Cisco Wide Area Application Services Command Reference

Software Version 6.2.3
March 5, 2019

Cisco Systems, Inc.
www.cisco.com
Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

CONTENTS

Preface 21

Audience 21

Document Organization 21

Document Conventions 22

Related Documentation 23

Obtaining Documentation and Submitting a Service Request 23

CHAPTER 1 **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

Using Global Configuration Mode 1-5

Using Interface Configuration Mode 1-6

Using ACL Configuration Modes 1-6

Using PKI Certificate Authority Configuration Mode 1-7

Using PKI Global Settings Configuration Mode 1-7

Using SSL Accelerated Service Configuration Mode 1-7

Using SSL Cipher List Configuration Mode 1-7

Using SSL Global Service Configuration Mode 1-7

Using SSL Host Peering Service Configuration Mode 1-8

Using SSL Management Service Configuration Mode 1-8

Using WCCP Configuration Mode 1-8

Command Modes Summary 1-9

Device Mode 1-10

Using Command-Line Processing 1-11

Checking Command Syntax 1-12

Using the no Form of Commands 1-13

Using System Help 1-13

Saving Configuration Changes 1-14

WAAS Directories on a WAE 1-14
Navigating WAAS Directories 1-14
Directory Descriptions 1-16
Managing WAAS Files Per Device 1-17

CHAPTER 2 Cisco WAAS Software Command Summary 2-1

CHAPTER 3 CLI Commands 3-1

EXEC Mode Commands 3-3
cd 3-4
clear arp-cache 3-5
clear bmc 3-6
clear cache 3-7
clear cache http-object-cache invalidate 3-9
clear cdp 3-10
clear connection 3-11
clear dre 3-12
clear ip 3-13
clear ipv6 3-14
clear license 3-15
clear logging 3-16
clear object-cache 3-17
clear service-policy 3-19
clear statistics 3-20
clear statistics accelerator 3-22
clear statistics accelerator http object-cache 3-23
clear statistics connection 3-24
clear statistics object-cache 3-26
clear transaction-log 3-27
clear users 3-28
clear windows-domain 3-30
clear windows-domain-log 3-31
clock 3-32
cms 3-33
cms secure-store 3-36

configure 3-39

copy cdrom 3-40

copy compactflash 3-41

copy disk 3-42

copy ftp 3-43

copy http 3-45

copy monitoring-log 3-47

copy running-config 3-48

copy scp 3-49

copy startup-config 3-51

copy sysreport 3-52

copy system-status 3-55

copy tech-support 3-56

copy tftp 3-58

cpfile 3-59

crypto delete 3-60

crypto export 3-61

crypto generate 3-63

crypto import 3-65

crypto pki 3-67

debug aaa accounting 3-68

debug aaa authorization 3-70

debug accelerator 3-72

debug accelerator http object-cache 3-77

debug accelerator mapi rpchttp-layer 3-78

debug accelerator object-cache-io 3-79

debug accelerator object-cache-ipc 3-80

debug accelerator object-cache-mgr 3-81

debug all 3-82

debug authentication 3-84

debug auto-discovery 3-86

debug buf 3-88

debug cdp 3-90

debug cli 3-92

debug cmm 3-94

debug cms 3-96

debug connection 3-98

debug dataserver 3-100

debug dhcp 3-102

debug dre 3-104

debug egress-method 3-106

debug encryption-service 3-108

debug fda 3-110

debug fdm 3-112

debug filtering 3-114

debug flow 3-116

debug generic-gre 3-118

debug hw-raid 3-120

debug imd 3-122

debug inline 3-124

debug key-manager 3-126

debug logging 3-128

debug monapi 3-130

debug nplogd 3-132

debug ntp 3-134

debug object-cache database 3-136

debug object-cache existence-cache 3-137

debug object-cache garbage-collection 3-138

debug object-cache ipc 3-139

debug object-cache load-monitor 3-140

debug rbcp 3-141

debug rmd 3-143

debug rpc 3-145

debug service-insertion 3-147

debug service-policy 3-149

debug snmp 3-151

debug standby 3-153

debug statistics 3-155

debug tfo 3-157

debug translog 3-159

debug wafs 3-161

debug wccp 3-163

delfile 3-165

deltree 3-166

dir 3-167

disable 3-169

disk 3-170

dnslookup 3-173

enable 3-174

exit 3-175

find-pattern 3-176

help 3-178

install 3-179

less 3-181

license add 3-182

lls 3-183

ls 3-184

lsusb 3-186

mkdir 3-187

mkfile 3-188

ntpdate 3-189

packet-capture 3-190

ping 3-192

ping6 3-193

pwd 3-195

reload 3-196

rename 3-197

restore 3-198

rmdir 3-202

scp 3-203

script 3-205

setup 3-206

show aaa accounting 3-207

show aaa authorization 3-209

show accelerator 3-210

show accelerator http object-cache 3-214

show alarms 3-215

show arp 3-218

show authentication 3-220

show auto-discovery 3-222

show auto-register 3-223

show banner 3-224

show bmc 3-225

show cache http-metadatacache 3-227

show cache object-cache 3-229

show cdp 3-231

show class-map 3-237

show clock 3-238

show cms 3-240

show cms secure-store 3-243

show crypto 3-245

show debugging 3-247

show device-id 3-248

show device-mode 3-249

show disks 3-251

show dre 3-259

show filtering list 3-260

show flash 3-262

show flow record 3-263

show hardware 3-264

show hosts 3-267

show inetd 3-268

show interception-method 3-269

show interface 3-270

show inventory 3-274

show ip access-list 3-275

show ip routes 3-277

show ipv6 3-278

show kdump 3-280

show kerberos 3-281

show key-manager 3-282

show license 3-283

show logging 3-284

show memory 3-285

show ntp 3-286

show object-cache 3-288

show peer optimization 3-289

show policy-map 3-290

show processes 3-291

show radius-server 3-293

show reload 3-295

show running-config 3-296

show service-insertion 3-298

show service-policy 3-304

show services 3-307

show smb-conf 3-308

show snmp 3-310

show ssh 3-316

show startup-config 3-317

show statistics accelerator 3-319

show statistics accelerator http object-cache 3-371

show statistics accelerator http preposition 3-373

show statistics aoim 3-374

show statistics application 3-378

show statistics authentication 3-381

show statistics auto-discovery 3-382

show statistics class-default 3-385

show statistics class-map 3-386

show statistics connection 3-387

show statistics connection auto-discovery 3-391

show statistics connection closed 3-393

show statistics connection conn-id 3-395

show statistics connection egress-methods 3-398

show statistics connection optimized 3-402

show statistics connection pass-through 3-405 show statistics crypto ssl ciphers 3-407

show statistics datamover 3-408

show statistics dre 3-410

show statistics filtering 3-414

show statistics flow 3-417

show statistics generic-gre 3-420

show statistics icmp 3-421

show statistics icmp6 3-423

show statistics ip 3-426

show statistics ipv6 3-429

show statistics netstat 3-432

show statistics object-cache 3-433

show statistics pass-through 3-435

show statistics peer 3-437

show statistics radius 3-440

show statistics service-insertion 3-442

show statistics services 3-443

show statistics sessions 3-444

show statistics snmp 3-445

show statistics system cpu 3-447

show statistics tacacs 3-449

show statistics tcp 3-451

show statistics tfo 3-455

show statistics udp 3-459

show statistics wccp 3-460

show statistics windows-domain 3-465

show sysfs volumes 3-467

show tacacs 3-468

show tcp 3-470

show tech-support 3-472

show telnet 3-475

show tfo tcp 3-476

show transaction-logging 3-478

show user 3-479

show users administrative 3-480

show version 3-482
show wccp 3-483
show windows-domain 3-490
show windows-domain encrypted services 3-492
shutdown 3-493
ssh 3-496
tcpdump 3-498
telnet 3-500
terminal 3-501
test 3-502
tethereal 3-503
top 3-506
traceroute 3-508
traceroute6 3-510
transaction-log 3-511
type 3-512
type-tail 3-513
vm 3-515
waas-tcptrace 3-517
whoami 3-519
windows-domain 3-520
write 3-523
zzdebugshell 3-524

Global Configuration Mode Commands 3-525

(config) aaa accounting 3-526
(config) aaa authorization commands 3-529
(config) accelerator epm 3-530
(config) accelerator http 3-531
(config) accelerator http object-cache enable 3-534
(config) accelerator http object-cache transparent enable 3-535
(config) accelerator http object-cache transparent basic 3-536
(config) accelerator http object-cache transparent standard 3-538
(config) accelerator http object-cache transparent advanced 3-540
(config) accelerator http object-cache transparent bypass 3-542
(config) accelerator http object-cache ott enable 3-544

(config) accelerator http object-cache connected enable 3-546

(config) accelerator http object-cache cws-check enable 3-547

(config) accelerator http preposition proxy server 3-548

(config) accelerator ica 3-549

(config) accelerator mapi 3-551

(config) accelerator object-cache enable 3-554

(config) accelerator smb 3-556

(config) accelerator smb preposition 3-560

(config) accelerator smb preposition dre 3-562

(config) accelerator ssl 3-563

(config) alarm overload-detect 3-565

(config) asset 3-567

(config) authentication configuration 3-568

(config)authentication enable 3-573

(config) authentication content-request 3-574

(config) authentication fail-over 3-578

(config) authentication login 3-580

(config) authentication strict-password-policy 3-585

(config) auto-discovery 3-587

(config) auto-register 3-588

(config) banner 3-590

(config) cdp 3-592

(config) central-manager 3-593

(config) clock 3-595

(config) cms 3-599

(config) crypto pki 3-602

(config) crypto ssl 3-604

(config) device mode 3-606

(config) disk disk-name 3-608

(config) disk cache 3-609

(config) disk encrypt 3-611

(config) disk error-handling 3-612

(config) disk logical shutdown 3-613

(config) disk object-cache extend 3-614

(config) dre 3-615

(config) end 3-616

(config) exec-timeout 3-617

(config) exit 3-618

(config) flow exporter 3-619

(config) flow record 3-621

(config) flow monitor 3-622

(config) help 3-623

(config) hostname 3-625

(config) inetd 3-627

(config) inline vlan-id-connection-check 3-628

(config) interception 3-629

(config) interception-method 3-631

(config) interface GigabitEthernet 3-633

(config) interface InlineGroup 3-638

(config) interface PortChannel 3-641

(config) interface standby 3-644

(config) interface TenGigabitEthernet 3-646

(config) interface virtual 3-650

(config) ip 3-653

(config) ip access-list 3-656

(config) ip icmp rate-limit unreachable 3-659

(config) ip unreachables df 3-661

(config) ipv6 3-662

(config) kerberos 3-664

(config) kernel kdb 3-666

(config) kernel kdump enable 3-668

(config) line 3-669

(config) logging console 3-670

(config) logging disk 3-672

(config) logging facility 3-674

(config) logging host 3-676

(config) ntp 3-678

(config) object-cache enable 3-680

(config) peer 3-681

(config) policy-map 3-682

(config) port-channel 3-684
(config) primary-interface 3-685
(config) radius-server 3-687
(config) service-policy 3-689
(config) smb-conf 3-691
(config) snmp-server access-list 3-694
(config) snmp-server community 3-695
(config) snmp-server contact 3-697
(config) snmp-server enable traps 3-698
(config) snmp-server group 3-701
(config) snmp-server host 3-703
(config) snmp-server location 3-705
(config) snmp-server mib 3-706
(config) snmp-server monitor user 3-708
(config) snmp-server notify inform 3-709
(config) snmp-server trap-source 3-710
(config) snmp-server trigger 3-712
(config) snmp-server user 3-715
(config) snmp-server view 3-717
(config) sshd 3-718
(config) ssh-key-generate 3-720
(config) stats-collector logging 3-721
(config) system jumbomtu 3-722
(config) tacacs 3-723
(config) tcp 3-726
(config) telnet enable 3-728
(config) tfo exception 3-729
(config) tfo optimize 3-730
(config) tfo tcp adaptive-buffer-sizing 3-731
(config) tfo tcp keepalive 3-732
(config) tfo tcp optimized-mss 3-733
(config) tfo tcp optimized-receive-buffer 3-734
(config) tfo tcp optimized-send-buffer 3-735
(config) tfo tcp original-mss 3-736
(config) tfo tcp original-receive-buffer 3-737

(config) tfo tcp original-send-buffer 3-738

(config) threshold-monitor 3-739

(config) username 3-741

(config) wccp access-list 3-743

(config) wccp router-list 3-745

(config) wccp shutdown 3-747

(config) wccp tcp-promiscuous service-pair 3-749

(config) windows-domain 3-751

Interface Configuration Mode Commands 3-755

(config-if) autosense 3-756

(config-if) bandwidth 3-757

(config-if) cdp 3-759

(config-if) channel-group 3-760

(config-if) description 3-761

(config-if) encapsulation dot1Q 3-762

(config-if) exit 3-763

(config-if) full-duplex 3-764

(config-if) half-duplex 3-766

(config-if) inline 3-768

(config-if) ip 3-770

(config-if) ip access-group 3-772

(config-if) load-interval 3-773

(config-if) mtu 3-774

(config-if) shutdown 3-775

(config-if) standby 3-776

Standard ACL Configuration Mode Commands 3-778

(config-std-nacl) delete 3-781

(config-std-nacl) deny 3-782

(config-std-nacl) exit 3-784

(config-std-nacl) list 3-785

(config-std-nacl) move 3-786

(config-std-nacl) permit 3-787

Extended ACL Configuration Mode Commands 3-789

(config-ext-nacl) delete 3-792

(config-ext-nacl) deny 3-793
(config-ext-nacl) exit 3-798
(config-ext-nacl) list 3-799
(config-ext-nacl) move 3-800
(config-ext-nacl) permit 3-801

Preposition Configuration Mode Commands 3-807
(config-preposition) accelerator http preposition dre enable 3-808
(config-preposition) accelerator http preposition task task-name 3-809
(config-preposition) credentials 3-812
(config-preposition) dscp 3-813
(config-preposition) duration 3-814
(config-preposition) enable 3-815
(config-preposition) ignore-hidden-dir 3-816
(config-preposition) max-cache 3-817
(config-preposition) max-file-size 3-818
(config-preposition) min-file-size 3-819
(config-preposition) name 3-820
(config-preposition) pattern 3-821
(config-preposition) recursive 3-822
(config-preposition) root 3-823
(config-preposition) scan-type 3-824
(config-preposition) schedule 3-825
(config-preposition) server 3-827
(config-preposition) use-proxy 3-828
(config-preposition) user-agent 3-829

PKI Certificate Authority Configuration Mode Commands 3-831
(config-ca) ca-certificate 3-833
(config-ca) description 3-834
(config-ca) revocation-check 3-835

PKI Global Settings Configuration Mode Commands 3-837
(config-pki-global-settings) ocsp 3-838
(config-pki-global-settings) revocation-check 3-839

SSL Accelerated Service Configuration Mode Commands 3-841
(config-ssl-accelerated) cipher-list 3-843

(config-ssl-accelerated) client-cert-key 3-844

(config-ssl-accelerated) client-cert-verify 3-845

(config-ssl-accelerated) client-version-rollback-check 3-846

(config-ssl-accelerated) description 3-847

(config-ssl-accelerated) inservice 3-848

(config-ssl-accelerated) protocol-chaining enable 3-849

(config-ssl-accelerated) server-cert-key 3-850

(config-ssl-accelerated) server-cert-verify 3-851

(config-ssl-accelerated) server-domain 3-852

(config-ssl-accelerated) server-ip 3-853

(config-ssl-accelerated) server-name 3-854

(config-ssl-accelerated) version 3-855

SSL Cipher List Configuration Mode Commands 3-857

(config-cipher-list) cipher 3-858

SSL Global Service Configuration Mode Commands 3-861

(config-ssl-global) cipher-list 3-863

(config-ssl-global) machine-cert-key 3-864

(config-ssl-global) version 3-865

SSL Host Peering Service Configuration Mode Commands 3-867

(config-ssl-peering) cipher-list 3-869

(config-ssl-peering) peer-cert-verify 3-870

(config-ssl-peering) version 3-871

SSL Management Service Configuration Mode Commands 3-873

(config-ssl-mgmt) cipher-list 3-875

(config-ssl-mgmt) peer-cert-verify 3-876

(config-ssl-mgmt) version 3-877

WCCP Configuration Mode Commands 3-879

(config-wccp-service) assignment-method 3-881

(config-wccp-service) egress-method 3-883

(config-wccp-service) enable 3-885

(config-wccp-service) exit 3-886

(config-wccp-service) failure-detection 3-887

(config-wccp-service) password 3-888

(config-wccp-service) redirect-method 3-889
(config-wccp-service) router-list-num 3-891
(config-wccp-service) weight 3-892

Service Node Configuration Mode Commands 3-895
(config-sn) authentication 3-897
(config-sn) description 3-898
(config-sn) enable 3-899
(config-sn) node-discovery enable 3-900
(config-sn) shutdown 3-902

Service Context Configuration Mode Commands 3-903

Class Map Configuration Mode Commands 3-905
(config-cmap) description 3-907
(config-cmap) match protocol 3-908
(config-cmap) match tcp 3-910

Policy Map Configuration Mode Commands 3-913
(config-pmap) class 3-915
(config-pmap) description 3-916

Policy Map Class Configuration Mode Commands 3-917
(config-pmap-c) optimize 3-919
(config-pmap-c) pass-through 3-921
(config-pmap-c) set ip dscp 3-923

APPENDIX A Acronyms and Abbreviations A-1

CLI COMMAND SUMMARY BY MODE

Preface

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

- Audience, page 21
- Document Organization, page 21
- Document Conventions, page 22
- Related Documentation, page 23
- Obtaining Documentation and Submitting a Service Request, page 23

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
Chapter 1, “Using the WAAS Command-Line Interface”	Describes how to use the command-line interface.
Chapter 2, “Cisco WAAS Software Command Summary”	Lists WAAS software commands, providing a brief description of each.

Chapter	Description
Chapter 3, "CLI Commands"	Provides detailed information for the following types of CLI commands for the WAAS software: • Commands you can enter after you log in to the WAAS device (EXEC mode). • Configuration mode commands that you can enter after you log in to the WAAS device, and then access configuration mode and its subset of modes. The description of each command includes the syntax of the command and any related commands, when appropriate.
Appendix A, "Acronyms and Abbreviations"	Defines the acronyms used in this publication.
CLI COMMAND SUMMARY BY MODE	Lists each command by command mode.

Document Conventions

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

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

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

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

Related Documentation

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

- *Release Note for Cisco Wide Area Application Services*
- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Command Reference* (this manual)
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services API Reference*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Installing the Cisco WAE Inline Network Adapter*

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.

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
- Using Command Modes
- Using Command-Line Processing
- Checking Command Syntax
- Using the no Form of Commands
- Using System Help
- Saving Configuration Changes
- WAAS Directories on a WAE
- Managing WAAS Files Per Device

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 a variety of WAE and WAVE appliances, WAE-NME and SM-SRE network modules, and as a virtual WAAS appliance (vWAAS).

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 platforms that are running 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 two 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 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
- Using EXEC Mode
- Using Global Configuration Mode
- Using Interface Configuration Mode
- Using ACL Configuration Modes
- Using PKI Certificate Authority Configuration Mode
- Using PKI Global Settings Configuration Mode

- Using SSL Accelerated Service Configuration Mode
- Using SSL Cipher List Configuration Mode
- Using SSL Global Service Configuration Mode
- Using SSL Host Peering Service Configuration Mode
- Using SSL Management Service Configuration Mode
- Using WCCP Configuration Mode

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.
- PKI certificate authority configuration mode—Configures public key infrastructure (PKI) encryption certificate authorities on a WAAS device. To use this mode, enter the **crypto pki ca** command.
- PKI global settings configuration mode—Configures OCSP and revocation checking on a WAAS device. To use this mode, enter the **crypto pki global-settings** command.
- SSL accelerated service configuration mode—Enables and configures secure socket layer (SSL) acceleration on your WAAS system. To use this mode, enter the **crypto ssl service accelerated-service** command.
- SSL cipher list configuration mode—Configures SSL encryption cipher lists on a WAAS device. To use this mode, enter the **crypto ssl cipher-list** command.
- SSL global service configuration mode—Enables and configures basic SSL acceleration settings on your WAAS system. To use this mode, enter the **crypto ssl services global-settings** command.
- SSL host peering service configuration mode—Configures SSL encryption peering services on a WAAS device. To use this mode, enter the **crypto ssl services host-service peering** command.

- SSL management service configuration mode—Configures SSL encryption management service parameters on a WAAS device. To use this mode, enter the **crypto ssl management-service** command.
- WCCP configuration mode—Configures WCCP service parameters on a WAAS device. To use this mode, enter the **wccp tcp-promiscuous** 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.

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>
```

- Comment—Any command line that begins with an exclaimation point (!) is considered a comment and is ignored.

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 1-14. 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
- PKI certificate authority configuration mode
- PKI global settings configuration mode
- SSL accelerated service configuration mode
- SSL cipher list configuration mode
- SSL global service configuration mode
- SSL host peering service configuration mode
- SSL management service configuration mode
- WCCP 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 Interface Configuration Mode

Use 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
  InlineGroup      Select an inline group interface to configure
  PortChannel      Ethernet Channel of interfaces
  Standby          Standby groups

WAE(config)# interface gigabitethernet ?
    <1-2>/ GigabitEthernet slot/port

WAE(config)# interface gigabitethernet 1/0
WAE(config-if)#
```

To exit interface configuration mode, 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 PKI Certificate Authority Configuration Mode

Use PKI certificate authority configuration mode to add and configure a certificate authority.

To enter this mode, use the **crypto pki ca** command from the global configuration mode.

To exit PKI certificate authority configuration mode, use the **exit** command to return to global configuration mode:

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

Using PKI Global Settings Configuration Mode

Use PKI global settings configuration mode to configure OCSP and revocation checking.

To enter this mode, use the **crypto pki global-settings** command from the global configuration mode.

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

```
WAE(config-pki-global-settings)# exit
WAE(config)#
```

Using SSL Accelerated Service Configuration Mode

Use SSL accelerated service configuration mode to enable and configure SSL acceleration on your WAAS system, and define services to be accelerated on the SSL path.

To enter this mode, use the **crypto ssl service accelerated-service** command from the global configuration mode.

To exit SSL accelerated service configuration mode, use the **exit** command to return to global configuration mode:

```
WAE(config-ssl-accelerated)# exit
WAE(config)#
```

Using SSL Cipher List Configuration Mode

Use SSL cipher list configuration mode to configure secure socket layer (SSL) encryption cipher lists on a WAAS device.

To enter this mode, use the **crypto ssl cipher-list** command from the global configuration mode.

To exit SSL cipher list configuration mode, use the **exit** command to return to global configuration mode:

```
WAE(config-cipher-list)# exit
WAE(config)#
```

Using SSL Global Service Configuration Mode

Use SSL global service configuration mode to enable and configure basic SSL acceleration settings on your WAAS system.

To enter this mode, use the **crypto ssl services global-settings** command from the global configuration mode.

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

```
WAE(config-ssl-global)# exit
WAE(config)#
```

Using SSL Host Peering Service Configuration Mode

Use SSL host peering service configuration mode to configure secure socket layer (SSL) encryption peering services on a WAAS device. SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections.

To enter this mode, use the **crypto ssl services host-service peering** command from the global configuration mode.

To exit SSL host peering service configuration mode, use the **exit** command to return to global configuration mode:

```
WAE(config-ssl-peering)# exit
WAE(config)#
```

Using SSL Management Service Configuration Mode

Use SSL management service configuration mode to configure SSL parameters used for secure communications between the Central Manager and the WAE devices.

To enter this mode, use the **crypto ssl management-service** command from the global configuration mode.

To exit SSL management service configuration mode, use the **exit** command to return to global configuration mode:

```
WAE(config-ssl-mgmt)# exit
WAE(config)#
```

Using WCCP Configuration Mode

Use WCCP configuration mode to configure the WCCP version 2 TCP promiscuous mode service.

To enter this mode, use the **wccp tcp-promiscuous** command from the global configuration mode.

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

```
WAE(config-wccp-service)# 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 **end** command. To enter privileged EXEC mode, use the **enable** command.
privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`WAE#`	To return to user EXEC mode, use the **disable** command. To enter global configuration mode, use the **configure** command.
global configuration	From privileged EXEC mode, use the **configure** command.	`WAE(config)#`	To return to privileged EXEC mode, use the **exit** command or press **Ctrl-Z**. To enter a configuration submode, use the specific command related to the submode.
interface configuration	From global configuration mode, use the **interface** command.	`WAE(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
standard ACL configuration	From global configuration mode, use the **ip access-list standard** command.	`WAE(config-std-nacl)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
extended ACL configuration	From global configuration mode, use the **ip access-list extended** command.	`WAE(config-ext-nacl)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
PKI certificate authority configuration	From global configuration mode, use the **crypto pki ca** command.	`WAE(config-ca)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
PKI global settings configuration	From global configuration mode, use the **crypto pki global-settings** command.	`WAE(config-pki-global-settings)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
SSL accelerated service configuration	From global configuration mode, use the **crypto ssl service accelerated-service** command.	`WAE(config-ssl-accelerated)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.

Table 1-1 WAAS Command Modes Summary (continued)

Command Mode	Access Method	Prompt	Exit Method
SSL cipher list configuration	From global configuration mode, use the **crypto ssl cipher-list** command.	`WAE(config-cipher-list)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
SSL global service configuration	From global configuration mode, use the **crypto ssl services global-settings** command.	`WAE(config-ssl-global)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
SSL host peering service configuration	From global configuration mode, use the **crypto ssl services host-service peering** command.	`WAE(config-ssl-peering)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
SSL management service configuration	From global configuration mode, use the **crypto ssl management-service** command.	`WAE(config-ssl-mgmt)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
WCCP configuration	From global configuration mode, use the **wccp tcp-promiscuous** command.	`WAE(config-wccp-service)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.

Device Mode

The WAAS software 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:

- WAAS Central Manager mode—Mode that the WAAS Central Manager uses.
- WAAS application accelerator mode—Mode that a WAAS Accelerator (data center WAEs and branch WAEs that run the WAAS software) uses to optimize and accelerate traffic. (default)

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[1]	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L	Repeats the current command line on a new line.

Table 1-2 Command-Line Processing Keystroke Combinations (continued)

Keystroke Combinations	Function
Ctrl-N or the Down Arrow key[1]	Enters the next command line in the history buffer.
Ctrl-P or the Up Arrow key[1]	Enters the previous command line in the history buffer.
Ctrl-T	Transposes the character at the cursor with the character to the left of the cursor.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or Backspace key	Erases a mistake when entering a command; 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
cd [*directory-name*]	Change Directory—Moves you from the current directory to the specified directory in the WAAS tree. If no directory is specified, **cd** takes you up one directory.
deltree *directory-name*	Remove Directory Tree—Deletes the specified directory and all subdirectories and files without displaying a warning message to you.
dir [*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 **lls** command.
ls [*directory-name*]	Show Directory Names—Lists the names of directories in the current directory path.

Table 1-3 WAAS Navigation Commands (continued)

Command	Description
lls [*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 **dir** command.
mkdir *directory-name*	Create Directory—Creates a directory of the specified name in the current directory path.
pwd	Present Working Directory—Lists the complete path from where this command is entered.
rmdir *directory-name*	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 *actona* subdirectory contains the commonly used Manager.log, Utilities.log, and Watchdog.log log files. See the *Cisco Wide Area Application Services Configuration Guide* 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 **show tech-support** EXEC command, and perhaps other output to Cisco TAC personnel if a problem arises.

Note The WAAS software uses the CONTENT file system for the data redundancy elimination (DRE) cache.

Managing WAAS Files Per Device

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

Table 1-5 WAAS File Management Commands

Command	Description
copy {*source* | *image*}	Copy—Copies the selected source file, image, or configuration information: • cdrom—Copies the file from the CDROM. • compactflash—Copies the file from the CompactFlash card. • disk—Copies the configuration or file from the disk. • ftp—Copies the file from the FTP server. • http—Copies the file from the HTTP server. • running-config—Copies information from the current system configuration. • startup-config—Copies information from the startup configuration. • sysreport—Copies system information. • system-status—Copies the system status for debugging reference. • tech-support—Copies system information for technical support. • tftp—Copies the software image from the TFTP server. • usb—Copies files from an external USB drive.
cpfile *source-filename destination-filename*	Copy File—Makes a copy of a source file, and puts it in the current directory.
delfile *filename*	Remove File—Deletes the specified file from the current directory path.
less *filename*	Display File Using LESS—Displays the specified file on the screen using the LESS program. The filename is case sensitive. Enter **q** to stop viewing the file and return to the directory.
mkfile *filename*	Create File—Creates a file of the specified name in the current directory path.
rename *old-filename new-filename*	Rename File—Renames the specified file with a new filename.
type *filename*	Display File—Displays the content of the specified file on the screen.
type-tail *filename* [*line* | follow | | {begin *LINE* | exclude *LINE* | include *LINE*}]	Display End of File—Displays the last few lines of the specified file. Can also be used to view the last lines of a file continuously as new lines are added to the file, to start at a particular line in the file, or to include or exclude specific lines in the file.
find-pattern *pattern*	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
```

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 6.2.3 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

Command	Description	CLI Mode	Device Mode
(config) aaa accounting	Configures AAA accounting.	global configuration	All
(config) aaa authorization commands	Configures AAA authorization.	global configuration	All
(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 ica	Enables the ICA application accelerator.	global configuration	application- accelerator
(config) accelerator mapi	Enables the MAPI application accelerator.	global configuration	application- accelerator
(config) accelerator smb	Enables the SMB application accelerator.	global configuration	application- accelerator
(config) accelerator ssl	Enables the SSL application accelerator.	global configuration	application- accelerator
(config) alarm overload-detect	Configures the detection of an alarm overload.	global configuration	All
(config) asset	Configures the tag name for the asset tag string.	global configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-wccp-service) assignment-method	Configures the WCCP assignment method.	WCCP configuration	application- accelerator
(config-sn) authentication	Configures the WN authentication key.	service node configuration	application- accelerator
(config) authentication configuration	Configures administrative authentication and authorization parameters.	global configuration	All
(config)authentication enable	Configures enable authentication to use local admin user account password instead of using external authentication servers.	global configuration	application- accelerator central manager
(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-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-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

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(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
(config-if) channel-group	Configures the port channel group for an interface.	interface configuration	All
(config-cipher-list) cipher	Configures a cipher suite on the cipher list.	cipher list configuration	All
(config-ssl-accelerated) cipher-list	Configures secure socket layer (SSL) encryption cipher lists on a WAAS device.	SSL accelerated service configuration	All
(config-ssl-global) cipher-list	Configures secure socket layer (SSL) encryption cipher lists on a WAAS device.	SSL global service configuration	All
(config-ssl-peering) cipher-list	Configures secure socket layer (SSL) encryption cipher lists on a WAAS device.	SSL host peering service configuration	All
(config-ssl-mgmt) cipher-list	Configures secure socket layer (SSL) encryption cipher lists on a WAAS device.	SSL management service configuration	All
clear arp-cache	Resets the ARP cache.	privileged-level EXEC	application- accelerator
clear cache	Resets the cached objects.	privileged-level EXEC	application- accelerator
clear cdp	Resets Cisco Discovery Protocol statistics.	privileged-level EXEC	All
clear connection	Resets one or more connections.	privileged-level EXEC	application- accelerator
clear dre	Clears DRE configurations.	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

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
clear statistics connection	Resets connection statistics.	privileged-level EXEC	All
clear transaction-log	Archives the working transaction log file.	privileged-level EXEC	application accelerator
clear users	Resets user connections or unlocks users that have been locked out.	privileged-level EXEC	All
clear windows-domain	Clears Windows domain server information.	privileged-level EXEC	All
clear windows-domain-log	Clears user connections and unlocks users that have been locked out.	privileged-level EXEC	All
(config-ssl-accelerated) client-cert-verify	Enables verification of client certificates.	SSL accelerated service configuration	All
(config-ssl-accelerated) client-cert-key	Configures a certificate and private key	SSL accelerated service configuration	All
(config-ssl-accelerated) client-version-rollback-check	Disables the client SSL version rollback check.	SSL accelerated service configuration	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 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

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
copy monitoring-log	Copies SMB statistics data to the local disk or an FTP server.	privileged-level EXEC	All
copy running-config	Copies information from the current system configuration.	privileged-level EXEC	All
copy scp	Copies files from an SCP server.	privileged-level EXEC	All
copy startup-config	Copies information from the startup configuration.	privileged-level EXEC	All
copy sysreport	Copies system troubleshooting information.	privileged-level EXEC	All
copy system-status	Copies the system status for debugging reference.	privileged-level EXEC	All
copy tech-support	Copies system information for technical support.	privileged-level EXEC	All
copy tftp	Copies the software image from the TFTP server.	privileged-level EXEC	All
copy usb	Copies files from an external USB drive.	privileged-level EXEC	All
cpfile	Copies a file to the current directory.	privileged-level EXEC	All
crypto delete	Removes SSL certificate and key files.	privileged-level EXEC	application- accelerator
crypto export	Exports SSL certificate and key files.	privileged-level EXEC	application- accelerator
crypto generate	Generates a self-signed certificate or a certificate signing request.	privileged-level EXEC	All
crypto import	Imports SSL certificate and key files.	privileged-level EXEC	application- accelerator
crypto pki	Initializes the PKI managed store.	privileged-level EXEC	All
(config) crypto pki	Configures public key infrastructure (PKI) encryption parameters.	global configuration	All
(config) crypto ssl	Configures secure sockets layer (SSL) encryption parameters.	global configuration	All
debug aaa accounting	Configures AAA accounting debugging.	privileged-level EXEC	All
debug aaa authorization	Configures AAA authorization debugging.	privileged-level EXEC	All
debug accelerator	Configures accelerator debugging.	privileged-level EXEC	application- accelerator
debug all	Configures all debugging.	privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
debug authentication	Configures authentication debugging.	privileged-level EXEC	All
debug auto-discovery	Configures auto discovery debugging.	privileged-level EXEC	application- accelerator
debug buf	Configures buffer manager debugging.	privileged-level EXEC	All
debug cdp	Configures CDP debugging.	privileged-level EXEC	All
debug cli	Configures CLI debugging.	privileged-level EXEC	All
debug cmm	Configures cluster membership manager debugging.	privileged-level EXEC	All
debug cms	Configures CMS debugging.	privileged-level EXEC	All
debug connection	Configures connection debugging.	privileged-level EXEC	application- accelerator
debug dataserver	Configures data server debugging.	privileged-level EXEC	All
debug dhcp	Configures DHCP debugging.	privileged-level EXEC	All
debug dre	Configures DRE debugging.	privileged-level EXEC	application- accelerator
debug egress-method	Configures egress method debugging.	privileged-level EXEC	application- accelerator
debug encryption-service	Configures encryption service debugging.	privileged-level EXEC	All
debug fda	Configures flow distribution agent service debugging.	privileged-level EXEC	All
debug fdm	Configures flow distribution manager service debugging.	privileged-level EXEC	All
debug filtering	Configures filtering debugging.	privileged-level EXEC	application- accelerator
debug flow	Configures network traffic flow debugging.	privileged-level EXEC	All
debug generic-gre	Configures generic GRE egress method debugging.	privileged-level EXEC	application- accelerator
debug hw-raid	Configures hardware RAID debugging.	privileged-level EXEC	All
debug imd	Configures interface manager debugging.	privileged-level EXEC	All
debug inline	Configures inline debugging.	privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
debug key-manager	Configures key manager debugging.	privileged-level EXEC	central-manager
debug logging	Configures logging debugging.	privileged-level EXEC	All
debug monapi	Configures monitoring API debugging.	privileged-level EXEC	central-manager
debug ntp	Configures NTP debugging.	privileged-level EXEC	All
debug rbcp	Configures RBCP debugging.	privileged-level EXEC	application- accelerator
debug rmd	Configures route manager debugging.	privileged-level EXEC	All
debug rpc	Configures record remote procedure calls debugging.	privileged-level EXEC	All
debug service-insertion	Configures service-insertion module debugging.	privileged-level EXEC	All
debug service-policy	Configures service policy debugging.	privileged-level EXEC	All
debug snmp	Configures SNMP debugging.	privileged-level EXEC	All
debug standby	Configures standby debugging.	privileged-level EXEC	application- accelerator
debug statistics	Configures statistics debugging.	privileged-level EXEC	All
debug tfo	Configures TFO flow optimization debugging.	privileged-level EXEC	application- accelerator
debug translog	Configures transaction logging debugging.	privileged-level EXEC	application- accelerator
debug wccp	Configures WCCP information debugging.	privileged-level EXEC	application- accelerator
(config-std-nacl) delete	Deletes a line from the standard ACL.	standard ACL configuration	All
(config-ext-nacl) delete	Deletes a line from the extended ACL.	extended ACL configuration	All
delfile	Deletes a file.	privileged-level EXEC	All
deltree	Deletes a directory and its subdirectories.	privileged-level EXEC	All
(config-std-nacl) deny	Adds a line to a standard access list that specifies the type of packets that you want the WAAS device to drop.	standard ACL configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-ext-nacl) deny	Adds a line to an extended access-list that specifies the type of packets that you want the WAAS device to drop.	extended ACL configuration	All
(config-ca) description	Configures a description for the certification authority.	certification authority configuration	All
(config-if) description	Configures the description for an interface.	interface configuration	All
(config-ssl-accelerated) description	Configures a description for SSL accelerated service.	SSL accelerated service configuration	All
(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
disable	Turns off the privileged EXEC commands.	privileged-level EXEC	All
disk	Configures the disks on the WAAS device.	privileged-level EXEC	All
(config) disk disk-name	Disables a RAID-1 disk for online removal.	global configuration	All
(config) disk cache	Configures Akamai cache and Object cache partitions	global configuration	application-accelerator
(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
(config) disk object-cache extend	Enables extended object cache.	global configuration	All
dnslookup	Resolves a DNS hostname.	user-level EXEC and privileged-level EXEC	All
(config) dre	Enables and configures DRE auto bypass and load monitor settings.	global configuration	application- accelerator
(config-wccp-service) egress-method	Configures the WCCP egress method.	WCCP configuration	application- accelerator
enable*	Accesses the privileged EXEC commands.	user-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-wccp-service) enable	Enables or disables WCCP.	WCCP configuration	application- accelerator
(config-if) encapsulation dot1Q	Sets the VLAN ID of traffic leaving an inline group 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
(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-wccp-service) exit	Exits from WCCP configuration mode.	WCCP configuration	application- accelerator
	Configures the maximum time for the inline interface to transition traffic to another port after a failure event.	interface configuration	All
(config-wccp-service) failure-detection	Configure the WCCP failure detection timeout.	WCCP configuration	application- accelerator
find-pattern	Searches for a particular pattern in a file.	privileged-level EXEC	All
(config) flow monitor	Configures network traffic flow monitoring.	global configuration	application- accelerator
(config-if) full-duplex	Sets the current interface to the full-duplex mode.	interface configuration	All
(config-if) half-duplex	Sets the current interface to half-duplex mode.	interface configuration	All
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

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) inetd	Enables FTP 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	application- accelerator
(config-ssl-accelerated) inservice	Enables the accelerated service.	SSL accelerated service configuration	All
install	Installs a new image into Flash memory.	privileged-level EXEC	All
(config) interception	Configures an interception access list.	global configuration	All
(config) interception-method	Configures an interception access list.	global configuration	application- accelerator appnav-controller
(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
(config) interface TenGigabitEthernet*	Configures a 10-Gigabit Ethernet interface. Provides access to interface configuration mode.	global configuration	All
(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 inline module.	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) ip icmp rate-limit unreachable	Limits the rate at which Internet Control Message Protocol (ICMP) destination unreachable messages are generated.	global configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) ip unreachables df	Enables the IP unreachable ICMP service.	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 enable	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-if) load-interval	Configures the statistics polling interval for an interface.	interface configuration	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 on the device hard disk.	user-level EXEC and privileged-level EXEC	All
lsusb	Lists the files and subdirectories in a directory on a USB storage device.	user-level EXEC and privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-ssl-global) machine-cert-key	Configures a certificate and private key.	SSL global service configuration	All
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) 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
packet-capture	Captures packets.	privileged-level EXEC	All
(config-wccp-service) password	Configures the WCCP service password.	WCCP configuration	application- accelerator
(config) peer	Enables/disables peer optimization.	global configuration	application- accelerator
(config-ssl-peering) peer-cert-verify	Enables verification of peer certificates.	SSL host peering service configuration	All
(config-ssl-mgmt) peer-cert-verify	Enables verification of peer certificates.	SSL management service configuration	All
(config-std-nacl) permit	Adds a line to a standard access list that specifies the type of packets that you want the WAAS device to permit for further processing.	standard ACL configuration	All
(config-ext-nacl) permit	Adds a line to an extended access list that specifies the type of packets that you want the WAAS device to permit for further processing.	extended ACL configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
ping	Sends the echo packets.	user-level EXEC and privileged-level EXEC	All
(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) radius-server	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-wccp-service) redirect-method	Configures the WCCP redirect method.	WCCP 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 the global settings revocation checking method.	PKI global-settings configuration	All
rmdir	Removes a directory.	privileged-level EXEC	All
(config-wccp-service) router-list-num	Configures the WCCP router list.	WCCP 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-ssl-accelerated) server-cert-key	Configures a certificate and private key.	SSL accelerated service configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-ssl-accelerated) server-cert-verify	Enables verification of server certificates.	SSL accelerated service configuration	All
(config-ssl-accelerated) server-domain	Configures the accelerated server domain and TCP port.	SSL accelerated service configuration	All
(config-ssl-accelerated) server-ip	Configures the accelerated server IP address and TCP port.	SSL accelerated service configuration	All
(config-ssl-accelerated) server-name	Configures the accelerated server hostname and TCP port.	SSL accelerated service configuration	All
(config) service-policy	Configures entities.	global configuration	application- accelerator
(config) service-policy	Configures optimization policy.	global 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.	user-level EXEC and privileged-level EXEC	All
show aaa authorization	Displays the AAA authorization configuration.	user-level EXEC and privileged-level EXEC	All
show accelerator	Displays the status and configuration of the application accelerators.	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.	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

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show bmc	Displays the Baseboard Management Controller information.	user-level EXEC and privileged-level EXEC	application- accelerator
show cache http-metadatacache	Displays HTTP metadata cache information.	privileged-level EXEC	application- accelerator
show cdp	Displays the CDP configuration.	privileged-level EXEC	All
show class-map	Displays the matching criteria configured for a class map.	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.	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
show debugging	Displays the state of each debugging option.	privileged-level EXEC	All
show device-id	Displays the device ID.	user-level EXEC and privileged-level EXEC	All
show device-mode	Displays the device mode.	privileged-level EXEC	All
show disks	Displays the disk configurations.	user-level EXEC and privileged-level EXEC	All
show filtering list	Displays TFO flow information for a WAE.	privileged-level EXEC	application- accelerator
show flash	Displays the flash memory information.	privileged-level EXEC	All
show flow record	Displays collection information for a WAE device.	EXEC	application-accelerator central-manager
show hardware	Displays the system hardware information.	privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.	user-level EXEC and privileged-level EXEC	All
show inetd	Displays the status of TCP/IP services.	privileged-level EXEC	All
show interception-method	Displays the interception method.	privileged-level EXEC	application- accelerator
show interface	Displays the hardware interface information.	privileged-level EXEC	All
show inventory	Displays the system inventory information.	privileged-level EXEC	All
show ip access-list	Displays the information about access lists that are defined and applied to specific interfaces or applications.	privileged-level EXEC	All
show ip routes	Displays the IP routing table.	privileged-level EXEC	All
show kdump	Displays the kernel crash dump information.	privileged-level EXEC	All
show kerberos	Displays the Kerberos authentication configuration.	user-level EXEC and privileged-level EXEC	All
show key-manager	Displays the key manager information for a WAAS device.	privileged-level EXEC	All
show license	Displays the license information.	privileged-level EXEC	All
show logging	Displays the system logging configuration.	user-level EXEC and privileged-level EXEC	All
show memory	Displays the memory blocks and statistics.	privileged-level EXEC	All
show ntp	Displays the NTP configuration status.	user-level EXEC and privileged-level EXEC	All
show peer optimization	Displays the configured serial peers for a WAE.	privileged-level EXEC	application- accelerator
show policy-map	Displays the configured policy map rules.	privileged-level EXEC	application- accelerator
show processes	Displays the process status.	privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show radius-server	Displays the RADIUS server information.	user-level EXEC and privileged-level EXEC	All
show reload	Displays scheduled reload information.	user-level EXEC and privileged-level EXEC	All
show running-config	Displays the current operating configuration.	privileged-level EXEC	All
show services	Displays information related to services.	privileged-level EXEC	All
show smb-conf	Displays the smb-conf configurations.	privileged-level EXEC	All
show snmp	Displays the SNMP statistics.	user-level EXEC and privileged-level EXEC	All
show ssh	Displays the status and configuration of the Secure Shell (SSH) service.	privileged-level EXEC	All
show startup-config	Displays the startup configuration.	privileged-level EXEC	All
show statistics accelerator	Displays the application accelerator statistics information.	privileged-level EXEC	application- accelerator
show statistics aoim	Displays AO (accelerator) Information Manager statistics.	privileged-level EXEC	application- accelerator
show statistics application	Displays the status of the application statistics.	privileged-level EXEC	All
show statistics authentication	Displays the authentication statistics.	user-level EXEC and privileged-level EXEC	All
show statistics auto-discovery	Displays TFO auto-discovery statistics for a WAE.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics class-default	Displays statistics information about the class-default class map.	privileged-level EXEC	application- accelerator
show statistics class-map	Displays statistics information about about class maps.	privileged-level EXEC	application- accelerator
show statistics connection	Displays the connection statistics for a WAE.	privileged-level EXEC	application- accelerator

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show statistics connection auto-discovery	Displays the auto-discovery connection statistics for a WAE.	privileged-level EXEC	application- accelerator
show statistics connection closed	Displays the closed connection statistics for a WAE.	privileged-level EXEC	application- accelerator
show statistics connection conn-id	Displays the connection ID statistics for a WAE.	privileged-level EXEC	application- accelerator
show statistics connection egress-methods	Displays detailed egress method-related information about the connection segments for a WAE.	privileged-level EXEC	application- accelerator
show statistics connection optimized	Displays optimized information about the connection segments for a WAE.	privileged-level EXEC	application- accelerator
show statistics connection pass-through	Displays pass through information about the connection segments for a WAE.	privileged-level EXEC	application- accelerator
show statistics crypto ssl ciphers	Displays crypto SSL cipher usage statistics.	privileged-level EXEC	application- accelerator
show statistics datamover	Displays internal datamover information.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics dre	Displays the Data Redundancy Elimination (DRE) statistics for a WAE.	privileged-level EXEC	application- accelerator
show statistics filtering	Displays TFO flow statistics for a WAE.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics flow	Displays the flow statistics.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics generic-gre	Displays the generic GRE tunnel statistics.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics icmp	Displays the ICMP statistics.	user-level EXEC and privileged-level EXEC	All
show statistics ip	Displays the IP statistics.	user-level EXEC and privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show statistics netstat	Displays the Internet socket connection statistics.	user-level EXEC and privileged-level EXEC	All
show statistics pass-through	Displays the pass-through statistics.	privileged-level EXEC	application- accelerator
show statistics peer	Displays the DRE peer statistics for a WAE.	privileged-level EXEC	application- accelerator
show statistics radius	Displays the RADIUS authentication statistics.	user-level EXEC and privileged-level EXEC	All
show statistics services	Displays the services statistics.	user-level EXEC and privileged-level EXEC	All
show statistics sessions	Displays the dynamic match session statistics.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics snmp	Displays the SNMP statistics.	user-level EXEC and privileged-level EXEC	All
show statistics system cpu	Displays detailed parameters of the cpu utilization.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics tacacs	Displays the TACACS+ authentication and authorization statistics.	user-level EXEC and privileged-level EXEC	All
show statistics tcp	Displays the Transmission Control Protocol statistics.	user-level EXEC and privileged-level EXEC	All
show statistics tfo	Displays the Transport Flow Optimization (TFO) statistics for a WAE.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics udp	Displays the User Datagram Protocol (UDP) statistics.	user-level EXEC and privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show statistics wccp	Displays the WCCP statistics for a WAE.	user-level EXEC and privileged-level EXEC	application- accelerator
show statistics windows-domain	Displays the Windows domain configuration.	user-level EXEC and privileged-level EXEC	All
show sysfs volumes	Displays system file system information.	privileged-level EXEC	application- accelerator
show sysfs volumes	Displays the system file system (SYSFS) information.	user-level EXEC and privileged-level EXEC	All
show tacacs	Displays the TACACS+ configuration.	user-level EXEC and privileged-level EXEC	All
show tcp	Displays the TCP configuration.	user-level EXEC and privileged-level EXEC	All
show tech-support	Displays the system information for Cisco technical support.	privileged-level EXEC	All
show telnet	Displays the Telnet services configuration.	privileged-level EXEC	All
show tfo tcp	Displays TFO TCP buffer information.	privileged-level EXEC	application- accelerator
show transaction-logging	Displays the transaction logging information for a WAE.	user-level EXEC and privileged-level EXEC	application- accelerator
show user	Displays information about a particular user.	privileged-level EXEC	All
show users administrative	Displays the administrative users.	user-level EXEC and privileged-level EXEC	All
show version	Displays the software version.	user-level EXEC and privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show wccp	Displays the WCCP information for a WAE.	user-level EXEC and privileged-level EXEC	application- accelerator
show windows-domain	Displays the Windows domain configuration.	user-level EXEC and privileged-level EXEC	All
(config-if) shutdown	Shuts down the specified interface.	interface configuration	All
shutdown	Shuts down the device (stops all applications and operating system).	privileged-level EXEC	All
(config) smb-conf	Manually configures parameters in the Samba configuration file, *smb-conf*.	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
ssh	Creates or deletes SNMP triggers on a MIB variable.	privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
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) stats-collector logging	Configures SMB statistics logging.	global configuration	application- accelerator
(config) system jumbomtu	Configures a jumbo MTU on all interfaces.	global configuration	application- accelerator
(config) tacacs	Configures the TACACS+ parameters on a WAAS device.	global configuration	All
(config) tcp	Configures the TCP parameters.	global configuration	All
tcpdump	Dumps the TCP traffic on the network.	privileged-level EXEC	All
telnet	Starts the Telnet client.	user-level EXEC and privileged-level EXEC	All
(config) telnet enable	Enables the Telnet services.	global configuration	All
terminal	Sets the terminal output commands.	user-level EXEC and privileged-level EXEC	All
test	Performs diagnostic tests and displays the results.	user-level EXEC and privileged-level EXEC	All
tethereal	Analyzes network traffic from the command line.	privileged-level EXEC	All
(config) tfo exception	Configures TFO exception handling.	global configuration	application- accelerator
(config) tfo optimize	Configures TFO optimization for DRE or full generic optimization on the WAE.	global configuration	application- accelerator
(config) tfo tcp adaptive-buffer-sizing	Configures TFO optimization with TCP adaptive buffer sizing.	global configuration	application- accelerator

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) tfo tcp keepalive	Configures TFO optimization with a TCP keepalive on a WAE.	global configuration	application- accelerator
(config) tfo tcp optimized-mss	Configures TFO optimization with an optimized-side TCP maximum segment size on a WAE.	global configuration	application- accelerator
(config) tfo tcp optimized-receive-buffer	Configures TFO optimization with an optimized-side receive buffer on a WAE.	global configuration	application- accelerator
(config) tfo tcp optimized-send-buffer	Configures TFO optimization with an optimized-side send buffer on a WAE.	global configuration	application- accelerator
(config) tfo tcp original-mss	Configures TFO optimization with an unoptimized-side TCP maximum segment size on the WAE.	global configuration	application- accelerator
(config) tfo tcp original-receive-buffer	Configures TFO optimization with an unoptimized-side receive buffer on a WAE.	global configuration	application- accelerator
(config) tfo tcp original-send-buffer	Configures TFO optimization with an unoptimized-side send buffer on a WAE.	global configuration	application- accelerator
(config) threshold-monitor	Configures monitoring thresholds in a WAAS deployment.	global configuration	application- accelerator
top	Displays the current top CPU activities.	privileged-level EXEC	All
traceroute	Traces the route to a remote host.	user-level EXEC and privileged-level EXEC	All
transaction-log	Forces the transaction logging for TFO and export on a WAE.	privileged-level EXEC	application- accelerator
type	Displays a file.	user-level EXEC and privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	user-level EXEC and privileged-level EXEC	All
(config) username	Establishes the username authentication.	global configuration	All
(config-ssl-accelerated) version	Specifies the type of SSL protocol to use for accelerated services.	SSL accelerated service configuration	All
(config-ssl-global) version	Specifies the type of SSL protocol to use for global services.	SSL global service configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-ssl-peering) version	Specifies the type of SSL protocol to use for management services.	SSL host peering service configuration	All
(config-ssl-mgmt) version	Specifies the type of SSL protocol to use for management services.	SSL management service configuration	All
vm	Initializes the virtual machine, and configures the host clock sync setting.	privileged-level EXEC	application- accelerator
(config) wccp access-list	Configures the IP access list for inbound Web Cache Coordination Protocol (WCCP) GRE-encapsulated traffic on a WAE.	global configuration	application- accelerator
(config) wccp router-list	Enables the WCCP flow protection feature on a WAE.	global configuration	application- accelerator
(config) wccp router-list	Creates a router list on a WAE for use in the WCCP Version 2 services.	global configuration	application- accelerator
(config) wccp shutdown	Sets the maximum time interval after which the WAE will perform a clean shut down.	global configuration	application- accelerator
(config) wccp tcp-promiscuous service-pair	Configures and enables the TCP promiscuous mode service on a WAE.	global configuration	application- accelerator
(config-wccp-service) weight	Configures the weight assigned to a WAE.	WCCP configuration	application- accelerator
waas-tcptrace	Lists WAAS devices in the path to a destination host.	user-level EXEC and privileged-level EXEC	All
whoami	Displays the name of the current user.	user-level EXEC and privileged-level EXEC	All
windows-domain	Accesses Windows domain utilities.	privileged-level EXEC	All
(config) windows-domain	Configures Windows domain server options.	global configuration	All
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the MIB persistence configuration to disk.	privileged-level EXEC	All

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.
- PKI Certificate Authority configuration mode commands that you can enter after you access certificate authority 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 PKI global settings configuration mode. See the "PKI Global Settings Configuration Mode Commands" section for a complete listing of commands.
- SSL accelerated service configuration mode commands that you can enter after you access SSL accelerated service configuration mode. See the "SSL Accelerated Service Configuration Mode Commands" section for a complete listing of commands.
- SSL cipher list configuration mode commands that you can enter after you access SSL cipher list configuration mode. See the "SSL Cipher List Configuration Mode Commands" section for a complete listing of commands.
- SSL global service configuration mode commands that you can enter after you access SSL global service configuration mode. See the "SSL Global Service Configuration Mode Commands" section for a complete listing of commands.
- SSL host peering service configuration mode commands that you can enter after you access SSL host peering service configuration mode. See the "SSL Host Peering Service Configuration Mode Commands" section for a complete listing of commands.

- SSL management service configuration mode commands that you can enter after you access SSL management service configuration mode. See the "SSL Management Service Configuration Mode Commands" section for a complete listing of commands.
- WCCP configuration mode commands that you can enter after you access WCCP configuration mode. See the "WCCP 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

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

cd *directoryname*

Syntax Description

directoryname	Directory name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

deltree

dir

lls

ls

mkdir

pwd

clear arp-cache

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

clear arp-cache [*ipaddress* | **interface** {**GigabitEthernet** *slot/port* | **PortChannel** *index* | **Standby** *grpNumber* | **TenGigabitEthernet** *slot/port* | **InlinePort** *slot/grpnumber* {**lan | wan**}}]

Syntax Description

ipaddress	(Optional) ARP entries for the IP address.
interface	(Optional) Clears all ARP entries on the designated interface.
GigabitEthernet *slot/port*	Clears the Gigabit Ethernet interface (slot/port).
PortChannel *index*	Clears the Port channel interface number (1-4).
Standby *grpNumber*	Clears the Standby group number (1-2).
TenGigabitEthernet *slot/port*	Clears the 10-Gigabit Ethernet interface (slot/port).
InlinePort *slot/grpnumber* {**lan** | **wan**}	Clears the inline port interface (slot/group). Specify **lan** for the LAN interface or **wan** for the WAN interface.

Defaults

No default behavior or values.

Note that on ISR-WAAS, the default-gateway (ISR host's interface address) cannot be cleared from ARP cache.

Command Modes

EXEC

Device Modes

application-accelerator

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 bmc

To clear the BMC logs and events, use the **clear bmc** EXEC command.

clear bmc [**event-log**]

Syntax Description

event-log	Clears BMC system events and logs.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows how to clear the entries recorded in the BMC system event log on the WAAS device:

```
WAE# clear bmc event-log
```

Related Commands

show bmc

clear cache

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

clear cache {**dre}**

clear cache http-metadatacache https {**conditional-response** | **redirect-response** | **unauthorized-response**}

clear cache http-metadatacache {**all** | **conditional-response** | **redirect-response** | **unauthorized-response**} [*url*]

Syntax Description

dre	Expires the DRE cache.
https	Clears cache entries for HTTPS metadata cache response types.
conditional-response	Clears cache entries for conditional responses (304).
redirect-response	Clears cache entries for redirect responses (301).
unauthorized-response	Clears cache entries for authorization required responses (401).
http-metadatacache	Clears the HTTP accelerator metadata cache.
all	Clears cache entries for all HTTP metadata cache response types.
url	Clears cache entries matching only the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

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.

The **clear cache dre** command may cause the system to reboot, but you are asked to confirm before the command continues and you are given a chance to save any configuration changes that have been made to the running configuration.

The **clear cache dre** command does not delete the DRE cache contents but expires it by removing markers in the content to prevent reuse. If you want to delete the cache contents, use the **disk delete-data-partitions** command.

Examples

The following example shows how to clear the HTTP metadata cache for conditional responses:

```
WAE# clear cache http-metadatacache conditional-response
```

Related Commands

license add

show cache http-metadatacache

show interface

show license

show wccp

clear cache http-object-cache invalidate

To clear the object cache, use the **clear cache http object-cache** EXEC command.

clear cache http-object-cache invalidate

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

This command clears all entries in the cache directory as a background task, but leaves entries up to 60 seconds prior to the command being given. It can take a few minutes to complete, but the CE is functional while the process is ongoing. Data on the disk remains and is not overwritten. Log entries appear indicating the beginning and end of the operation.

Examples

The following example shows how to clear the HTTP object cache:

```
WAE# clear cache http-object-cache invalidate
```

clear cdp

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

clear cdp {**counters** | **table**}

Syntax Description

counters	Clears the CDP counters.
table	Clears the CDP tables.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

```
WAE# clear cdp counters
```

Related Commands

license add

show interface

show license

show wccp

clear connection

To reset one or more connections, use the **clear connection** EXEC command.

clear connection [**client-ip** {*ip_address* | *hostname*} | **client-port** *port* | **flow-id** *id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*]

Syntax Description

client-ip	Resets the connections with the specified client IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	Resets the connections with the specified client port number. The port number is from 1 to 65535.
flow-id *id*	Resets the connection with the specified number identifier.
server-ip	Resets the connections with the specified server IP address or hostname.
server-port *port*	Resets the connections with the specified server port number. The port number is from 1 to 65535.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows how to reset connection number 45 on the WAAS device:

```
WAE# clear connection flow-id 45
```

The following example shows how to reset connections with server port 80 on the WAAS device:

```
WAE# clear connection server-port 80
```

Related Commands

show statistics connection

clear dre

To clear DRE configurations, use the **clear dre** EXEC command.

clear dre auto-bypass [{*ip_address* | *hostname*} *port* **]**

Syntax Description

ip_address	(Optional) IP address of a server.
hostname	(Optional) Hostname of a server.
port	(Optional) A port number in the range from 1 to 65535.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to clear all DRE auto-bypass entries:

```
WAE# clear dre auto-bypass
```

The following example shows how to clear the DRE auto-bypass entry for a specific port on a specific server:

```
WAE# clear dre auto-bypass server 1.2.3.4 17
```

Related Commands

show dre

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

access-list	Clears the access list statistical information.
counters	Clears the IP access list counters.
acl-num	(Optional) Counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
acl-name	(Optional) 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 ipv6

To clear IPv6 neighbor cache entries, use the **clear ipv6 neighbors** EXEC command.

clear ipv6 neighbors {GigabitEthernet [*slot number/port***] | Portchannel [***Etherchannel index***] | standby [***standby index***] }**

clear ipv6 neighbors virtual *slot/port*

Syntax Description

GigabitEthernet *slot number/port*	Clears the neighboring ipv6 cache entries for the GigabitEthernet interface.
PortChannel *index*	Clears the neighboring ipv6 cache entries for the EtherChannel device (1-4).
standby *grpNumber*	Clears the neighboring ipv6 cache entries for the standby device (1-2).
virtual	Clear neighboring ipv6 cache entries for Virtual Ethernet device (1-2)

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to clear the neighboring cache entries for a GigabitEthernet interface on the WAAS device:

```
WAE# clear ipv6 neighbors GigabitEthernet 0/0
vWAAS# clear ipv6 neighbors virtual 1/0
```

Related Commands

show ipv6

show interface

show license

show wccp

clear ip

clear license

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

clear license [*license-name*]

Syntax Description

license-name	Name of the software license to remove. The following license names are supported: • Transport—Enables basic DRE, TFO, and LZ optimization. • Enterprise—Enables the EPM, HTTP, MAPI, SSL, and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization. You cannot remove this license if the virtualization licenses are installed. You must remove both of those licenses first.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to clear the licensing configuration on the WAAS device:

```
WAE# clear license
```

Related Commands

license add

show interface

show license

show wccp

clear logging

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

clear 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

The **clear logging** command removes all current entries from the *syslog.txt* file but does not make an archive of the file. It puts a “Syslog cleared” message in the *syslog.txt* file to indicate that the syslog has been cleared.

Examples

The following example shows how to clear all entries in the *syslog.txt* file on the WAAS device:

```
WAE# clear logging

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

Related Commands

license add

show interface

show license

show wccp

clear object-cache

To remove objects from object cache that match specified criteria, use the **clear object-cache** EXEC command.

clear object-cache [accelerator *ao-name*] **all**

clear object-cache [accelerator *ao-name*] **server {server-ip** *server-ip* | **server-host** *hostname*}

clear object-cache [accelerator *ao-name*] **url** *path*

Syntax Description

accelerator *ao-name*	(Optional) The name of the application accelerator specified, such as HTTP.
all	Clears all objects from the object cache. If you specify **all**, you will be prompted to confirm this action. Note that for WAAS Version 6.0, **all** is used only with accelerator HTTP.
server	Clears objects from the object cache of the server with the specified server IP address or hostname.
server-host *hostname*	Clears objects from the object cache of the specified server hostname.
server-ip *server-ip*	Clears objects from the object cache of the specified server IP address.
url *path*	Clears objects from the object cache for the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **clear object-cache** command removes all objects from the object cache, or all objects from cache that match specified criteria, such as AO name, server IP address or hostname, or path of a specified URL.

Examples

The following example shows how to clear objects from object cache that match the criteria of the SMB AO and the URL www.sampletestdomain.com.

```
WAE# clear object-cache accelerator http url www.sampletestdomain.com
```

Related

clear statistics object-cache

clear service-policy

To clear class map and policy map counters for optimization policies, use the **clear service-policy** EXEC command.

clear service-policy [**type** { **waas**}] **counters**

Syntax Description

type	Specifies the type of counters to clear.
waas	Clears WAAS optimization class map and policy map counters.
counters	Clears the class map and policy map counters.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

When specified without the **type** keyword, this command clears counters for WAAS optimization class maps and policy maps.

Examples

The following example shows how to clear WAAS optimization class map and policy map counters:

```
WAE# clear service-policy counters
```

Related Commands

show class-map

show policy-map

show statistics class-map

show statistics policy-sub-class

clear statistics

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

clear statistics {**all** | **authentication** | **auto-discovery** {**all** | **blacklist**} | **class-map**{**waas**} | **datamover** | **dre** [**global**] **| exporter | filtering | flow monitor type performance-monitor tcpstat-v1** | **generic-gre** | **icmp** | **inline** | **ip** | **ipv6** {**internal**} | **pass-through** | **peer dre** | **punt** | **radius** | | **snmp** | **tacacs** | **tcp** | **tfo** | **udp** | **wccp** | **windows-domain** | **windows-print**}

Syntax Description

all	Clears all statistics.
authentication	Clears authentication statistics.
auto-discovery	Clears the auto-discovery statistics.
blacklist	Clears the auto-discovery statistics for the blacklist.
class-map	Clears all class map statistics.
waas	Clears all statistics for WAAS class maps.
datamover	Clears all of the data mover statistics.
dre	Clears the Data Redundancy Elimination (DRE) statistics.
exporter	Clears the exporter statistics.
global	(Optional Clears the global DRE statistics.
filtering	Clears the filter table statistics.
flow	Clears the network traffic flow statistics.
monitor	Clears the monitor flow performance statistics.
tcpstat-v1	Clears the tcpstat-v1 collector statistics.
generic-gre	Clears the generic GRE statistics.
icmp	Clears the ICMP statistics.
inline	Clears the inline interception statistics.
ip	Clears the IP statistics.
ipv6	Clears IPv6 statistics.
pass-through	Clears all of the pass-through statistics.
peer dre	Clears all peer DRE statistics.
punt	Clears all the punt statistics.
radius	Clears the RADIUS statistics.
snmp	Clears the SNMP statistics.
tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
tfo	Clears the TCP flow optimization (TFO) statistics.
udp	Clears the UDP statistics.
wccp	Clears all of the WCCP statistics.
windows-domain	Clears the Windows domain statistics.

Defaults

No default behavior or values.

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.

Note that from software version 6.x onwards, **clear statistics snmp** does not clear all statistical counters due to net snmp implementation.

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 {**epm** | **generic** | **http** | **mapi** | **smb** | **ssl**}

Syntax Description

epm	Clears the statistics for the EPM application accelerator.
generic	Clears the statistics for generic accelerator.
http	Clears the statistics for the HTTP application accelerator.
mapi	Clears the statistics for the MAPI application accelerator.
ssl	Clears the statistics for the SSL application accelerator.
smb	Clears the statistics for the SMB application accelerator, ***except*** for statistics on signed SMB bytes counters. To clear statistics for signed SMB bytes (read from/written to LAN, read from/written to WAN), use **clear statistics accelerator generic**, which clears all accelerator statistics, including signed SMB bytes counters.

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 SMB application accelerator on the WAAS device:

```
WAE# clear statistics accelerator smb
```

Related Commands

clear statistics

clear statistics connection

clear statistics accelerator http object-cache

To clear object cache statistics for a WAAS device, use the **clear statistics accelerator HTTP object-cache** EXEC command.

clear statistics accelerator http object-cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use this command to clear object cache statistics.

Example

The following example shows how to clear object cache statistics for a WAAS device.

```
WAE# clear statistics accelerator http object-cache
```

Related

show statistics accelerator http object-cache

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* | {**epm** | **http** | **ica** | **mapi** | **smb** | **ssl** | **tfo** | **wansecure**} **dre** | **peer-id** *peer_id* | **server-ip** {*ip_address* | *hostname*} **| server-port** *port*]

Syntax Description

conn-id *connection_id*	Clears connection statistics for the connection with the specified number identifier.
optimized	Clears connection statistics for optimized connections.
client-ip	(Optional) Clears connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Clears the connection statistics for the client with the specified port number. The port number is from 1 to 65535.
epm	(Optional) Clears connection statistics for connections optimized by the EPM application accelerator.
http	(Optional) Clears connection statistics for connections optimized by the HTTP application accelerator.
ica	(Optional) Clears connection statistics for connections optimized by the ICA application accelerator.
mapi	(Optional) Clears connection statistics for connections optimized by the MAPI application accelerator.
smb	(Optional) Clears connection statistics for connections optimized by the SMB application accelerator.
ssl	(Optional) Clears connection statistics for connections optimized by the SSL application accelerator.
tfo	(Optional) Clears connection statistics for connections optimized by the TFO application accelerator.
wansecure	(Optional) Clears connection statistics for connections optimized by the WAN secure application accelerator.
dre	(Optional) Clears connection statistics for connections optimized by the DRE feature.
peer-id *peer_id*	(Optional) Clears the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295.
server-ip	(Optional) Clears the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Clears the connection statistics for the server with the specified port number. The port number is from 1 to 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 statistics object-cache

To clear statistics from object cache, use the **clear statistics object-cache** EXEC command.

clear statistics object-cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **clear statistics object-cache** command clears all statistical counters from the object cache.

Examples

The following example shows how to clear all statistics from the object cache:

```
WAE# clear statistics object-cache
```

Related

clear object-cache

clear transaction-log

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

clear transaction-log {**accelerator** | **flow**}

Syntax Description

accelerator	Clears the accelerator transaction log file.
flow	Clears the TFO transaction log.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

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*}]

Syntax Description

administrative	(Optional) Clears the connections (logins) of administrative users authenticated through a remote login service.
locked-out	(Optional) Unlocks specified locked-out user accounts.
all	Specifies all user accounts.
username *username*	Specifies the 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. Only locally authenticated administrative users can run this command.

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
```

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

To clear Windows domain server information for a WAAS device, use the **clear windows-domain** EXEC command.

clear windows-domain encryption-service blacklist {**identity** *tagName* | **service** *spn*}

Syntax Description

identity *tagName*	Clears identity information.
service *spn*	Clears service information.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **clear windows-domain** EXEC command to clear Windows domain server information.

Examples

The following example shows how to clear the Windows domain server information:

```
WAE(config)# clear windows-domain encryption-service blacklist identity some-id
```

Related Commands

show windows-domain

clear windows-domain-log

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

clear windows-domain-log

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 clear all entries in the Windows domain log file on the WAAS device:

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

Related Commands

license add

show interface

show license

show wccp

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

read-calendar	Reads the calendar and updates the system clock.
set *time day month year*	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).
update-calendar	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** {**config**}| **create** | **delete**

Syntax Description

config-sync	Sets the node to synchronize configuration with the WAAS Central Manager.
deregister	Removes the device registration record and its configuration on the WAAS Central Manager.
force	(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.
lcm	Configures local/central management on a WAAS device that is registered with the WAAS Central Manager.
enable	Enables synchronization of the WAAS network configuration of the device with the local CLI configuration.
disable	Disables synchronization of the WAAS network configuration of the device with the local CLI configuration.
maintenance	Cleans and reindexes the embedded database tables.
full	Specifies a full maintenance routine for the embedded database tables.
regular	Specifies a regular maintenance routine for the embedded database tables.
recover	Recovers the identity of a WAAS device.
identity *word*	Specifies the identity of the recovered device (identification key set on the Central Manager).
restore *filename*	Restores the database management tables using the backup local filename.
validate	Validates the database files.
database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
backup	Backs up the database management tables.
config	Backs up only configuration tables.
create	Creates the embedded database management tables.
delete	Deletes the embedded database files.

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.

Note For a vWAAS device, the model type must be configured before enabling management services.

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.

After the backup is complete, use the **copy disk ftp** command to move the backup file to a remote system.

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.

Note All CMS-related commands are disabled when running the **cms restore** command.

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

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

cms secure-store {**init** | **open** | **change** | **clear** | **reset** | **mode**{**user-passphrase** | **auto-passphrase**}}

Syntax Description

init	Initializes secure store encryption on the WAE device and opens the secure store. This option is valid only on WAE devices.
open	Activates secure store encryption (the WAAS device encrypts the stored data using secure store encryption). On WAEs, secure store encryption must already be initialized using the **cms secure-store init** command. This option is valid on all types of devices. On the Central Manager, this command is valid only when in user-provided passphrase mode and it prompts you to enter the secure store encryption pass phrase.
change	Changes the secure store encryption pass phrase and encryption key. On the Central Manager, this command prompts you to enter 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. After this option is used, the Central Manager is in user-provided passphrase mode. This option is valid only on the primary Central Manager and WAE devices.
clear	Disables secure store encryption. This option is valid only on WAE devices. **Note** If a Windows Domain User Account Identity has been configured on the device or the device group for encrypted-mapi acceleration, you will not be able to clear the secure store on the device. You must remove the Windows domain user account identity configuration from the device or device group before you can clear secure store.
reset	Resets secure store to the uninitialized state. You must initialize but not open secure store encryption and you must be in user-provided passphrase mode, to use this option. This option is valid only on primary Central Manager devices.
mode	Sets the secure store mode of opening. This option is valid only on primary Central Manager devices.
user-passphrase	Sets secure store to require a user-provided pass phrase to open after a reboot.
auto-passphrase	Sets secure store to automatically open after a reboot by using a unique system-generated pass phrase.

Defaults

A new Central Manager is configured for auto-generated passphrase mode with the secure store open.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Secure store encryption provides strong 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.

On a new Central Manager, secure store is initialized and open and in auto-generated passphrase mode. The only options are to change the pass phrase (which sets the secure store to user-provided passphrase mode) or to change to user-provided passphrase mode. To change to user-provided passphrase mode, use the **cms secure-store mode user-passphrase** command.

Note There may be a delay of a few minutes for the any changes you submit with the **cms secure-store** command to take effect. There may also be a delay for any changes to take effect if you submit changes at the WAAS CM **Configure** > **Security** > **Secure Store Settings** window.

For secure store on the Central Manager, the data is encrypted using a key encryption key generated from the pass phrase 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 can use your own password to enable secure store, but it is not necessary in auto-generated passphrase mode (the default), where the Central Manager generates a unique password automatically. A user-supplied 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

If you are using the user-provided passphrase mode, 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 and services that use encryption (such as the SSL application accelerator) are not available. If you are using the auto-generated passphrase mode (the default), the Central Manager automatically opens the secure store after a reboot by using its own generated pass phrase.

The secure store passphrase mode on the primary Central Manager is replicated to the standby Central Manager (within the standard replication time). If the primary Central Manager is switched to auto-generated passphrase mode, the standby Central Manager secure store changes to the open state. If the primary Central Manager is switched to user-provided passphrase mode or the passphrase is changed, the standby Central Manager secure store changes to the initialized but not open state and an alarm is raised. You must manually open the secure store on the standby 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 and dynamic share 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 a Central Manager that is configured in user-provided passphrase mode and you forget the secure store password. This command deletes all encrypted data, certificate and key files, and key manager keys. The secure store is left in the open state using auto-generated passphrase mode. For the complete procedure for resetting the secure store, see the "Resetting Secure Store Encryption on a Central Manager" section on page 9-17 in the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to change the pass phrase mode of the secure store encryption on the WAAS Central Manager:

```
waas-cm# cms secure-store mode user-passphrase
Stopping cms.
Do you wish to switch to User-provided passphrase mode? [yes]/no :y


The passphrase must adhere to the following rules
*******************************************************************
* 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 new passphrase:
Confirm passphrase:

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

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

copy cdrom install *filedir filename*

Syntax Description

install *filedir filename*	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

write

copy compactflash

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

copy compactflash install *filename*

Syntax Description

install *filename*	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

write

copy disk

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

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

Syntax Description

ftp	Copies to a file on an FTP server.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server to which the local file is copied.
remotefilename	Name of the local file once it has been copied to the FTP server.
localfilename	Name of the local file to be copied.
startup-config *filename*	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

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 wow-recovery {*hostname* | *ip-address*} *remotefiledir remotefilename*

Syntax Description

disk	Copies a file to a local disk.
hostname	Hostname of the specific server.
ip-address	IP (IPV4/IPv6) address of the specific server.
remotefiledir	Directory on the FTP server where the image file to be copied is located.
remotefilename	Name of the file to be copied.
localfilename	Name of the copied file as it appears on the local disk.
install	Copies the file from an FTP server and installs the software release or firmware file to the local device.

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. This command can also be used to install a BIOS or other firmware update by specifying the appropriate update file.

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.

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

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# copy ftp install upgradeserver /bios/update53/derived/ bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
 .
 .
 .
Primary BIOS flashed successfully
Cleanup BIOS related files that were downloaded....
The new software will run after you reload.
WAE#
```

Related Commands

install

reload

show running-config

show startup-config

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

install	Copies the file from an HTTP server and installs the software release file to the local device.
hostname	Name of the HTTP server.
ip-address	IP (IPV4/IPv6) address of the HTTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
port *portnum*	(Optional) Specifies the port number (1–65535) to connect to the HTTP server (the default is 80).
proxy *proxy_portnum*	(Optional) Allows the request to be redirected to an HTTP proxy server. HTTP proxy server port number (1–65535).
username *username password*	(Optional) Specifies the username and password to access the HTTP proxy server.

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.

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# copy ftp install upgradeserver /bios/update53/derived/ bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
 .
 .
 .
```

Related Commands

install

reload

show running-config

show startup-config

write

copy monitoring-log

To copy SMB statistics data to the local disk or an FTP server, use the **copy monitoring-log** EXEC command.

copy monitoring-log {**disk** *filename* | **ftp** {*hostname* | *ip-address*} *remotefiledir remotefilename*}

Syntax Description

disk *filename*	Copies the statistics in CSV format to the specified local disk file in the /local/local1 directory.
ftp	Copies the statistics in CSV format to the specified remote file on an FTP server.
hostname	Name of the FTP server.
ip-address	IP (IPV4/IPv6) address of the FTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this command to write the last 14 days of statistics data that has been collected by the **stats-collector logging** global configuration command. The data is written as a CSV file compressed in tar archive format.

Examples

The following example shows how to copy statistics data to an FTP server:

```
WAE# copy monitoring-log ftp 10.1.1.1 mydir mystats
```

Related Commands

(config) stats-collector logging

copy running-config

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

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

Syntax Description

disk *filename*	Copies the current system configuration to a disk file. Specify the name of the file to be created on a disk.
startup-config	Copies the running configuration to startup configuration (NVRAM).
tftp	Copies the running configuration to a file on a TFTP server.
hostname	Hostname of the TFTP server.
ip-address	IP (IPV4/IPv6) address of the TFTP server.
remotefilename	Remote filename of the configuration file to be created on the TFTP server. Use the complete pathname.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

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

write

copy scp

To securely copy configuration or image files from a source to a destination location, use the **copy scp** EXEC command.

copy scp {{**disk** {*hostname* | *ip-address*} *remote_dir remote_file local_file*} | {**install** {*hostname* | *ip-address*} *remote_dir remote_file*}}

Syntax Description

disk	Copies the current system configuration to a disk file.
hostname	Hostname of the SCP server.
ip-address	IP (IPV4/IPv6) address of the SCP server.
remote_dir	Remote directory where the system information file is to be created on the SCP server.
remote_file	Remote filename of the system information file to be created on the SCP server.
local_file	Name of the copied file as it appears on the local disk.
install	Copies the file from a source server and installs the software release or firmware file to the local device.
hostname	Hostname of the SCP server.
ip-address	IP address of the SCP server.
remote_dir	Remote directory where the system information file is to be created on the SCP server.
remote_file	Remote filename of the system information file to be created on the SCP server.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **copy scp disk** EXEC command to copy a file from an SCP server to a SYSFS partition on the WAAS device.

Use the **copy scp install** EXEC command to install a software release or firmware file from an SCP server on a WAAS device.

Examples

The following example shows how to securely install the software release or firmware file from a source to a destination location:

```
WAE#copy scp install 2.43.65.21 /work/admin ruby.test.bin
```

```
Enter usename for remote scp server: admin

                                 WARNING!!!
                    READ THIS BEFORE ATTEMPTING TO LOGON

      This System is for the use of authorized users only.  Individuals
      using this computer without authority, or in excess of their
      authority, are subject to having all of their activities on this
      system monitored and recorded by system personnel.  In the course
      of monitoring individuals improperly using this system, or in the
      course of system maintenance, the activities of authorized users
      may also be monitored.  Anyone using this system expressly
      consents to such monitoring and is advised that if such
      monitoring reveals possible criminal activity, system personnel
      may provide the evidence of such monitoring to law enforcement
      officials.

      Cisco Acceptable Use Policy:
      http://wwwin.cisco.com/infosec/policies/acceptableuse.shtml

admin@2.43.65.21's password:
ruby.test.bin        100% |*****************************|   432 MB    00:13
Backing up existing version WAAS 5.1.0-b67, built on 02:20:49 Nov 29 2012 by damaster
Converting Manifest files ...  Done
Rebuilding image based on current software ...  Done
Backing up flash configuration ...  Done
Reclaiming unused flash safe state sectors ...SSMGR RETURNING: 4 (Success)
Done.
Detected OE594
Installing phase3 bootloader...
Installing WAE 64-bit image.
buildsysimg: short write on /swstore/comp.basesystem: Inappropriate ioctl for device
/swstore/default_ruby_installer.sh: problem running buildsysimg
Remove /swstore/backup to free up space.
Installing system image to flash... The new software will run after you reload.
```

Related Commands

install

copy sysreport

copy tech-support

copy startup-config

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

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

Syntax Description

disk *filename*	Copies the startup configuration to a disk file. Specify the name of the startup configuration file to be copied to the local disk.
running-config	Copies the startup configuration to running configuration.
tftp	Copies the startup configuration to a file on a TFTP server.
hostname	Hostname of the TFTP server.
ip-address	IP (IPV4/IPv6) address of the TFTP server.
remotefilename	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

write

copy sysreport

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

copy sysreport disk *filename* [**start-date** {*day month* **|** *month day*} *year* [**end-date** {*day month* | *month day*} *year*]]

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

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

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

copy sysreport usb *filename* [**start-date** {*day month* **|** *month day*} *year* [**end-date** {*day month* | *month day*} *year*]]

Syntax Description

disk *filename*	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.
ftp	Copies system information to a FTP server.
hostname	Hostname of the server.
ip-address	IP(IPV4/IPv6) address of the server.
remotedirectory	Remote directory where the system information file is to be created on the server.
remotefilename	Remote filename of the system information file to be created on the server.
scp	Copies system information to a SCP server.
hostname	Hostname of the server.
ip-address	IP address of the server.
remotedirectory	Remote directory where the system information file is to be created on the server.
remotefilename	Remote filename of the system information file to be created on the server.
start-date	(Optional) Specifies the start date of the information in the generated system report.
day month	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.
year	Start date year (1993–2035).
end-date	(Optional) Specifies the 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.
day month	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.

year	End date year (1993–2035).
tftp	Copies system information to a TFTP server.
start-date	(Optional) Specifies the start date of the information in the generated system report.
day month	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.
year	Start date year (1993–2035).
end-date	(Optional) Specifies the 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.
usb *filename*	Copies system information to a USB flash drive installed in a WAVE-294/594/694/7541/7571/8541 device. Specify the name of the file to be created on the USB flash drive. Note that .tar.gz is appended to the filename that you specify.

Defaults

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

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

A system report is a comprehensive report, which you must generate before contacting Cisco technical support. The system report contains output from many commands and system logs, including show commands, network and other statistics, graphs, log content, and configuration settings.

Note The **copy sysreport** command consumes significant CPU and disk resources and can adversely affect system performance while it is running. The system report can be from 30 MB to 100MB in size, or larger, depending on your system configuration.

- Before you run the **copy sysreport** command:
  - Before generating a system report, use the **test** command to run diagnostic tests, so that diagnostic information is also included in the system report.
  - Before generating a system report on a WAAS CM or standby WAAS CM, make a database backup by using the **cms database backup** command.
- To generate a system report and store it on an FTP server, use the following form of the sysreport command:

  copy sysreport ftp *server-ip*

- Generating the system report:

  When you run the **copy sysreport disk** command, the system report must be saved to the local1 directory.

  Note When you run the **copy sysreport disk** command, the system report save process differs depending on the version of WAAS you are running.

  For WAAS versions 6.1.x and later, the **copy sysreport disk** command saves the system report to the present working directory. Therefore, you must be in the **local1** directory path when you run the **copy sysreport disk** command. If you are not in the local1 directory, the error message "Could not generate sysreport in location *your-current-location*" is displayed.

  To display your present working directory, use the pwd command. To change your directory, use the cd command.

  For WAAS versions earlier than 6.1.x, the **copy sysreport disk** command saves the system report to the local1 directory, irregardless of your present working directory. Therefore, you can be in any system directory when you run the **copy sysreport disk** command, and the system report is saved to the local1 directory.

- Storing the completed system report:

  Because the system report is such a large file, after you run the **copy sysreport disk** command, move the report file out of the disk, to save significant disk space. To do this, follow these steps:

  1. `WAE# copy generatedSysreport-name ftp server-name`
     The generated system report is copied from the current disk location and a copy is stored to a non-current-disk destination.
  2. `WAE# delfile generatedSysreport-name`
     The original generated system report on the current disk is deleted.

Examples

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

```
WAE# copy sysreport disk mysysinfo start-date 1 March 2016 end-date March 31 2016
```

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

```
WAE# copy sysreport ftp myserver / myfile start-date 1 March 2016 end-date March 31 2016
```

Related Commands

cms

pwd

show running-config

show startup-config

test

copy system-status

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

copy system-status disk *filename*

Syntax Description

disk *filename*	Specifies the name of the file to be created on the disk.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example shows how to copy the system status to a disk file:

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

Related Commands

install

reload

show running-config

show startup-config

write

copy tech-support

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

copy tech-support {**disk** *filename* | **ftp** {*hostname* | *ip-address*} *remotedirectory remotefilename* | **scp** {*hostname* | *ip-address*} *remotedirectory remotefilename* | **tftp** {*hostname* | *ip-address*} *remotefilename*}

Syntax Description

disk *filename*	Copies system information for technical support to a disk file. Specify the name of the file to be created on disk.
ftp	Copies system information for technical support to an FTP server.
hostname	Hostname of the server.
ip-address	IP (IPV4/IPv6) address of the server.
remotedirectory	Remote directory of the system information file to be created on the server. Use the complete pathname.
remotefilename	Remote filename of the system information file to be created on the server.
scp	Copies system information for technical support to an SCP server
hostname	Hostname of the server.
ip-address	IP address of the server.
remotedirectory	Remote directory of the system information file to be created on the server. Use the complete pathname.
remotefilename	Remote filename of the system information file to be created on the server.
tftp	Copies system information for technical support to a TFTP server.

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

reload

show running-config

show startup-config

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*

Syntax Description

disk	Copies an image from a TFTP server to a disk file.
hostname	Hostname of the TFTP server.
ip-address	IP (IPV4/IPv6) address of the TFTP server.
remotefilename	Name of the remote image file to be copied from the TFTP server. Use the complete pathname.
localfilename	Name of the image file to be created on the local disk.
running-config	Copies an image from a TFTP server to the running configuration.
startup-config	Copies an image from a TFTP server to the startup configuration.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to copy configuration or image data from a TFTP server to the running configuration:

```
WAE# copy tftp running-config
```

Related Commands

install

reload

show running-config

show startup-config

write

cpfile

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

cpfile *oldfilename newfilename*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Only SYSFS files can be copied.

Examples

The following example shows how to create a copy of a file:

```
WAE# cpfile fe512-194616.bin fd512-194618.bin
```

Related Commands

deltree

dir

lls

ls

mkdir

pwd

rename

crypto delete

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

crypto delete {**ca-certificate** *filename* | **pkcs12** {*filename* | **admin** }}

Syntax Description

ca-certificate *filename*	Deletes a certificate authority certificate file.
pkcs12 *filename*	Deletes a PKCS12 format file. (PKCS12 files contain both the private encryption key and the public key certificate.)
admin	Deletes the certificate and key for the Central Manager admin service, if a custom certificate and key were installed. This option can be used only on the Central Manager.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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.

If you use the **crypto delete pkcs12 admin** command to delete a custom certificate and key that were installed for the Central Manager admin service, the admin service uses its built-in self-signed certificate.

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** | **admin** | *filename*} {**pem-cert-key** | **pem-cert-only** | **pem-key-only** | **pkcs12**}}{**disk** *pathname* | **ftp** *address* | **sftp** *address* | **terminal** | **tftp** *address*}

Syntax Description

ca-certificate *filename*	Exports a certificate authority certificate file.
pkcs12	Exports a PKCS12 format file. (PKCS12 files contain both the private encryption key and the public key certificate.)
factory-self-signed	Specifies that the SSL PKCS file is to be self-signed.
admin	Specifies that the certificate and key are for the Central Manager admin service. This option can be used only on the Central Manager.
filename	Name of the PKCS12 file to be exported.
pem-cert-key	Exports both the certificate and key in PEM format.
pem-cert-only	Exports only the certificate in PEM format.
pem-key-only	Exports only the key in PEM format.
pkcs12	Exports both the certificate and key in PKCS12 format.
disk *pathname*	Exports to a disk. Type the disk filename including the full path.
ftp *address*	Exports to FTP. Type the FTP server’s IP address or hostname.
sftp *address*	Exports to secure FTP. Type the secure FTP server’s IP address or hostname.
terminal	Exports to a terminal. (Not available for **crypto export pkcs12**.)
tftp *address*	Exports to TFTP. Type the TFTP server’s IP address or hostname.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

```
WAE# crypto export ca-certificate mycert.ca ftp 1.2.3.4 dir1 mycert.ca
```

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:

```
WAE# crypto export pkcs12 myfile.p12 pkcs12 disk /local1/myfile.p12
```

Related Commands

crypto delete

crypto generate

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 rsa modulus	Generates a certificate signing request (CSR)
rsa modulus	Generates a self-signed certificate.
1024 | **1536** | **2048** | **512** | **768**	Specifies the size (number of bits) used for the RSA modulus for a CSR or a self-signed certificate. **Note** The valid size for the RSA modulus for a self-signed certificate is dependent on the WAAS Version used. Refer to the crypto generate command Usage Guidelines for how to specify the RSA modulus size for WAAS Version 6.1.x and earlier, and for WAAS Version 6.2.x and later.
disk *pathname*	Generates the file to a disk. Type the disk filename including the full path.
ftp *address*	Generates the file to FTP. Type the FTP server's IP address or hostname.
sftp *address*	Generates the file to secure FTP. Type the secure FTP server's IP address or hostname.
terminal	Generates the file to a terminal.
tftp *address*	Generates the file to TFTP. Type the TFTP server's IP address or hostname.
self-signed-cert *filename*	Generates a self-signed SSL encryption certificate. The filename of the self-signed certificate to be generated must have the .p12 file extension.
exportable	(Optional) Allows the self-signed certificate to be exported.
rsa modulus	Specifies 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

Usage Guidelines

The valid size (number of bits) for the RSA modulus for a self-signed certificate is dependent on the WAAS version:

- *For WAAS Version 6.1.x and earlier,* the valid RSA module size is 512, 768, 1024, 1536, or 2048.

Note A self-signed certificate on WAAS Version 6.1.x or earlier with an RSA modulus size of 512 is *not* compatible with Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later. A self-signed certificate on WAAS Version 6.1.x or earlier with an RSA modulus size of 512 *is* compatible with Internet Explorer 8 and later.

If you have previously configured the RSA modulus size as 512: to access the WAAS CM with Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later, you must regenerate the self-signed certificate with an RSA modulus size of **2048**, and then upgade to the specified version of Mozilla FireFox or Google Chrome.

- *For WAAS Version 6.2.x and later,* the valid RSA module size is 768, 1024, 1536, or 2048. The RSA module size 512 is *not* used with WAAS Version 6.2.x and later.

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 2048-bit RSA modulus.

```
WAE# crypto generate self-signed-cert myfile.p12 exportable rsa modulus 2048
Generating a 2048bit 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
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 import** EXEC command.

crypto import ca-certificate *filename* {**disk** *pathname* | **ftp** *host* | **http** *host* | **scep** *url* | **sftp** *host* | **terminal** | **tftp** *host*}

crypto import pkcs12 {*filename* | **admin**} [**exportable**] [**ignore-cert-chain-order**] **pem-cert-key** {**disk** *pathname* | **ftp** *host* | **http** *host* | **scep** *url* | **sftp** *host* | **terminal** | **tftp** *host*}

crypto import pcsk12 {*filename* | **admin**} [**exportable**] [**ignore-cert-chain-order**] **pkcs12** {**disk** *pathname* | **ftp** *host* | **http** *host* | **sftp** *host* | **terminal** | **tftp** *host*}

Syntax Description

ca-certificate *filename*	Imports a certificate authority certificate file. The name of the CA certificate file to be imported (PEM format) must have .ca extension.
pkcs12 *filename*	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. DSA-encoded certificates are not supported and will not be imported.
admin	Specifies that the certificate and key are for the Central Manager admin service. This option can be used only on the Central Manager.
exportable	(Optional) Configures the imported certificate to be exportable.
ignore-cert-chain-order	(Optional) Allows the **crypto import** command to import a certificate chain that does not have a strict order.
pem-cert-key	Imports both the certificate and key in PEM format. When you use the **pem-cert-key** keyword, 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**.
pkcs12	Imports both the certificate and key in PKCS12 format.
disk *pathname*	Imports from a disk. Type the disk filename including the full path.
ftp *address*	Imports from FTP. Type the FTP server's IP address or hostname.
sftp *address*	Imports from secure FTP. Type the secure FTP server's IP address or hostname.
scep *url*	Imports from a SCEP server. Type the SCEP server's IP address.
terminal	Imports from a terminal.
tftp *address*	Imports from TFTP. Type the TFTP server's IP address or hostname.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The Central Manager admin service uses a self-signed certificate and key by default. You can use the **crypto import pkcs12 admin** command to import a custom certificate and key in PKCS12 or PEM format. If you delete the custom certificate and key, the self-signed certificate and key again become active.

Note DSA certificates and keys cannot be imported.

Examples

The following example shows how to import a CA certificate file named mycert.ca from a TFTP server:

```
WAE# crypto import ca-certificate mycert.ca tftp 00.00.00.00
```

Related Commands

crypto delete

crypto export

crypto generate

crypto pki

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

crypto pki managed-store initialize

Syntax Description

managed-store	Specifies managed store commands.
initialize	Initializes the PKI managed store.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows how to initialize the PKI managed store:

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

Related Commands

crypto export

crypto generate

crypto import

debug aaa accounting

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

debug aaa accounting

undebug aaa accounting

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

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 23.

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 **undebug** 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 aaa authorization

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

debug aaa authorization

undebug aaa authorization

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

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

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

```
WAE# debug aaa authorization
```

Related Commands

show debugging

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

no debug accelerator generic [**connection** | **misc** | **shell** | **stats** | **all**]

debug accelerator http [**bypass-list** | **cli** | **conditional-response** | **connection** | **dre-hints** | **metadatacache** | **redirect-response** | **shell** | **subnet** | **supress-server-encoding** | **transaction** | **unauthorized-response** | **all**]

no debug accelerator http [**bypass-list** | **cli** | **conditional-response** | **connection** | **dre-hints** | **metadatacache** | **redirect-response** | **shell** | **subnet** | **supress-server-encoding** | **transaction** | **unauthorized-response** | **all**]

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

no debug accelerator mapi [**all** | **Common-flow** | **DCERPC-layer** | **EMSMDB-layer** | **IO** | **ROP-layer** | **ROP-parser** | **RPCHTTP-layer** | **RCP-parser** | **shell** | **Transport** | **Utilities**]

debug accelerator ica [**all** | **ao-connectionmgr** | **ao-parser** | **cgp** | **connection** | **crypto** | **detectionparser** | **failure** | **hash** | **ica** | **initialization | io | main | pipe | shell**]

no debug accelerator ica [**all** | **ao-connectionmgr** | **ao-parser** | **cgp** | **connection** | **crypto** | **detectionparser** | **failure** | **hash** | **ica** | **initialization | io | main | pipe | shell**]

debug accelerator smb [**cli** | **cmd-close** | **cmd-create** | **cmd-lock** | **cmd-others** | **cmd-query-info** | **cmd-read** | **cmd-set-info** | **cmd-write** | **flow** | **large-data-flush** | **lock-manager** | **meta-data** | **named-pipe** | **not-found-cache** | **packeter** | **parser** | **read-ahead** | **shell** | **vfn** | **all**]

no debug accelerator smb [**cli** | **cmd-close** | **cmd-create** | **cmd-lock** | **cmd-others** | **cmd-query-info** | **cmd-read** | **cmd-set-info** | **cmd-write** | **flow** | **large-data-flush** | **lock-manager** | **meta-data** | **named-pipe** | **not-found-cache** | **packeter** | **parser** | **read-ahead** | **shell** | **vfn** | **all**]

debug accelerator ssl [**accelerated-svc** | **alarm** | **all** | **am** | **am-generic-svc** | **bio** | **ca** | **ca-pool** | **cipherlist** | **client-to-server** | **dataserver** | **flow-shutdown** | **generic** | **ocsp** | **oom-manager** | **openssl-internal | parser** | **peering-svc** | **session-cache** | **shell** | **sm-alert** | **sm-generic| sm-io** | **sm-pipethrough** | **synchronization** | **verify** | **waas-to-waas**]

no debug accelerator ssl [**accelerated-svc** | **alarm** | **all** | **am** | **am-generic-svc** | **bio** | **ca** | **ca-pool** | **cipherlist** | **client-to-server** | **dataserver** | **flow-shutdown** | **generic** | **ocsp** | **oom-manager** | **openssl-internal | parser** | **peering-svc** | **session-cache** | **shell** | **sm-alert** | **sm-generic| sm-io** | **sm-pipethrough** | **synchronization** | **verify** | **waas-to-waas**]

debug accelerator wansecure [**all** | **flow** | **mux** | **ocsp** | **shell** | **ssl**]

no debug accelerator wansecure [**all** | **flow** | **mux** | **ocsp** | **shell** | **ssl**]

Syntax Description

generic	Enables generic accelerator debugging.
connection	Enables accelerator connection debugging.
misc	Enables generic accelerator miscellaneous debugging.
shell	Enables accelerator shell debugging.
stats	Enables generic accelerator statistics debugging.
all	Enables all accelerator debugging of a specified type.
http	Enables HTTP accelerator debugging.
bypass-list	Enables HTTP accelerator bypass list debugging.
cli	Enables configuration CLI debugging.
conditional-response	Enables HTTP accelerator metadata cache conditional response debugging.
dre-hints	Enables HTTP accelerator DRE hinting debugging.
metadatacache	Enables HTTP accelerator metadata cache debugging.
redirect-response	Enables HTTP accelerator metadata cache redirect response debugging.
subnet	Enables HTTP accelerator subnet configuration debugging.
supress-server-encoding	Enables HTTP accelerator supress-server-encoding debugging.
transaction	Enables HTTP accelerator transaction debugging.
unauthorized-response	Enables HTTP accelerator metadata cache unauthorized response debugging.
ica	Enables ICA accelerator debugging.
ao-connectionmgr	Enables ICA AO-ConnectionMgr debugging.
ao-parser	Enables ICA AO-Parser debugging.
cgp	Enables ICA CGP debugging.
connection	Enables ICA AO-Connection debugging.
crypto	Enables ICA CRYPTO debugging.
detectionparser	Enables ICA detectionparser debugging.
failure	Enables ICA allocation failure debugging.
hash	Enables ICA HASH debugging.
ica	Enables ICA parsing debugging.
initialization	Enables ICA initialization debugging.
io	Enables ICA IO debugging.
main	Enables ICA main debugging.
pipe	Enables ICA pipe debugging.
shell	Enables ICA shell debugging.
mapi	Enables MAPI accelerator debugging.
Common-flow	Enables MAPI common flow debugging.
DCERPC-layer	Enables MAPI DCERPC layer flow debugging.
EMSMDB-layer	Enables MAPI EMSMDB layer flow debugging.

IO	Enables MAPI IO flow debugging.
ROP-layer	Enables MAPI ROP layer flow debugging.
ROP-parser	Enables MAPI ROP parser flow debugging.
RCP-parser	Enables MAPI RCP parser flow debugging.
RPCHTTP-layer	Enable MAPI RPCHTTP-layer flow debugs
shell	Enables MAPI shell flow debugging.
Transport	Enables MAPI transport flow debugging.
Utilities	Enables MAPI utilities flow debugging.
smb	Enables SMB accelerator debugging.
cmd-close	Enables SMB close commands debugging.
cmd-create	Enables SMB create commands debugging.
cmd-lock	Enables SMB lock commands debugging.
cmd-others	Enables SMB other commands debugging.
cmd-query-info	Enables SMB query-info commands debugging.
cmd-read	Enables SMB read commands debugging.
cmd-set-info	Enables SMB set-info commands debugging.
cmd-write	Enables SMB write commands debugging.
flow	Enables SMB flow debugging.
large-data-flush	Enables SMB large data flush debugging.
lock-manager	Enables SMB lock manager debugging.
meta-data	Enables SMB meta data debugging.
named-pipe	Enables SMB named pipe debugging.
not-found-cache	Enables SMB not-found metadata cache debugging.
packeter	Enables SMB packeter debugging.
parser	Enables SMB parser debugging.
read-ahead	Enables SMB read-ahead debugging.
shell	Enables SMB shell debugging.
vfn	Enables SMB VFN debugging.
ssl	Enables SSL accelerator debugging.
accelerated-svc	Enables accelerated service debugging.
alarm	Enables SSL AO alarm debugging.
am	Enables SSL auth manager debugging.
am-generic-svc	Enables SSL am generic service debugging.
bio	Enables SSL bio layer debugging.
ca	Enables SSL cert auth module debugging.
ca-pool	Enables SSL cert auth pool debugging.
cipherlist	Enables SSL cipher list debugging.
client-to-server	Enables SSL client-to-server datapath debugging.
dataserver	Enables SSL dataserver debugging.
flow-shutdown	Enables SSL flow shutdown debugging.
ocsp	Enables SSL ocsp debugging.

oom-manager	Enables SSL oom-manager debugging.
openssl-internal	Enables SSL openssl internal debugging.
parser	Enables SSL accelerator parser debugging.
peering-svc	Enables SSL peering service debugging.
session-cache	Enables SSL session cache debugging.
shell	Enables SSL shell debugging.
sm-alert	Enables SSL session manager alert debugging.
sm-generic	Enables SSL session manager generic debugging.
sm-io	Enables SSL session manager i/o debugging.
sm-pipethrough	Enables SSL session manager pipethrough debugging.
synchronization	Enables SSL synchronization debugging.
verify	Enables SSL certificate verification debugging.
waas-to-waas	Enables SSL waas-to-waas datapath debugging.
client-ip *ip-addr*	Specifies the client IP address.
server-ip *ip-addr*	Specifies the server IP address.
wansecure	Enables WANSECURE debugging.
flow	Enables WANSECURE flow debugging.
mux	Enables WANSECURE mux debugging.
ocsp	Enables WANSECURE ocsp debugging.
shell	Enables WANSECURE shell debugging.
ssl	Enables WANSECURE ssl debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The output associated with the **debug accelerator** *name module* command for an application accelerator is written to the file *name*ao-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 23.

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 **undebug** 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 accelerator http object-cache

To enable object-cache debugging, use the **debug accelerator http object-cache** EXEC command.

debug accelerator http object-cache {all | configuration | gate-keeper | logger | preposition | response-headers | statistics | traffic-plugin}

Syntax Description

all	Enable all object-cache debugging.
configuration	Enable configuration debugging.
gate-keeper	Enable gate keeper debugging.
logger	Enable logger debugging.
preposition	Enable cache prepositioning debugging.
response-headers	Enable debugging headers in HTTP response.
statistics	Enable statistics debugging.
traffic-plugin	Enable traffic plugin debugging.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **debug accelerator http object-cache** EXEC command to enable debugging for all object-cache debugging, or to specifying debugging for a particular object-cache area, such as configuration, cache preposition, or statistics.

Examples

The following example shows how to enable debugging for all parameters for the HTTP object cache:

```
WAE# debug accelerator http object-cache all
```

debug accelerator mapi rpchttp-layer

To enable debugging of the MAPI RPC HTTP accelerator, use the **debug accelerator mapi rpchttp** EXEC command. To disable debugging, use the **no** form of this command.

debug accelerator mapi rpchttp-layer

no debug accelerator mapi rpchttp-layer

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **debug accelerator mapi rpchttp-layer** EXEC command to enable debugging of the mapi RPC HTTP application accelerator.

Examples

The following example shows how to enable debugging for the MAPI object cache i/o:

```
WAE# debug accelerator mapi rpchttp-layer
```

Related Commands

debug accelerator

debug accelerator object-cache-io

To enable debugging of a specified accelerator object cache i/o debugging, use the **debug accelerator object-cache-io enable** EXEC command. To disable debugging, use the **no** form of this command.

debug accelerator *ao-name* **object-cache-io**

no debug accelerator *ao-name* **object-cache-io**

Syntax Description

ao-name	The name of the application accelerator specified for i/o debugging: SMB or HTTP.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **debug accelerator object-cache-io** EXEC command to enable debugging for object cache i/o data for a specified application accelerator.

Examples

The following example shows how to enable debugging for the MAPI object cache i/o:

```
WAE# debug accelerator smb object-cache-io
```

Related Commands

debug accelerator object-cache-ipc

debug accelerator object-cache-mgr

debug object-cache ipc

debug accelerator object-cache-ipc

To enable debugging of IPC transport data for a specified accelerator object cache, use the **debug accelerator object-cache-ipc enable** EXEC command. To disable debugging, use the **no** form of this command.

debug accelerator *ao-name* **object-cache-ipc**

no debug accelerator *ao-name* **object-cache-ipc**

Syntax Description

ao-name	The name of the application accelerator specified for ipc message debugging: SMB or HTTP.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **debug accelerator object-cache-ipc** EXEC command to enable debugging for object cache IPC transport data for a specified application accelerator.

Examples

The following example shows how to enable debugging for IPC transport data for the MAPI object cache.

```
WAE# debug accelerator smb object-cache-ipc
```

Related Commands

debug accelerator object-cache-io

debug accelerator object-cache-mgr

debug object-cache database

debug accelerator object-cache-mgr

To enable debugging of of the object cache storage manager for a specified accelerator object cache, use the **debug accelerator object-cache-mgr enable** EXEC command. To disable debugging, use the **no** form of this command.

debug accelerator *ao-name* **object-cache-mgr**

no debug accelerator *ao-name* **object-cache-mgr**

Syntax Description

ao-name	The name of the application accelerator specified for object cache storage manager debugging: SMB or HTTP.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **debug accelerator object-cache-mgr** EXEC command to enable debugging for the object cache storage manager for a specified application accelerator.

Examples

The following example shows how to enable debugging for the object cache storage manager for the MAPI application accelerator.

```
WAE# debug accelerator smb object-cache-mgr
```

Related Commands

debug accelerator object-cache-io

debug accelerator object-cache-ipc

debug object-cache database

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

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

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 23.

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 **undebug** 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 {**user** | **windows-domain**}

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

Syntax Description

user	Enables debugging of the user login against the system authentication.
windows-domain	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 23.

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 **undebug** 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 auto-discovery

To trace connections in the auto discovery module, use the **debug auto-discovery** EXEC command. To disable debugging**,** use the **undebug** form of this command.

debug auto-discoveryconnection

undebug auto-discovery connection

Syntax Description

This command has no arguments or keywords.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable auto discovery connection debugging:

```
WAE# debug auto-discovery connection
```

Related Commands

show debugging

debug buf

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

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

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

Syntax Description

all	Enables all buffer manager debugging.
dmbuf	Enables only dmbuf debugging.
dmsg	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 23.

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 **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**}

Syntax Description

adjacency	Enables CDP neighbor information debugging.
events	Enables CDP events debugging.
ip	Enables CDP IP debugging.
packets	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 23.

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 **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**}

Syntax Description

all	Enables all CLI debugging.
bin	Enables CLI command binary program debugging.
parser	Enables CLI command parser 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 23.

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 **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 cmm

To monitor and record cluster membership manager debugging, use the **debug cmm** EXEC command. To disable debugging, use the **undebug** form of this command.

debug cmm {**all** | **cli** | **events** | **ipc** | **misc** | **packets** | **shell** | **timers**}

undebug cmm {**all** | **cli** | **events** | **ipc** | **misc** | **packets** | **shell** | **timers**}

Syntax Description

all	Enables all cluster membership manager (CMM) debugging.
cli	Enables CMM CLI debugging.
events	Enables CMM state machine event debugging.
ipc	Enables CMM ipc message debugging.
misc	Enables CMM miscellaneous debugging.
packets	Enables CMM packet debugging.
shell	Enables CMM infra debugging.
timers	Enables CMM state machine timer 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

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

```
WAE# debug cmm all
```

Related Commands

show debugging

debug cms

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

debug cms{router-config | stats}

undebug cms

Syntax Description

router-config	Enables debug only router configuration from CM
stats	Enables debug only statistics

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 23.

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 **undebug** 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 connection

To enable connection-specific debugging, use the **debug connection** EXEC command. To disable debugging, use the **undebug** form of this command.

debug connection {**all** | **access-list** *acl-name*}

undebug connection {**all** | **access-list** *acl-name*}

Syntax Description

all	Enables all connection-specific debugging.
access-list *acl-name*	Enables access list connection debugging. Access list name is an alphanumeric identifier up to 30 characters, beginning with a letter.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all connection-specific debug monitoring:

```
WAE# debug connection all
```

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

all	Enables all data server debugging.
clientlib	Enables data server client library module debugging.
server	Enables data server module 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 23.

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 **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

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

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 23.

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 **undebug** 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** | **chunking** | **connection** {**aggregation** [*acl*] | **cache** [*acl*] | **chunking** [*acl*] | **core** [*acl*] | **message** [*acl*] | **misc** [*acl*] | *acl*} | **core** | **lz** | **message** | **misc** | **nack** | **packet**}

undebug dre {**aggregation** | **all** | **cache** | **chunking** | **connection** {**aggregation** [*acl*] | **cache** [*acl*] | **chunking** [*acl*] | **core** [*acl*] | **message** [*acl*] | **misc** [*acl*] | *acl*} | **core** | **lz** | **message** | **misc** | **nack** | **packet**}

Syntax Description

aggregation	Enables DRE chunk-aggregation debugging.
all	Enables the debugging of all DRE commands.
cache	Enables DRE cache debugging.
chunking	Enables DRE chunking debugging.
connection	Enables DRE connection debugging.
acl	ACL to limit connections traced.
core	Enables DRE core debugging.
lz	Enables DRE lz debugging.
message	Enables DRE message debugging for a specified connection.
misc	Enables DRE other debugging for a specified connection.
nack	Enables DRE NACK debugging.
packet	Enables DRE packet 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 23.

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 **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

Syntax Description

connection	(Optional) Enables egress method connection 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 23.

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 **undebug** 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 encryption-service

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

debug encryption-service {**all** | **application-layer** | **cfgmgr** | **dcerpc-layer** | **gss** | **io** | **secure-store** | **server** | **shell** | **transport-lib** | **utilities**}

undebug encryption-service {**all** | **application-layer** | **cfgmgr** | **dcerpc-layer** | **gss** | **io** | **secure-store** | **server** | **shell** | **transport-lib** | **utilities**}

Syntax Description

all	Enables debugging of all encryption services components.
application-layer	Enables debugging of the encryption services application layer.
cfgmgr	Enables debugging of the encryption services configuration manager.
dcerpc-layer	Enables debugging of the encryption services dcerpc layer.
gss	Enables debugging of the encryption services gss.
io	Enables debugging of the encryption services io.
secure-store	Enables debugging of the encryption services secure store.
server	Enables debugging of the encryption services server.
shell	Enables debugging of the encryption services shell.
transport-lib	Enables debugging of the encryption services transport library.
utilities	Enables debugging of the encryption services utilities.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable debugging of all encryption services components:

```
WAE# debug encryption-services all
```

Related Commands

show debugging

debug fda

To monitor and record flow distribution agent debugging, use the **debug fda** EXEC command. To disable debugging, use the **undebug** form of this command.

debug fda {**all** | **events** | **infra** | **messages**}

undebug fda {**all** | **events** | **infra** | **messages**}

Syntax Description

all	Enables all flow distribution agent debugging.
events	Enables only flow distribution agent event debugging.
infra	Enables only flow distribution agent infra debugging.
messages	Enables only flow distribution agent message 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all flow distribution agent debug monitoring:

```
WAE# debug fda all
```

Related Commands

show debugging

debug fdm

To monitor and record flow distribution manager debugging, use the **debug fdm** EXEC command. To disable debugging, use the **undebug** form of this command.

debug fdm {**all** | **events** | **infra** | **messages**}

undebug fdm {**all** | **events** | **infra** | **messages**}

Syntax Description

all	Enables all flow distribution manager debugging.
events	Enables only flow distribution manager event debugging.
infra	Enables only flow distribution manager infra debugging.
messages	Enables only flow distribution manager message 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

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

```
WAE# debug fdm all
```

Related Commands

show debugging

debug filtering

To trace filtering connections setup, use the **debug filtering** EXEC command. To disable debugging**,** use the **undebug** form of this command.

debug filtering connection

undebug filtering connection

Syntax Description

connection	(Optional) Enables filtering module connection 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable filtering module connection debugging:

```
WAE# debug filtering connection
```

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 **undebug** form of this command.

debug flow monitor type performance-monitor tcpstat-v1

undebug flow monitor type performance-monitor tcpstat-v1

Syntax Description

monitor	Enables monitor flow performance debugging commands.
tcpstat-v1	Enables tcpstat-v1 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 23.

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 **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 type performance-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 **undebug** form of this command.

debug generic-gre

undebug 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

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 23.

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 **undebug** 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 hw-raid

To monitor and record hardware RAID debugging , use the **debug hw-raid** EXEC command. To disable debugging, use the **undebug** form of this command.

debug hw-raid {**all** | **cli** | **daemon**}

undebug hw-raid {**all** | **cli** | **daemon**}

Syntax Description

all	Enables all hardware RAID debug commands.
cli	Enables hardware RAID CLI debugging.
daemon	Enables hardware RAID daemon 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all hardware RAID debug monitoring:

```
WAE# debug hw-raid all
```

Related Commands

show debugging

debug imd

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

debug imd {**all** | **cli** | **infra** | **nprm** | **stats**}

undebug fdm {**all** | **cli** | **infra** | **nprm** | **stats**}

Syntax Description

all	Enables all interface manager debugging.
cli	Enables only interface manager cli debugging.
infra	Enables only interface manager infra debugging.
nprm	Enables only interface manager nprm debugging.
stats	Enables only interface manager stats 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

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

```
WAE# debug imd all
```

Related Commands

show debugging

debug inline

To enable inline module debugging, use the **debug inline** EXEC command. To disable debugging, use the **undebug** form of this command.

debug inline {**debug** | **info** | **warn**}

undebug inline {**debug** | **info** | **warn**}

Syntax Description

debug	Sets the debug level to debug.
info	Sets the debug level to info.
warn	Sets the debug level to warn.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to set the log level for inline modules to warning level:

```
WAE# debug inline warn
```

Related Commands

show debugging

debug key-manager

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

debug key-manager

undebug key-manager

Syntax Description

key-manager	(Optional) Enables key manager debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

central-manager (primary only)

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable monitoring API 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 **undebug** form of this command.

debug logging all

undebug logging all

Syntax Description

all	Enables all logging 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 23.

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 **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 monapi

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

debug monapi

undebug monapi

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

central-manager (primary only)

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable monitoring API debug monitoring:

```
WAE# debug monapi
```

Related Commands

show debugging

debug nplogd

To monitor and record NP log daemon debugging, use the **debug nplogd** EXEC command. To disable debugging, use the **undebug** form of this command.

debug nplogd all

undebug nplogd all

Syntax Description

This command has no arguments or keywords.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable NP log daemon debug monitoring:

```
WAE# debug nplogd all
```

Related Commands

show debugging

debug ntp

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

debug ntp

undebug ntp

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

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 23.

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 **undebug** 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 object-cache database

To enable debugging of the object cache database, use the **debug object-cache database** EXEC command. To disable debugging, use the **no** form of this command.

debug object-cache database

no debug object-cache database

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 **debug object-cache database** EXEC command to enable debugging for the object cache database.

Examples

The following example shows how to enable debugging for the object cache database.

```
WAE# debug object-cache database
```

Related Commands

debug object-cache existence-cache

debug object-cache garbage-collection

debug object-cache ipc

debug object-cache load-monitor

debug object-cache existence-cache

To enable debugging of the object cache existence cache database, use the **debug object-cache existence-cache database** EXEC command. To disable debugging, use the **no** form of this command.

debug object-cache existence-cache

no debug object-cache existence-cache

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 **debug object-cache existence-cache** EXEC command to enable debugging for the existence cache, which maintains information on whether or not an object is present in the object databases.

Examples

The following example shows how to enable debugging for the object cache existence cache.

```
WAE# debug object-cache existence-cache
```

Related Commands

debug object-cache database

debug object-cache garbage-collection

debug object-cache ipc

debug object-cache load-monitor

debug object-cache garbage-collection

To enable debugging of the object cache garbage collection function, use the **debug object-cache garbage-collection** EXEC command. To disable debugging, use the **no** form of this command.

debug object-cache garbage-collection

no debug object-cache garbage-collection

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 **debug object-cache garbage-collection** EXEC command to enable debugging of the object cache garbage collection function, which collects objects that are either invalid or rarely used.

Examples

The following example shows how to enable debugging for the object cache garbage collection function.

```
WAE# debug object-cache garbage-collection
```

Related Commands

debug object-cache database

debug object-cache existence-cache

debug object-cache ipc

debug object-cache load-monitor

debug object-cache ipc

To enable debugging of object cache IPC transport data, use the **debug object-cache ipc enable** EXEC command. To disable debugging, use the **no** form of this command.

debug object-cache ipc

no debug object-cache ipc

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 **debug object-cache ipc** EXEC command to enable debugging of object cache IPC transport data.

Examples

The following example shows how to enable debugging for object cache IPC transport data.

```
WAE# debug object-cache ipc
```

Related Commands

debug accelerator object-cache-ipc

debug object-cache database

debug object-cache existence-cache

debug object-cache garbage-collection

debug object-cache load-monitor

debug object-cache load-monitor

To enable debugging of the object cache load monitor function, use the **debug object-cache load-monitor enable** EXEC command. To disable debugging, use the **no** form of this command.

debug object-cache load-monitor

no debug object-cache load-monitor

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 **debug object-cache load-monitor** EXEC command to enable debugging of the object cache load monitor function, which monitors disk load and usage.

Examples

The following example shows how to enable debugging for the object cache load monitor function.

```
WAE# debug object-cache load-monitor
```

Related Commands

debug object-cache database

debug object-cache existence-cache

debug object-cache garbage-collection

debug object-cache ipc

debug rbcp

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

debug rbcp

undebug rbcp

Syntax Description

This command has no arguments or keywords.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable RBCP debug monitoring:

```
WAE# debug rbcp
```

Related Commands

show debugging

debug rmd

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

debug rmd {**all** | **cli** | **infra** | **nprm**}

undebug rmd {**all** | **cli** | **infra** | **nprm**}

Syntax Description

all	Enables all route manager debugging.
cli	Enables only route manager cli debugging.
infra	Enables only route manager infra debugging.
nprm	Enables only route manager nprm 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

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

```
WAE# debug rmd all
```

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 **undebug** form of this command.

debug rpc {**detail** | **trace**}

undebug rpc {**detail** | **trace**}

Syntax Description

detail	Displays RPC logs of priority detail or higher.
trace	Displays RPC logs of priority trace or higher.

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 23.

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 **undebug** 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 service-insertion

To trace connections in the service-insertion module, use the **debug service-insertion** EXEC command. To disable debugging, use the **undebug** form of this command.

debug service-insertion connection

undebug service-insertion connection

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

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all service-insertion module debug monitoring:

```
WAE# debug service-insertion connection
```

Related Commands

show debugging

debug service-policy

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

debug service-policy type {**waas**}

undebug service-policy type waas}

Syntax Description

waas	Enables WAAS service policy 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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable WAAS service policy debug monitoring:

```
WAE# debug service-policy waas
```

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

all	Enables all SNMP debug commands.
cli	Enables SNMP CLI debugging.
main	Enables SNMP main debugging.
mib	Enables SNMP MIB debugging.
traps	Enables SNMP trap debugging.

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 23.

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 **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 standby

To enable standby debugging, use the **debug standby** EXEC command. To disable debugging, use the **undebug** form of this command.

debug standby [all]

undebug standby [all]

Syntax Description

all	(Optional) Enables standby debugging using all debug features.

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 23.

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 **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

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

```
WAE# debug standby all
```

Related Commands

show debugging

debug statistics

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

debug statistics {**all** | **ao** | **client** | **collector** | **ipc** | **messages** | **serializer** | **sqm**}

undebug statistics {**all** | **ao** | **client** | **collector** | **ipc** | **messages** | **serializer** | **sqm**}

Syntax Description

all	Enables all statistics debug commands.
ao	Enables statistics acceleration debugging.
client	Enables statistics client debugging.
collector	Enables statistics collector debugging.
ipc	Enables statistics IPC debugging.
messages	Enables statistics messages/buffers debugging.
serializer	Enables statistics serializer debugging.
sqm	Enables statistics computation debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

services-controller

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 23.

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 **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 statistics 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 {**all** | **buffer-mgr** | **dre-flow** | **netio** | **scheduler**}

undebug tfo {**all** | **buffer-mgr** | **dre-flow** | **netio** | **scheduler**}

Syntax Description

all	Enables all TFO debugging.
buffer-mgr	Enables TFO data-buffer from buffer manager debugging.
dre-flow	Enables TFO DRE flow debugging for all connections.
netio	Enables TFO connection debugging for the network input/output module.
scheduler	Enables TFO scheduler 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 23.

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 **undebug** 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 **undebug** form of this command.

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

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

Syntax Description

detail	Enables transaction log detailed debugging.
export	Enables transaction log FTP export debugging.
info	Enables transaction log high level 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 23.

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 **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 the WAFS Device Manager component, use the **debug wafs** EXEC command. To disable debugging, use the **undebug** form of this command.

debug wafs manager {**debug** | **error** | **info** | **warn**}

undebug wafs manager {**debug** | **error** | **info** | **warn**}

Syntax Description

manager	Sets the logging level for the Device Manager.
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

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 23.

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 **undebug** 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 manager 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 **undebug** form of this command.

debug wccp {**all** | **detail** | **error** | **events** | **packets**}

undebug wccp {**all** | **detail** | **error** | **events** | **packets**}

Syntax Description

all	Enables all WCCP debugging functions.
detail	Enables the WCCP detail debugging.
error	Enables the WCCP error debugging.
events	Enables the WCCP events debugging.
packets	Enables the WCCP packet-related information 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 23.

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 **undebug** 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*

Syntax Description

filename	Name of the file to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

deltree

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

deltree *directory*

Syntax Description

directory	Name of the directory tree to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **deltree** 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.

Examples

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

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

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

dir

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

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **dir** 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 **lls** 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
-------------  ------------------------          -----------
```

```
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 the admin 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 delete-data-partitions

disk delete-preserve-software

disk disk-name *diskxx* **enable force**

disk disk-name disk*xx* **replace**

disk insert *diskname*

disk recreate-raid

disk scan-errors *diskname*

Syntax Description

delete-partitions *diskname*	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. 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.
delete-data-partitions	Deletes all data partitions on all logical drives. Data partitions include the CONTENT, PRINTSPOOL, and GUEST partitions. These partitions include all DRE cache files and print spool files.
delete-preserve-software	Deletes all disk and data partitions and preserves current software version and CM registration details.
disk-name *diskxx* **enable force**	Reenables a defunct drive (with or without removing it) that has been previously shut down. **Note** This option is available only on RAID-5 systems.
disk-name disk*xx* **replace**	Shuts down the physical disk with the name disk*xx* (disk00, disk01, etc.) so that it can be replaced in the RAID-5 array. **Note** This option is available only on RAID-5 systems.
insert *diskname*	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). **Note** This option is available only on WAE-612 models.
recreate-raid	Recreates the RAID-5 array. **Note** This option is available only on RAID-5 systems.
scan-errors *diskname*	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). For RAID-5 systems, this command scans the logical RAID device for errors. On these systems, there is no *diskname* option.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The WAAS software supports hot-swap functionality for both failed disk replacement and scheduled disk maintenance. On the WAE-612, use the **disk disk-name** *diskxx* **shutdown** global configuration command to shut down a disk for scheduled disk maintenance. (For the scheduled disk maintenance procedure, see the chapter "Maintaining Your WAAS System" in the *Cisco Wide Area Application Services Configuration Guide*.)

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-612 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.

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

Caution 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.

The **disk delete-data-partitions** command deletes the DRE caches.

After using the **disk delete-data-partitions** command, you must reload the device. The data partitions are automatically re-created and the caches are initialized, which can take several minutes. DRE optimization is not done until the DRE cache has finished initializing. The **show statistics dre** EXEC command reports "TFO: Initializing disk cache" until then. It is best not to interrupt DRE cache initialization by reloading the device again until after cache initialization has finished. However, if DRE cache initialization is interrupted, on the next reboot the disk is checked, which takes extra time, and DRE initialization is completed again.

When you upgrade to software version 6.1.1, and execute **disk-delete-preserve-software** command for the first time, all data and system partitions are re-created.
Use the **disk delete-preserve-software c**ommand if you want to delete all existing data and system partitions, and yet want to preserve the software version and the device registration details with the Central Manager. This changes the software store partition size from 1 GB to 2GB. This command is applicable for all vWAAS devices, ISR WAAS devices and SM-SRE devices.

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 object-cache extend

show disks

dnslookup

To resolve a host or domain name to an IP address(IPv4/IPv6), use the **dnslookup** EXEC command.

dnslookup {*hostname* | *domainname*| *IPv4/IPv6 address*}

Syntax Description

hostname	Name of DNS server on the network.
domainname	Name of domain.
ip-address	IPv4 or IPv6 address

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how the **dnslookup** command is used to resolve the hostname *myhost* to IP address172.31.69.11

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

The following example shows how the **dnslookup** command is used to resolve the hostname *abd.com* to IP address 192.168.219.25:

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

The following example shows how the **dnslookup** command is used to resolve an IP address used as a hostname to 10.0.11.0:

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

The following example shows how the **dnslookup** command is used to resolve an IP address to a hostname:

```
WAE# dnslookup 2012:3:3:3::8
official hostname: CM.cisco.com
          address:2012:3:3:3::8
```

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 the admin password when prompted for a password.

If using TACACS+ authentication, there is an enable password feature in TACACS+ that allows an administrator to define a different enable password for each user. If a TACACS+ user enters the **enable** EXEC command to access privileged EXEC mode, that user must enter the admin password defined by the TACACS+ server.

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

Examples

The following example shows how to access privileged EXEC mode:

```
WAE> enable
WAE#
```

Related Commands

disable

exit

exit

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

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

All modes

Device Modes

application-accelerator

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*}

Syntax Description

binary *reg-express filename*	Does not suppress the binary output. Specifies the regular expression to be matched and the filename.
count *reg-express filename*	Prints the number of matching lines. Specifies the regular expression to be matched and the filename.
lineno *reg-express filename*	Prints the line number with output. Specifies the regular expression to be matched and the filename.
match *reg-express filename*	Prints the matching lines. Specifies the regular expression to be matched and the filename.
nomatch *reg-express filename*	Prints the nonmatching lines. Specifies the regular expression to be matched and the filename.
recursive *reg-express filename*	Searches a directory recursively. Specifies the regular expression to be matched and the filename.
case	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/
```

```
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) on the WAAS device, use the **install** EXEC command.

install *filename*

Syntax Description

filename	Specifies the name of the *.bin* file you want to install.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **install** command loads the system image into flash memory and copies the disk-based software component to the software file system (swfs) partition. This command can also be used to install a BIOS or other firmware update by specifying the appropriate update file.

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

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.

Examples

The following example shows how to load the system image contained in the *wae512-cache-300.bin* file:

```
WAE# install wae512-cache-300.bin
```

Related Commands

copy disk

reload

less

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

less *file_name*

Syntax Description

file_name	Name of the file to be displayed.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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.

Examples

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

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

Related Commands

type

license add

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

license add *license-name*

Syntax Description

license-name	Name of the software license to add. The following license names are supported: • Transport—Enables basic DRE, TFO, and LZ optimization. • Enterprise—Enables the EPM, HTTP, MAPI, SSL, and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to install the enterprise license:

```
WAE# license add Enterprise
```

Related Commands

clear arp-cache license

show license

lls

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

lls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a long list of files.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **lls** 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 **dir** command.

Examples

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
          4096  Thu Feb 16 12:29:30 2006  <DIR>    var
           508  Sat Feb 25 13:18:35 2006           wdd.sh.signed
```

Related Commands

dir

lls

ls

ls

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

ls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a list of files.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **ls** *directory* command to list the filenames and subdirectories within a particular directory.

Use the **ls** command to list the filenames and subdirectories of the current working directory.

Use the **pwd** command to view the present working directory.

Examples

The following example shows how to display the files and subdirectories that are listed within the root directory:

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

Related Commands

dir

lls

pwd

lsusb

To view a list of files or subdirectory names within a directory on a USB storage device, use the **lsusb** EXEC command.

lsusb [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a list of files.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **lsusb** *directory* command to list the filenames and subdirectories within a particular directory on the USB device.

Use the **lsusb** command to list the filenames and subdirectories of the current working directory on the USB device.

This command is available only on WAAS devices that support external USB storage devices.

Examples

The following example shows how to display the files and subdirectories that are listed within the root directory of a USB device:

```
WAE# lsusb
directory1
afile.txt
bfile.txt
```

Related Commands

dir

lls

ls

pwd

mkdir

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

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

```
WAE# mkdir /oldpaxfiles
```

Related Commands

cpfile

dir

lls

ls

pwd

rename

rmdir

mkfile

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

mkfile *filename*

Syntax Description

filename	Name of the file that you want to create.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **mkfile** EXEC command to create a new file in any directory of the WAAS device.

Examples

The following example shows how to create a new file, *traceinfo*, in the root directory:

```
WAE# mkfile traceinfo
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

ntpdate

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

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

Syntax Description

hostname	NTP hostname.
ip-address	NTP server IP (IPV4/IPv6) address.
key	(Optional) Specifies to use authentication with the NTP server.
authentication-key	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

packet-capture

To capture packets on a device interface, use the **packet-capture** EXEC command.

packet-capture interface {**GigabitEthernet** *slot/port* | **TenGigabitEthernet** *slot/port* | **PortChannel** *index* | **standby** *grpnumber*} **access-list** {*acl-name* | *acl-num*}} [**file-size** *size* [**number-of-files** *num* | **stop-after-num-files** *num*]] | **packet-size** | **non-encapsulated** | [*capture-filename*]

packet-capture interface {**GigabitEthernet** *slot/port* | **TenGigabitEthernet** *slot/port* | **PortChannel** *index* | **standby** *grpnumber*} {**access-list** {*acl-name* | *acl-num*} | **destination-ip** {*hostname* | *ip-address*} | **destination-port** *port* | **source-ip** {*hostname* | *ip-address*} | **source-port** *port*} [**file-size** *size* [**number-of-files** *num* | **stop-after-num-files** *num*]] | **packet-size** | **non-encapsulated** | [*capture-filename*]

packet-capture decode [**destination-ip** {*hostname* | *ip-address*} | **destination-port** *port* | **source-ip** {*hostname* | *ip-address*} | **source-port** *port*] [**file-size** *size* [**number-of-files** *num* | **stop-after-num-files** *num*]] | **packet-size** | **non-encapsulated** | *capture-filename*

Syntax Description

interface	Specifies the source interface from which to capture packets.
GigabitEthernet *slot/port*	Specifies a Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
TenGigabitEthernet *slot/port*	Specifies a 10-Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
PortChannel *index*	Specifies a port channel interface (1-4).
standby *grpnumber*	Specifies a standby group (1-2).
access-list	Specifies an access list for which to capture packets on the specified interface.
file-size *size*	(Optional) Specifies the maximum file size for captured output, from 1–100000 KB. After a file fills to capacity, another output file is created according to the following keywords.
number-of-files *num*	(Optional) Specifies the maximum number of output files to create (1–500), after which earlier files are overwritten as needed for more captured data.
stop-after-num-files *num*	(Optional) Specifies the maximum number of output files to create (1–500), after which packet capture is stopped.
packet-size	The maximum number of capture bytes per packet.
non-encapsulated	Captures packets that are not SIA encapsulated.
capture-filename	(Optional) Specifies the name of a file to which output is saved. If no file is specified, output is sent to the console.
destination-ip	Captures packets matching the specified destination IPv4 or IPv6 address.
hostname	Captures packets matching the specified destination or source hostname.
ip-address	Destination or source IP address.
destination-port *port*	Captures packets matching the specified destination port.
source-ip	Captures packets matching the specified source IPv4 or IPv6 address.
source-port *port*	Captures packets matching the specified source port.
decode	Decodes captured packets.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The following are usage guidelines for the packet-capture command:

- Either packet capture or debug capture can be active, but not both simultaneously.

  The **packet-capture** command is preferred over the deprecated commands **tcpdump** and **tethereal**,
- For WAAS Version 6.2.1 and later, you can run the **packet-capture** command in multiple sessions (telnet or ssh) on the same or different interfaces, up to a maximum of five sessions, that print in the WAE.

Examples

The following example shows how to capture packets on a normal interface:

```
WAE(config)# ip access-list extended 100 permit tcp any any range 23 35
WAE(config)# exit
WAE# packet-capture interface gig 0/1 access-list 100 mycapture
```

Related Commands

tcpdump

tethereal

ping

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

ping [**management**] {*hostname* | *ip-address*}

Syntax Description

management	Uses the designated management interface for the ping.
hostname	Hostname of system to ping.
ip-address	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#
```

Related Commands

traceroute

ping6

To send echo packets for diagnosing basic network connectivity on IPv6 networks, use the **ping6** EXEC command.

ping6 {*hostname* | *ip-address*}[**management**]

Syntax Description

hostname	Hostname of system to ping.
ip-address	IPv6 address of system to ping.
management	Uses the designated management interface for the ping.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

To use the **ping6** 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**.

When you use a device’s management interface to establish connectivity to another device, using **ping6 command,** and the management interface goes down, the communication will still succeed if the address of the end device is reachable from any other interface.

Examples

The following example shows how to send echo packets to a machine with address 2013:1:1:10::5

to verify its availability on the network:

```
WAE# ping 2013:1:1:10::5

PING 2013:1:1:10::5(2013:1:1:10::5) 56 data bytes
64 bytes from 2013:1:1:10::5: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 2013:1:1:10::5: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 2013:1:1:10::5: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 2013:1:1:10::5: icmp_seq=4 ttl=64 time=0.029 ms
64 bytes from 2013:1:1:10::5: icmp_seq=5 ttl=64 time=0.029 ms

--- 2013:1:1:10::5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.018/0.028/0.037/0.006 ms
```

Related Commands

traceroute6

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

force	(Optional) Forces a reboot without further prompting.
in *m*	(Optional) Schedules a reboot after a specified interval (1-10080 minutes).
cancel	(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

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

rename *oldfilename newfilename*

Syntax Description

oldfilename	Original filename.
newfilename	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

factory-default	Resets the device configuration and data to their manufactured default status.
preserve	(Optional) Preserves certain configurations and data on the device.
basic-config	(Optional) Selects basic network configurations.
rollback	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

central-manager

Usage Guidelines

Use the **restore** 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.

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 l00 - DAS)    140011MB(136.7GB)
  disk01: Normal                (h00 c00 i01 l00 - 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: oe612-4.0.0.340

Compiled 17:26:17 Mar 25 2006 by cnbuild

System was restarted on Mon Mar 27 15:25:02 2006.
The system has been up for 3 days, 21 hours, 9 minutes, 17 seconds.

WAE# show version last
    Nothing is displayed.
WAE# show version pending
WAAS 4.0.1 Version Y
WAE# reload
...... reloading ......
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
...
WAE# restore rollback
```

```
WAE# reload
...... reloading ......
```

Because flash memory configurations were removed after the **restore** command was used, the **show startup-config** command does not return any flash memory data. The **show running-config** command returns the default running configurations.

Related Commands

reload

show disks

show running-config

show startup-config

show version

rmdir

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

rmdir *directory*

Syntax Description

directory	Name of the directory that you want to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **rmdir** EXEC command to remove any directory from the WAAS file system. The **rmdir** command only removes empty directories.

Examples

The following example shows how to delete the *oldfiles* directory from the *local1* directory:

```
WAE# rmdir /local1/oldfiles
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

scp

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

scp [**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

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

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **scp** command uses SSH for transferring data between hosts.This command is enabled by default.

This command prompts you for passwords or pass phrases when needed for authentication.

Related Commands

ssh

script

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

script {**check** | **execute**} *file_name*

Syntax Description

check	Checks the validity of the script.
execute	Executes the script. The script file must be a SYSFS file in the current directory.
file_name	Name of the script file.

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*.

For proper display of the **setup** command, leave the terminal length set to the default value of 24 lines.

show aaa accounting

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

show aaa accounting

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 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: • Exec • Command level 0 • Command level 15 • System
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.

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

Field	Description
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. 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.
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 aaa authorization

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

show aaa authorization

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 aaa authorizaiton** EXEC command to display configuration and state information related to AAA authorization.

Examples

Table 3-2 describes the fields shown in the **show aaa authorization** command display.

Table 3-2 Field Descriptions for the show aaa authorization Command

Field	Description
Authorization Type	AAA authorization configuration for the following types of user accounts: • Command level 0 • Command level 15
Protocol	Authorization protocol that is configured.

Related Commands

(config) aaa authorization commands

show accelerator

To display the status and configuration of the application accelerators, use the **show accelerator** EXEC command.

show accelerator [**detail** | **epm** | **http** [**debug**]| **ica** | **interposer-ssl | mapi** | **smb | ssl** | **wansecure**]

Syntax Description

detail	(Optional) Displays the license information, configuration state, and operational state for all accelerators, and additional accelerator and policy engine configuration.
epm	(Optional) Displays the status for the EPM application accelerator.
http	(Optional) Displays the status for the HTTP application accelerator.
debug	(Optional) Displays more detailed status for the HTTP application accelerator.
ica	(Optional) Displays the status for the ICA application accelerator.
mapi	(Optional) Displays the status for the MAPI application accelerator.
smb	(Optional) Displays the status for the SMB application accelerator.
ssl	(Optional) Displays the status for the SSL application accelerator.
wansecure	(Optional) Displays the status for the WAN secure application accelerator.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays the output for the **show accelerator http** command:

```
wae# show accelerator http
Accelerator     Licensed        Config State    Operational State
-----------     --------        ------------    -----------------
http            Yes             Enabled         Running

HTTP:
   Accelerator Config Item            Mode        Value
   -----------------------            ----        ------
   Suppress Server Encoding           Default     Disabled
                 Access-List          Default     All
   DRE Hints                          User        Enabled
                 Access-List          Default     All
   Metadatacache                      User        Enabled
                 Access-List          Default     All
   HTTPS Metadatacache                User        Enabled
                 Access-List          Default     All
                 MaxAge               Default     86400
                 MinAge               Default     60
                 Filter-extension     Default     All
                 Redirect             Default     Enabled
                 Unauthorized           Default        Enabled
                 Conditional            Default        Enabled

   Policy Engine Config Item            Value
   -------------------------            -----
   State                                Registered
   Default Action                       Use Policy
   Connection Limit                     200
   Effective Limit                      200
   Keepalive timeout                    5.0 seconds
```

The following example displays the output for the **show accelerator smb** command:

```
wae# show accelerator smb

Accelerator     Licensed        Config State    Operational State
-----------     --------        ------------    -----------------
smb             Yes             Enabled         Running

SMB:
   Accelerator Config Item              Mode           Value
   -----------------------              ----           ------
   WanSecure Mode                       Default        auto
   MultiChannel Status                  Default        Enabled
   Encryption Status                    Default        L7-opt-enable
   Digital signing alarm                Default        Disabled
   Change Notification size             Default        10
   DRE hints                            Default        Enabled
   Highest dialect                      Default        smb3-02
       Exceed action                    Default        handoff
   Matches dialect                      Default        smb3-02
       Action                           Default        none
   Named pipe optimization              Default        Enabled
       Resp. cache lifetime (s)         Default        20
       Sess. cache lifetime (s)         Default        30
       NamedPipe-cache size (KB)        Default        300         (default: 300
 maximum: 900)
   NF metadata cache opt                Default        Enabled
       Max size (MB)                    Default        32
       Aging (s)                        Default        30
       Bypass patterns                  Default
   SMB Print optimization               Default        Enabled
   SMB Object Cache support             Default        Enabled
   SMB Load-bypass support              Default        Enabled
   SMB Object Cache Operational         User           Up
   Microsoft Office optimization        Default        Enabled
   SMB2 Read-caching opt                Default        Enabled
   SMB2 Guestbit opt                    Default        Enabled
   SMB3 Read-caching opt                Default        Enabled
   Optimization bypass pattern          Default        \\.pst |.ini
   Smb2 Dir opt                         Default        Enabled
      Smb2-Dir-opt-cache size (MB)      Default        55          (default: 55 maximum:
55)
      Smb2-Dir-opt-pre-fetch            Default        Enabled
   Read-ahead opt                       Default        Enabled
       Buffer size (MB)                 Default        110         (default: 110 maximum:
220)
   Directory listing opt                Default        Enabled
   SMB3 Async-write opt                 Default        Enabled
       Quota threshold (MB)             Default        20
       Quota aging time (s)             Default        60
   SMB2 Async-write opt                 Default        Enabled
       Quota threshold (MB)             Default        20
       Quota aging time (s)             Default        60
   Async-write opt                      Default        Enabled
```

```
       Quota threshold (MB)            Default        20
       Quota aging time (s)            Default        60
   Metadata-opt                        Default        Enabled
       Metadata-cache size (MB)        Default        75          (default: 75 maximum:
75)
   smb2-Batch-close-opt                Default        Enabled
   smb2-Invalid-fid-opt                Default        Enabled
   smb3-Batch-close-opt                Default        Enabled
   smb3-Invalid-fid-opt                Default        Enabled
   large-pkt                           Default        Disabled
   Iobuf size (MB)                     Default        50          (default: 50 maximum:
100)
       Max iobuf size for 1 pkt(KB)    Default        65
       Directory aging time            Default        30
   Dynamic share                       Default
   Oplock opt                          Default        Enabled
       Client OS patterns              Default        Mac OS
   Signing opt                         Default        Enabled
           Unwrap opt                  Default        Enabled
   SMB Preposition DRE                 Default        Disabled

   Policy Engine Config Item           Value
   -------------------------           -----
   State                               Registered
   Default Action                      Use Policy
   Connection Limit                    750
   Effective Limit                     740
   Keepalive timeout                   5.0 seconds
```

Table 3-3 describes the fields shown in the **show accelerator** command display for all application accelerators. Specific application accelerators display additional configuration status information.

Table 3-3 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).
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.

Table 3-3 Field Description for the show accelerator Command (continued)

Field	Description
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 accelerator.

If you use the **show accelerator http** or the **show accelerator smb** command, the output contains an extra section called Accelerator Config Item, which appears before the Policy Engine Config Item section. In the Accelerator Config Item section, each item shows the status of an HTTP accelerator configuration item. The Mode column shows Default if the item is configured with the default setting or User if the item is configured with a different setting by the user. The Value column shows the current value of the item (Enabled, Disabled, or an alpha-numeric setting).

Related Commands

(config) accelerator epm

(config) accelerator http

(config) accelerator ica

(config) accelerator mapi

(config) accelerator nfs

(config) accelerator smb

(config) accelerator ssl

show statistics accelerator

show accelerator http object-cache

To display HTTP object cache configuration and status information for a WAAS device, use the **show accelerator http object-cache** EXEC command.

show accelerator http object-cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the show accelerator http object-cache command to display HTTP object cache configuration and status information for a WAAS device.

Examples

The following example shows output from the **show accelerator http object-cache** command:

```
HTTP Object-cache Version
-------------------------------

                                   Mode        Value
                                   ----        ------
Object-cache                       User         Enabled
              Transparent          Default     Enabled
              Connected            Default     Disabled
              OTT                  Default     Disabled
              Default Profile      Default     standard

              Host-profile-count   Default     0
```

Related

show statistics accelerator http object-cache

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

critical	Displays critical alarm information.
detail	(Optional) Displays detailed information for each alarm.
support	(Optional) Displays additional information about each alarm.
history	Displays information about the history of various alarms.
start_num	(Optional) Alarm number that appears first in the alarm history.
end_num	(Optional) Alarm number that appears last in the alarm history.
major	Displays information about major alarms.
minor	Displays information about minor alarms.
status	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 3-4 describes the fields shown in the **show alarms history** command display.

Table 3-4 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.
Module/Submodule	Software module affected.
Instance	Object that this alarm event is associated with. For example, for an alarm event with the Alarm ID disk_failed, the instance would be the name of the disk that failed. The Instance field does not have predefined values and is application specific.

Table 3-5 describes the fields shown in the **show alarms status** command display.

Table 3-5 Field Descriptions for the show alarms status Command

Field	Description
Critical Alarms	Number of critical alarms.
Major Alarms	Number of major alarms.

Table 3-5 Field Descriptions for the show alarms status Command (continued)

Field	**Description**
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 Address Resolution Protocol (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.

On an ISR-WAAS device, no ARP entries are present for IP addresses on the same subnet as the ISR-WAAS device; there is an entry only for the defined gateway.

The ARP cache is cleared based on the gc_stale_time; the default time is 60 seconds.

Cache entry states, described in Table 3-6, function as follows:

1. An entry in the ARP table with a Reachable state is moved to the Stale state after the ReachableTime is exceeded, or an UnsolicitedNeighbor advertisement is received.
2. After an entry in the ARP table is moved to the Stale state, it sends an ARP request and is moved to the Delay state. It remains in the Delay state until it receives an acknowledgment.
3. Depending on the next action, the entry is then moved to the Reachable state or the Probe state:
   - If the entry receives an acknowledgment on time, it is moved to the Reachable state.
   - If the entry does not receive an acknowledgment on time, it is moved to the Probe state.

Examples

Table 3-6 describes the fields shown in the **show arp** command display.

Table 3-6 Field Descriptions for the show arp Command

Field	Description
Protocol	Type of protocol.
State	Cache entry state. There are five possible cache entry states: Incomplete, Reachable, Stale, Delay, and Probe. • Incomplete—Address resolution on the cache is in progress: a Neighbor Solicitation has been sent to the solicited-mode address of the target, but the corresponding Neighbor Advertisement has not yet been received. • Reachable—Within the last ReachableTime milliseconds, positive confirmation has been received that the forward path to the neighbor is functioning properly. While in Reachable state, no special action occurs as packets are sent. • Stale—Within the last ReachableTime milliseconds, no positive confirmation has been received that the forward path to the neighbor is functioning properly. While in Stale state, no action occurs until a packet is sent. **Note** The Stale state is entered after an unsolicited Neighbor Discovery message is received, which updates the cached linked-layer address. Receipt of this message does *not* confirm reachability. Reachability is verified only after the entry is actually used. The Stale state ensures that reachability is verified quickly if the entry is actually being used. • Delay—More than the ReachableTime milliseconds has elapsed since receipt of the last positive confirmation that the forward path to the neighbor is functioning properly, and a packet was sent within the specified DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within the DELAY_FIRST_PROBE_TIME seconds of entering the Delay state, a Neighbor Solicitation is sent, and the state is changed to the Probe state. • Probe—Neighbor Solicitations are retransmitted every RetransTime seconds to confirm reachability, until a reachability confirmation is received.
Address	IP address of the hostname.
Flags	Current ARP flag status.
Hardware Addr	Hardware IP address given as six hexadecimal bytes separated by colons.
Type	Type of wide-area network.
Interface	Name and slot/port information for the interface.

show authentication

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

show authentication {**user** | **strict-password-policy**}

Syntax Description

user	Displays authentication configuration for user login to the system.
strict-password-policy	Displays strict password policy configuration information.

s

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

To display the strict password policy configuration information , use the **show authentication strict-password-policy** EXEC command.

Examples

Table 3-7 describes the fields shown in the **show authentication user** command display.

Table 3-7 Field Descriptions for the show authentication user Command

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

Table 3-7 Field Descriptions for the show authentication user Command (continued)

Field	Description
Windows domain RADIUS TACACS+ Local	Operation status of the authentication service. Values are enabled or disabled. Priority status of each authentication service. Values are primary, secondary, or tertiary.

Table 3-8 describes the fields in the **show authentication strict-password-policy** command display. If the strict password policy is not enabled, the command displays, “Strict password policy is disabled.”

Table 3-8 Field Description for the show authentication strict-password-policy Command

Field	Description
Password validity	Number of days for which strict passwords are valid.
Password expiry warning	Number of days in advance that users are warned before strict passwords expire.
Maximum login retry attempts	Number of login retry attempts allowed before the user is locked out.

Related Commands

(config) authentication configuration

(config) authentication strict-password-policy

clear arp-cache

show statistics authentication

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*]}] | **asymmetric-connections**}

Syntax Description

blacklist	Displays the entries in the blacklist server table.
netmask *netmask*	(Optional) Displays the network mask to filter the table output (A.B.C.D/).
list	Lists TCP flows that the WAE is currently optimizing or passing through.
|	(Optional) Specifies the output modifier.
begin *regex*	Begins with the line that matches the regular expression. You can enter multiple expressions.
exclude *regex*	Excludes lines that match the regular expression. You can enter multiple expressions.
include *regex*	Includes lines that match the regular expression. You can enter multiple expressions.
asymmetric-connections	Displays asymmetric connections.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **asymmetric-connections** option displays the last 1000 asymmetric connections seen on the device.

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 3-9 describes the output in the **show auto-register** command display.

Table 3-9 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

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 3-10 describes the fields shown in the **show banner** command display.

Table 3-10 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 bmc

To display the Baseboard Management Controller (BMC) system event log, use the **show bmc** EXEC command.

show bmc {**info** | **fru** | **event-log [all** | **event** | **range** | |**]** | **management** |}

Syntax Description

info	Displays the BMC information.
fru	Displays the BMC Field Replaceable Unit.
event-log	Displays the BMC system event log (by default, the last 10 events).
all	Displays all events from the BMC system event log.
event	Displays a single event number from the BMC system event log.
range	Displays the range of events from the BMC system event log.
management	Displays the BMC management related information.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following is a sample output from the **show bmc** command:

```
WAE#show bmc ?
event-log   Display BMC System Event Log (default is the last 10 events)
fru         Display BMC Field Replaceable Unit
info        Display BMC information
management  Display BMC management information

WAVE-694-K9#sh bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.44
IPMI Version              : 2.0
Manufacturer ID           : 5771
Manufacturer Name         : Unknown (0x168B)
Product ID                : 161 (0x00a1)
Product Name              : Unknown (0xA1)
Device Available          : yes
Provides Device SDRs      : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info     :
    0x0b
    0x04
    0x1b
    0x01
SEL Information
Version          : 1.5 (v1.5, v2 compliant)
Entries          : 4
Free Space       : 9136 bytes
Percent Used     : 0%
Last Add Time    : 05/20/2011 05:26:56
Last Del Time    : 05/20/2011 05:26:55
Overflow         : false
Supported Cmds   : 'Delete' 'Reserve'
Self Test Results    : passed
System Power         : on
Power Overload       : false
Power Interlock      : inactive
Main Power Fault     : false
Power Control Fault  : false
Power Restore Policy : always-off
Last Power Event     :
Chassis Intrusion    : inactive
Front-Panel Lockout  : inactive
Drive Fault          : false
Cooling/Fan Fault    : false
Current Time     : 05/24/2011 06:45:29


WAVE-694-K9#sh bmc fru
FRU Device Description : Builtin FRU Device (ID 0)
 Chassis Type           : Rack Mount Chassis
 Chassis Part Number    : 800-34889-01
 Chassis Serial         : FCH1445V03Y
 Board Mfg Date         : Mon May  2 22:00:00 2011
 Board Mfg              : CISCO
 Board Serial           : FCH1448709T
 Board Part Number      : 74-7814-01
 Product Manufacturer   : CISCO
 Product Name           : WAVE-694-K9
 Product Version        : V01
 Product Extra          : Wide Area Virtualization Engine
 Product Extra          : Small fan: FAN-WAVE-40MM=
 Product Extra          : Big fan: FAN-WAVE-60MM=

WAE#show bmc event-log
all    Display all events from BMC System Event Log
event  Display a single event number from BMC System Event Log
range  Display the range of events from BMC System Event Log
|      Output Modifiers

WAE#show bmc manangement
Watchdog Timer Use:     SMS/OS (0x44)
Watchdog Timer Is:      Started/Running
Watchdog Timer Actions: Power Cycle (0x03)
Pre-timeout interval:   0 seconds
Timer Expiration Flags: 0x00
Initial Countdown:      900 sec
Present Countdown:      740 sec
```

Related Commands

clear bmc

show cache http-metadatacache

To display HTTP metadata cache information for a WAE, use the **show cache http-metadatacache** EXEC command.

show cache http-metadatacache https {**conditional-response** | **redirect-response** | **sharepoint-prefetch** | **unauthorized-response**}

show cache http-metadatacache {**all** | **conditional-response** | **redirect-response** | **sharepoint-prefetch** | **unauthorized-response**} [*url*]

Syntax Description

https	Displays cache entries for HTTPS metadata cache response types, which includes the active entries only, not the URLs.
conditional-response	Displays cache entries for conditional responses (304).
redirect-response	Displays cache entries for redirect responses (301).
sharepoint-prefetch	Displays cache entries of the prefetched data.
unauthorized-response	Displays cache entries for authorization required responses (401).
all	Displays cache entries for all HTTP metadata cache response types.
url	(Optional) Displays cache entries that match only the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-11 describes the fields shown in the **show cache http-metadatacache all** command display.

Table 3-11 Field Descriptions for the show cache http-metadatacache all Command

Field	Description
Redirect Cache	
Active HTTP entries	Number of current HTTP redirect cache entries.
Active HTTPS entries	Number of current HTTPS redirect cache entries.
Max Entries	Maximum number of redirect cache entries allowed.
URL	URL and expiration time (in seconds) for each redirect cache entry.
Conditional Cache	
Active HTTP entries	Number of current HTTP conditional cache entries.

Table 3-11 Field Descriptions for the show cache http-metadatacache all Command (continued)

Field	**Description**
Active HTTPS entries	Number of current HTTPS conditional cache entries.
Max Entries	Maximum number of conditional cache entries allowed.
URL	URL and expiration time (in seconds) for each conditional cache entry.
Unauthorized Cache	
Active HTTP entries	Number of current HTTP unauthorized cache entries.
Active HTTPS entries	Number of current HTTPS unauthorized cache entries.
Max Entries	Maximum number of unauthorized cache entries allowed.
URL	URL and expiration time (in seconds) for each unauthorized cache entry.

Related Commands

(config) accelerator http

clear cache

show cache object-cache

To display a list of individual objects in the cache, one per line, use the **show cache object-cache** EXEC command.

show cache object-cache [accelerator *ao-name***] {server-ip** *server-ip* **| server-host** *hostname* **| url** *path***}**

Syntax Description

accelerator *ao-name*	(Optional) The name of the application accelerator specified, such as EPM or MAPI.
server-host *hostname*	Displays a list of individual objects in the cache for the specified server hostname.
server-ip *server-ip*	Displays a list of individual objects in the cache for the specified server IP address.
url *path*	Displays a list of individual objects in the cache for the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show cache object-cache** command to display a list of individual objects in the cache, one per line. You can display a list of all individual objects, or only those that match specified criteria, such as server IP address or hostname, or path of a specified URL.

Examples

The following is sample output from the **show cache object-cache** command:

```
show cache object-cache


URL                                       Size (KB)   State

------------------------------------------------------------

http://www.sampletestdomain.com/a.jpg     10          DEL_PEND
SMB://10.1.1.1/share1/z.doc               25          COMPLETE
```

```
**** Object  1 *******
Object General information
==========================
owner_ao: 15
resource_id: 253
stored_obj_id: 253
state:  OC_OBJ_STATE_CREATED
url_hash:  9381385200752939448
url:  /local/local1/test2.txt
server_ip:  0.0.0.1
hostname:  10.10.10.10
port:  8080
stored_offset:  9381385200752939448
stored_size:  1000
last_access_time:  16738851
hit_count:  2
flag:  NODUP
Object's Protocol Related Information
=======================================

size:  18446744073709551615
last_modified_time:  7814
expiration_time:  18446744073709551615
protocol_req_metadata_size:  0
protocol_resp_metadata_size:  0x100
Object's Storage Related Information
====================================
local_path:
/object-cache1/ocdata/smb_ao/fd/0_82316
022a7fc51b8
extent_list_size:  16
extent_list :
(0,1000)

*********** END OF Object Information ***********
```

Related

show object-cache

show statistics object-cache

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* | **TenGigabitEthernet** *slot/port* | **InlinePort** *slot/port* {**lan** | **wan**}]

show cdp neighbors
[**detail** | **GigabitEthernet** *slot/port* [**detail**] | **TenGigabitEthernet** *slot/port* [**detail**] |
InlinePort *slot/port/*{**lan**/**wan**}[**detail**]]

show cdp {**holdtime** | **run** | **timer** | **traffic**}

Syntax Description

entry	(Optional) Displays information for a specific CDP neighbor entry.
*****	Specifies all neighbors.
neighbor	CDP neighbor entry to display.
protocol	(Optional) Displays the CDP protocol information.
version	(Optional) Displays the CDP version.
interface	Displays the interface status and configuration.
GigabitEthernet *slot/port*	(Optional) Displays the Gigabit Ethernet configuration for the designated interface.
TenGigabitEthernet *slot/port*	(Optional) Displays the 10-Gigabit Ethernet configuration for the designated interface.
InlinePort *slot/port* {**lan** | **wan**}	(Optional) Displays Inline Port configuration for the designated interface.
neighbors	Displays CDP neighbor entries.
detail	(Optional) Displays detailed information.
holdtime	Displays the length of time that CDP information is held by neighbors.
run	Displays the CDP process status.
timer	Displays the time when CDP information is resent to neighbors.
traffic	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. This command supports VLAN (802.1Q) tagged packets

Note The CDP protocol is not supported for OVS (Open Virtual Switch) on RHEL KVM on CentOS, therefore the **show cdp** command cannot be used for vWAAS on RHEL KVM on CentOS.

Examples

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

Table 3-12 Field Descriptions for the show cdp Command

Field	Description
Sending CDP packets every XX seconds	Interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.
Sending a holdtime value of XX seconds	Time (in seconds) that the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.
Sending CDPv2 advertisements is XX	Transmission status for sending CDP Version-2 type advertisements. Possible values are enabled or not enabled.

Table 3-13 describes the fields shown in the **show cdp entry** *neighbor* command display.

Table 3-13 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: R—Router S—Switch H—Host I—IGMP device r—Repeater

Table 3-13 Field Descriptions for the show cdp entry Command (continued)

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

Table 3-14 describes the fields shown in the **show cdp entry** *neighbor* **protocol** command display.

Table 3-14 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 3-15 describes the fields shown in the **show cdp entry** *neighbor* **version** command display.

Table 3-15 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 3-16 describes the field in the **show cdp holdtime** command display.

Table 3-16 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 3-17 describes the fields shown in the **show cdp interface** command display.

Table 3-17 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.

Table 3-17 Field Descriptions for the show cdp interface Command (continued)

Field	Description
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 3-18 describes the fields shown in the **show cdp neighbors** command display.

Table 3-18 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 where the device is connected. Gig refers to a Gigabit Ethernet interface, Ten refers to a 10 Gigabit Ethernet interface, and Inline refers to an inline interface.
Holdtime	Time, in seconds, that the current device will hold the CDP advertisement from a transmitting router before discarding it.
Capability	Capability code discovered on the device. This is the type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router S—Switch H—Host I—IGMP device r—Repeater
Platform	Product number of the device.
Port ID (outgoing port)	Port number of the device.

Table 3-19 describes the fields shown in the **show cdp neighbors detail** command display.

Table 3-19 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 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.

Table 3-19 Field Descriptions for the show cdp neighbors detail Command (continued)

Field	Description
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.
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 3-20 describes the field in the **show cdp run** command display.

Table 3-20 Field Description for the show cdp run Command

Field	Description
CDP is XX.	Whether CDP is enabled or disabled.

Table 3-21 describes the field in the **show cdp timer** command display.

Table 3-21 Field Description for the show cdp timer Command

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

Table 3-22 describes the fields shown in the **show cdp traffic** command display.

Table 3-22 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.
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 3-22 Field Descriptions for the show cdp traffic Command (continued)

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

Related Commands

(config) cdp

(config-if) cdp

clear arp-cache

debug cdp

show class-map

To display the matching criteria configured for an optimization class map, use the **show class-map** EXEC command.

show class-map type { **waas**} [*classmap-name*]

Syntax Description

waas	Displays the specified WAAS optimization class map, or all class maps if no class map is specified.
classmap-name	Class map name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

This command displays the matching criteria for all class maps or a specified class map in the active policy. It also displays the number of flows that have matched each condition, in all uses of the class map, including in nested policy maps.

Related Commands

(config) class-map

show policy-map

show policy-sub-class

show statistics class-default

show statistics class-map

show clock

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

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

Syntax Description

detail	(Optional) Displays detailed information; indicates the clock source (NTP) and the current summer time setting (if any).
standard-timezones	(Optional) Displays information about the standard time zones.
all	Displays all of the standard time zones (approximately 1500 time zones). Each time zone is listed on a separate line.
details *timezone*	Displays detailed information for the specified time zone.
regions	Displays the region name of all the standard time zones. All 1500 time zones are organized into directories by region.
zones *region-name*	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 3-23 describes the field in the **show clock** command display.

Table 3-23 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 3-24 describes the fields shown in the **show clock detail** command display.

Table 3-24 Field Descriptions for the show clock detail Command

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

Related Commands

clock

(config) clock

show cms

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

show cms {**database content** {**dump** *filename* | **text** | **xml**} | **info** | **secure-store** | **device status** *name*}

Syntax Description

database	Displays embedded database maintenance information.
content	Writes the database content to a file.
dump *filename*	Dumps all database content to a text file. Specifies the name of the file to be saved under local1 directory.
text	Writes the database content to a file in text format.
xml	Writes the database content to a file in XML format.
info	Displays CMS application information.
secure-store	Displays the status of the CMS secure store.
device status *name*	Displays status for the device or device group indicated by *name*, the name of the device or device group.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show cms device status** command is not available on a standby Central Manager.

Examples

Table 3-25 describes the fields shown in the **show cms info** command display for WAAS application engines.

Table 3-25 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.

Table 3-25 Field Descriptions for the show cms info Command for WAAS Application Engines (continued)

Field	Description
Current WAAS Central Manager	Address of the Central Manager as currently configured in the **central-manager address** global configuration command. This address may differ from the registered address if a standby Central Manager is managing the device instead of the primary Central Manager with which the device is registered.
Registered with WAAS Central Manager	Address of the Central Manager with which the device is registered.
Status	Connection status of the device to the Central Manager. This field may contain one of 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 3-26 describes the fields shown in the **show cms info** command display for WAAS Central Managers.

Table 3-26 Field Descriptions for the show cms info Command for WAAS Central Managers

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

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

Table 3-27 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 **show cms database content text** command requests the management service to write its current configuration to an automatically generated file in text format.

Table 3-28 describes the field in the **show cms database content xml** command display.

Table 3-28 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 **show cms database content xml** 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 3-29):

Table 3-29 Status Messges for the show cms secure-store Command

Message	Description
WAE Messages	
`secure-store not initialized`	Secure store is not initialized.
`secure-store is initialized, enter pass-phrase to open store`	Secure store is initialized and not open.
`secure-store initialized and open`	Secure store is initialized and open.
Central Manager Messages	
`Secure store is in CM 'auto-generated passphrase' mode in 'Open' state.`	Secure store is initialized and open and in the auto-passphrase mode.
`Secure store is in 'User-provided passphrase' mode in 'Not Open' state. Use the command 'cms secure-store open' to open the secure store.`	Secure store is initialized but not open because it is in the user-passphrase mode and the passphrase has not been entered.
`Secure store is in 'User-provided passphrase' mode in 'Open' state.`	Secure store is initialized and open and the user-passphrase has been entered.

Examples

The following is sample output from the **show cms secure-store** command:

```
WAE# show cms secure-store
Secure store is in 'User-provided passphrase' mode in 'Open' state.


***** WARNING : If Central Manager device is reloaded, you must reopen Secure St
```

```
ore with the correct passphrase. Otherwise disk encryption features will not operate on
WAE(s).*****
```

Related Commands

cms secure-store

show crypto

To display crypto layer information, use the **show crypto** EXEC command.

show crypto {**certificate-detail** {**factory-self-signed** | **management** | **admin** | *filename*} | **certificates** | **ssl services** {**accelerated-service** *service* | **host-service peering**}}

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.
admin	Displays the certificate details for the Central Manager admin service certificate. This option can be used only on the Central Manager.
filename	Filename of the certificate to display.
certificates	Displays a summary of all PKI certificates. This option can be used only on the WAE.
ssl services	Displays status of SSL services. This option can be used only on the WAE.
accelerated-service *service*	Displays status of SSL accelerated service with the specified service name.
host-service peering	Displays status of the SSL host peering service.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-30 describes the fields in the **show crypto certificate-detail** command display.

Table 3-30 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.

Table 3-30 Field Descriptions for the show crypto certificate-detail Command

Field	Description
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	
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	Actual certificate follows until the End Certificate line.
END CERTIFICATE	Line that signifies the end of the certificate.

Table 3-31 describes the fields in the **show crypto certificates** command display.

Table 3-31 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	Name of the holder of the certificate.
Issuer	Who signed the certificate.

Related Commands

show statistics crypto ssl ciphers

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**, **rbcp**, **tfo**, **translog**, 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-id

To display the device ID of a WAAS device, use the **show device-id** EXEC command.

show device-id

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

This command displays the device ID, as follows:

```
WAE# show device-id
System Device ID is: 00:1a:64:f2:22:37
```

Related Commands

(config) peer

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** | **profile-branch**}

Syntax Description

configured	Displays the configured device mode, which has not taken effect yet.
current	Displays the current device mode.
profile-branch	Displays the branch profile mode, for use with the WAVE-7571, which enables the device to function as a branch device.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following is sample output from the **show device mode** command. It displays the current mode in which the WAAS device is operating.

```
WAE# show device-mode current

Current device mode: application-accelerator
```

Table 3-32 describes the field in the **show device-mode current** command display.

Table 3-32 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
```

Table 3-33 describes the field in the **show device-mode configured** command display.

Table 3-33 Field Description for the show device-mode configured Command

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

Related Commands

(config) device mode

show disks

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

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

Syntax Description

cache-details	Displays data cache details.
details	Displays currently effective configurations with more details.
failed-disk-id	Displays a list of disk serial numbers that have been identified as failed.
failed-sectors	Displays a list of failed sectors on all the disks.
disk_name	(Optional) Name of the disk for which failed sectors are displayed (disk00 or disk01).
tech-support	Displays SSD/HDD attributes for SSD/HDD devices. Displays hard drive diagnostic information and information about impending disk failures. Displays all available information from the RAID controller, including disk status (logical and physical), disk vendor ID, and serial numbers. This command replaces the **show disk smart-info** EXEC command.
details	(Optional) Displays more detailed SMART disk monitoring information.
fwlogs	(Optional) Displays disk controller firmware logs (available only on WAVE-75xx/85xx devices).

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.

Note When the system software recovery procedure is used and the system reboots and begins optimizing traffic, the show **disks details command** may show that the /dre1 partition is 98% or more used, due to the preallocation of DRE cache space. Use the **show statistics dre** command to display the actual DRE cache usage.

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 3-34 describes the fields shown in the **show disks failed-disk-id** command display.

Table 3-34 Field Description for the show disks failed-disk-id Command

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

The following is sample output from the **show disks cache- details** command.

```
WAE# show disks cache-details
Mode # oc-weight2
Name           Default MB     Existing MB    Configured MB Configured %

-----------------------------------------------------------------------------------------

Akamai          189440 MB       189440 MB        64512 MB       20.26%

Object-cache    129024 MB       129024 MB        253952 MB       79.74%

Disk cache has been configured. Please reload for the new config to take effect.
```

Table 3-35 describes the fields shown in the **show disks cache-details** command display.

Table 3-35 Field Description for the show disks cache-details Command

Field	Description
Mode	Currently configured mode for data cache partitions for Akamai cache and Object cache.
Name	Name of the cache.
Default MB	Default size alloted to Akamai cache or Object cache.
Existing MB	Current size used by Akamai cache or Object cache.
Configured MB	User configured size to be used by Akamai cache or Object cache. Takes effect after a reload. After a reload the configured size and the existing size is the same.
Configured %	User configured percentage of the total available space for Akamai Cache or Object Cache.

Table 3-36 describes the fields shown in the **show disks details** command display.

Table 3-36 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	Availability of the disk: Present, Not present or Not responding, Not used (*), or Online (for RAID-5 disks). Disk identification number and type, for example: (h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB). Lists attributes such as serial number, the technology family(SATA/SAS) and the capacity of the SSD or HDD.
disk01	Same type of information is shown for each disk.
RAID Logical drive information	RAID-5 logical drive status and error conditions and total size. (Only shown for RAID-5 systems.)
Mounted filesystems	Table containing the following column heads:

Table 3-36 Field Descriptions for the show disks details Command (continued)

Field	Description
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name “md1” indicates that the partition is a raided partition and that the RAID type is RAID-1.
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 feature	Indicates whether 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 3-37 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 3-37 Field Descriptions for the show disks tech-support Command (RAID-1)

Field	Description
disk00—disk05	Number of drives shown depends on the hardware platform.
SSD Statistics Lifetime remaining	Displays the percentage remaining lifetime of the SSD disk.
Total bytes written	Displays total bytes written to the SSD disk.
Write Amplification Factor	Displays the quotient of data written to physical NAND internally by the SSD itself divided by data transferred to the SSD from the host.
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 3-38 describes the fields shown in the **show disks tech-support** command display for a RAID-5 appliance.

Table 3-38 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.
Logical drives/Offline/Critical	Number of logical drives, number of drives that are offline, and number of critical alarms.
Controller Version Information	

Table 3-38 Field Descriptions for the show disks tech-support Command (RAID-5) (continued)

Field	Description
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	
Device #	Device number for which the information applies.
Device is a xxxx	Type of device.
State	State of the device: Online or Offline.

Table 3-38 Field Descriptions for the show disks tech-support Command (RAID-5) (continued)

Field	Description
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 3-39 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 3-39 Field Descriptions for the show disks tech-support details Command

Field	Description
disk00—disk05	Number of drives shown depends on the hardware platform.
Device	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time hh:mm:ss, year, clock standard. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.
Current Drive Temperature	Temperature of the drive in degrees Celsius.
Manufactured in week XX of year	Manufacturing details.

Table 3-39 Field Descriptions for the show disks tech-support details Command (continued)

Field	Description
Current start stop count	Number of times the device has stopped or started.
Recommended maximum start stop count	Maximum recommended count used to gauge the life expectancy of the disk.
Error counter log	Table displaying the error counter log. Counters for various types of disk errors.

Related Commands

disk

(config) disk error-handling

show tech-support

show dre

To view DRE configuration information, use the **show dre** EXEC command.

show dre [**auto-bypass**]

Syntax Description

auto-bypass	Displays the auto bypass table entries.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following is sample output from the **show dre** EXEC command:

```
WAE# show dre

DRE configuration:
  Mac-id: 50:3d:e5:9c:8f:a5
  DRE-peer-id: 50:3d:e5:9c:8f:a5-01319249ed67-92f8dea8
  Max concurrent connections: 200, max fan-out: 700
  DRE auto bypass threshold 7074 MB
```

Related Commands

clear dre

(config) dre

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*]}]

Syntax Description

|	(Optional) Output modifier.
begin *regex*	Begins with the line that matches the regular expression. You can enter multiple expressions.
exclude *regex*	Excludes lines that match the regular expression. You can enter multiple expressions.
include *regex*	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     0xcba709c0(0xcba70a00)   E
   10.99.11.200:1425    10.99.22.200:80     0xcba70780(0xcba707c0)   E
   10.99.11.200:1439    10.99.22.200:5222   0xcba703c0(0xcba70b40)   Sr
   10.99.11.200:1440    10.99.22.200:5222   0xcba70400(0xcba70440)   Sr
   10.99.22.200:1984    10.99.11.200:80     0xcba70600(0xcba70640)   E
   10.99.22.200:1800    10.99.11.200:23     0xcba70480(0x0       )   PE
   10.99.11.200:1392    10.99.22.200:80     0xcba70f80(0x0       )   E
   10.99.22.200:20      10.99.11.200:1417   0xcba701c0(0xcba70180)   E
   10.99.11.200:1417    10.99.22.200:20     0xcba70180(0x0       )   E
   10.99.22.200:1987    10.99.11.200:80     0xcba70240(0xcba70200)   E
```

```
10.99.11.200:1438     10.99.22.200:5222  0xcba70900(0xcba70580)   Sr
10.99.22.200:1990     10.99.11.200:80    0xcba70100(0xcba70140)   E
10.99.22.200:80       10.99.11.200:1426  0xcba70740(0xcba70700)   E
10.99.22.200:80       10.99.11.200:1425  0xcba707c0(0xcba70780)   E
10.99.22.200:1985     10.99.11.200:80    0xcba70a40(0xcba70a80)   E
10.99.22.200:80       10.99.11.200:1410  0xcba70500(0xcba70540)   E
10.99.22.200:80       10.99.11.200:1398  0xcba70a00(0xcba709c0)   E
10.99.22.200:80       10.99.11.200:1392  0xcba70f40(0xcba70f80)   E
10.0.19.5:54247       10.1.242.5:80      0xc9e5b400(0xc9e5b100)   ED
```

Note 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

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 3-40 describes the fields shown in the **show flash** command display.

Table 3-40 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 or bytes used by the system image.
Bootloader, rescue image, and other reserved areas, or Rescue image Bootloader & others	Number of sectors used by the bootloader, rescue image, and other reserved areas. On some devices, the number of bytes used by the rescue image is shown separately from the number of bytes used by the bootloader and other areas.
XX sectors total, XX sectors free, or Total Used Total Free	Total number of sectors in the flash memory and the number of free sectors available. Some devices show the total number of bytes used and the total free bytes available.

show flow record

To display collection information for a WAAS device, use the **show flow record** EXEC command. Collection information includes source and destination address, source and destination port, class name, number of optimized and unoptimized packets, input/output information for DRE and LZ compression, and average latency encode/decode information for DRE and LZ compression.

show flow record {*RecordName* **[template] | waas-all }**

Syntax Description

RecordName	The name of the flow record
template	The identity of the template associated with this flow record.
waas-all	Collects all WAAS statistics.

Defaults

No default behavior or values.

Device Modes

application-accelerator

central-manager

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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 3-41 describes the fields shown in the **show hardware** command display. The display may vary depending on the hardware platform.

Table 3-41 Field Descriptions for the show hardware Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) *year* by Cisco Systems, Inc. Cisco Wide Area Application Services (universal-k9) Software Release *X.X.X* (build b*nnn month day year*)	Software application, copyright, release, and build information. Displays universal-k9 for the full software image, accelerator-k9 for the accelerator only software image, and universal-npe-k9 or accelerator-npe-k9 for the NPE versions of those images. The NPE image versions have the disk encryption feature disabled for use in countries where disk encryption is not permitted.
Version	Device model identifier and 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.
Device Id	The device ID.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.

Table 3-41 Field Descriptions for the show hardware Command (continued)

Field	Description
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 (appears once for each CPU core).
Total X CPU	Number of CPUs on the device. Also reports number of cores and threads available on multi-core devices.
XXXX Mbytes of Physical memory	Number of megabytes of physical memory on the device.
XXXX Mbytes of flash memory	Number of megabytes of flash memory on the device.
X CD ROM drive	Number of CD-ROM drives on the device (if applicable).
X GigabitEthernet interfaces X TenGigabitEthernet interfaces	Number of Gigabit Ethernet and 10-Gigabit Ethernet interfaces on the device.
X InlineGroup interfaces	Number of InlineGroup interfaces on the device (if applicable).
X Console interface	Number of console interfaces on the device.
X external USB interface	Number of USB interfaces on the device.
Device Model Number	Product model 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.
Mainboard info	
Model	Hardware model identifier of the device.
Serial Number	Serial number of the WAE.
Detailed Memory Device (DIMM) configuration	Size and location of the installed memory.
List of all disk drives	
Physical disk information or RAID Physical disk information	Disks listed by number.
disk00, and so on	Availability of the disk: Present, Not present or not responding, or Not used (*). For RAID disks: ONLINE or OFFLINE. For each disk, shows the size and disk identification number.
RAID Logical drive information	Size and other information about the RAID logical drive (appears only if the device contains a logical RAID drive).
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.

Table 3-41 Field Descriptions for the show hardware Command (continued)

Field	Description
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 feature	Whether the disk encryption feature is enabled or disabled.
Primary Power Supply Unit	Whether the primary power supply is installed and powered. (Shown for devices that support reporting power supply information.)
Redundant Power Supply Unit	Whether the redundant power supply is installed and powered. (Shown for devices that support reporting redundant power supply information.)
Total number of system fans is	Number of fans installed in the device. (Shown for devices that support reporting fan information.)

Related Commands

show disks

show version

show hosts

To view the hosts on a WAAS device, use the **show hosts** EXEC command.

show hosts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

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 3-42 describes the fields shown in the **show hosts** command display.

Table 3-42 field Descriptions for the show hosts Command

Field	Description
Domain names	Domain names used by the WAE to resolve the IP address.
Name Server(s)	IP address of the DNS name server or servers.
Host Table	
hostname	FQDN (hostname and domain) of the current device.
inet address	IP address of the current host device.
aliases	Name configured for the current device based on the **host** global configuration command.

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 3-43 describes the fields shown in the **show inetd** command display.

Table 3-43 Field Descriptions for the show inetd Command

Field	Description
Inetd service configurations:	
ftp	Status of whether the FTP service is enabled or disabled.

Related Commands

(config) inetd

show interception-method

To display the configured interception method, use the **show interception-method** EXEC command.

show interception-method

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 interception-method** command:

```
WAE# show interception-method
Interception-method: wccp
WCCP Interception :
Configured State :  Enabled
Operational State : Enabled

Services Enabled on this WAE:
        TCP Promiscuous 61
```

Related Commands

(config) interception-method

show interface

To display the hardware interface information for a WAAS device, use the **show interface** EXEC command.

show interface {**GigabitEthernet** *slot/port* | **InlineGroup** *slot/grpnumber* | **InlinePort** *slot/grpnumber* {**lan** | **wan**} | **PortChannel** *index* | **standby** *grpnumber* | **virtual** *slot/port* | **TenGigabitEthernet** *slot/port* } [**detail**]

Syntax Description

GigabitEthernet *slot/port*	Displays Gigabit Ethernet interface device information. Slot and port number for the Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
InlineGroup *slot/grpnumber*	Displays the inline group information and the slot and inline group number for the selected interface.
InlinePort	Displays the inline port information and the slot and inline group number for the selected interface.
lan	Displays the inline port information for the LAN port.
wan	Displays the inline port information for the WAN port.
PortChannel *index*	Displays the port channel interface (1-4) device information.
standby *grpnumber*	Displays the standby group (1-2) information.
virtual *slot/port*	Displays the virtual interface device information. Slot and port number for the virtual interface. The slot range is 1–2; the port range is 0.
TenGigabitEthernet *slot/port*	Displays 10-Gigabit Ethernet interface device information. Slot and port number for the Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show interface** command displays hardware interface information for a WAAS device, such as interface operating mode, interception statistics, packets sent, and active optimized flows.

Note When you use the **show interface PortChannel** *index* **detail** command on an interface with an AppNav Controller, the output may display an error count larger than zero (0) for the Length Error Frames Received counter. The displayed error count does not impact WAAS performance: the packets will not be dropped and will undergo further processing.

Note If a WAAS device is running for an extended period of time (13 hours or more) without a restart, output for the **show interface** command may erroneously show input errors for the device. To clear these statistics, reload the device, run the **show interface** command, and the input errors count will be cleared to zero.

Examples

The following is sample output from the **show interface** command. It displays information for GigabitEthernet interface 0 in slot 0:

```
WAE-231-03# show interface gigabitethernet 0/0
Ethernet Address                     : 50:3d:e5:9c:8f:a5
Internet Address                     : 2.43.65.52
Netmask                              : 255.255.255.0
IPv6 Enabled                         : Yes
IPv6 Link Local Address              : fe80::4e4e:35ff:fe44:c74f
IPv6 Autoconfig Enabled              : No
IPv6 Global unicast address(es)      : 2001:420:54ff:13::457:88/119
                                     : 2001:1::1/64
IPv6 ND DAD attempts                 : 1
Admin State                          : Up
Operation State                      : Running
Maximum Transfer Unit Size           : 1500
Input Errors                         : 0
Input Packets Dropped                : 0
Packets Received                     : 4074292
Output Errors                        : 0
Output Packets Dropped               : 0
Load Interval                        : 30
Input Throughput                     : 12538 bits/sec, 13 packets/sec
Output Throughput                    : 23235 bits/sec, 11 packets/sec
Packets Sent                         : 3334662
Auto-negotiation                     : On
Full Duplex                          : Yes
Speed                                : 1000 Mbps
```

Table 3-44 describes the fields shown in the **show interface GigabitEthernet** command. Most of the other **show interface** command options display similar output.

Table 3-44 Field Descriptions for the show interface GigabitEthernet command

Field	Description
Description	Description of the interface, including member interfaces. Displayed only for logical interfaces.
lsp	Displayed only if interface is configured with link state propagation.
flow sync	Flow synchronization status. .
Ethernet address	Layer-2 MAC address.
Internet address	Internet IP address configured for this interface.
Netmask	Netmask configured for this interface.
IPv6 Enabled	Displays yes only if IPv6 configuration is enabled for this interface.
IPv6 Link Local Address	Single link-local address for this interface.

Table 3-44 Field Descriptions for the show interface GigabitEthernet command (continued)

Field	Description
IPv6 Global unicast address(es)	IPv6 address configured for this interface.
IPv6 ND DAD attempts	Number of Duplicate Address Detection attempts
Admin State	Administrative state.
Operational State	Administrative state.
Maximum Transfer Unit Size	Current configured MTU value.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Packets Received	Total number of packets received by this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Load Interval	Interval at which the interface is polled for statistics and to calculate throughput.
Input Throughput	Input throughput in bits per second and packets per second.
Output Throughput	Output throughput in bits per second and packets per second.
Packets Sent	Total number of packets sent from this interface.
Auto-negotiation	State of auto-negotiation for transmission speed and mode. Shown only for physical interfaces.
Full Duplex	State of full duplex transmission mode. Shown only for physical interfaces.
Speed	Configured speed. Shown only for physical interfaces.

Table 3-45 describes the fields shown in the **show interface InlineGroup** command.

Table 3-45 Field Descriptions for the show interface InlineGroup command

Field	Description
General Statistics Of The Group	
Internet address	Internet IP address configured for this interface.
Netmask	Netmask configured for this interface.
Interface Operating Mode	Operating mode of interface: • Intercept—Intercepting traffic • Bypass—Bypassing traffic.
Standard NIC Mode	Standard NIC mode. Off when in inline mode.
Disable Bypass Mode	Unused.
Watchdog Timer	Watchdog timer status.
Timer frequency(in ms)	Timer frequency in ms. If the timer is not reset before this interval, the interface switches into bypass mode.

Table 3-45 Field Descriptions for the show interface InlineGroup command (continued)

Field	Description
Autoreset Frequency(in ms)	WAAS resets the watchdog timer at this interval.
The watchdog timer expiry(in ms)	Watchdog timer expiration in ms.
VLAN IDs configured for interception	List of VLAN IDs configured for interception. All means all VLANS are configured for interception.
Inline Port Statistics Of The Group (WAN port and LAN port shown in separate columns)	
Packets Received Inline	Number of packets received by this interface.
Packets Bridged	*For WAAS versions earlier than 6.x:* Number of non-TCP packets or other packets that the device does not want to intercept. *For WAAS Version 6.x and later:* All packets, including non-TCP packets or other packets, are incremented in the Packets Forwarded counter.
Packets Forwarded	*For WAAS versions earlier than 6.x:* Number of packets considered for optimization or pass-through, including host-generated packets. *For WAAS Version 6.x and later:* All packets, including non-TCP packets or other packets, are incremented in the Packets Forwarded counter.
Active flows on the interface	Number of active flows on the interface.

Related Commands

(config) interface GigabitEthernet

(config) interface InlineGroup

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 3-46 describes the fields shown in the **show inventory** command display.

Table 3-46 Field Descriptions for the show inventory Command

Field	Description
Name	Chassis for an appliance or slot number for an installed interface card.
DESCR	Description of the device.
PID	Product identification (ID) number of the device.
VID	Version ID number of the device. Displays as 0 if the version number is not available.
SN	Serial number of the device.

Related Commands

show tech-support

show ip access-list

To display the access lists that are defined and applied to specific interfaces or applications on a WAAS device, use the **show ip access-list** EXEC command.

show ip access-list [*acl-name* | *acl-num*]

Syntax Description

acl-name	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl-num	(Optional) Information for a specific access list, using a numeric identifier (0–99 for standard access lists and100–199 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 and what rules are being hit. 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

Interception access lists are shown under the Application access list references section.

Examples

Table 3-47 describes the fields shown in the **show ip access-list** command display.

Table 3-47 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.
XXX TCAM Entries	Number of remaining TCAM entries on an ANC.

Table 3-47 Field Descriptions for the show ip access-list Command (continued)

Field	Description
Standard IP access list	Name of a configured standard IP access list. Displays a list of the conditions configured for this list.
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: *interface slot/port* *interface direction* *access list number*
Application access list references	List of applications and the access lists with which they are associated, displayed in the following format: *application type* *access list type and number* *associated port*

Related Commands

clear arp-cache

(config) interception

(config) ip access-list

show ip routes

To display the IP routing table for a WAAS device, use the **show ip routes** EXEC command.

show ip routes [**data** | **management**]

Syntax Description

data	Displays the routing table for data traffic.
management	Displays the routing table for management traffic.

Defaults

Displays the routing table for both data and management traffic.

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 interfaces, any user-configured static routes, and the default gateway. The last line in the Data Routes table shows the default route.

Examples

Table 3-48 describes the fields shown in the **show ip routes** command display.

Table 3-48 Field Descriptions for the show ip routes Command

Field	Description
Destination	Destination IP addresses for each route.
Netmask	Netmask for each route.
Gateway	Gateway address for each route.
Interface	Interface on which each route is configured.

Related Commands

(config) ip

(config-if) ip

show ipv6

To display the IPv6 configuration for a WAAS device, use the **show ipv6** EXEC command.

show ipv6 {**neighbors** {**virtual** *slot/port* | **GigabitEthernet** [*slot number/port*] | **Portchannel** [*Etherchannel index*] | **standby** [*standby index*] } | **routes {data | management**}}

Syntax Description

neighbors	Displays the information for IPv6 neighbors.
virtual *slot/port*	Display information for Virtual Ethernet device
GigabitEthernet [*slot number/port*]	Display information for GigabitEthernet device
Portchannel [*Etherchannel index*	Displays information for Etherchannel device
standby [*standby index*]	Displays information for Standby interfaces
routes	Displays the v6 routing table.
data	Display ipv6 static route to send data traffic
management	Display ipv6 static route to send management traffic

Defaults

Displays the neighbor details and routing table for both data and management traffic.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show ipv6** command displays the IPv6 configuration on a WAAS device, This includes the ipv6 address, local-link addresses and the default gateway of all the cached entries for the neighbor interfaces on a WAAS device. The **show ipv6 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 interfaces, any user-configured static routes, and the default gateway. The last line in the Data Routes table shows the default route

Examples

Table 3-49 describes the fields shown in the **show ipv6** command display.

Table 3-49 Field Descriptions for the show ipv6 Command

Field	Description
IPv6 Address	Configured IPv6 address on the interface
Interface Link Layer Address	Link Local address
State	Operation State

Table 3-49 Field Descriptions for the show ipv6 Command

Field	Description
Destination	Destination IP addresses for each route.
Nexthop	Netmask for each route.
Interface	Interface on which each route is configured.

Related Commands

(config) 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 3-50 describes the fields shown in the **show kdump** command display.

Table 3-50 Field Descriptions for the show kdump Command

Field	Description
Kdump state	Enabled or not enabled.
Kdump operation	Operational or not operational.
Kdump installed	If the kdump package is not installed, this line alerts you.
Kdump crashkernel	Crash kernel information (Memory @ Base Address).

Related Commands

(config) kernel kdump enable

(config) logging console

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 3-51 describes the fields shown in the **show kerberos** command display.

Table 3-51 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 key-manager

To display the key manager information for a WAAS Central Manager, use the **show key-manager** EXEC command.

show key-manager {**key-token** | **status**}

Syntax Description

key-token	Displays the encryption key token for each registered WAE device.
status	Displays the encryption status for each registered WAE device.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

central-manager

Usage Guidelines

This command is not available on a standby Central Manager.

Examples

Table 3-52 describes the fields shown in the **show key-manager key-token** command display. The set of fields is displayed for each key used on each WAE registered to the Central Manager.

Table 3-52 Field Descriptions for the show key-manager key-token Command

Field	Description
WAE Device	WAE device name.
Key Token	The encryption token.
Creation Time	Time the encryption key was created.
Encryption Algorithm	Type of encryption algorithm used.
Type	Type of key.

Related Commands

(config) disk encrypt

cms secure-store

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
```

Related Commands

clear arp-cache

license add

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 memory	Total amount of system memory in kilobytes (KB), not including the amount reserved for the rescue kernel.
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.

Syntax Description

This command has no arguments or keywords.

show ntp

To display the NTP parameters for a WAAS device, use the **show ntp** EXEC command.

show ntp status

Syntax Description

status	Displays the NTP status.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-54 describes the fields shown in the **show ntp status** 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 (**l**ocal, **u**nicast, **m**ulticast, or **b**roadcast).
when	Indicates when the last packet was received from the server in seconds.
poll	Time check or correlation polling interval in seconds.
reach	8-bit reachability register. If the server was reachable during the last polling interval, a 1 is recorded; otherwise, a 0 is recorded. Octal values 377 and above indicate that every polling attempt reached the server.
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 object-cache

To display global statistics about the cache, use the **show object-cache** EXEC command.

show object-cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show object-cache** command to display global statistics about the cache,

The following is sample output from the **show object-cache** command:

```
show object-cache


Accelerator        Config State            Operational State
-----------        ------------            -----------------
ObjectCache        Enabled                 Running

More details :
Object Cache Mount Path: /object-cache1
Object Cache Storage Size: 242227 MB
```

Related

show cache object-cache

show statistics object-cache

show peer optimization

To display the configured serial peers for a WAAS device, use the **show peer optimization** EXEC command.

show peer optimization

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 example shows how to display the device IDs of the configured nonoptimizing peer devices:

```
WAE# show peer optimization
Configured Non-optimizing Peers:
        Peer Device Id: 00:21:5e:28:87:54
```

Related Commands

show device-id

(config) peer

show policy-map

To display the policy map rules configured for an optimization class map, use the **show policy-map** EXEC command.

show policy-map type {**waas**} [*policymap-name*]

Syntax Description

waas	Displays the specified WAAS optimization policy map, or all policy maps if no policy map is specified.
classmap-name	Policy map name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

This command displays the policy rules for all policy maps or a specified policy map. It also displays the number of flows that have matched each class map and the total number of flows that have matched the policy. For nested policy maps, a match is counted for each policy map involved in the classification of a connection.

Related Commands

(config) policy-map

show class-map

show policy-sub-class

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

cpu	(Optional) Displays CPU utilization.
debug *pid*	(Optional) Prints the system call and signal traces for a specified process identifier to display system progress.
memory	(Optional) Displays memory allocation processes.
system	(Optional) Displays system load information in terms of updates.
delay *secs*	(Optional) Specifies the delay between updates, in seconds (1–60).
count *num*	(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. For real time CPU utilization information, use the top EXEC command.

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.

Note CPU utilization and system performance are severely affected when you use these commands. We therefore recommend that you avoid using these commands, especially the **show processes debug** command, unless it is absolutely necessary.

Examples

Table 3-55 describes the fields shown in the **show processes** command display.

Table 3-55 Field Descriptions for the show processes Command

Field	Description
CPU utilization	CPU utilization since the last reload as a percentage for user, system overhead, and idle. Includes average usage (calculated every 10 minutes).
Overall current CPU utilization	Current CPU utilization over all CPUs in the system.
PID	Process identifier.
STATE	Current state of corresponding processes. R = running S = sleeping in an interruptible wait D = sleeping in an uninterruptible wait or swapping Z = zombie T = traced or stopped on a signal
PRI	Priority of processes.
User T	User time utilization in seconds.
Sys T	System time utilization in seconds.
COMMAND	Process command.
Total	Total available memory in bytes.
Used	Memory currently used in bytes.
Free	Free memory available in bytes.
Shared	Shared memory currently used in bytes.
Buffers	Buffer memory currently used in bytes.
Cached	Cache memory currently used in bytes.
SwapTotal	Total available memory in bytes for swap purposes.

Related Commands

top

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 3-56 describes the fields shown in the **show radius-server** command display.

Table 3-56 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 reload

To display scheduled reload information, use the **show reload** EXEC command.

show reload

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Related Commands

reload

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 [interface | no-policy | policy | snmp | wccp]

Syntax Description

no-policy	(Optional) Does not display the policy engine configuration.
interface	(Optional) Displays interface configuration.
policy	(Optional) Displays policy engine configuration.
snmp	(Optional) Displays SNMP configuration.
wccp	(Optional) Displays WCCP configuration.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this EXEC command in conjunction with the **show startup-config** command to compare the information in running memory to the startup configuration used during bootup.

Examples

The following is sample output from the **show running-config** command. It displays the currently running configuration of a WAAS device.

```
NO-HOSTNAME-10-78-108-140#show running-config
! waas-universal-k9 version 6.0.1 (build b2 Jun 12 2015)
!
device mode central-manager
!
!hostname NO-HOSTNAME-10-78-108-140
!
!primary-interface GigabitEthernet 0/0 ipv4
!
primary-interface GigabitEthernet 0/0 ipv6
!
interface GigabitEthernet 0/0
 ip address 10.78.108.140 255.255.255.0
 ipv6 address autoconfig
 exit
interface GigabitEthernet 0/1
 shutdown
 exit
!
ip default-gateway 10.78.108.1
```

```
!
!!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
bmc lan ip address set-to-factory-default
no bmc lan enable
no bmc serial-over-lan enable
!
!
ntp server 10.78.108.125
!
!
!
!
username admin password 1 ****
username admin privilege 15
!
!
!
!
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
!
inetd enable ftp
!
!
sshd enable
!
!
!
!
!
!
! End of WAAS configuration
```

Related Commands

configure

copy running-config

copy startup-config

show service-insertion

To display information about the entities (WNs, WNGs, ANCs, ANCG, and a service context) defined in an AppNav Cluster configuration and the cluster status, use the **show service-insertion** EXEC command.

show service-insertion {**data-path mtu** | **pass-through offload** | **service-context** [**detail**] | **appnav-controller** *ip-address* | **appnav-controller-group** | **service-node** [*ip-address*] | **service-node-group** [*sngroupname*]}

Syntax Description

data-path mtu	Displays the MTU of the data path from this device to each of the other ANCs in the cluster.
pass-through offload	Displays the pass-through offload configuration.
service-context	Displays service context information. Available only on ANCs.
detail	Displays service context information and includes details about the ANCG, ANCs, and WNGs that are part of the service context.
appnav-controller *ip-address*	Displays information about the specified ANC. Available only on ANCs.
appnav-controller-group	Displays information about the ANCG. Available only on ANCs.
service-node [*ip-address*]	Displays information about the WN on this device or the specified device. If an IP address is specified, the information is the local device's view of the specified device.
service-node-group *sngroupname*	Displays information about the specified WNG. If the group name is not specified, it shows information about all WNGs. Available only on ANCs.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command returns minimal information if the entity or service context is disabled, or if the entity is not attached to the service context.

Although software version 6.x.x does not support Video and CIFS traffic acceleration, the Video and CIFS load markers have been retained in the **show service-insertion service-node** command for backward compatibility. This is to ensure that an AppNav Controller in version 5.x.x is able to forward a request for traffic acceleration to a Service Node in version 6.x.x.

Examples

Table 3-57 describes the fields shown in the **show service-insertion service-context** command display

Table 3-57 Field Descriptions for the show service-insertion service-context Command

Field	Description
Service Context	Service context name.
Service Policy	Name of the AppNav policy map that is attached to the service context.
Cluster protocol ICIMP version	Cluster ICIMP protocol version.
Cluster protocol DMP version	Cluster DMP protocol version.
Time service context was enabled	Time the service context was enabled.
Current FSM state	Current cluster finite state machine state: • Operational—Stable and operational. All ANCs in the cluster have converged on a stable view of the devices in the cluster. • Degraded—Partially stable state and operational. All ANCs cannot converge on a stable view of devices in the cluster but cluster can operate in pass-through mode. • Converging—Performing the convergence process due to a device change. Devices are exchanging information about each device's view of the cluster. • Admin Disabled—Configured but not enabled. • Initializing—Cluster is initializing. • Internal Error—Internal error condition due to convergence failing after 5 minutes.
Time FSM entered current state	Time the cluster finite state machine entered the current state.
Last FSM state	Last cluster finite state machine state. See the Current FSM State field for details.
Time FSM entered last state	Time the cluster finite state machine entered the last state.
Joining state	Current joining state: • Started—Device has started to join the cluster gracefully. • Completed—The graceful join operation completed successfully. • Aborted—Graceful join was started and then disabled before completing. • Not Configured—Device did not join the cluster gracefully. • Unknown—State is unknown (default).
Time joining state entered	Time the device entered the joining state.

Table 3-57 Field Descriptions for the show service-insertion service-context Command

Field	Description
Cluster operational state	Cluster operational state: • Operational—All ANCs are redirecting new flows to WNs. This is the overall cluster state if all ANCs have a FSM state of Operational or a cluster was Operational and a device is added. (This makes the FSM state go to Converging, but the operational state stays as Operational because the existing devices are handling new flows.) • Degraded—ANCs are not redirecting new flows to WNs but existing flows may be redirected to WNs. New flows are passed through. This is the overall cluster state if any ANCs have a FSM state other than Operational.
Interception Readiness State	Interception readiness state of this device: • Ready—Ready to intercept traffic. This state occurs two minutes after the cluster has reached stable convergence. (This state can exist even with a degraded cluster operational state because traffic is passed through in these cases.) • Not Ready—Not ready to intercept traffic (could be due to cluster convergence)
Device Interception State	Interception state of this device: • Shutdown—Device is not intercepting traffic. • Not Shutdown—Device is intercepting traffic. • Unknown—State is unknown (default).
Stable AC View	IP addresses of the ANCs in the stable view of this device. The stable view is the view of the devices after the convergence period in which all ANCs in the cluster have implicitly agreed on the view of all devices in the cluster.
Stable SN View	IP addresses of the WNs in the stable view of this device.
Current AC View	IP addresses of the ANCs in the current view of this device. The current view is the immediate view of the devices in the cluster. This could differ from the stable view if a device was newly added.
Current SN View	IP addresses of the WNs in the current view of this device.

Table 3-58 describes the additional fields shown in the **show service-insertion service-context detail** command display. The AppNav Controller Group and AppNav Controller sections of this table also describe the fields shown in the **show service-insertion appnav-controller-group** command display. The AppNav Controller section of this table also describes the fields shown in the **show service-insertion appnav-controller** command display.

The Service Node Group and Service Node sections of this table also describe the fields shown in the **show service-insertion service-node-group** command display. The Service Node section of this table also describes the fields shown in the **show service-insertion service-node** command display.

Table 3-58 Field Descriptions for the show service-insertion service-context detail Command

Field	Description
Service Context	Service context name.
Service Context configured state	State of service context (enabled or disabled). If disabled, some output fields are not shown.
AppNav Controller Group	ANCG name.
Member AppNav Controller count	Number of ANCs in the ANCG.
Members	IP addresses of the member ANCs in the ANCG.
Member (removed from config) AppNav Controller count	Number of ANCs that have been recently removed from the ANCG. These appear until the cluster converges on agreement that these are removed.
Members (removed from config)	IP addresses of the member ANCs recently removed from the ANCG.
An AppNav Controller section appears for each ANC in the cluster.	
AppNav Controller	IP address of the ANC. A (local) indication means that this is the device on which you are running this command.
AppNav Controller ID	Identifier for the ANC.
Current status of AppNav Controller	Current status of communication to this ANC: • Alive—This device can communicate with the ANC. • Alive (Removed from config)—This device was recently removed from the configuration but can still communicate with the ANC. • Dead—This device cannot communicate with the ANC. • Inactive—This device was added to a full cluster that had recently removed an ANC. Until the removal process completes or the removed ANC stops responding, this device cannot join the cluster and remains in Inactive state.
Time current status was reached	Time current status was reached.
Joining status of AppNav Controller	Current joining status of the ANC: • Joining—The ANC is in the process of joining the cluster defined on the local ANC. • Joined—The ANC has successfully joined the cluster defined on the local ANC.
Secondary IP address	IP address that the ANC is using as its source address when communicating with this ANC.
Cluster protocol ICIMP version	Cluster ICIMP protocol version running on this ANC.
Cluster protocol incarnation number	Internal information.

Table 3-58 Field Descriptions for the show service-insertion service-context detail Command (continued)

Field	Description
Cluster protocol last sent sequence number	Internal information.
Cluster protocol last received sequence number	Internal information.
Current AC View of AppNav Controller	IP addresses of the member ANCs in the ANCG, as viewed by this ANC.
Current SN View of AppNav Controller	IP addresses of the member WNs in the ANCG, as viewed by this ANC.
A Service Node Group section appears for each WNG in the cluster.	
Service Context	Service context name.
Service Context configured state	State of service context (enabled or disabled). If disabled, some output fields are not shown.
Service Node Group name	WNG name.
Service Node Group ID	Identifier for the WNG.
Member Service Node count	Number of WNs in the WNG.
Members	IP addresses of the member WNs in the WNG.
A Service Node section appears for each WN in the WNG.	
Service Node	IP address of the WN.
Service Node ID	Identifier for the WN.
Current status of Service Node	Current status of communication to this WN: • Alive—This device can communicate with the WN. • Dead—This device cannot communicate with the WN due to connectivity or not configured. • Excluded—This device can communicate with the WN, but another ANC cannot communicate with the WN. New flows are not redirected to this WN by any ANC, but existing flows could still be redirected if the device had previously been Alive and receiving flows.
Time current status was reached	Time current status was reached.
Secondary IP address	IP address that the WN is using as its source address when communicating with this ANC.
Cluster protocol DMP version	Cluster ICIMP protocol version running on this WN.
Cluster protocol incarnation number	Internal information.
Cluster protocol last sent sequence number	Internal information.

Table 3-58 Field Descriptions for the show service-insertion service-context detail Command (continued)

Field	Description
Cluster protocol last received sequence number	Internal information.
Accelerator State (appears for each WN in the WNG)	
Accl	Application accelerator name.
State	Application accelerator state: • GREEN—Operating normally and accepting new flows. • YELLOW—Servicing existing flows but not accepting new flows due to overload, license removed, or policy engine timeout. • RED—Not running due to not configured, not licensed, or unresponsive.
For	Amount of time the application accelerator has been in this state.
SNG Availability per Accelerator (for the whole WNG)	
Accl	Application accelerator name.
Available	Availability status: • Yes—In GREEN state on at least one WN in the WNG. • No—In YELLOW or RED state on all WNs in the WNG.
Since	Amount of time the application accelerator has been available.

Related Commands

(config) service-policy

show statistics service-insertion

show service-policy

To display information about the optimization use the **show service-policy** EXEC command.

show service-policy type {**waas** {**application-name** | **dynamic** [**app-id** {*app-id* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**}| **detail** | **dm-index** *index* | **server-ip** *ip_address* | **server-port** *port*]| **epm** | **status**}}

Syntax Description

dynamic	Displays policy information for dynamic matched flows.
detail	(Optional) Displays detailed policy information for dynamic matched flows.
server-ip *ip_address*	(Optional) Displays the policy information for dynamic matched flows for the server with the specified IP address.
server-port *port*	(Optional) Displays the policy information for dynamic matched flows for the server with the specified port number (1–65535). **Note** The CIFS application accelerator is removed from WAAS v6.0.1, but the CIFS policy is continued for two ports: Port 139 and Port 445. For these ports only, the SMB application accelerator runs on CIFS policy. Therefore, an alarm generated by SMB on Port 139 or Port 445 is seen as a CIFS alarm.
epm	Displays policy information for EPM flows
status	Displays how many policy resources are in use and available.
waas	Displays WAAS optimization policy information.
application-name	Displays the configured application names on the device.
app-id *app-id*	Displays the policy information for dynamic matched flows for the application with the specified application number (0-1023) or the specified traffic type.
mapi **ms-ad-rep** **ms-exch-nspi** **ms-frs** **ms-frs-api** **ms-rfr** **ms-sql** **msn-messenger** **netlogon**	Microsoft Exchange MAPI aka Exchange Server Store EMSMDB, Microsoft Active Directory Replication (drsuapi), Microsoft Active Directory Name Service Provider (NSP), Microsoft File Replication Services (FRS), Microsoft File Replication API, Microsoft Exchange Directory RFR Interface, Microsoft SQL, Microsoft Messenger Service, Netlogon RPC
dm-index *index*	Displays the policy information for dynamic matched flows for the application with the specified DM index.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-59 describes the fields shown in the **show service-policy type waas status** command display.

Table 3-59 Field Descriptions for the show service-policy type waas status Command

Field	Description
Application names	Number of total allowed, used, and available WAAS application names.
Class Maps	Number of total allowed, used, and available WAAS class maps.
Matches	Number of total allowed, used, and available WAAS match conditions.
Optimization policy map	Name of optimization policy map in use.

Table 3-60 describes the fields shown in the **show service-policy type waas application-name** command display.

Table 3-60 Field Descriptions for the show service-policy type waas application-name Command

Field	Description
Number of application names	Number of defined WAAS application names.
#	Number of a defined application.
Application Name	Name of a defined application.
Occurrences	Number of occurrences of the application in the policy map.

Table 3-61 describes the fields shown in the **show service-policy type waas epm** command display.

Table 3-61 Field Descriptions for the show service-policy type waas epm Command

Field	Description
Keyword	An EPM-related application name.
App-Id	Application ID.
UUID	UUID associated with this traffic type.
Ref Count	Number of times this application is referenced in the policy map.
Hits	Number of hits on this application since the device started up.
SC Add Count	Number of ???.

The following is sample output from the **show service-policy type waas epm** command:

```
ANC# show service-policy type waas epm
Keyword             App-Id    UUID
----------------    --------  ----------------------------------------
mapi                78        a4f1db00ca471067b31f00dd010662da
     Ref Count:          1  Hits:          0  SC Add Count =          0
```

```
ms-ad-rep            1252      e35142354b0611d1ab0400c04fc2dcd2
     Ref Count:          1  Hits:          0  SC Add Count =          0

ms-exch-nspi         1249      f5cc5a184264101a8c5908002b2f8426
     Ref Count:          1  Hits:          0  SC Add Count =          0

ms-rfr               1253      1544f5e0613c11d193df00c04fd7bd09
     Ref Count:          1  Hits:          0  SC Add Count =          0

ms-frs               1250      f5cc59b44264101a8c5908002b2f8426
     Ref Count:          1  Hits:          0  SC Add Count =          0

ms-sql               4098      3f99b9004d87101b99b7aa0004007f07
     Ref Count:          1  Hits:          0  SC Add Count =          0
```

Related Commands

(config) service-policy

show services

To display services-related information for a WAAS device, use the **show services** EXEC command.

show services {**ports** [*port-num*] | **summary**}

Syntax Description

ports	Displays services by port number.
port-num	(Optional) Up to 8 port numbers (1–65535).
summary	Displays the services summary.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following is sample output from the **show services** 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
```

```
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** | **engineID** | **event** | **group** | **stats** | **user**}

Syntax Description

alarm-history	Displays SNMP alarm history information.
engineID	Displays local SNMP engine identifier.
event	Displays events configured through the Event MIB. This keyword applies only to application-accelerator device mode.
group	Displays SNMP groups.
stats	Displays SNMP statistics.
user	Displays SNMP users.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

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.

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 **ssh** 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 **show** output.
Comment:	Description of the trigger function and use. For example: License is not valid.
Sample:	Basis on which the test sample is being evaluated. For example: Abs (Absolute) or Delta.
Freq:	Frequency. Number of seconds to wait between trigger samplings. To encourage consistency in sampling, the interval is measured from the beginning of one check to the beginning of the next and the timer is restarted immediately when it expires, not when the check completes.
Test:	Type of trigger test to perform based on the SNMP trigger configured. The Test field may contain the following types of tests: Absent—Absent existence of a test Boolean—Boolean value test Equal—Equality threshold test Falling—Falling threshold test Greater-than—Greater-than threshold test Less-than—Less-than threshold test On-change—Changed existence test Present—Present present test Rising—Rising threshold test
Wildcard	True or False.
ObjectOwner:	Name of the object owner who created the trigger using the **snmp-server trigger** global configuration command or by using an SNMP interface. "CLI" is the default owner.
Object:	String identifying the object.
Boolean Entry:	
Value:	Object identifier of the MIB object to sample to see whether the trigger should fire.

Table 3-66 Field Descriptions for the show snmp event Command (continued)

Field	Description
Cmp:	Comparison. Type of boolean comparison to perform. The numbers 1–6 correspond to these Boolean comparisons: unequal (1) equal (2) less (3) lessOrEqual (4) greater (5) greaterOrEqual (6)
Start:	Starting value for which this instance will be triggered.
ObjOwn:	Object owner.
Obj:	Object.
EveOwn:	Event owner.
Eve:	Event. Type of SNMP event. For example: CLI_EVENT.
Delta Value Table:	Table containing trigger information for delta sampling.
(0):	
Thresh:	Threshold value to check against if the trigger type is threshold.
Exis:	Type of existence test to perform. Values are 1 or 0.
Read:	Indicates whether the MIB instance has been queried or not.
OID:	Object ID (Same as MIB instance).
val:	Value ID.
(2):	MIB instance on which the trigger is configured. This is the second management trigger listed in the **show** output. The fields are repeated for each instance listed in this **show** command.

Table 3-67 describes the fields shown in the **show snmp group** command display.

Table 3-67 Field Descriptions for the show snmp group Command

Field	Description
groupname	Name of the SNMP group, or collection of users who have a common access policy.
security_model	Security model used by the group (either v1, v2c, or v3).
readview	String identifying the read view of the group.
writeview	String identifying the write view of the group.
notifyview	string identifying the notify view of the group.

Table 3-68 describes the fields shown in the **show snmp stats** command display.

Table 3-68 Field Descriptions for the show snmp stats Command

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Table 3-69 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

(config) snmp-server view

(config) snmp-server 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 the SSH version 2 protocol only.	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

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

To display application accelerator general statistics for a WAAS device, use the **show statistics accelerator** EXEC command.

show statistics accelerator detail

show statistics accelerator epm [**detail**]

show statistics accelerator generic {**connections** {**epm** | **http** | **ica** | **mapi** | **smb** | **ssl** }| **detail**}

show statistics accelerator http [**debug** | **detail** | **https**]

show statistics accelerator ica [**detail**]

show statistics accelerator mapi [**detail**]

show statistics accelerator mapi detail rpchttp

show statistics accelerator smb [**debug | detail | inc Print | request**]

show statistics accelerator ssl [**detail** | **payload** {**http** | **other**}]

show statistics accelerator wansecure [**detail**]

Syntax Description

detail	(Optional) Displays detailed statistics.
epm	Displays statistics for the EPM application accelerator.
generic	Displays statistics for the generic application accelerator.
connections	Displays generic connection statistics.
http	Displays statistics for the HTTP application accelerator.
ica	Displays statistics for the ICA application accelerator.
mapi	Displays statistics for the MAPI application accelerator.
mapi rpchttp	Displays statistics for the MAPI RPC HTTP application accelerator.
smb	Displays statistics for the SMB application accelerator.
request	Displays SMB application accelerator statistics on requests.
ssl	Displays statistics for the SSL application accelerator.
wansecure	Displays statistics for the WAN secure application accelerator.
debug	(Optional) Displays debug statistics.
https	Displays statistics for the HTTPS application accelerator.
payload	(Optional) Displays the SSL payload type.
other	Displays the unidentified protocol flows within SSL.

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 epm detail** command display.

Table 3-71 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 3-72 describes the fields shown in the **show statistics accelerator generic connections detail** command display. This command shows the aggregated statistics for all connections.

Table 3-72 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.

Table 3-72 Field Descriptions for the show statistics accelerator generic Command (continued)

Field	Description
Time Statistics were Last Reset/Cleared	Local time accelerator was last started or restarted, or the **clear statistics** command was executed since accelerator was last started or restarted.
Total Handled Connections	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented. 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. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
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	Number of WAN side connections currently established and either in use or free for fast connection use. 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 **clear statistics accelerator** command.
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 **clear statistics accelerator** command.
Global Generic AO Connection Statistics	
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. 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. 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.

Table 3-72 Field Descriptions for the show statistics accelerator generic Command (continued)

Field	Description
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	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).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
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 3-72 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: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched

Table 3-73 describes the fields shown in the **show statistics accelerator http detail** command display.

Table 3-73 Field Descriptions—show statistics accelerator http detail 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 **clear statistics accelerator [http | all]** command was executed since accelerator was last started or restarted.

Table 3-73   Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total Handled Connections	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented. 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. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total Optimized Connections	Connections previously and currently optimized by the HTTP 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.	Number of WAN side connections currently established and either in use or free for fast connection use. 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 **clear statistics accelerator [http | all]** command.
Current Pending Connections	Number of SYN requests queued waiting for for accelerator to accept.
Maximum Active Connections	Highest number of active connections since accelerator was last started/restarted. Not cleared using the **clear statistics accelerator [http | all]** command.
Total Time Saved (ms)	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.
Current Active Connections Free for Fast Connection Use	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. Decremented when an available idle active connection is reused or its idle timeout (5 secs) is reached. Not cleared using the **clear statistics accelerator [http | all]** command.

Table 3-73 Field Descriptions—show statistics accelerator http detail 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. 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.
Current Active Connections with Object-cache optimization	The total number of current active connections with object-cache optimization.
Percentage of Connection Time Saved	(Total Time Saved / (Total Time Saved + Total Round Trip Time For All Connections)) * 100.
Object Cache Caching Type	
Object cache transactions served from cache	The total number of object cache transactions served from cache.
Object cache request bytes for cache-hit transactions	The total number of object cache request bytes for cache-hit transactions.
Object cache response bytes for cache-hit transactions	The total number of object cache response bytes for cache-hit transactions.
Object cache response time saved for cache-hit transactions	The total number of object cache response time saved for cache-hit transactions.
Avg. response time saved per cache-hit transaction (ms)	The average response time saved per cache-hit transaction, in milliseconds.
Percentage response time savings for cache-hit transactions	The total percentage response time savings for cache-hit transactions.
Avg. response time saved for connections with RTT [00-20] (ms)	The average response time saved for connections with RTT, in the range 00-20, in milliseconds.

Table 3-73 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Avg. response time saved for connections with RTT [20-50] (ms)	The average response time saved for connections with RTT, in the range 20-50, in milliseconds.
Avg. response time saved for connections with RTT [50-90] (ms)	The average response time saved for connections with RTT, in the range 50-90, in milliseconds.
Avg. response time saved for connections with RTT [90+] (ms)	The average response time saved for connections with RTT, in the range 90+, in milliseconds.
Object cache transactions requiring freshness check	The total number of object cache transactions requiring freshness check.
Object cache responses not cached	The total number of object cache responses not cached.
Object cache responses stored in cache	he total number of object cache responses stored in cache.
Object cache WAN response bytes for freshness check	The total number of object cache WAN response bytes requiring freshness check.
Object cache WAN response bytes not cached	The total number of object cache WAN response bytes not cached.
Object cache WAN response bytes stored in cache	The total number of object cache WAN response bytes stored in cache.
Object cache LAN response bytes for freshness check	The total number of object cache LAN response bytes requiring freshness check.
Object cache Percentage cache-hit transactions	The percentage of object cache cache-hit transactions.
Object cache Percentage cache-hit bytes	The percentage of object-cache cache-hit bytes.
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. This statistic should match the Total Fast Connections on the peer WAE.
Total SYN Timeouts	Total number of SYN timeouts because the HTTP accelerator was temporarily busy.
Total Time for Metadata Cache Miss (ms)	Total time for metadata cache misses, in milleseconds.
RTT saved by Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving redirect (301) responses, in milliseconds.
RTT saved by Authorization Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving authentication required (401) responses, in milliseconds.
RTT saved by Content Refresh Check Metadata Cache (ms)	Round trip time saved by caching and locally serving conditional (304) responses, in milliseconds.
Total Time Saved by Fast Connection Use (ms)	Total time saved by fast connection reuse, in milliseconds.
Total Locally Served Redirect Responses	Number of locally served redirect (301) responses.

Table 3-73 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total Locally Served Unauthorized Responses	Number of locally served authentication required (401) responses.
Total Locally Served Conditional Responses	Number of locally served conditional (304) responses.
Total Remotely Served Redirect Responses	Number of remotely served redirect (301) responses (cache misses).
Total Remotely Served Unauthorized Responses	Number of remotely served authentication required (401) responses (cache misses).
Total Remotely Served Conditional Responses	Number of remotely served conditional (304) responses (cache misses).
Total Requests with URL Longer than 255 Characters	Number of requests not cached because the URL is longer than 255 characters.
Total Requests with HTTP Pipelining	Number of requests not cached due to HTTP pipelining.
Total Transactions Handled	Number of HTTP transactions handled.
Total Server Compression Suppression	Number of times server compression was suppressed.
Total Requests Requiring Server Content-Revalidation	Number of requests that required content to be revalidated with the origin server, as specified by a Cache-Control header.
Total Responses not to be Cached	Number of 200, 301, 304, and 401 responses not to be cached, as specified by a Cache-Control header.
Total Connections Expecting Authentication	Number of connections expecting authentication.
Total Connections with Unsupported HTTP Requests	Number of connections with unsupported HTTP requests.
Total Connections with Unsupported HTTP Responses	Number of connections with unsupported HTTP responses.
Total Hints Sent to DRE Layer to Flush Data	Number of DRE hints to flush data.
Total Hints Sent to DRE Layer to Skip LZ	Number of DRE hints to skip LZ compression.
Total Hints Sent to DRE Layer to Skip Header Information	Number of DRE hints to skip header information.
Total ACL Lookups for Subnet feature	Total number of system calls made for ACL lookup.
Total Sessions using Global enable/disable settings	Total number of sessions using global configuration for all four HTTP AO optimization features.
Total Sessions using ACL-selected settings	Total number of sessions using subnet configuration for at least one HTTP AO optimization feature.
Total sessions using SharePoint optimization	Number of sessions using SharePoint optimization feature to access objects from SharePoint server.
Total sessions using SharePoint pre-fetch optimization	Number of sessions where pre-fetch optimization for SharePoint objects ((MS Office applications) is enabled.

Table 3-73 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total SharePoint objects prefetched	Number of SharePoint objects that have been prefetched due to client requests.
Total locally served SharePoint prefetch objects	Number of SharePoint objects that have been prefetched and have been displayed on the client.
Total RTT saved by SharePoint optimization (ms)	Total response time (in milliseconds) saved in accessing SharePoint objects by enabling SharePoint optimization.
Total RTT saved by SharePoint prefetch cache hit (ms)	Total response time (in milliseconds) saved in accessing SharePoint data that has already been prefetched and stored in the cache.
Total remotely served SharePoint prefetch objects	Number of SharePoint objects that have been prefetched and displayed remotely.
Total time for SharePoint cache miss (ms)	Total time (in milliseconds) lost in accessing SharePoint data that is not already stored in the cache.
Total time for SharePoint prefetch cache miss (ms)	Total time (in milliseconds) lost in finding prefetched data that was not stored in cache.
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).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
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 3-73 Field Descriptions—show statistics accelerator http detail 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: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
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.
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	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 3-74 describes the fields shown in the **show statistics accelerator http debug** command display.

Table 3-74 Field Descriptions—show statistics accelerator http debug Command

Field	Description
Total HTTP Parser Errors	Number of times that various HTTP parser errors occurred.
Total HTTP Transactions	HTTP transaction statistics.
Total Memory Allocation Errors	Number of times that various memory allocation errors occurred.
Total HTTP Requests	Number of various HTTP requests received.
Total HTTP Responses	Number of various HTTP responses.
Total HTTP Requests Processing Errors	Number of various HTTP request processing errors.
Total HTTP Responses Processing Errors	Number of various HTTP response processing errors.
Total HTTP 1-0 Requests	Total HTTP 1.0 requests.
Total HTTP 1-1 Requests	Total HTTP 1.1 requests.
Total HTTP 1-0 Responses	Total HTTP 1.0 responses.
Total HTTP 1-1 Responses	Total HTTP 1.1 responses.
Total 301 Cached Responses	Total 301 cached responses.
Total 301 Non-Cached due to Long HTTP Header	Number of 301 responses not cached due to a long HTTP header.
Total 301 Non-Cached due to Unsupported HTTP Header	Number of 301 responses not cached due to an unsupported HTTP header.
Total 301 Non-Cached due to Cache Control Directives	Number of 301 responses not cached due to cache control directives.
Total 301 Non-Cached due to Authentication Flag Being Set	Number of 301 responses not cached due to the authentication flag being set.
Total 301 Non-Cached due to Metadata Cache Thrashing Limit	Number of 301 responses not cached due to metadata cache thrashing limit.
Total 301 Non-Cached due to a long URL	Number of 301 responses not cached due to a long URL. The URL length includes the length of the destination IP address.
Total 301 Non-Cached due to a Webdav Method	Number of 301 responses not cached due to a webdav method.
Total 401 Cached Responses	Total 401 cached responses.
Total 401 Non-Cached due to Long HTTP Header	Number of 401 responses not cached due to a long HTTP header.
Total 401 Non-Cached due to Unsupported HTTP Header	Number of 401 responses not cached due to an unsupported HTTP header.
Total 401 Non-Cached due to Cache Control Directives	Number of 401 responses not cached due to cache control directives.
Total 401 with Unsupported Authentication Mechanism	Number of 401 responses with unsupported authentication mechanisms.

Table 3-74 Field Descriptions—show statistics accelerator http debug Command (continued)

Field	Description
Total 401 Non-Cached due to Metadata Cache Thrashing Limit	Number of 401 responses not cached due to metadata cache thrashing limit.
Total Type-2 401 responses	Number of 401 responses that use type 2 NTLM authentication.
Total 401 Non-Cached due to a long URL	Number of 401 responses not cached due to a long URL.
Total 401 Non-Cached due to a Webdav Method	Number of 401 responses not cached due to a webdav method.
Total HTTP Requests With Cache Control Checks	Total HTTP requests with cache control checks.
Total HTTP Responses With Cache Control Checks	Total HTTP responses with cache control checks.
Total Conditional Requests with max-age header	Total conditional requests with max-age header.
Total Conditional Requests with 'If-Range' Header	Total conditional requests with If-Range header.
Total Conditional Requests with If-None-Match header	Total conditional requests with If-None-Match header.
Total Conditional Requests With If-None-Match value >63 chars	Total conditional requests with If-None-Match value longer than 63 characters.
Total Conditional Requests with If-Modified-Since header	Total conditional requests with If-Modified-Since header.
Total Conditional Requests with invalid If-Modified-Since header	Total conditional requests with invalid If-Modified-Since header.
Total Conditional Requests with Connection: Keep-alive header	Total conditional requests with Connection: Keep-alive header.
Total Conditional Requests with Connection: Close header	Total conditional requests with Connection: Close header.
Total Conditional Requests with an HTTP Parser Error	Total conditional requests with an HTTP parser error.
Total Conditional Requests Cache Lookup Failure	Total conditional requests with a cache lookup failure.
Total Conditional Requests not Matching Etag/LM values in cache	Total conditional requests with nonmatching Etag or Last Modified values in the cache (such requests are not served from the cache).
Total Memory Allocation Errors in Conditional Request Process	Total memory allocation errors in conditional request processing.
Total Cache Pointer Errors in Conditional Request Process	Total cache pointer errors in conditional request processing.
Total 200/304 Cached Responses	Total 200/304 cached responses.
Total 200/304 Non-Cached due to Metadata Cache Thrashing Limit	Total 200/304 noncached responses due to metadata cache thrashing limit.

Table 3-74 Field Descriptions—show statistics accelerator http debug Command (continued)

Field	Description
Total 200/304 Non-Cached due to Vary Header	Total 200/304 noncached responses due to having a Vary header.
Total 200 Responses with no Etag/LM	Total 200 responses with no Etag or Last Modified header (such responses are not cached).
Total 200/304 Responses with max-age header	Total 200/304 responses with max-age header.
Total 200/304 Responses with s-maxage header	Total 200/304 responses with s-maxage header.
Total 200/304 Responses with Expires header	Total 200/304 responses with Expires header.
Total 200/304 Responses with Invalid Expires header	Total 200/304 responses with invalid Expires header.
Total 200/304 Responses with Etag header	Total 200/304 responses with Etag header.
Total 200/304 Responses with Too Long Etag value (> 64 chars)	Total 200/304 responses with Etag value that is longer than 64 characters.
Total 200/304 Responses with Last-Modified header	Total 200/304 responses with Last-Modified header.
Total 200/304 Responses with invalid Last-Modified header	Total 200/304 responses with invalid Last-Modified header.
Total 200/304 Responses with Content-Type header	Total 200/304 responses with Content-Type header.
Total 200/304 Responses with Server Header	Total 200/304 responses with Server header.
Total 200/304 Responses too long Server Header (>99 chars)	Total 200/304 responses with Server header that is longer than 99 characters.
Total 200/304 Responses with Content-Location Header	Total 200/304 responses with Content-Location header.
Total 200/304 Responses too long Content-Location (>99 chars)	Total 200/304 responses with Content-Location header that is longer than 99 characters.
Total 304 Response Not Cached Because of Filter-Extension	Total 304 responses not cached because of Filter-Extension.
Total 304 Responses with an HTTP Parser Error	Total 304 responses with an HTTP parser error.
Total 304 Memory Allocation Errors in 304 Response Process	Total 304 memory allocation errors in 304 response processing.
Total 304 Cache Pointer Errors in 304 Response Process	Total 304 cache pointer errors in 304 response processing.
Total 200 OK with object size less than 1 KB	Total 200 OK responses with object size less than 1 KB.
Total 200 OK with object size less than 5 KB	Total 200 OK responses with object size less than 5 KB.

Table 3-74 Field Descriptions—show statistics accelerator http debug Command (continued)

Field	Description
Total 200 OK with object size less than 8 KB	Total 200 OK responses with object size less than 8 KB.
Total 200 OK with object size more than 8 KB	Total 200 OK responses with object size more than 8 KB.
Total Connections Bypassed due to URL Based Bypass List	Total connections bypassed due to URL-based bypass list.
Total Connections Bypassed due to IP Based Bypass List	Total connections bypassed due to IP-based bypass list.
Total Connections Not Been Reused due to Unread WAN Data	Total connections not reused due to unread WAN data.
Total Connections with first message initiated from server	Total connections with first message initiated from server.

Table 3-75 describes the fields shown in the **show statistics accelerator http https** command display.

Table 3-75 Field Descriptions—show statistics accelerator http https Command

Field	Description
Total Optimized HTTPS Connections	HTTPS connections previously and currently optimized by the HTTP Accelerator.
Total Handled HTTPS Connections	HTTPS connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted. Never decremented. 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. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total Active HTTPS Connections	Number of HTTPS connections currently being handled and optimized by both SSL and HTTP optimization.
Total Proxy-Connect HTTPS Connections	Total number of HTTPS connection started as HTTP and upgraded to HTTPS. For such connections both SSL and HTTP optimizations are applied.
Total Proxy-Connect HTTPS Insert Failures	Number of HTTPS connections started as HTTP for which the SSL optimization upgrade failed.
RTT saved by HTTPS Content Refresh Check Metadata Cache (ms)	Round trip time saved by caching and locally serving conditional (304) responses, in milliseconds.
RTT saved by HTTPS Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving redirect (301) responses, in milliseconds.

Table 3-75 Field Descriptions—show statistics accelerator http https Command (continued)

Field	Description
RTT saved by HTTPS Authorization Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving authentication required (401) responses, in milliseconds.
Total Locally Served HTTPS Conditional Responses	Number of locally served conditional (304) responses.
Total Locally Served HTTPS Redirect Responses	Number of locally served redirect (301) responses.
Total Locally Served HTTPS Unauthorized Responses	Number of locally served authentication required (401) responses.
Total Remotely Served HTTPS Conditional Responses	Number of remotely served conditional (304) responses (cache misses).
Total Remotely Served HTTPS Redirect Responses	Number of remotely served redirect (301) responses (cache misses).
Total Remotely Served HTTPS Unauthorized Responses	Number of remotely served authentication required (401) responses (cache misses).
Total Hints Sent to DRE Layer to Skip Header Information - HTTPS	Number of DRE hints to skip header information.
Total Hints Sent to DRE Layer to Flush Data - HTTPS	Number of DRE hints to flush data.
Total Hints Sent to DRE Layer to Skip LZ - HTTPS	Number of DRE hints to skip LZ compression.
Total Server Compression Suppression - HTTPS	Number of times server compression was suppressed.
Total Time Saved from all HTTPS metadata cache hits	Total round-trip time saved by the three metadata caches (conditional response, redirect response, and unauthorized response) in milliseconds.
Total Time HTTPS Cache Miss (ms)	Total time for HTTPS metadata cache misses, in milleseconds.
Total HTTPS Requests Requiring Server Content-Revalidation	Number of requests that required content to be revalidated with the origin server, as specified by a Cache-Control header.
Total HTTPS Responses not to be Cached	Number of 200, 301, 304, and 401 responses not to be cached, as specified by a Cache-Control header.
Total HTTPS Connections Bypassed due to URL Based Bypass List	Number of connection flows that are bypassed due to a URL based bypass list.
Total HTTPS Connections Bypassed due to IP Based Bypass List	Number of connection flows that are bypassed due to a bypass list entry.
Total HTTPS sessions using SharePoint optimization	Number of HTTPS sessions using the SharePoint optimization feature to access objects from the SharePoint server.
Total HTTPS sessions using SharePoint prefetch optimization	Number of HTTPS sessions where the prefetch optimization for SharePoint objects (MS Office applications) is enabled.

Table 3-75 Field Descriptions—show statistics accelerator http https Command (continued)

Field	Description
Total HTTPS SharePoint objects prefetched	Number of SharePoint objects that have been prefetched due to client requests using HTTPS sessions.
Total HTTPS locally served SharePoint prefetch objects	Number of SharePoint objects that have been prefetched and have been displayed on the client using HTTPS sessions.
Total HTTPS RTT saved by SharePoint optimization (ms)	For HTTPS sessions, the total response time (in milliseconds) saved in accessing SharePoint objects by enabling the SharePoint optimization.
Total HTTPS RTT saved by SharePoint prefetch cache hit (ms)	For HTTPS sessions, the total response time (in milliseconds) saved in accessing SharePoint data that has already been prefetched and stored in the cache.
Total HTTPS remotely served SharePoint prefetch objects	For HTTPS sessions, the number of SharePoint objects that have been prefetched and displayed remotely.
Total HTTPS time for SharePoint cache miss (ms)	For HTTPS sessions, the total time (in milliseconds) lost in accessing SharePoint data that is not already stored in the cache.
Total HTTPS time for SharePoint prefetch cache miss (ms)	For HTTPS sessions, the total time (in milliseconds) lost in finding prefetched data that was not stored in the cache.

Table 3-76 describes the fields shown in the **show statistics accelerator ica detail** command display.

Table 3-76 Field Descriptions—show statistics accelerator ica detail Command

Field	Description
Global Statistics	
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 since the accelerator was started, from start to finish.
Total Connections Handed-off with Compression Policies Unchanged	Total number of connections received by the accelerator but to which only generic optimizations were done (no acceleration).
Total Dropped Connections	Total number of connections dropped for reasons other than client/server socket errors or close.
Current Active Connections	Total number of current active connections being handled by the ICA accelerator.
Current Pending Connections	Total number of connections pending to be accepted.
Maximum Active Connections	Maximum number of active connections handled by the accelerator.

Table 3-76 Field Descriptions—show statistics accelerator ica detail Command (continued)

Field	Description
Current Active SSL Connections	Total number of SSL connections currently being handled by the accelerator.
Current Active Non-SSL Connections	Total number of non-SSL connections currently being handled by the accelerator
Current Active CGP Connections	Total number of CGP (Common Gateway Protocol) connections currently being handled by the accelerator.
Current Active ICA Connections	Total number of ICA connections currently being handled by the accelerator.
Total SSL Connections	Total number of SSL connections.
Total non-SSL Connections	Total number of non-SSL connections.
Total CGP Connections	Total number of CGP connections.
Total ICA Connections	Total number of ICA connections being handled by the accelerator.
Total CGP Reconnections	Total number of CGP reconnections being handled by the accelerator.
Total Sessions Client Version 13.1	Total number of ICA sessions with client version (Citrix Receiver) 13.1.
Total Sessions Client Version 13.0	Total number of ICA sessions with client version (Citrix Receiver) 13.0.
Total Sessions Client Version 12.1	Total number of ICA sessions with client version (online plugin) 12.1.
Total Sessions Client Version 12.0	Total number of ICA sessions with client version (online plugin) 12.0.
Total Sessions Client Version 11.2	Total number of ICA sessions with client version (online plugin) 11.2.
Total Sessions Client Version 11.0	Total number of ICA sessions with client version (online plugin) 11.0.
Total Sessions Other Client Versions	Total number of ICA sessions with other client versions.
Total Sessions with No Encryption	Total number of ICA sessions with no encryption.
Total Sessions with Basic Encryption	Total number of ICA sessions with basic encryption.
Total Sessions with RC5_40 Encryption	Total number of ICA sessions with RC5 40-bit encryption.
Total Sessions with RC5_56 Encryption	Total number of ICA sessions with RC5 56-bit encryption.
Total Sessions with RC5_128 Encryption	Total number of ICA sessions with RC5 128-bit encryption.
Total Sessions with RC5_128 Logon-Only Encryption	Total number of ICA sessions with RC5 128-bit logon-only encryption.
Connections Handed Off Because of Unrecognized Protocol	Total number of ICA connections handed off because of unrecognized protocol.

Table 3-76 Field Descriptions—show statistics accelerator ica detail Command (continued)

Field	Description
Connections Handed Off Because of Unsupported Client Version	Total number of ICA connections handed off because of unsupported client version.
Connections Handed Off Because of Unknown CGP Session ID	Total number of ICA connections handed off because of unknown CGP session ID.
Connections Handed Off Because of Client on Denied List	Total number of ICA connections handed off because of client on Denied list.
Connections Handed Off Because of Resource Limit	Total number of ICA connections handed off because of resource limit.
Connections Handed Off Because of Other Reasons	Total number of ICA connections handed off because of other reasons.
Connections Disconnected Because of Unsupported Client Version	Total number of ICA connections disconnected because of unsupported client version.
Connections Disconnected Because of I/O Error	Total number of ICA connections disconnected because of I/O error.
Connections Disconnected Because of Parsing Error	Total number of ICA connections disconnected because of parsing error.
Connections Disconnected Because of Resource Limit	Total number of ICA connections disconnected because of resource limit.
Connections Disconnected Because of Session in Use	Total number of ICA connections disconnected because of session in use.
Connections Disconnected Because of Other Reasons	Total number of ICA connections disconnected because of other reasons.
Active MSI Very High Connections	Number of active MSI very high priority connections.
Active MSI High Connections	Number of active MSI high priority connections.
Active MSI Medium Connections	Number of active MSI medium priority connections.
Active MSI Low Connections	Number of active MSI low priority connections.
Active non-MSI Connections	Number of active non-MSI connections.
Total MSI Very High Connections	Total number of MSI very high priority connections.
Total MSI High Connections	Total number of MSI high priority connections.
Total MSI Medium Connections	Total number of MSI medium priority connections.
Total MSI Low Connections	Total number of MSI low priority connections.
Total non-MSI Connections	Total number of non-MSI connections.
LAN bandwidth (kb/s)	LAN bandwidth speed, in kilobtyes per second.

Table 3-77 describes the fields shown in the **show statistics accelerator mapi detail** command display.

Table 3-77 Field Descriptions—show statistics accelerator mapi detail Command

Field	Description
Global Statistics	
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.
Total Secured Connections	Number of connections to Outlook clients that use encryption. Such connections are not accelerated by the MAPI accelerator but are passed through.
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.

Table 3-77 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
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.
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.
Number of Write Stream Requests	Number of write stream requests.
Minimum Async Write Stream Buffer Size (bytes)	Minimum size of the asynchronous request stub sent on the WAN, calculated from the minimum stub size across all sessions.
Maximum Async Write Stream Buffer Size (bytes)	Maximum size of the asynchronous request stub sent on the WAN, calculated from the maximum stub size across all sessions.
Average Async Write Stream Buffer Size (bytes)	Average size of the asynchronous request stub sent on the WAN, calculated by taking the average of the stub size across all sessions.
Current 2000 Accelerated Sessions	Number of accelerated sessions to Outlook 2000 clients. Sessions (users), not TCP connections.
Current 2003 Accelerated Sessions	Number of accelerated sessions to Outlook 2003 clients. Sessions (users), not TCP connections.
Current 2007 Accelerated Sessions	Number of accelerated sessions to Outlook 2007 clients. Sessions (users), not TCP connections.
Current 2010 Accelerated Sessions	Number of accelerated sessions to Outlook 2010 clients. Sessions (users), not TCP connections.
Current 2013 Accelerated Sessions	Number of accelerated sessions to Outlook 2013 clients. Sessions (users), not TCP connections.
Current 2016 Accelerated Sessions	Number of accelerated sessions to Outlook 2016 clients. Sessions (users), not TCP connections.
Current Exchange to Exchange Accelerated Sessions	Number of accelerated sessions between the exchange servers.
Current 2003 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2003 clients.
Current 2007 Accelerated Secured Sessions	Number of accelerated secured sessions to Outlook 2007 clients.
Current 2010 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2010 clients.
Current 2013 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2013 clients.

Table 3-77 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Current 2016 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2016 clients.
Lower than 2000 Sessions	Number of sessions to clients using a version of Outlook lower than Outlook 2000. Such connections are not accelerated by the MAPI accelerator but are passed through.
Unsupported Higher Client Version Sessions	Number of sessions to clients using a version of Outlook higher than that supported. Such connections are not accelerated by the MAPI accelerator but are passed through.
Async Write Optimization Statistics	
Current Number Of Async Write Stubs On WAN	Current number of asynchronous requests on the WAN.
Current Number Of Requests Queued Due To Flow Control	Current number of client session flows that were blocked due to threshold limit.
Current Number Of Requests Queued Due To RopBackOff	Current number of client session flows that were blocked due to ropbackoff response.
Total Number Of RopBackOff Response Received	Total number of ropbackoff responses received across all connections.
Total RopBackOff Duration (msec)	Cumulative time of ropbackoff durations across all connections, in milliseconds.
Total Wait Time Of Requests Queued Due To FlowControl (msec)	Cumulative wait time of requests queued due to flow control across all connections, in milliseconds.
Total Wait Time Of Requests Queued Due To RopBackOff (msec)	Cumulative wait time of requests queued due to ropbackoff across all connections, in milliseconds.
Connection Hand-Off Reasons	Number of connections handed off from the MAPI accelerator to the generic accelerator for various reasons.
Total Handled RPC TCP Connections	The total handled RPC TCP connections handled during this session.
Total Handled RPCH HTTP Connections	The total handled RPCH HTTP connections handled since the accelerator was started or its statistics last reset.
Total Handled RPCH HTTPS Connections	The total handled RPCH HTTPS connections handled since the accelerator was started or its statistics last reset.
Total Optimized RPC TCP Connections	The total optimized RPC TCP connections.
Total Optimized RPCH HTTP Connections	The total optimized RPCH HTTP connections.
Total Optimized RPCH HTTPS Connections	The total optimized RPCH HTTPS connections.
Total Handled RPCH Virtual Sessions	The total handled RPCH virtual sessions.
Total Optimized RPCH Virtual Sessions	The total optimized RPCH virtual sessions,
Total Pipe-Through Virtual Sessions	The total pipe-through virtual sessions.
Association Group (AG) Statistics	

Table 3-77 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Average Active AGs In The Last Hour	Average number of active AGs in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average Active Connections Used By AGs In The Last Hour	Average number of active connections used by AGs in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average Active AGs In The Last 5min	Average number of active AGs in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Average Active Connections Used By AGs In The Last 5min	Average number of active connections used by AGs in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Current Active AGs	Number of current active AGs.
Current Active Connections Used By AGs	Number of current active connections used by AGs.
Max Active AGs Since Last Reset/Cleared	Number of max active AGs since last reset/cleared.
Active Connections When Max Active AGs Since Last Reset/Cleared	Number of active connections when max active AGs since last reset/cleared.
Max Active Connections Within an AG Since Last Reset/Cleared	Number of max active connections within an AG since last reset/cleared.
Max Total Active Connections Since Last Reset/Cleared	Number of max total active connections since last reset/cleared.
AGs When Max Total Active Connections Since Last Reset/Cleared	Number of AGs when max total active connections since last reset/cleared.
Total AGs	Number of total AGs.
Total Handed Off AGs due to Reservation Failure	Number of total handed off AGs due to reservation failure.
Total Handed Off AGs Tracked by MAPI AO	Number of total handed off AGs tracked by MAPI AO.
Current Handed Off AGs Tracked by MAPI AO	Number of current handed off AGs tracked by MAPI AO.
Reserved Connections Pool Statistics	
Current In-Use Connections	Number of current in-use connections.
Current Reserved (Unused) Connections	Number of current reserved but still not used connections.
Average In-Use Connections in Last One Hour	Average number of average in-use connections in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average Reserved (Unused) Connections in Last One Hour	Average number of average reserved but unused connections in the last hour. This number is zero if statistics were reset/cleared within one hour.

Table 3-77 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Average In-Use Connections in Last 5min	Average number of average in-use connections in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Average Reserved (Unused) Connections in Last 5min	Average number of reserved (unused) connections in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Configured Maximum Reserved (Unused) Connections	Maximum reserved connections configured but not used.
ReadAhead (RAH) Optimization Statistics	Several statistics for read ahead optimization, including the number of active read aheads and bytes read by the read ahead optimizer.
Exchange Server Error Statistics	Number of errors of various types that were returned by the Exchange server.
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).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
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 3-77 Field Descriptions—show statistics accelerator mapi detail 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: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Rejected Connections Of Interest Due To Unavailable Resources	Number of connections rejected due to unavailable resources. Incremented when a new MAPI connection arrives that matches an existing MAPI specific dynamic policy but there are no resources available in the reserved pool to accept it; the connection is passed through.
Rejected Connections Of Interest Due To Unavailable Peer	Number of connections rejected due to unavailable peer. Incremented when a new MAPI connection arrives that matches an existing MAPI specific dynamic policy but there is no remote MAPI peer or the remote peer is unable to accept it; the connection is passed through.
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.

Table 3-77 Field Descriptions—show statistics accelerator mapi detail 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 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	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 3-78 describes the fields shown in the s***how statistics accelerator mapi detail rpchttp*** command display.

Table 3-78 Field Descriptions for the show statistics accelerator mapi detail rpchttp Command

Field	Description
Number of active IN channels	Count of current active IN channel RPCHTTP(S) connections.
Number of active OUT channels	Count of current active OUT channel RPCHTTP(S) connections.
Number of active optimized sessions	Count of current active RPCHTTP(S) Virtual sessions. This count is equal to the current active IN/OUT channel count.
Number of active RPC HTTP(S) clients	Number of outlook clients currently optimized for RPCHTTP(S).
Number of RPC HTTP connections optimized since uptime	Total count of the RPCHTTP(S) connections optimized. This count is the total of the IN and OUT channels optimized. This count is equal to 2 times the 'Number of Optimized RPCH Virtual Sessions' counter.
Number of Handled RPCH Virtual Sessions	Total count of the RPCHTTP(S) virtual session handled by MAPI AO.
Number of Optimized RPCH Virtual Sessions	Total count of the RPCHTTP(S) virtual sessions optimized. This counter is half of the 'Number of RPC HTTP connections optimized since uptime' counter.
Number of Pipe-through Virtual Sessions	Total number of RPCHTTP(S) sessions handed over without optimization. This counter is equal to 'Number of Handled RPCH Virtual Sessions' - 'Number of Optimized RPCH Virtual Sessions'

Table 3-79 describes the fields shown in the **show statistics accelerator smb detail** command display.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total Handled Connections	Number of connections handled since the accelerator was started or its statistics last reset.
Total Optimized Connections	Number of connections previously and currently optimized by the accelerator.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections initially accepted by the SMB accelerator, but later handed off to generic optimization without poliby changes so the current negotiated policies for compression (DRE/LZ) will be used.
Total Dropped Connections	Number of connections dropped.
Total Active Connections	Number of connections currently being optimized by the SMB accelerator.
Current Pending Connections	Number of connections that have been determined to be accelerated by the SMB accelerator, and have been queued to be picked up by the accelerator.
Maximum Active Connections	Maximum value reached by the Current Active Connections counter. This counter will be reset if the accelerator is restarted or statistics are cleared.
Total Number of SMB1 Sessions Optimized	Total number of SMB1 sessions optimized by the accelerator.
Total Number of SMB1 Signed Sessions (L4 Opt)	Total number of SMB1 signed sessions (Layer 4 optimization).
Total Number of SMB1 Sessions Not Optimized	Total number of SMB1 sessions not optimized by the accelerator.
Total Number of SMB2 Sessions Not Optimized (handoff on request)	Total number of SMB2 sessions not optimized by the accelerator.
Total Number of SMB2 Sessions (L4 optimization, handoff on request)	Total number of SMB2 sessions optimized (Layer 4 optimization)
Total Number of SMB2_0 Sessions Optimized	Total number of SMB2 sessions optimized.
Total Number of SMB2 _0 Signed Sessions (L4 Opt)	Number of SMB2_0 signed sessions (Layer 4 optimization)
Total Number of SMB2 _0 Signed Sessions (L7Opt)	Number of SMB2_0 signed sessions (Layer 7 optimization)
Total Number of SMB2_0 Sessions Not Optimized	Number of SMB2_1 session optimized.
Total Number of SMB2_1 Sessions Optimized	Number of SMB2_1 sessions optimized.
Total Number of SMB2_1 Signed Sessions (L4 Opt)	Number of SMB2_1 signed sessions (Layer 4 optimization)

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total Number of SMB2_1 Signed Sessions (L7 Opt)	Number of SMB2_1 signed sessions (Layer 7 optimization)
Total Number of SMB2_1 Sessions Not Optimized	Number of SMB2_1 sessions not optimized.
Total Number of SMB3_0 Sessions Optimized:	Total number of SMB3 sessions optimized.
Total Number of SMB3_0 Sessions Not Optimized:	Total number of SMB3 sessions not optimized by the accelerator.
Total Number of SMB3_0 Sessions Optimized (L4 Opt)	Number of SMB3_0 sessions (Layer 4 optimization).
Total Number of SMB3_0 Sessions Not Optimized	Total number of SMB3 sessions not optimized by the accelerator.
Total Number of Signed SMB3_0 Signed Sessions Optimized	Number of optimized signed SMB3_0 sessions.
Total Number of Signed SMB3_0 Signed Sessions (L4/Not Optimized)	Number of signed SMB3_0 sessions not optimized. (Layer 4)
Total Number of Signed SMB3_02 Signed Sessions Optimized	Number of optimized signed SMB3_02 sessions.
Total Number of Signed SMB3_02 Signed Sessions (L4/Not Optimized)	Number of signed SMB3_02 sessions not optimized. (Layer 4)
Total Number of SMB3_02 Signed Sessions (L7 opt)	Number of signed SMB3_02 signed sessions optimized. (Layer 7)
Total Number of SMB3_02 Encrypted Sessions not optimized	Number of encrypted SMB3_02 sessions not optimized.
Total Number of SMB3_0 Encrypted Sessions (L4 opt)	Total number of SMB 3_0 encrypted sessions using Layer 4 optimization.
Total Number of SMB3_0 Encrypted Sessions (L7 opt)	Total number of SMB 3_0 encrypted sessions using Layer 7 optimization.
Total Number of SMB3_02 Encrypted Sessions (L4 opt)	Total number of SMB 3_02 encrypted sessions using Layer 4 optimization.
Total Number of SMB3_02 Encrypted Sessions (L7 opt)	Total number of SMB 3_02 encrypted sessions using Layer 7 optimization.
Total Number of Requests Processed	Number of requests processed (including successful and unsuccessful responses).
Total Number of Signed Requests Processed	Number of signed requests processed (including successful and unsuccessful responses).
Total Number of Encrypted Requests Processed	Number of encrypted requests processed (including successful and unsuccessful responses)
Total Number of Requests Served Locally	Number of requests served locally by the WAAS device.
Total Number of Signed Requests Served Locally	Number of signed requests served locally by the WAAS device.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total Number of Encrypted Requests Served Locally	Number of encrypted requests served locally by the WAAS device.
Total Number of Requests Sent to File Servers	Number of requests sent to file servers.
Total Number of Signed Requests Sent to File Servers	Number of signed requests sent to file servers.
Total Number of Encrypted Requests Sent to File Servers	Number of encrypted requests sent to file servers.
Total Number of SMB1 Requests Processed	Number of SMB1 requests processed (including successful and unsuccessful responses).
Total Number of SMB2 Requests Processed	Number of SMB2 requests processed (including successful and unsuccessful responses).
Total Number of SMB2 Signed Requests Processed	Number of signed SMB2 requests processed (including successful and unsuccessful responses).
Total Number of VFN Requests Processed	Number of VFN requests processed (including successful and unsuccessful responses).
Total Number of Active Requests	Number of active SMB requests.
Total Number of Open Files	Number of open files on the WAE. The SMB accelerator performs below the optimum level if there are too many open files. The maximum value of the open-file count is platform-dependent. Use **(config) threshold-monitor** to configure monitoring thresholds.
Total Number of Bytes Read from Cache	Number of bytes read from cache.
Total Number of Bytes Written to Cache	Number of bytes written to the cache.
Total SMB Object Cache Read bytes	Number of SMB Object Cache read bytes.
Total SMB Object Cache Write bytes	Number of SMB Object Cache write bytes.
Object cache load bypass read	Total number of read request that were sent to server because of object cache load.
Object cache load bypass write	Total number of write requests which are not cached in object cache because of load
Object cache load bypass read bytes	Total number of read bytes that went to the server because of object cache load
Object cache load bypass write byte	Total number of write bytes which are not written to object cache because of object cache load.
Total Number of Bytes Written to LAN (Original)	Number of unoptimized bytes written to the LAN.
Total Number of Bytes Read from LAN (Original)	Number of unoptimized bytes read from the LAN.
Total Number of Bytes Read from WAN (Optimized)	Number of optimized bytes read from the WAN.
Total Number of Bytes Written to WAN (Optimized)	Number of optimized bytes written to the WAN.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
SMB preposition gain %	Gain percent when a file is served locally from cache because it was previously cached using preposition.
Total Number of Signed SMB Bytes Read from LAN (Original)	Number of unoptimized signed SMB bytes read from the LAN.
Total Number of Signed SMB Bytes Written to LAN (Original)	Number of unoptimized signed SMB bytes writte to the LAN.
Total Number of Signed SMB Bytes Read from WAN (L4 Optimized)	Number of Layer 4 optimized signed SMB bytes read from the WAN.
Total Number of Signed SMB Bytes Written to WAN (L4 Optimized)	Number of Layer 4 optimized signed SMB bytes written to the WAN.
Total Number of Encrypted SMB Bytes read from LAN (Original):	Number of unoptimized encrypted bytes read from the LAN.
Total Number of Encrypted SMB Bytes written to LAN (Original)	Number of unoptimized encrypted bytes written to the LAN.
Total Number of Encrypted SMB Bytes read from WAN (L4 Optimized)	Number of encrypted optimized bytes read from the WAN.
Total Number of Encrypted SMB Bytes Written to WAN(L4 Optimized)	Number of encrypted optimized bytes written to the WAN.
Average Response Time (ms) for Requests Served Locally	Average response time for requests served locally, in milliseconds.
Average Signed Response Time (ms) for Requests Served Locally	Average response time for signed requests served locally, in milliseconds
Average Response Time (ms) for Requests Sent to File Servers	Average response time for requests sent to file servers, in milliseconds.
Average Signed Response Time (ms) for Requests Sent to File Servers	Average response time for signed requests sent to file servers, in milliseconds.
Total Round Trip Time (ms) for All Requests	Total round trip time for all requests, in milliseconds.
Total Amount of Time Saved (ms) Due to Optimization	Total time saved due to optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Read-ahead	Total time saved due to read-ahead, in milliseconds.
Total Amount of Time Saved (ms) Due to Metadata Optimization	Total time saved due to metadata optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Microsoft Optimization	Total time saved due to Microsoft optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Not-found-metadata Cache	Total time saved due to not-found metadata cache, in milliseconds.
Total Amount of Time Saved (ms) Due to Async Request Handling	Total time saved due to asynchronous request handling, in milliseconds.
Total Amount of Time Saved (ms) Due to DCE-RPC Optimization	Total time saved due to DCE-RPC optimization, in milliseconds.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total Amount of Time Saved (ms) Due to Print Optimization	Total time saved due to print optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Other Optimization	Total time saved due to other, non-print optimization, in milliseconds.
Current Allocated Memory Usage of Not-found Metadata Cache	Currentallocated memory usage of not-found metadata cache.
Number of Entries in Not-found Metadata Cache	Number of entries in not-found metadata cache.
Not-found Metadata Cache Hit Count	Number of not-found metadata cache hits.
Not-found Metadata Cache Access Attempts Count	Number of not-found metadata cache access attempts.
Not-found Metadata Cache Allowed Access Count	Number of not-found metadata cache allowed accesses.
Not-found Metadata Cache Update Attempts Count	Number of not-found metadata cache update attempts.
Not-found Metadata Cache Allowed Updates Count	Number of not-found metadata cache allowed updates.
Not-found Metadata Cache Hash Bucket Count	Number of not-found metadata cache hash buckets. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster.
Read-ahead Buffer Hit Rate (%)	The hit rate of the read-buffer, as a percent.
Read-ahead Buffer Hit Count	Number of read-ahead buffer hits.
Read-ahead Buffer Hit Bytes	Number of read-ahead buffer hits, in bytes.
Read-ahead Buffer Miss Bytes	Number of read-ahead buffer misses, in bytes.
Read-ahead Buffer Total Bytes Read from Files Servers	Number of read-ahead buffer bytes read from file servers.
Read-ahead Buffer Pass-through Bytes	Number of read-ahead buffer pass-through bytes.
Read-ahead Buffer Wait Blocks	Number of read-ahead buffer wait blocks.
Read-ahead Buffer Active IO Blocks	Number of read-ahead buffer active IO blocks.
Read-ahead Buffer Block Size in Bytes	The read-ahead buffer block size, in bytes.
Read-ahead Buffer Usage (in Blocks)	The read-ahead buffer usage, in blocks.
Read-ahead Buffer Total Size (in Blocks)	Total size of the read-ahead buffer, in blocks.
Read-ahead Buffer Blocks Evicted	Number of read-ahead buffer blocks evicted.
Read-ahead Buffer Blocks Evicted Before Use	Number of read-ahead buffer blocks evicted before use.
Read-ahead Buffer Blocks Invalidated	Number of read-ahead buffer blocks invalidated.
Total Number of Files in Read-ahead Buffer	Number of files in the read-ahead buffer.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Read-ahead Buffer Last Evicted Item Age (Seconds)	The age of the last evicted item in the read-ahead buffer, in seconds.
Read-ahead Buffer Min Eviction Age (Seconds)	The minimum amount of time, in seconds, before an item is evicted from the read-ahead buffer.
Metadata Cache Total Size (Bytes)	The size of the metadata cache, in bytes.
Metadata Cache Hit Rate (%)	The hit rate of the metdata cache, as a percent.
Metadata Cache Hit Count	Number of metadata cache hits.
Total Number of File Oplocks Acquired on Behalf of the Client	Number of opportunistic locks acquired on behalf of the client.
Total Number of Write-opt Requests Served Locally	Number of write-optimization requests served locallyu.
Total Number of Other Requests Served Locally	Number of other requests served locally.
Total Number of Metadata Cached Resources	Number of metadata cached references.
Total SMB1 Named Pipe Open Requests Processed	Number of SMB1 NT_Create_AndX requests for non \spoolss pipe seen by the edge WAE.
Total SMB1 Named Pipe Open Requests Served Locally	Number of SMB1 NT_Create_AndX requests for non \spoolss pipe served locally by the edge WAE, due to cached-open and delayed-close optimization.
Total SMB1 Named Pipe Open Requests Forward to Server	Number of SMB1NT_Create_AndX requests for non \spoolss pipe that were forwarded to the server by the edge WAE (requests that could not be served locally).
Total SMB1 Named Pipe Close requests processed	Number of SMB1 Close requests for non \spoolss pipe see by the edge WAE.
Total SMB1 Named Pipe Close requests served locally	Number of SMB1 Close requests for non \spoolss pipe served locally by the edge WAE as part of delayed-close optimization.
Total SMB1 Named Pipe Close requests forwarded to server	Number of SMB1 Close requests for non \spoolss pipe that were forwarded to the server by the dge WAE (requests that could not be served locally). This total includes only the Close requests that are sent synchronously to the server (when the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests that are first served locally and then sent to the server at a later point in time).
Named Pipe Cache Access Attempts Count	Number of named pipe cache access attempts.
Named Pipe Cache Hit Count	Number of named pipe cache hits.
Named Pipe Entry Count	Number of named pipe entries.
Named Pipe Cache Size	The size of the named pipe cache.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total Amount of Time Saved (ms) Due to Print Optimization	Total time saved (since the last counters were cleared) due to all print optimizations being performed, in milliseconds.
Total SMB1 Print Open requests	Number of SMB1 NT_Create_AndX requests for \spoolss pipe seen by the edge WAE.
Total SMB1 Print Open requests served locally	Number of SMB1 NT_Create_AndX requests for \spoolss pipe served locally by the edge WAE due to cached open and delayed close optimization.
Total SMB1 Print Open requests forwarded to server	Number of SMB1 NT_Create_AndX requests for \spoolss pipe forwarded to the server by the edge WAE (could not be served locally).
Total SMB1 Print Close requests processed	Number of SMB1 Close requests for \spoolss pipe seen by the edge WAE.
Total SMB1 Print Close requests served locally	Number of SMB1 Close requests served locally by the edge WAE as part of delayed close optimization.
Total SMB1 Print Close requests forwarded to the server	Number of SMB1 Close requests forwarded to the server by the edge WAE (could not be served locally). This total includes only the Close requests that are sent *synchronously* to the server (the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests first served locally and then sent to the server at a later point in time).
Print SMB1 Documents Spooled count	Number of SMB1 Transact EndDocPrinter messages (DCE-RPC opnum 23) for the \spoolss pipe seen by the edge WAE.
Print SMB1 Pages Spooled count	Number of SMB1 Transact EndDocPrinter messages (DCE-RPC opnum 20) for the \spoolss pipe seen by the edge WAE. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async Write count	Number of SMB1 Write_AndXmessages for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization.
Print SMB1 Async StartPagePrinter count	Number of SMB1 Transact StartPagePrinter messages (DCE-RPC opnum 18) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Print SMB1 Async EndPagePrinter count	Number of SMB1 Transact EndPagePrinter messages (DCE-RPC opnum 20) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async WritePrinter count	Number of SMB1 Transact WritePagePrinter messages (DCE-RPC opnum 19) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Remote Command Count	The number of SMB1 Transact commands for the \spoolss pipe seen by the edge WAE that are not parsed and are sent to the core.
Total Number of Read Requests with Office Optimization	Number of read requests with Microsoft Office optimization.
Total Number of Write Requests with Office Optmization	Number of write requests with Microsoft Office Optimization.
Total SMB1_Create_AndX requests processed	Number of SMB1 Create_AndX requests processed.
Total SMB1_Write_AndX requests processed	Number of SMB1 Write_AndX requests processed.
Total SMB1_Write_AndX requests served locally	Number of SMB1 Write_AndX requests served locally.
Total SMB1_Write_AndX requests forwarded to file server	Number of SMB1 Write_AndX requests forwarded to the file server.
Total SMB1_Read_AndX requests processed	Number of SMB1 Read_AndX requests processed.
Total SMB1_Read_AndX requests served locally	Number of SMB1 Read_AndX requests served locally.
Total SMB1_Read_AndX requests forwarded to file server	Number of SMB1 Read_AndX requests forwarded to the file server.
Total SMB1_Cancel requests processed	Number of SMB1 cancel requests processed.
Total SMB1_Delete Requests Processed	Number of SMB1 delete requests processed.
Total SMB1_Delete Requests Served Locally	Number of SMB1 delete requests served locally.
Total SMB1_Delete Requests Forwarded to File Server	Number of SMB1 delete requests forwarded to the file server.
Total SMB1_Delete_Dir Requests Processed	Number of SMB1 delete directory requests processed.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total SMB1_Delete_Dir Requests Served Locally	Number of SMB1 delete directory requests served locally.
Total SMB1_Delete_Dir Requests Forwarded to File Server	Number of SMB1 delete directory requests forwarded to the file server.
Total SMB1_Create_Temp Requests Processed	Number of SMB1 create temporary directory requests processed.
Total SMB1_Check_Dir Requests Processed	Number of SMB1 check directory requests processed.
Total SMB1_Check_Dir Requests Served Locally	Number of SMB1 check directory requests served locally.
Total SMB1_Check_Dir Requests Forwarded to File Server	Number of SMB1 check directory requests forwarded to the file server.
Total SMB1_Close Requests Processed	Number of SMB1 close requests processed.
Total SMB1_Close Requests Served Locally	Number of SMB1 close requests served locally.
Total SMB1_Close Requests Forwarded to File Server	Number of SMB1 close requests forwarded to the file server.
Total SMB1_Rename Requests Processed	Num ber of SMB1 rename requests processed.
Total SMB1_Rename Requests Served Locally	Number of SMB1 rename requests served locally.
Total SMB1_Rename Requests Forwarded to Server	Number of SMB1 rename requests forwarded to the file server.
Total SMB1_Session_Setup Requests Processed	Number of SMB1 session setup requests processed.
Total SMB1_Tree_Connect_AndX Requests Processed	Number of SMB1 Tree_Connect_AndX requests processed.
Total SMB1_Tree_Disconnect Requests Processed	Number of SMB1 Tree_Disconnect requests processed.
Total SMB1_Logoff Requests Processed	Number of SMB1 logoff requests processed.
Total SMB1_Negotiate Requests Processed	Number of SMB1 negotiate requests processed.
Total SMB1_Query_Path_Info Requests Processed	Number of SMB1 query path information requests processed.
Total SMB1_Query_Path_Info Requests Served Locally	Number of SMB1 query path information requests served locally.
Total SMB1_Query_Path_Info Requests Forwarded to File Server	Number of SMB1 query path information requests forwarded to the file server.
Total SMB1_Query_File_Info Requests Processed	Number of SMB1 query file information requests processed.
Total SMB1_Query_File_Info Requests Served Locally	Number of SMB1 query file information requests served locally.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total SMB1_Query_File_Info Requests Forwarded to File Server	Number of SMB1 query file information requests forwarded to the file server.
Total SMB1_Set_Path_Info Requests Processed	Number of SMB1 set path information requests processed.
Total SMB1_Set_Path_Info Requests Served Locally	Number of SMB1 set path information requests served locally.
Total SMB1_Set_Path_Info Requests Forwarded to File Server	Number of SMB1 set path information requests forwarded to the file server.
Total SMB1_Set_File_Info Requests Processed	Number of SMB1 set file information requests processed.
Total SMB1_Set_File_Info Requests Served Locally	Number of SMB1 set file information requests served locally.
Total SMB1_Set_File_Info Requests Forwarded to File Server	Number of SMB1 set file information requests forwarded to the file server.
Total SMB1_Find_First Requests Processed	Number of SMB1 find first requests processed.
Total SMB1_Find_First Requests Served Locally	Number of SMB1 find first requests served locally.
Total SMB1_Find_First Requests Forwarded to File Server	Number of SMB1 find first requests forwarded to the file server.
Total SMB1_Find_Next Requests Processed	Number of SMB1 find next requests processed.
Total SMB1_Find_Next Requests Served Locally	Number of SMB1 find next requests served locally.
Total SMB1_Find_Next Requests Forwarded to File Server	Number of SMB1 find next requests forwarded to the file server.
Total SMB1_Create_Dir Requests Processed	Number of SMB1 create directory requests processed.
Total SMB1_Trans2_Create_Dir Requests Processed	Number of SMB1 Transaction2 create directory requests processed.
Total SMB1_Query_FS_Info Requests Processed	Number of SMB1 query file share information requests processed.
Total SMB1_Query_FS_Info Requests Served Locally	Number of SMB1 query file share information requests served locally.
Total SMB1_Query_FS_Info Requests Forward to File Server	Number of SMB1 query file share information requests forwarded to the file server.
Total SMB1_Set_Security_Desc Requests Processed	Number of SMB1 set security descriptor requests processed.
Total SMB1_IOCTL Requests Processed	Number of SMB1 input/output control requests processed.
Total SMB1_OPEN_ANDX Requests Processed	Number of SMB1 Open_AndX requests processed.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total SMB1_OPEN_ANDX Requests Served Locally	Number of SMB1 Open_AndX requests served locally.
Total SMB1_OPEN_ANDX Requests Forwarded to File Server	Number of SMB1 Open_AndX requests forwarded to the file server.
Total SMB1 Transact Notify Requests Processed	Number of SMB1 transact notify requests processed.
Total SMB1 Transact Notify Requests Served Locally	Number of SMB1 transact notify requests served locally.
Total SMB1 Transact Notify Requests Forwarded to File Server	Number of SMB1 transact notify requests forwarded to the file server.
Total SMB1 Transact Create Requests Processed	Number of SMB1 transact create requests processed.
Total SMB1 Transact Create Requests Served Locally	Number of SMB1 transact create requests served locally.
Total SMB1 Transact Create Requests Forwarded to File Server	Number of SMB1 transact create requests forwarded to the file server.
Total SMB1_Locking_AndX Requests Processed	Number of SMB1 Locking_AndX requests processed.
Total SMB1_Locking_AndX Requests Served Locally	Number of SMB1 Locking_AndX requests served locally.
Total SMB1_Locking_AndX Requests Forwarded to File Server	Number of SMB1 Locking_AndX requests served locally.
Total SMB1 Transaction Requests Processed	Number of SMB1 transaction requests processed.
Total SMB1 Transaction Requests Served Locally	Number of SMB1 transacation requests served locally.
Total SMB1 Transaction Requests Forwarded to File Server	Number of SMB1 transaction requests forwarded to the file server.
Total SMB1_Set_Information Requests Processed	Number of SMB1 set information requests processed.
Total SMB1_Set_Information Requests Served Locally	Number of SMB1 set information requests served locally.
Total SMB1_Set_Information Requests Forwarded to File Server	Number of SMB1 set information requests forwarded to the file server.
Total SMB1_Set_Information2 Requests Processed	Number of SMB1 set information2 requests processed.
Total SMB1_Set_Information2 Requests Served Locally	Number of SMB1 set information2 requests served locally.

Table 3-79 Field Descriptions for the show statistics accelerator smb detail Command (continued)

Field	Description
Total SMB1_Set_Information2 Requests Forwarded to File Server	Number of SMB1 set information2 requests forwarded to the file server.
Total SMB1_Query_Information Requests Processed	Number of SMB1 query information requests processed.
Total SMB1_Query_Information Requests Served Locally	Number of SMB1 query information requests served locally.
Total SMB1_Query_Information Requests Forwarded to File Server	Number of SMB1 query information requests forwarded to the file server.
Total SMB1_Query_Information2 Requests Processed	Number of SMB1 query information2 requests processed.
Total SMB1_Query_Information2 Requests Served Locally	Number of SMB1 query information2 requests served locally.
Total SMB1_Query_Information2 Requests Forwarded to File Server	Number of SMB1 query information2 requests forwarded to the file server.
Total SMB1_NTRename Requests Processed	Number of SMB1 NT rename requests processed.
Total SMB1_FindClose2 Requests Processed	Number of SMB1 find close2 requests processed.
Total SMB1_Write Requests Processed	Number of SMB1 write requests processed.
Total SMB2_Read requests Processed	Number of SMB2 read requests processed.
Total SMB2_Write requests Processed	Number of SMB2 write requests processed.
Directory-Browsing Active nodes	Number of active directory browsing created directory browsing active files being served from the WAAS device's RAM.
Directory-Browsing Total nodes	Total number of directory browsing files that can be created in the WAAS device's RAM.
Directory-Browsing Total Size used in Bytes	Total RAM memory (in bytes) used by directory browsing requests.
Directory-Browsing Nodes Evicted	Total number of directories/files removed because they were not being used to free up limited memory space.
Total SMB2_Query_Directory requests processed	Number of SMB2 query directory requests processed
Total SMB2_Query_Directory requests served locally	Number of SMB2 query directory requests served locally from the WAAS device RAM infrastructure.
Total SMB2_Query_Directory forwarded to file server	Number of SMB2 query directory requests that could not be served locally from the WAAS device and were forwarded to the file server.
Total SMB2_Compound requests served locally	Number of SMB2 compound query requests (2) served locally from the WAAS device RAM infrastructure.

Table 3-80 describes the fields shown in the **show statistics accelerator smb debug** command display.

Table 3-80 Field Descriptions for the show statistics accelerator smb d ebug Command (continued)

Field	Description
Total SMB Object Cache Open calls	Total number of SMB Object open calls made by the SMB Acceleration Accelerator to the Object Cache (OC) API.
Total SMB Object Cache Open success	Total number of SMB Object Cache calls that were successfully answered by the object cache API.
Total SMB Object Cache Open failure	Total number of SMB Object Cache calls that failed to be answered by the object cache API
Total SMB Object Cache Open failure due to load bypass	Total number of SMB Object Cache calls that failed to be answered by the object cache API due to network latency.
Total SMB Object Cache Read success	The total number of successful read requests sent to the OC.
Total SMB Object Cache Read calls	The total number of read requests sent to the OC.
Total SMB Object Cache Read failure	The total number of failed read requests.
Total SMB Object Cache Read failure due to load bypass	The total number of failed read requests due to network latency.
Total SMB Object Cache Read failure due to version check	The total number of failed read requests due to version mismatch.
Total SMB Object Cache Write success	Total number of SMB data that has been successfully written to object cache
Total SMB Object Cache Write calls	Total number of write requests sent to OC.
Total SMB Object Cache Write failure	Total number of write requests that could not be written to OC.
Total SMB Object Cache Write failure due to load bypass	Total number of write requests that failed due to network latency.
Total SMB Object Cache Write issued with overwrite flag set	Total number of calls to object cache write with differentiator as the overwriteflag, so that it overwrites existing data or writes to offset.
Total SMB Object Cache Write issued when load bypass was set	Total number of object cache writes issued with load bypass flag.
Total SMB Object Cache Duplicate calls	Total number of duplicate calls to open object in object cache.
Total SMB Object Cache Duplicate success	Total number of successful duplicate calls to open object in object cache.
Total SMB Object Cache Duplicate failure	Total number of unsuccessful duplicate calls to open object in object cache.
Total SMB Object Cache Close calls	Total number of close file requests sent to OC.
Total SMB Object Cache Close success	Total number of successful close file request done by OC.
Total SMB Object Cache Close failure	Total number of files that could not be successfully closed by the OC.
Total SMB Object Cache Delete calls	Total number of delete file requests sent to the OC.

Field	Description
Total SMB Object Cache Delete success	Total number of files that were successfully deleted from the OC after receiving a response from the server.
Total SMB Object Cache Delete failure	Total number of files that were could not be deleted from the OC even after receiving a response from the server.
Total SMB Object Cache SetMetaData calls	Total number of object meta-data set calls sent to object cache.
Total SMB Object Cache SetMetaData success	Total number of successful object meta-data set calls sent to object cache.
Total SMB Object Cache SetMetaData failure	Total number of unsuccessful object meta-data set calls sent to object cache.
Total SMB Object Cache Rename calls	Total number of requests made to the server for renaming the files.
Total SMB Object Cache Rename success	Total number of files that were successfully renamed by the OC.
Total SMB Object Cache Rename failure	Total number of files that could not be renamed by the OC because of no response from the server.
Total SMB Object Cache GetNextHole calls	Total number of get next hole calls sent to object cache to see if there is any hole in the data after the offset. This enables to understand what to read next in read ahead from server after the offset.
Total SMB Object Cache GetNextHole success	Total number of successful get next hole calls sent to object cache.
Total SMB Object Cache GetNextHole failure	Total number of unsuccessful get next hole calls sent to object cache.
Total SMB Object Cache GetNextHole that returned no hole	Total number of get next hole calls sent to object cache for which no holes were identified.
Total SMB Object Cache GetNextHole that returned hole	Total number of get next hole calls sent to object cache for which holes were identified.
Total SMB Object Cache GetNextData calls	Total number of get next data calls sent to object cache to look for next available data in the object cache after offset. This enables to return the data after offset and finds the length of data that is available.
Total SMB Object Cache GetNextData success	Total number of successful get next data calls sent to object cache to look for next available data in the object cache after offset.
Total SMB Object Cache GetNextData failure	Total number of unsuccessful get next data calls sent to object cache to look for next available data in the object cache after offset.
Total SMB Object Cache GetNextData that returned no data	Total number of get next data calls sent to object cache to look for next available data in the object cache after offset that did not find the next available object.
Total SMB Object Cache GetNextData that returned data	Total number of get next data calls sent to object cache to look for next available data in the object cache after offset and that returned the next available object.

Table 3-81 describes the fields shown in the **show statistics accelerator smb | inc Print** command display.

Table 3-81 Field Descriptions for the show statistics accelerator smb | inc Print Command

Field	Description
Total Amount of Time Saved (ms) Due to Print Optimization	Total time saved due to all the optimizations being performed on all the \spoolss pipes (one print job can open multiple \spoolss pipes) and for all the print jobs since the last time the counters were cleared.
Total SMB1 Print Open Requests Processed	The total number of calls to open (NTCreate_AndX).
Total SMB1 Print Open requests served locally	Number of SMB1 NT_Create_AndX requests for \spollss pipe served locally by the edge WAE due to cached open and delayed close optimization.
Total SMB1 Print Open requests forwarded to server	Number of SMB1 NT_Create_AndX requests for \spoolss pipe which were forwarded to the file server by the edge WAE (requests that could not be served locally).
Total SMB1 Print Close requests processed	Number of SMB1 Close requests for the \spoolss pipe seen by the edge WAE.
Total SMB1 Print Close requests served locally	Number of SMB1 Close requests for the \spoolss pipe served locally by the edge WAE as part of delayed close optimization.
Total SMB1 Print Close requests forwarded to the server	Number of SMB1 Close requests for the \spoolss pipe that were forwarded to the file server by the edge WAE (requests that could not be served locally). This total includes only the Close requests that are sent synchronously to the server (the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests first served locally and then sent to the server at a later point in time).
Print SMB1 Documents Spooled count	Number of SMB1 Transact EndDocPrinter messages for the spoolss pipe seen by the edge WAE.
Print SMB1 Pages Spooled count	Number of SMB1 Transact EndParePrinter messages for the \spoolss pipe seen by the edge WAE.
Print SMB1 Async Write count	Number of SMB1 Write_AndXmessages for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization.
Print SMB1 Async StartPagePrinter count	Number of SMB1 Transact StartPagePrinter messages (DCE-RPC opnum 18) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.

Table 3-81 Field Descriptions for the show statistics accelerator smb | inc Print Command (continued)

Field	Description
Print SMB1 Async EndPagePrinter count	Number of SMB1 Transact EndPagePrinter messages (DCE-RPC opnum 20) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async WritePrinter count	Number of SMB1 Transact WritePagePrinter messages (DCE-RPC opnum 19) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Remote Command Count	The number of SMB1 Transact commands for the \spoolss pipe seen by the edge WAE that are not parsed and are sent to the core.

Table 3-82 describes the fields shown in the **show statistics accelerator ssl detail** command display.

Table 3-82 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 **clear stat accelerator all** or **clear stat accelerator ssl** commands were never issued. Otherwise it will show the time at which the **clear stat accelerator all** or **clear stat accelerator ssl** commands were last issued.
Total Handled Connections	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.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Total Optimized Connections	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	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.
Total Dropped Connections	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	Number of connections currently being optimized by the SSL accelerator.
Current Pending Connections	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	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	Number of bytes read by the SSL accelerator from the original side of the flow.
Total Reads on LAN	Number of read operations performed by the SSL accelerator on the original side of the flow.
Total LAN Bytes Written	Number of bytes written by the SSL accelerator on the original side of the flow.
Total Writes on LAN	Number of write operations performed by the SSL accelerator on the original side of the flow.
Total WAN Bytes Read	Number of bytes read by the SSL accelerator from the optimized side of the flow.
Total Reads on WAN	Number of read operations performed by the SSL accelerator on the optimized side of the flow.
Total WAN Bytes Written	Number of bytes written by the SSL accelerator on the optimized side of the flow.
Total Writes on WAN	Number of write operations performed by the SSL accelerator on the optimized side of the flow.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Total LAN Handshake Bytes Read	Number of bytes read from the original side of flows during the handshake phase of flows.
Total LAN Handshake Bytes Written	Number of bytes written to the original side of flows during the handshake phase of flows.
Total WAN Handshake Bytes Read	Number of bytes read to the optimized side of flows during the handshake phase of flows.
Total WAN Handshake Bytes Written	Number of bytes written to the optimized side of flows during the handshake phase of flows.
Total Accelerator Bytes Read	SSL accelerator internal counter. (Bytes read from original side of DRE).
Total Accelerator reads	SSL accelerator internal counter. (Read operations performed on original side of DRE).
Total Accelerator Bytes Written	SSL accelerator internal counter. (Bytes written to original side of DRE).
Total Accelerator Writes	SSL accelerator internal counter. (Write operations performed on original side of DRE).
Total DRE Bytes Read	SSL accelerator internal counter. (Bytes read from optimized side of DRE).
Total DRE Reads	SSL accelerator internal counter. (Read operations performed on the optimized side of DRE).
Total DRE Bytes Written	SSL accelerator internal counter. (Bytes read from optimized side of DRE).
Total DRE Writes	SSL accelerator internal counter. (Write operations performed on the optimized side of DRE).
Number of forward DNS lookups issued	Number of forward DNS lookups that were issued.
Number of forward DNS lookups failed	Number of forward DNS lookup failures.
Number of flows with matching host names	Number of flows where server host name matched accelerated service configuration.
Number of reverse DNS lookups issued	Number of reverse DNS lookups that were issued.
Number of reverse DNS lookups failed	Number of reverse DNS lookup failures.
Number of reverse DNS lookups cancelled	Number of reverse DNS lookups that were cancelled.
Number of flows with matching domain names	Number of flows where server domain name matched accelerated service configuration.
Number of flows with matching any IP rule	Number of flows where the server IP address matched 'IP any' rule.
Total Failed Handshakes	Number of connections that ended during the handshake phase.
Pipe-through due to cipher mismatch	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.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Pipe-through due to version mismatch	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 non-matching domain name	Number of connections bypassed by SSL accelerator because the destination domain did not match the domains specified to be accelerated.
Pipe-through due to unknown reason	Number of connections bypassed by SSL accelerator because of unknown reasons.
Pipe-through due to detection of non-SSL traffic	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	Number of connections that used SSL version 3 on the original side of the flow.
Total TLSv1 Negotiated on LAN	Number of connections that used TLS version 1 on the original side of the flow.
Total SSLv3 Negotiated on WAN	Number of connections that used SSL version 3 on the optimized side of the flow.
Total TLSv1 Negotiated on WAN	Number of connections that used TLS version 1 on the optimized side of the flow.
Total SSLv3 Negotiated on Peer	Number of connections that used SSL version 3 on the control connection between WAAS devices.
Total TLSv1 Negotiated on Peer	Number of connections that used TLS version 1 on the control connection between WAAS devices.
Total renegotiations requested by server	Number of SSL “Hello Request” messages detected by the SSL accelerator.
Total SSL renegotiations performed	Number of SSL renegotiation attempts (successful and unsuccessful) detected by the SSL accelerator.
Total number of failed renegotiations	Number of unsuccessful SSL renegotiations detected by the SSL accelerator.
Flows dropped due to renegotiation timeout	Number of flows dropped due to renegotiation timeout.
[W2W-Srvr] Number of session hits	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	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 timedout	Number of SSL sessions that were not reused because they were timed out.
[W2W-Srvr] Number of sessions deleted because of cache full	Number of sessions evicted from inter-WAAS session cache to make room for new sessions.
[W2W-Srvr] Number of bad sessions deleted	Number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
[W2W-Comm] Number of sessions inserted into cache	Number of sessions inserted into the inter-WAAS session cache
[W2W-Comm] Number of sessions evicted from cache	Number of sessions evicted from the inter-WAAS session cache.
[W2W-Comm] Number of sessions in cache	Number of session currently cached in the inter-WAAS session cache.
[W2W-Clnt] Number of session hits	Number of times an inter-WAAS session resumption was successful on flows where this WAE was the Edge WAE.
[W2W-Clnt] Number of session misses	Number of times an inter-WAAS full SSL handshake was carried out, on flows where this WAE was the Edge WAE.
[W2W-Clnt] Number of sessions timedout	Number of SSL sessions that were not reused because they were timed out.
[W2W-Clnt] Number of sessions deleted because of cache full	Number of sessions evicted from inter-WAAS session cache to make room for new sessions.
[W2W-Clnt] Number of bad sessions deleted	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	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	Number of times a client-requested session was not found in the client-facing session cache.
[C2S-Srvr] Number of sessions timedout	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	Number of sessions evicted from the client-facing session cache to make room for new sessions.
[C2S-Srvr] Number of bad sessions deleted	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	Number of sessions inserted into the client-facing session cache.
[C2S-Srvr] Number of sessions evicted from cache	Number of sessions evicted from the client-facing session cache.
[C2S-Srvr] Number of sessions in cache	Number of sessions currently cached in the client-facing session cache.
[C2S-Clnt] Number of session hits	Number of times a Core-WAE requested session was successfully reused between the Core WAE and server.
C2S-Clnt] Number of session misses	Number of times a full SSL handshake had to be carried out between the Core WAE and server.
[C2S-Clnt] Number of sessions timedout	Number of times a session in the server-facing session cache could not be reused because it was timed out.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
[C2S-Clnt] Number of sessions deleted because of cache full	Number of sessions evicted from the server-facing session cache to make room for new sessions.
[C2S-Clnt] Number of bad sessions deleted	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	Number of sessions inserted into the server-facing session cache.
[C2S-Clnt] Number of sessions evicted from cache	Number of sessions evicted from the server-facing session cache.
[C2S-Clnt] Number of sessions in cache	Number of sessions currently cached in the server-facing session cache.
Total Successful Certificate Verifications	Number of times a certificate was successfully verified (could be client or server).
Total Failed Certificate Verifications	Number of times a certificate verification failed (could be for various reasons, other counters may indicate why).
Failed certificate verifications due to invalid certificates	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	Number of certificate verification attempts deemed unsuccessful based on results of OCSP revocation check.
Failed Certificate Verifications (non OCSP)	Number of certificate verification attempts deemed unsuccessful based on results of the certificate verification operation.
Total Failed Certificate Verifications due to Other Errors	Number of certificate verification failures due to other problems (including internal errors). An inspection of the SSL accelerator errorlog may indicate the reasons.
Total OCSP Connections Outstanding	Number of OCSP requests currently in progress.
Total OCSP Requests Processed	Number of OCSP requests completed (including successful and unsuccessful responses).
Maximum Concurrent OCSP Requests	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	Number of OCSP requests that were completed with a valid response from the OCSP responder.
Total Successful OCSP Requests Returning OK Status	Number of OCSP request where the certificate status was OK.
Total Successful OCSP Requests with 'NONE' Revocation	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	Number of OCSP requests where the certificate status was REVOKED.
Total Successful OCSP Requests Returning UNKNOWN Status	Number of OCSP requests where the responder did not know the status of the certificate.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Total Failed OCSP Requests	Number of OCSP requests which could not be completed successfully.
Total Failed OCSP Requests due to Other Errors	Number of OCSP requests deemed failed due to internal errors.
Total Failed OCSP Requests due to Connection Errors	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	Number of OCSP requests deemed failed because no response was received from the OCSP responder.
Total Failed OCSP Requests due to Insufficient Resources	Number of OCSP requests deemed failed because there was insufficient memory to carry out the revocation check.
Total OCSP Bytes Read	Number of bytes read from connections to OCSP responders.
Total OCSP Write Bytes	Number of bytes written to connections to OCSP responders.
Flows dropped due to verification check	Number of connections dropped by this WAE because verification of the client or server certificate failed.
Flows dropped due to revocation check	Number of connections dropped by this WAE because revocation check of the client or server certificate failed.
Flows dropped due to other reasons	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 3-83 describes the fields shown in the **show statistics accelerator ssl payload http** command display.

Table 3-83 Field Descriptions—show statistics accelerator ssl payload http Command

Field	Description
Total Optimized Connections	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.
Successful HTTP accelerator insertions	Number of connections where the SSL accelerator successfully inserted the HTTP accelerator.
Unsuccessful HTTP accelerator insertions	Number of connections where the SSL accelerator was unsuccessfully in inserting the HTTP accelerator.

Table 3-84 describes the fields shown in the **show statistics accelerator ssl payload other** command display.

Table 3-84 Field Descriptions—show statistics accelerator ssl payload other Command

Field	Description
Total Optimized Connections	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.

Related Commands

show accelerator

show statistics connection closed

show statistics accelerator http object-cache

To display object cache statistics for a WAAS device, use the **show statistics accelerator http object-cache** EXEC command.

show statistics accelerator http object-cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use **show statistics accelerator http object-cache** to display a summary of the number of HTTP transactions to the specified host. The top hosts list is always displayed after the cache-type statistics, and contains between 0-10 hosts. This same information can be displayed in graphics form in the Monitor > Caching >Akamai Connect section of the WCM.

Note Depending on which cache types are enabled and what traffic is seen, the output may show statistics for any or all of the following cache types: bypass, standard, advanced, connected cache, OTT-youtube, OTT-generic, or unknown.

Examples

The following example shows sample output from the **show statistics accelerator http object-cache** command:

```
HTTP:
   Object Cache Statistics
   -----------------------

Object Cache Caching Type:                                         ott-youtube
   Object cache transactions served from cache:                       7
   Object cache request bytes for cache-hit transactions:             5560
   Object cache response bytes for cache-hit transactions:            962534
   Object cache transactions requiring freshness check:               1
   Object cache responses not cached:                                 43
   Object cache responses stored in cache:                            295
Object Cache Caching Type:                                         standard
   Object cache transactions served from cache:                       31
   Object cache request bytes for cache-hit transactions:             10770
   Object cache response bytes for cache-hit transactions:            50235
   Object cache response time savings for cache-hit transactions:     5546
   Average response time saved per cache-hit transactions (ms)        5
   Percentage response time saving for cache-hit transactions:        60
   Object cache transactions requiring freshness check:               3
   Object cache responses not cached:                                 364
   Object cache responses stored in cache:                            65

Object cache top hosts ordered by:                                 hit count

   Object cache host name:
au.download.windowsupdate.com
      Object cache transaction count:                     197
      Object cache WAN response bytes:                    54245680
      Object cache LAN response bytes:                    54260258
   Object cache host name:
 r13---sn-hp576ne7.googlevideo.com
      Object cache transaction count:                     123
      Object cache WAN response bytes:                    40209279
      Object cache LAN response bytes:                    41180077
   Object cache host name:                             s.youtube.com
      Object cache transaction count:                     102
      Object cache WAN response bytes:                    43160
      Object cache LAN response bytes:                    54551
Object cache top hosts ordered by:             Total Response Time Savings

   Object cache host name:              www.carnival.com
      Object cache transaction count:                     31
      Object cache WAN response bytes:                    15
      Object cache WAN response bytes:                    329919
      Object cache LAN response bytes:                    1706503
      Object cache response time savings (ms):            6565476
```

Related

show statistics accelerator

show statistics accelerator http preposition

To display preposition task status information for a WAAS device, use the **show statistics accelerator http preposition** EXEC command.

show statistics accelerator http preposition

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use **show statistics accelerator http preposition** to display task status information for a WAAS device.

Examples

The following example shows output from the **show statistics accelerator http preposition** command:

```
Preposition Task                          mytask1
   Status                                COMPLETE
   Error                                     None
   Start Time:                2014-11-24 14:53:00
   End Time:                  2014-11-24 14:53:03
   Transaction Count:                           1
   Byte count:                               2229
   Refresh object count:                        0
   Refresh object bytes                         0
   Cache store object count                     1
   Cache store object bytes                  2229
   Uncacheable object count                     0
   Uncacheable object bytes                     0
```

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**]

Syntax Description

local	(Optional) Displays statistics only for all locally registered application accelerators.
peer	Displays statistics only for all peer WAAS devices encountered.
detail	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 3-85 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 3-85 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.
Number of Peers	Number of known or encountered peer WAAS devices.

Table 3-85 Field Descriptions for the show statistics aoim Command (continued)

Field	Description
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.
Peer AOIM Statistics	
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	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.
#CONNS	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.
Detailed AOIM Statistics	
Policy Engine Statistics	

Table 3-85 Field Descriptions for the show statistics aoim Command (continued)

Field	Description
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).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
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.

Table 3-85 Field Descriptions for the show statistics aoim Command (continued)

Field	Description
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
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.
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	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 [**name** *app_name* | **savings** [**appname** *app_name*]]

Syntax Description

name *app_name*	(Optional) Statistics for the specified application.
savings	(Optional) Savings statistics applications.
appname *app_name*	(Optional) Savings statistics for the specified application.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show statistics application** 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 **name** keyword.

Table 3-86 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, "Predefined Application Policies" in the *Cisco Wide Area Application Services Configuration Guide*.

Note If the HTTP connection to the client aborts while the file transfer is in progress, the **show statistics application** command output may display a higher total for optimized traffic than for original traffic. This is because the HTTP cache always caches the complete file, even if the connection to the client is aborted before the file transfer has completed.

Table 3-86 app_name Variable Values for the show statistics application Command

app_name Values			
Authentication	Backup	CAD	Call-Management
Citrix	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	SSL	Storage

Table 3-86 app_name Variable Values for the show statistics application Command

app_name Values			
Streaming	Systems-Management	Version-Management	VPN
Web			

Examples

Table 3-87 describes the statistics for each class of application that are displayed by the **show statistics application** EXEC command.

Table 3-87 Statistic Descriptions for the show statistics application Command

Statistic	**Description**
Opt TCP Plus	Optimized traffic on the WAN side, optimized at the TFO and DRE/LZ/accelerator levels.
Orig TCP Plus	Original traffic on the LAN side, optimized at the TFO and DRE/LZ/accelerator levels.
Opt Preposition	Optimized traffic on the WAN side, initiated by the WAE device for preposition purposes.
Orig Preposition	Original traffic (unoptimized) on the LAN side, initiated by the WAE device for preposition purposes.
Opt TCP Only	Optimized traffic on the WAN side, optimized at the TFO level only.
Orig TCP Only	Original traffic on the LAN side, optimized at the TFO level only.
Internal Client	Traffic initiated by the WAE device.
Internal Server	Traffic terminated by the WAE device.
PT Client	Pass-through traffic going from the client to the server.
PT Server	Pass-through traffic going from the server to the client
Opt TCP Plus	Optimized traffic on the WAN side, optimized at the TFO and DRE/LZ/accelerator levels.
Preposition	Traffic initiated by the WAE device for preposition purposes.
Opt TCP Only	Optimized traffic on the WAN side, optimized at the TFO level only.
Internal Client	Traffic initiated by the WAE device.
Internal Server	Traffic terminated by the WAE device.
Auto-Discovery	Connections in auto-discovery.
PT No Peer ...	Pass-through reasons.
PT Overall	Total passed-through traffic for all reasons.

Table 3-88 describes the result values shown for the statistics in the **show statistics application** command display.

Table 3-88 Result Value Descriptions for the show statistics application Command

Result	Description
Bytes	Amount of traffic shown as a count of the number of bytes.
Packets	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

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**]

Syntax Description

blacklist	(Optional) Displays the blacklist server statistics.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-89 describes the result values shown for the statistics in the **show statistics application** command display.

Table 3-89 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.

Table 3-89 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 nostate state	Number on non-SYN packets dropped that were in the nostate 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 AO	Auto-discovery failed because the peer accelerator is not compatible with the accelerator on this WAE.

Table 3-89 Result Value Descriptions for the show statistics auto-discovery Command

Result	Description
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	Address of the internal server.
External server	Address of the external server.
Auto discovery success FOR	
Internal client	Address of the internal client.
External client	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	Number of SYN packets received indicating WAE’s device ID.
SYN retransmit count resets	Number of resets to the SYN retransmission count.
SYN-ACK sequence number resets (syncookies)	Number of SYN-ACK packets received with a sequence number reset.
SYN-ACKs found with our device id	Number of SYN-ACK packets received indicating WAE’s device ID.
SYN-ACKs found with mirrored options	Number of SYN-ACK packets received with mirrored options.
Connections taken over for MAPI optimization	Number of connections taken over for MAPI acceleration from an overloaded serial cluster peer.

Related Commands

show auto-discovery

show statistics filtering

show statistics tfo

show statistics connection closed

show statistics class-default

To display statistics information about the class-default class map, use the **show statistics class-default** EXEC command.

show statistics class-default top-talkers

Syntax Description

top-talkers	Displays the statistics for the top 10 ports with the most traffic.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics class-default top-talkers** EXEC command to view statistics for traffic matched by the class-default class map. Statistics are displayed for the top 10 ports by traffic volume.

Examples

The following shows an example of output from the **show statistics class-default top-talkers** command.

```
WAE# show statistics class-default top-talkers
Rank   Port   Vol %                    Bytes                 Packets
----  -----  ------  ----------------------  ----------------------
        All  100.00              45759836065                63801873
  1      80   94.44              43216161904                52890647
  2     443    1.92                877275192                 4744341
  3    9182    0.00                    88010                     330
  4   34182    0.00                    87985                     324
  5   14660    0.00                    87894                     326
  6   49468    0.00                    82857                     299
  7   44180    0.00                    82746                     304
  8   29641    0.00                    82104                     292
  9   47835    0.00                    81966                     304
 10   20362    0.00                    81957                     314
```

Related Commands

clear statistics

show class-map

show statistics class-map

show statistics class-map

To display statistics information about class maps, use the **show statistics class-map** EXEC command.

show statistics class-map type { **waas**
[**name** *classmap-name* | **summary** [**active** | **all**]]}

Syntax Description

waas	Displays statistics for the specified WAAS optimization class map, or all class maps if no class map is specified.
name *classmap-name*	Displays statistics for the specified WAAS optimization class map.
summary	Displays summary statistics for all WAAS optimization class maps that have active and completed connections.
active	Displays summary statistics for all WAAS optimization class maps that have currently active connections.
all	Displays summary statistics for all WAAS optimization class maps.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics class-map** EXEC command to view statistics for class maps.

Related Commands

show class-map

show statistics class-default

show statistics connection

To display all connection statistics for a WAAS device, use the **show statistics connection** 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***} |**
client-ip {*ip_address* | *hostname*} **| client-port** *port* |
closed |
detail [**client-ip** {*ip_address* | *hostname*} | **client-port** *port* **| peer-id** *peer_id* | **server-ip**
{*ip_address* | *hostname*} **| server-port** *port*] **|**
egress methods |
optimized |
pass-through |
peer-id *peer_id* |
server-ip {*ip_address* | *hostname*} **|**
server-port *port*] |
conn-id *connection_id*

Syntax Description

auto-discovery	Displays currently active auto-discovery connections
client-ip	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
closed	Displays closed connections for client, server and peer along with their details.
detail	(Optional) Displays detailed connection statistics.
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).
egress-methods	Displays detailed information on the egress-methods
optimized	Displays currently active optimized connections.
pass-through	Display currently active pass-through connections.
conn-id *connection_id*	(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.

Note For pass-through entries, a new connection immediately replaces an old connection. If a connection termination takes less than 10 seconds, then the new connection replaces it. However, WAAS has pass-through connection entry for both new and old connections (connections lasting 10 seconds or more). Therefore, in a scenario where pass-through entries take 10 seconds or more to expire, the output from **show statistics connection** will show totals for both old and new connections.

Unlike optimized flow, WAAS does not inspect each packet at TCP level to confirm when the connection got reset. Therefore, when there is no activity for 10 seconds, the pass-through flow entry get removed. The pass-through flows are then a count of pass-through flows seen in less than 10 seconds.

Examples

Table 3-90 describes the fields shown in the **show statistics connection** command display.

Table 3-90 Field Descriptions for the show statistics connection 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 Reserved Flows	Number of connections reserved for the MAPI accelerator. It appears for all accelerators.
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.

Table 3-90 Field Descriptions for the show statistics connection Command (continued)

Field	Description
Dest IP:Port	IP address and port of the outgoing destination connection.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, S = SSL, W = WAN secure, X = signed SMB
Reduction Ratio (RR)	Relative reduction ratio (in bytes) for a particular connection.
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	Connection type (see Table 3-91).

Table 3-91 describes the possible values found in the ConnType field.

Table 3-91 Connection Types

ConnType	Description
Accelerator Non-Optimized	Connection has been initiated from an external client to an external server and is not optimized.
Accelerator Optimized	Connection has been initiated from an internal client to an external server and is optimized.
App Dyn Mtch Non-Optimized	Connection has been forced through an application dynamic match and is non-optimized by an application accelerator, even though the connection may be optimized by TFO+DRE+LZ.
App Dyn Mtch Optimized	Connection has been forced through an application dynamic match to be optimized, even though the connection may be handled as pass-through.
PT AD Int Error	Connection encountered an internal error during processing by the TFO auto discovery SYN cache.
PT App Cfg	Policy action for this application is configured as pass-through.
PT App Override	Connection is pass-through because the internal application has explicitly requested that the connection not be optimized. This state would only occur if the connection would have otherwise been optimized.
PT Asym Client	Connection is pass-through due to the WAE only seeing one side of the TCP connection (where the src is the client and the dst is the server).
PT Asym Server	Connection is pass-through due to the WAE only seeing one side of the TCP connection (where the dst is the client and the src is the server).
PT Dst Cfg	Policy action for this application is configured as pass-through in the peer WAE.
PT FB Int Error	Connection encountered an internal error during processing by the filter bypass module.

Table 3-91 Connection Types

ConnType	Description
PT_Glb Cfg	Global action is configured as pass-through; that is, TFO, DRE, or LZ are disabled globally on the WAE.
PT In Progress	Connection was already established when the first packet was seen by the WAE.
PT Interception ACL	Connection is pass-through due to an interception ACL denying optimization.
PT Intermediate	Connection is pass-through due to the WAE being in the middle of the best local and remote WAE's (relative to the client and server).
PT No Peer	Connection is pass-through due to no peer WAE being found during TFO auto-discovery.
PT Non-Optimizing Peer	Connection is pass-through because the only peer found is a serially clustered peer and optimization is disabled to the peer.
PT Overload	TFO application has indicated it is overloaded (that is, the maximum number of optimized connections has been exceeded). New connections not handled by an application accelerator are configured as pass-through.
PT PE Int Error	Connection encountered an internal error during processing by the policy engine.
PT Rjct Capabilities	Connection is pass-through due to auto discovery finding that the peer WAE does not have the required capabilities.
PT Rjct Resources	Connection is pass-through due to auto discovery finding that the peer WAE does not have the required resources.
PT Server Blacklist	Connection is pass-through because the server is on the TFO blacklist as not supporting TCP Option (0x21) being present in the SYN packet.

Related Commands

clear arp-cache

show statistics accelerator

show statistics connection egress-methods

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*

Syntax Description

auto-discovery	(Optional) Displays active connection statistics for auto-discovery connections.
client-ip	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(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

This command displays the statistics for auto-discovery TCP connections. This information is updated in real time.

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 3-92 describes the fields shown in the **show statistics connection auto-discovery** display.

Table 3-92 Field Descriptions for the show statistics connection auto-discovery 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	MAC address of the peer device.

O-ST	Origin state of the connection.
	E = Established, S = Syn, A = Ack, F = Fin, R = Reset,
	s = sent, r = received, O = Options, P = Passthrough

T-ST	Terminal state of the connection.
	E = Established, S = Syn, A = Ack, F = Fin, R = Reset,
	s = sent, r = received, O = Options, P = Passthrough

ConnType	Type of the connection (see Table 3-91).

Related Commands

show statistics accelerator

show statistics connection egress-methods

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
[**detail | dre** | **epm** | **http** | **mapi** | **ssl** | **tfo |** [**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

detail	(Optional) Displays detailed closed connection statistics.
dre	(Optional) Displays closed connection statistics for connections optimized by the DRE feature.
epm	(Optional) Displays closed connection statistics for connections optimized by the EPM application accelerator.
http	(Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.
mapi	(Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.
ssl	(Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.
tfo	(Optional) Displays closed connection statistics for connections optimized by the TFO application accelerator.
client-ip	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
conn-id *connection_id*	(Optional) Displays closed connection statistics for the connection with the specified identifier.
peer-id *peer_id*	(Optional) Displays the closed connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(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 closed** 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.

Examples

Table 3-93 describes the fields shown in the **show statistics connection closed** command display.

Table 3-93 Field Descriptions for the show statistics connection closed 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.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, S = SSL, W = WAN secure, X = signed SMB

Related Commands

clear arp-cache

show statistics accelerator

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*

Syntax Description

connection_id	(Optional) Connection statistics for the connection with the specified identifier number.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **show statistics connection conn-id** command displays the statistics for individual TCP connections. This information is updated in real time.

Examples

Table 3-94 describes the fields shown in the **show statistics connection conn-id** command display.

Table 3-94 Field Descriptions for the show statistics connection conn-id Command

Field	Description
Connection Information	
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.
Preposition Flow	Flow was originated by an accelerator to acquire data in anticipation of its future use: true or false.
Policy Details: Configured	Name of the configured application policy.

Table 3-94 Field Descriptions for the show statistics connection conn-id Command (continued)

Field	Description
Policy Details: Derived	Name 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 rear and written on the original (incoming) side and the optimized (outgoing) side.
DRE Stats	
Encode	Statistics for compressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for compressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for compression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
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.
Connection Details	
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.
TFO Stats	
Conn-Type	Type of connection (see Table 3-91).
Policy	Policy in use on connection.

Table 3-94 Field Descriptions for the show statistics connection conn-id Command (continued)

Field	Description
EOT State [write | req | ack | read | ack]	End of transmission state for data written and read.
Socket States	Socket states, including **read-shut**, **write-shut**, **close**, **choke**, and **envoy**.
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	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

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*

Syntax Description

client-ip	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(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):

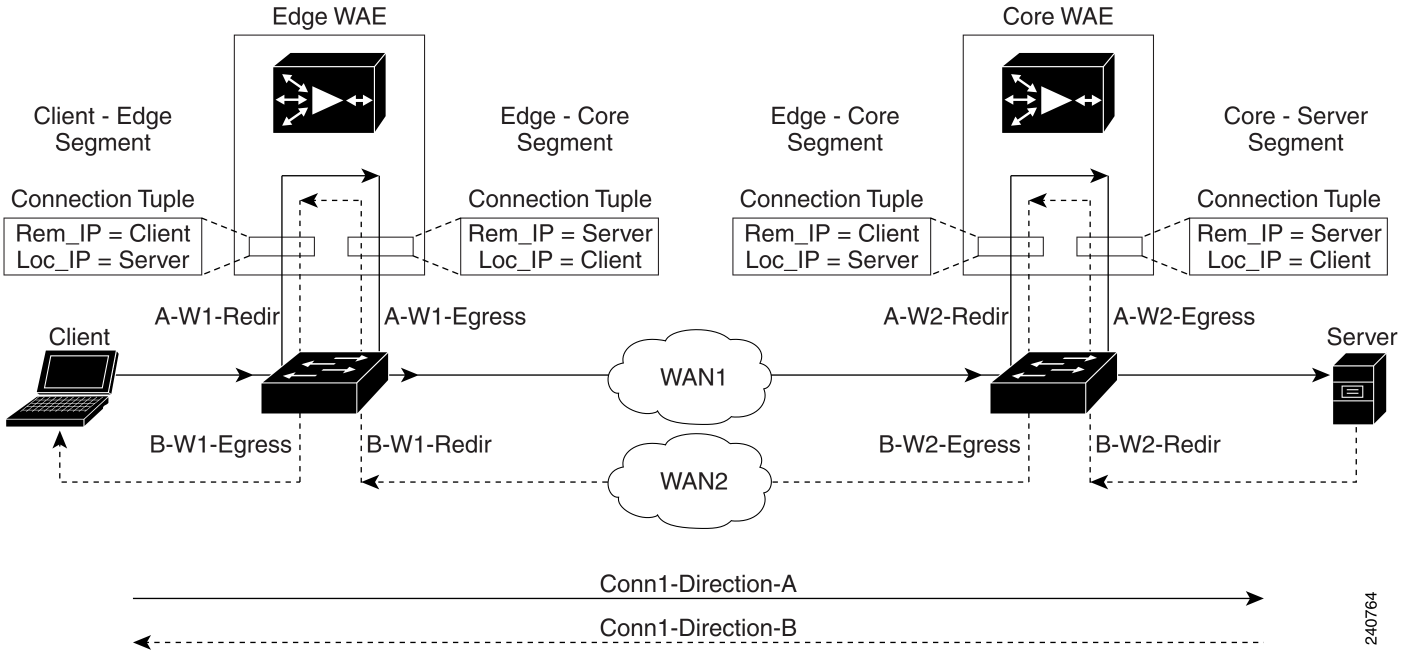
- Between the client and the Edge WAE
- Between the Edge WAE and the Core WAE
- Between the Core WAE and the server

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 3-95.) 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 3-95 describes the fields shown in the **show tfo egress-methods connection** command display.

Table 3-95 Field Descriptions for the show tfo egress-methods connection Command

Field	Description
TUPLE	
Local-IP:Port	IP address and port number of the local device in the connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the connection tuple.
MATE	
Local-IP:Port	IP address and port number of the local device in the mate connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the mate connection tuple.
Egress method	Egress method being used.
WCCP Service | Bucket	WCCP service number and bucket number for the connection tuple and mate connection tuple.
Tuple Flags	Flags for intercept method and intercept mechanism. This field may contain the following values: WCCP or NON-WCCP as the intercept method; L2 or GRE as the intercept mechanism; or PROT showing whether this tuple is receiving packets through the flow protection mechanism.
Intercepting device (ID)	
ID IP address	IP address of the intercepting device.
ID MAC address	MAC address of the intercepting device.
ID IP address updates	Number of IP address changes for the intercepting device.
ID MAC address updates	Number of MAC address changes for the intercepting device.
Memory address	Memory address.

Each time a packet enters the connection tuple, the intercepting device IP address or MAC address is recorded. The updates field in the command output indicates whether the intercepting device IP address or intercepting device MAC address has been recorded. If, for example, the ID MAC address updates field is zero (0), the MAC address was not recorded, and the ID MAC address field will be blank. The recorded intercepting device information is used when a packet egresses from the WAE.

If the egress method for the connection tuple is IP forwarding, the updates fields are always zero (0) because the intercepting device information is neither required nor recorded for the IP forwarding egress method.

If the intercept method is WCCP GRE redirect and the egress method is WCCP GRE, only the IP address field is updated and recorded. The MAC address information is neither required nor recorded because the destination address in the GRE header only accepts an IP address.

If the intercept method is WCCP L2 redirect and the egress method is WCCP GRE, both the MAC address and the IP address fields are updated and recorded because incoming WCCP L2 packets contain only a MAC header. The MAC address is recorded and the intercepting device IP address is derived from a reverse ARP lookup and is then recorded, also. When packets egress the connection tuple in this scenario, they will have a GRE header with the destination IP address of the intercepting device that was recorded.

The updates count may be greater than 1 in certain topologies. For example, in a redundant router topology, where for the same direction of the same connection between two hosts, packets may be coming in from different intercepting routers. Each time a packet comes in, the intercepting device MAC or IP address is compared against the last recorded address. If the MAC or IP address has changed, the updates field is incremented and the new MAC or IP address is recorded.

Related Commands

show statistics tfo

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* |
{**http** | **ica** | **mapi** | **smb** **|** **ssl** | **wansecure** | {**detail** | **dre** { **all** | **savings** | {**http** | **ica** | **mapi** | **smb** **|** **ssl** | **wansecure**}}]

Syntax Description

optimized	(Optional) Displays active connection statistics for optimized connections.
client-ip	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).
http	(Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.
ica	(Optional) Displays closed connection statistics for connections optimized by the ICA application accelerator.
mapi	(Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.
smb	(Optional) Displays the connection statistics for connections optimized by the SMB application accelerator.
ssl	(Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.
wansecure	(Optional) Displays closed connection statistics for connections optimized by the WAN secure application accelerator.
dre	(Optional) Displays closed connection statistics for connections optimized by the DRE feature.
all	(Optional) Displays all the connection statistics for connections of the filtered type.
savings	(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 3-96 describes the fields shown in the **show statistics connection optimized** command display.

Table 3-96 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 Reserved Flows	Number of reserved connections.
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	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, S = SSL, W = WAN secure, X = signed SMB

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*

Syntax Description

pass-through	Displays active connection statistics for pass-through connections.
client-ip	Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	Displays the closed connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	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

The **show statistics connection pass-through** 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.

Examples

Table 3-97 describes the fields shown in the **show statistics connection pass-through** command display.

Table 3-97 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	MAC address of the peer device.
ConnType	Status of the connection (see Table 3-92).

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 3-98 describes the fields shown in the **show statistics crypto ssl ciphers** command display.

Table 3-98 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

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 3-99 describes the fields shown in the **show statistics datamover** command display.

Table 3-99 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 *n*	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 3-99 Field Descriptions for the show statistics datamover Command (continued)

Field	Description
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 dre

To display Data Redundancy Elimination (DRE) general statistics for a WAE, use the **show statistics dre** EXEC command,

show statistics dre [**detail**]

Syntax Description

detail	(Optional) Specifies to show detail.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Example 1

Table 3-100 describes the fields shown in the **show statistics dre detail** command display. This command shows the aggregated statistics for all connections.

Table 3-100 Field Descriptions for the show statistics dre detail 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). 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.
Cache details	
Replaced (last hour)	Amount of cache replaced within the last hour.
Connections	
Total (cumulative)	Total cumulative connections.
Active	Number of active 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).

Table 3-100 Field Descriptions for the show statistics dre detail 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.
Avg msg size	Average message size.
Message size distribution	Message sizes divided into six size groups. Number of messages in each group and their distribution percentage.
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).
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 DRE. Number of messages, number of bytes.
Avg latency: ms	Average latency introduced to compress a message.
Avg msg size	Average message size.
Message size distribution	Message sizes divided into six size groups. Number of messages in each group and their distribution percentage.
Connection details	
Encode bypass due to: last partial chunk	Number of bypassed partial chunks and total size of bypassed chunks.
Nacks: total	Total NACKs.
R-tx: total	Total number of retransmissions.
Encode LZ latency: ms per msg, avg msg size	Encoding LZ latency in milliseconds per message and average message size in bytes.
Decode LZ latency: ms per msg, avg msg size	Decoding LZ latency in milliseconds per message and average message size in bytes.

Table 3-100 Field Descriptions for the show statistics dre detail Command

Field	Description
Cache write detail	
Disk size saving due to unidirectional mode	Amount of cache disk space saved due to using unidirectional caching mode.

Example 2

The following example shows output from the **`show statistics dre`** command.

```
Cache:
    Status: Usable, Oldest Data (age): 14d16h
    Total usable disk size:  77822 MB,  Used: 96.69%
WAE-337-06#sh statistics dre

Cache:
    Status: Usable, Oldest Data (age): 14d17h
    Total usable disk size:  77822 MB,  Used: 96.69%

Connections:   Total (cumulative): 9   Active: 9

Encode:
   Overall: msg:       1398, in:   2586 KB, out:   2318 KB, ratio:  10.38%
       DRE: msg:       1389, in:   2549 KB, out:   2381 KB, ratio:   6.57%
DRE Bypass: msg:       1398, in:  38235 B
        LZ: msg:       1347, in:   2384 KB, out:   2253 KB, ratio:   5.49%
 LZ Bypass: msg:         51, in:  35814 B
    Avg latency:      0.334 ms, Avg msg size:   1894 B
  Message size distribution:
    0-1K=7%  1K-5K=88%  5K-15K=3%  15K-25K=0%  25K-40K=0%  >40K=0%
Decode:
   Overall: msg:         27, in:  14140 B, out:  29223 B, ratio:  51.61%
       DRE: msg:         27, in:  29770 B, out:  29079 B, ratio:   0.00%
DRE Bypass: msg:         27, in:    144 B
        LZ: msg:         27, in:  14140 B, out:  30076 B, ratio:  52.99%
 LZ Bypass: msg:          0, in:      0 B
    Avg latency:      0.061 ms, Avg msg size:   1082 B
```

Example 3

The following example shows sample output using the **`cwoDre`** parameter. The output provides two types of MIB DRE statistics—DRE cache statistics and DRE performance statistics:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsStatus.0 = STRING: Usable
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsAge.0 = STRING: 14d17h
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsTotal.0 = Counter64: 77822 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 96 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitUsage.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrDataUnit.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitAge.0 = STRING: 0s
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockUsage.0 = Counter64: 1695 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrSigblock.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockAge.0 = STRING: 14d17h
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeCompressionRatio.0 = Gauge32: 9 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeCompressionLatency.0 = Counter64: 0 ms
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeAvgMsgSize.0 = STRING:   1991 B
```

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeCompressionRatio.0 = Gauge32: 51 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeCompressionLatency.0 = Counter64: 0 ms
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeAvgMsgSize.0 = STRING:   1082 B
```

Related Commands

show statistics peer

show statistics encryption-services

To display encryption-services general statistics for a WAE, use the **show statistics encryption-services** EXEC command,

show statistics encryption-services {interposer-ssl (detail) | sake}

Syntax Description

interposer-ssl	Displays interposer-ssl statistics
sake	Displays sake statistics

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Example 1

Table 3-101 describes the fields shown in the **show statistics interposer-ssl detail** command.

Table 3-101 Field Descriptions for the show statistics interposer-ssl detail 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 clear statistics accelerator [interposer-ssl | all] command was executed since accelerator was last started or restarted.
Total Handled Connections	Total number of handled connections by the Interposer.
Total Optimized Connections	Total number of optimized connections by the Interposer.
Total Connections Handed-off	Connections initially accepted by Interposer accelerator, but later handed off to generic optimization without policy changes
Total Dropped Connections	Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources)
Current Active Connections	Number of WAN side connections currently established
Maximum Active Connections	Highest number of active connections since accelerator was last started/restarted.
Number of flows with matching IP	Number of connection that flows with the matching ip i.e configured in accelerated service.

Table 3-101 Field Descriptions for the show statistics interposer-ssl detail Command

Field	Description
Number of flows with matching SNI	Number of connection that flows with the matching server name.
Total requests to SAKE	Total number of requests sent to the SAKE server
Total responses from SAKE	Total number of responses from the SAKE server
Total Failed Certification Validations	Total Number of Failed Certificate validation.
Total Connections Dropped due to OCSP failures	Total Number of connection pushdown due OCSP failures.
Interposer SSL Detailed Statistics	
Total Pushdown Flows	Total number of flows that were pushed down due to various reasons.
Pushdown due to cipher mismatch	Number of connections pushed down by Interposer- SSL accelerator because the SSL cipher negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
Pushdown due to unsupported SSL version	Number of connections pushed down by Interposer- SSL accelerator because the SSL version negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
Pushdown due to detection of non-SSL traffic	Number of connections pushed down by the Interposer- SSL accelerator because the content of the flow did not appear to contain SSL messages.
Pushdown due to ASVC not found	Number of connections pushed down by the Interposer- SSL accelerator because no matching accelerated service was found for the content of the flow.
Pushdown due to unknown reason	Number of connections pushed down by the Interposer- SSL accelerator because of unknown reasons.
Total Handled Flows	
Total SSLv3	Total number of connection that are negotiated with the SSL version SSLv3.
Total TLS	
Total TLS1.0	Total number of connection that are negotiated with the SSL version TLS1.0 in Handshakes
Total TLS 1.1	Total number of connection that are negotiated with the SSL version TLS1.1 in Handshakes
Total TLS1.2	Total number of connection that are negotiated with the SSL version TLS1.2 in Handshakes
SSL Handshake classification	
Total SSL Handshakes	Total number of all handshakes seen by the WAE since the last reset.

Table 3-101 Field Descriptions for the show statistics interposer-ssl detail Command

Field	Description
Total Full SSL Handshakes	Total number of connections that performed a full handshake exchanging cryptographic information.
Total SSL Resumptions	Total number of connections that perform a resumption (either with session-id or session-ticket) handshake.
Session-Id	Number of SSL Handshakes with Resumption with Session-Id.
Session-Ticket	Number of SSL Handshakes with Resumption with Session-Ticket
Fallback to Full SSL Handshakes	Total number of resumption failures that result in a fallback to full handshake.
Total SSL renegotiations	Total number of renegotiated SSL handshakes.
Total number of failed renegotiations	Total number of renegotiation handshakes that resulted in failures.
Certificate Validation	
Total Certificate Validation Requests	Total number of client and server certificate validation attempted by SMART-SSL accelerator. Total Number of Certificate Validation Requests without OCSP revocation check
Total Successful Certificate Validations	Total Number of successful Certificate Validation done by the SMART-SSL accelerator without OCSP revocation check.
Total Trusted Certificate Store Refresh	Total number of times CA trusted pool is updated. In other words, total number of trusted certificate store refresh.
OCSP	
Total OCSP validation requests initiated	Number of OCSP validation requests that were initiated by the SMART-SSL accelerator based on configuration settings.
Total OCSP validation responses completed	Number of OCSP validation requests that were completed with a valid response from the OCSP responder.
Total OCSP requests that timed out	Number of OCSP requests deemed failed because no response was received from the OCSP responder.
Total Successful OCSP requests with GOOD status	Number of OCSP requests where the OCSP certificate status was "GOOD"
Total Successful OCSP requests with NONE status	Number of OCSP requests where the OCSP status was deemed OK because of fallback to method configuration: NONE.
Total Successful OCSP requests with REVOKED status	Number of OCSP requests where the OCSP certificate status was REVOKED.
Total Successful OCSP requests with UNKNOWN status	Number of OCSP requests where the responder did not know the status of the certificate.
Total OCSP requests pending	Number of OCSP requests currently in progress.
Total OCSP requests with a corrupted certificate	Number of OCSP requests where certificate verification attempts failed because the certificate was corrupted.

Table 3-101 Field Descriptions for the show statistics interposer-ssl detail Command

Field	Description
Total OCSP requests with failed certificate verification	Number of OSCP requests where certificate verification attempts failed.
Total OCSP requests that encountered internal error	Number of OCSP requests deemed failed due to internal errors.

Table 3-102 describes the fields shown in the **show statistics sake detail** command.

Table 3-102 Field Descriptions for the show statistics sake detail Command

Field	Description
SAKE Server Statistics	
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 clear statistics accelerator [interposer-ssl | all] command was executed since accelerator was last started or restarted.
ASVC Config Channel	This indicates that the SMART-SSL accelerator is ready to receive the configuration from CLI or CM.
Number of ISM Connected	Total number of Interposer Session Manager participating in the SSL handshake.
Accelerated Service Count	Number of configured accelerated services.
Number of Sake Requests Received	Total number of Accelerated services configured on SAKE server.
Number of Sake Pending Requests	Total number of SAKE requests pending to be served.
Number of Sake Success Responses	Total number of successful SAKE responses.
Number of flows with matching SN	The total number of connections requests that matched the SNI (Service Name Indicator) to find the right accelerated service.
Number of Sake Error Responses	Total number of requests that resulted in errors.
SAKE Server Detailed Statistics	
Number of requests per Crypto	Total number of crypto requests serviced by SAKE server.
DHE key exchange	Number of SAKE Requests that originates from DHE Handshakes.
ECDHE Key exchange	Number of SAKE Request that is carried with ECDHE algorithm at the time of the connection between interposer and sake.
RSA key exchange	Number of SAKE Request that is carried with RSA algorithm at the time of the connection between interposer and sake.
Client Authentication	Number of SAKE Request when server asks for the client Authentication

Table 3-102 Field Descriptions for the show statistics sake detail Command

Field	Description
Number of requests per ASVC	Number of connection that flows to that particular Accelerated Service.
ASVC-ngssl	Number of requests to SAKE from a particular Accelerated Service.

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 3-103 describes the fields shown in the **show statistics filtering** command display.

Table 3-103 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.
Internal client syn packets dropped	Number of syn packets generated by a process on the WAE that were dropped.

Table 3-103 Field Descriptions for the show statistics filtering Command (continued)

Field	Description
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 recvd 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.
SYN packets sent with non-opt option due to MAPI	Number of syn packets sent with the non-optimizing option due to the MAPI accelerator.
Internal Server conn. not optimized due to Serial Peer	Number of server connections not optimized because this device is in a serial cluster and is passing through the connections to its serial peer.

Table 3-103 Field Descriptions for the show statistics filtering Command (continued)

Field	Description
Duplicate packets to synq dropped	Number of dropped syn packets that were retransmitted and received for a connection while it was being processed in synq (without impacting the connection).
Number of ICMP Fragmentation Needed messages sent	Number of ICMP fragmentation needed messages sent.
Incorrect length or checksum received on Syn	Number of syn packets received with incorrect length or checksum.
Dropped optimized timewait sockets	Number of sockets in the time-wait state from a previous optimized connection that were dropped due to a new connection request.
Dropped non-optimized timewait sockets	Number of sockets in the time-wait state from a previous nonoptimized connection that were dropped due to a new connection request.

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 type performance-monitor tcpstat-v1**} | **monitor** *MonitorName* | **exporter** *ExporterName*

Syntax Description

filters	Displays flow filter statistics.
monitor type	Displays flow performance statistics.
tcpstat-v1	Displays tcpstat-v1 collector statistics.
monitor *MonitorName*	Displays statistics for a specified flow monitor.
exporter *ExporterName*	Displays statistics for a specified exporter.

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 flow filters** command display.

Table 3-104 Field Descriptions for the show statistics flow filters Command

Field	Description
Number of Filters	Number of filters.
Status	Status of whether the filters are enabled or disabled.
Capture Mode	Operation of the filter. Values include FILTER or PROMISCUOUS. The promiscuous operation is not available in WAAS.
Server	IP address list of the servers for which flows are being monitored.
Flow Hits	Number of flow hits for each server.
Flags	Flags identifying the flows. CSN: Client-Side Non-Optimized (Edge) SSO: Server-Side Optimized (Edge) CSO: Client-Side Optimized (Core) SSN: Server-Side Non-Optimized (Core) PT: Pass Through (Edge/Core/Intermediate) IC: Internal Client

Table 3-105 describes the fields shown in the **show statistics flow monitor** command display.

Table 3-105 Field Descriptions for the show statistics flow monitor Command

Field	Description
Host Connection	
Configured host address	IP address of the tcpstat-v1 console for the connection.
Connection State	State of the connection.
Connection Attempts	Number of connection attempts.
Connection Failures	Number of connection failures.
Last connection failure	Date and time of the last connection failure.
Last configuration check sent	Date and time that the last configuration check was sent.
Last registration occurred	Date and time that the last registration occurred.
Host Version	Version number of the tcpstat-v1 console for the connection.
Collector Connection	
Collector host address:port	IP address and port number of the tcpstat-v1 aggregator identified through the host connection.
Connection State	State of the connection.
Connection Attempts	Number of connection attempts.
Connection Failures	Number of connection failures.
Last connection failure	Date and time of the last connection failure.
Last configuration check sent	Date and time that the last configuration check was sent.
Last update sent	Date and time that the last update was sent.
Updates sent	Number of updates sent.
Summaries discarded	Number of summaries that were discarded because disk space allocated for storage has reached its limit. The numbers in this field indicate when summaries are being collected faster than they are able to be transferred to the collector. Counters in this field generate a data_update alarm.
Last registration occurred	Date and time that the last registration occurred.
Host Version	Version number of the tcpstat-v1 aggregator for the connection.
Collection Statistics	
Collection State	State of the summary collection operation.
Summaries collected	Number of summaries collected. Summaries are packet digests of the traffic that is being monitored.
Summaries dropped	Total number of summaries dropped. This is the sum of the following subcategories.
Dropped by TFO	Number of packets that were dropped by TFO because of an error, such as not being able to allocate memory.

Table 3-105 Field Descriptions for the show statistics flow monitor Command (continued)

Field	Description
Dropped due to backlog	Number of packets that were dropped because the queue limit has been reached. This counter indicates whether the flow monitor application can keep up with the number of summaries being received.
Summary backlog	Number of packets that are waiting in the queue to be read by the collector module on the WAE.
Last drop occurred	Date and time that the last packet drop occurred.

Related Commands

clear arp-cache

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 3-106 describes the fields shown in the **show statistics generic-gre** command display.

Table 3-106 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 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 3-107 describes the fields shown in the **show statistics icmp** command display.

Table 3-107 Field Descriptions for the show statistics icmp Command

Field	Description
ICMP messages received	Total number of Internet Control Message Protocol (ICMP) messages which the entity received, including all those counted as ICMP input errors.
ICMP messages receive failed	Number of ICMP messages which the entity received but determined as having ICMP-specific errors, such as bad ICMP checksums, bad length, and so forth.
Destination unreachable	Number of ICMP messages of this type received.
Timeout in transit	Number of ICMP messages of this type received.
Wrong parameters	Number of ICMP messages of this type received.
Source quenches	Number of ICMP messages of this type received.
Redirects	Number of ICMP messages of this type received.
Echo requests	Number of ICMP messages of this type received.
Echo replies	Number of ICMP messages of this type received.
Timestamp requests	Number of ICMP messages of this type received.
Timestamp replies	Number of ICMP messages of this type received.
Address mask requests	Number of ICMP messages of this type received.
Address mask replies	Number of ICMP messages of this type received.

Table 3-107 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 icmp6

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 3-108 describes the fields shown in the **show statistics icmp6** command display.

Table 3-108 Field Descriptions for the show statistics icmp6 Command

Field	Description
ICMP6 messages received	Total number of Internet Control Message Protocol (ICMP) messages which the entity received, including all those counted as ICMP6 input errors.
ICMP6 messages receive failed	Number of ICMP6 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 ICMP6 messages that can not be delivered to its destination address for reasons other than congestion.
Large packets	Number of ICMP6 messages that have packets larger than the MTU size specified.
Timeout in transit	Number of ICMP6 messages that failed to reach its destination due to extra time taken during transit, than the set limit.
Wrong parameters	Number of ICMP6 messages with erroneous parameters in its header etc.
Echo requests	Number of echo requests sent during the ping request to check and confirm the connectivity to the neighbor device.
Echo replies	Number of echo replies generated in response to the echo request.
Group member queries	Number of groups who would want to receive the ICMP6 packets

Table 3-108 Field Descriptions for the show statistics icmp6 Command (continued)

Field	Description
Group member responses	Number of groups who would want to receive the ICMP6 packets
Group member reductions	
Router solicits	Number of router solicitations messages sent by host in order to prompt routers to generate router advertisements
Router advertisements	Number of periodic router advertisement messages or in response to a router solicitation.
Neighbor solicits	Neighbor solicitation messages to request the link-layer address of a target device while also providing their own link-layer address to the target.
Neighbor advertisements	Number of neighbor advertisements in response to neighbor solicitations.
Redirects	Number of neighbor redirect messages of this type received.
MLDv2 reports	Type of Multicast Listener Discovery v2 message.
Type 134	Number of advertisement messages sent out.
ICMP6 messages sent	Total total number of ICMP6 messages which this entity attempted to send. This counter includes all those counted as ICMP output errors.
Destination unreachable	Number of ICMP6 sent messages that can not be delivered to its destination address for reasons other than congestion.
Large packets	Number of ICMP6 messages that have packets larger than the MTU size specified.
Time exceeded	Number of ICMP messages of this type sent out.
Wrong parameters	Number of ICMP messages of this type sent out.
Echo requests	Number of echo requests sent during the ping request it to check and confirm the connectivity to the neighbor device.
Echo replies	Number of echo replies generated in response to the echo request.
Group member queries	Number of ICMP messages of this type sent out.
Group member responses	Number of ICMP messages of this type sent out.
Group member reductions	Number of ICMP messages of this type sent out.
Router solicits	Number of ICMP messages of this type sent out.
Router advertisements	Number of ICMP reply Packet from the device to neighbor.
Neighbor solicits	Number of ICMP request to the neighbor device.
Neighbor advertisements	Number of responses from the device against the request coming from the client device.
Redirects	Number of neighbor redirect messages of this type received.
MLDv2 reports	Type of Multicast Listener Discovery v2 message.
Type 133	Number of Neighbor advertisement message sent out.

Table 3-108 Field Descriptions for the show statistics icmp6 Command (continued)

Field	Description
Type 135	Number of Neighbor solicits message sent out.
Type 143	Number of Home Agent Address Discovery message send 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 3-109 describes the fields shown in the **show statistics ip** command display.

Table 3-109 Field Descriptions for the show statistics ip Command

Field	Description
IP statistics	
Total packets in	Total number of input datagrams received from interfaces, including all those counted as input errors.
with invalid address	Number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as 0.0.0.0) and addresses of unsupported classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
with invalid header	Number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatches other format errors, time-to-live exceeded errors, and errors discovered in processing their IP options.
forwarded	Number of input datagrams for which this entity was not their final IP destination, and as a result, an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were source-routed by way of this entity, and the source-route option processing was successful.

Table 3-109 Field Descriptions for the show statistics ip Command (continued)

Field	Description
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).
Total packets out	Total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
dropped	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (such as, for lack of buffer space). This counter includes datagrams counted in the forwarded field if any such packets meet this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in the forwarded field which meet this no-route criterion, including any datagrams that a host cannot route because all of its default gateways are down.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Total number of IP datagrams that have been successfully fragmented at this entity.
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented because their Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Related Commands

clear arp-cache

(config) ip

(config-if) ip

show ip routes

show statistics ipv6

To display IPv6 statistics for a WAAS device, use the **show statistics ipv6** EXEC command.

show statistics ipv6 internal

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-110 describes the fields shown in the **show statistics ipv6 internal** command display.

Table 3-110 Field Descriptions for the show statistics ipv6 Command

Field	Description
IPv6 statistics internal	
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 large errors	Number of error messages sent by the device.
with invalid headers	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.
dropped (no route)	Number of packets dropped on device without knowing the destination device.
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
truncated packets	Number of modified packet without any acknowledgment.

Table 3-110 Field Descriptions for the show statistics ipv6 Command (continued)

Field	Description
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).
multicast packets	Total number of multicast packets.
octets	Total number of octets
multicast octets	Total number of multicast octets in the IPv6 packet.
broadcast octets	Total number of broadcast octets in the IPv6 packet
Total packets out forwarded	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.
requests	Total number of requests received of the above type.
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.
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.
multicast packets	Total number of multicast packets out forwarded.
octets	Total number of octets out forwarded.
multicast octets	Total number of multicast octets in the out forwarded packets.
broadcast octets	Total number of broadcast octets in the out forwarded packets.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Total number of IP datagrams that have been successfully fragmented at this entity.

Table 3-110 Field Descriptions for the show statistics ipv6 Command (continued)

Field	Description
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

(config) ip

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 3-111 describes the fields shown in the **show statistics netstat** command display.

Table 3-111 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 object-cache

To display a list of statistics use the **show statistics object-cache** EXEC command.

show statistics object-cache [accelerator *ao-name***] {server-ip** *server-ip* **| server-host** *hostname* **| url** *path* **} [detail]**

Syntax Description

accelerator *ao-name*	(Optional) The name of the application accelerator specified, such as SMB or MAPI.
server-host *hostname*	Displays a list of individual objects in the cache for the specified server hostname.
server-ip *server-ip*	Displays a list of individual objects in the cache for the specified server IP address.
url *path*	Displays a list of individual objects in the cache for the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).
detail	(Optional) Displays detailed statistics for the object cache. x shows field descriptions for **show statistics object-cache detail**.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics object-cache** command to display statistics for the cache. You can display all statistics, or

Examples

The following is sample output from the **show statistics object-cache** command:

```
Object Cache Storage Assigned: 236.00 GB, Used: 0.00 GB

    Objects Created: 0
    Objects Deleted: 0
    Objects Evicted: 0
    Max Objects: 1, 0.00 GB
    Current Objects 1, 0.00 GB

          Creating: 0
          Created: 1
          Complete: 0
          Pending Delete: 0
          Updating: 0
```

```
Objects by size:

     0 - 32K:       1
     32KB - 256KB:  0
     256KB - 1MB:   0
     1MB - 10MB:    0
     10MB - 100MB:  0
     100MB - 1GB:   0
     Over 1GB:      0
```

Table 3-112 describes the fields shown in the **show statistics object-cache** command display.

Table 3-112 Field Descriptions for the show statistics object-cache Command

Field	Description
Object Cache Storage Assigned	Total disk space assigned for the object cache disk cache.
(Object Cache Storage Assigned) Used	Total disk space currently used by objects on the disk.
Objects Created	Total number of objects created.
Objects Deleted	Total number of objects deleted by the AO.
Objects Evicted	Total number of objects evicted by the garbage collector.
Max Objects	Maximum number of objects in the object cache at any given point of time.
Current Objects	Current number of objects.
SMB Objects	Total number of objects created by the SMB AO.

Related

(config) accelerator object-cache enable

(config) object-cache enable

show cache object-cache

show object-cache

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 3-113 describes the fields shown in the **show statistics pass-through** command display.

Table 3-113 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.
PT In Progress: Bytes	Number of bytes passed through in progress.
PT In Progress: Packets	Number of packets passed through in progress.
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.
Rjct No License	Number of connections passed through due to no license.
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).

Table 3-113 Field Descriptions for the show statistics pass-through Command (continued)

Field	Description
In Progress	Number of connections passed through due to connections seen by the WAE mid-stream.
Intermediate	Number of connections passed through because the WAE was in between two other WAEs.
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.
Peer Override	Number of connections passed through due to an upstream serial peer handling optimization and telling this WAE not to optimize the connection.
Bad AD Options	Number of connections passed through due to invalid auto discovery options.
Non-optimizing Peer	Number of connections passed through because the only peer found is configured as a non-optimizing serial peer.
Interception ACL	Number of connections passed through due to an interception ACL denying them.

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

dre	Displays the peer DRE statistics.
context *context-value*	Displays peer statistics for the specified context (0–4294967295).
peer-id *peer-id*	(Optional) Specifies the MAC address of the peer (0–4294967295).
peer-ip *ip_address*	(Optional) Specifies the IP address of the peer.
peer-no *peer-no*	(Optional) Specifies the peer number.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-114 describes the fields shown in the **show statistics peer dre detail** command display. This command shows the peer DRE device connection information.

Table 3-114 Field Descriptions for the show statistics peer dre detail Command

Field	Description
Current number of peers with active connections	Number of peer devices with active connections to this device.
Maximum number of peers with active connections	Maximum number of peer devices with active connections to this device (since reboot).
Active peer details	
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.
IP reported from peer	IP address reported from the peer device.

Table 3-114 Field Descriptions for the show statistics peer dre detail Command (continued)

Field	Description
Cache	DRE cache data statistics as shown by the peer.
Used disk:	Number of megabytes (MB) used on the disk for the DRE cache.
Age:	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s).
Connections:	
Total (cumulative):	Number of cumulative connections that have been processed.
Active:	Number of connections that are still open.
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. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for compression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for compression.
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Decode	Statistics for decompressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for decompressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were decompressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for decompression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for decompression.

Table 3-114 Field Descriptions for the show statistics peer dre detail Command (continued)

Field	Description
Latency (Last 3 sec): [max | avg]	Maximum time to decompress one message for both DRE and LZ in milliseconds (ms). Average time to decompress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Connection details	
Encode bypass due to: last partial chunk	Number of bypassed partial chunks and total size of bypassed chunks.
Nacks: total	Total NACKs.
R-tx: total	Total number of retransmissions.
Encode LZ latency: ms per msg, avg msg size	Encoding LZ latency in milliseconds per message and average message size in bytes.
Decode LZ latency: ms per msg, avg msg size	Decoding LZ latency in milliseconds per message and average message size in bytes.
Cache write detail	
Disk size saving due to unidirectional mode	Amount of cache disk space saved due to using unidirectional caching mode.

Related Commands

show statistics connection closed

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 3-115 describes the fields shown in the **show statistics radius** command display.

Table 3-115 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 3-115 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 service-insertion

To display statistics about the entities (WNs, WNGs, ANCs, ANCG, and a service context) defined in an AppNav Cluster configuration, use the **show statistics service-insertion** EXEC command.

show statistics service-insertion {**appnav-controller** *ip_address* | **appnav-controller-group** [**detail**] | **data-path** | **service-context** | **service-node** [*ip_address*] | **service-node-group** [**detail** | **name** *sng-name*]}

Syntax Description

appnav-controller *ip_address*	(Optional) Displays statistics about the specified ANC.
appnav-controller-group	(Optional) Displays ANCG statistics for the service context.
detail	(Optional) Displays detailed statistics.
data-path	(Optional) Displays data path statistics.
service-context	(Optional) Displays service context statistics.
service-node	(Optional) Displays service node (WN) statistics.
ip_address	(Optional) Displays service node statistics of the specified node.
service-node-group	(Optional) Displays statistics for all the service node groups (WNGs) in the service context.
name *sng-name*	(Optional) Displays statistics of the specified node group (WNG).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Related Commands

show statistics appnav-controller

show service-insertion

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 3-116 describes the fields shown in the **show statistics services** command display.

Table 3-116 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 sessions

To display the dynamic match session statistics, use the **show statistics sessions** EXEC command.

show statistics sessions [**detail**] [**app-id** {*app-id* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**}]

Syntax Description

detail	(Optional) Displays the detailed session statistics for all of the dynamic match sessions or for the specified traffic type.
app-id *app-id*	(Optional) Displays the session statistics for dynamic matched flows for the application with the specified application number (0-1023) or the specified traffic type.
mapi **ms-ad-rep** **ms-exch-nspi** **ms-frs** **ms-frs-api** **ms-rfr** **ms-sql** **msn-messenger** **netlogon**	Microsoft Exchange MAPI aka Exchange Server Store EMSMDB, Microsoft Active Directory Replication (drsuapi), Microsoft Active Directory Name Service Provider (NSP), Microsoft File Replication Services (FRS), Microsoft File Replication API, Microsoft Exchange Directory RFR Interface, Microsoft SQL, Microsoft Messenger Service, Netlogon RPC

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **show statistics sessions** command displays session statistics for all the dynamic matched flows. You can optionally specify an application ID or traffic type identifier to see session statistics for only that traffic type.

The **show statistics sessions details** command displays detailed session statistics for all the dynamic matched flows. You can optionally specify an application ID or traffic type identifier to see detailed session statistics for only that traffic type.

Related Commands

(config) policy-map

show class-map

show policy-map

show policy-sub-class

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 3-117 describes the fields shown in the **show statistics snmp** command display.

Table 3-117 Field Descriptions for the show statistics snmp Command

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.

Table 3-117 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 system cpu

To display the detailed parameters of the cpu utilization, use the **show statistics system cpu** EXEC command.

show statistics system cpu

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 system cpu** command to display statistics for the system cpu utilization.

Examples

The following is sample output from the **show statistics system cpu** command:

```
WAE# show statistics system cpu
CPU overload protection params:
State:                      Normal
CPU utilization:
   samples average:         8%
   current probe:           8%
Config thresholds:
   high:                    98%
   low:                     90%
Config sampling window:     4 samples
Sampling intervals in secs:
   current:                 10
   config (normal state):   10
   config (overload state): 30
```

Table

Field	Description
State	The current system-level state-- normal, overloaded or disabled. When the CPU utilization percentage is lower than the threshold used, it is in the normal state; otherwise it is overloaded. When this functionality is disabled through its CLI "no threshold-monitor system cpu enable", this state would become disabled.
CPU utilization	

Field	Description
samples average	The reading obtained from Linux during last sampling time by the system.
current probe	The reading taken right after executing this show command. When the sampling window is wide, this reading shows the value between the sampling instances.
Config thresholds	
high	The configured high threshold above which the system goes into the overloaded state when it is normal. But in the overloaded state, it doesn't go back to the normal state until the CPU utilization goes below the low threshold.
low	The configured low threshold below which the system goes into the normal state when it is overloaded. But in the normal state, it doesn't transition into the overloaded state until the CPU utilization goes above the high threshold.
Config sampling window	The configured sampling window size for the moving average. The number of the most recent CPU utilization samples taken in calculating the latest CPU utilization percentage.The result is the average of the given number of samples.
Sampling intervals in secs	
current	When the show command is issued, usually the Sysload is in the inactive state between sampling moments. The current sample rate determines the duration of the current inactive state. The duration can be different from the configured sampling rate, if the configured values are changed between sampling instances before the current inactive state expires.
config (normal state)	The configured sampling rate for the normal state.
config (overload state)	The configured sampling rate for the overloaded state.

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 3-118 describes the fields shown in the **show statistics tacacs** command display.

Table 3-118 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 3-118 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

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 3-119 describes the fields shown in the **show statistics tcp** command display.

Table 3-119 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 3-119 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.

Table 3-119 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 3-119 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
TCP Reno recovery fail	Number of TCP Reno recovery failures.
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

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*]

Syntax Description

connection	(Optional) Displays aggregated TFO connection statistics.
detail	(Optional) Displays detailed TFO statistics.
peer	(Optional) Displays DRE peer statistics.
peer-id *peer-id*	(Optional) Displays peer statistics for peer ID.
peer-ip *peer-ip*	(Optional) Displays peer statistics for peer IP.
peer-no *peer-no*	(Optional) Displays peer statistics for peer number.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-120 describes the fields shown in the **show statistics tfo** command. The Policy Engine Statistics and Auto-Discovery Statistics sections are displayed only when you use the **detail** option.

Table 3-120 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	Socket between two WAEs (WAN socket) closed before completing writing into it.
AO socket close while waiting to write	Socket between the WAE and the client/server (LAN socket) closed before completing writing into it.

Table 3-120 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
WAN socket error close while waiting to read	Socket between two WAEs (WAN socket) closed before completing reading from it.
AO socket error close while waiting to read	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	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.
AckQ Control	Shows the total and current number of connections blocked due to a full ack queue.
Scheduler	Scheduler queue sizes and number of jobs processed by each queue.
Policy Engine Statistics	
Session timeouts	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.

Table 3-120 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
Total timeouts	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	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the TFO component registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with TFO enabled • Restart of the TFO component by the Node Manager
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: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use TFO. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched

Table 3-120 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
Auto-Discovery Statistics	
Total connections queued for accept	Total number of connections added to the TFO connection accept queue by auto discovery.
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

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 3-121 describes the fields shown in the **show statistics udp** command display.

Table 3-121 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

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 output of this command differs depending on the device mode of the WAE.

Examples

Table 3-122 describes the fields shown in the **show statistics wccp gre** command display for an application accelerator device.

Table 3-122 Field Descriptions for the show statistics wccp Command on a WAE

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 non-WCCP packets received	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.

Table 3-122 Field Descriptions for the show statistics wccp Command on a WAE (continued)

Field	Description
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. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.

Table 3-122 Field Descriptions for the show statistics wccp Command on a WAE (continued)

Field	Description
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.
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 received on loopback	Number of packets that are dropped by the WAE because they were received on the loopback interface.

Table 3-122 Field Descriptions for the show statistics wccp Command on a WAE (continued)

Field	Description
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).
Packets fragmented for bypass	Number of bypass GRE packets that do not contain enough data to hold an IP header.
Packets fragmented for egress	Number of egress 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.
WCCP Loop Packets detected	Number of WCCP loop packets detected.
WCCP Loop Packets dropped	Number of WCCP loop packets dropped.

Table 3-123 describes the fields shown in the **show statistics wccp** command display for an ANC device.

Table 3-123 Field Descriptions for the show statistics wccp Command on an ANC

Field	Description
WCCP Stats for Router	Router address. This section appears for each WCCP router.
Packets Received from Router	Packets received from the router.
Bytes Received from Router	Bytes received from the router.
Packets Transmitted to Router	Packets sent to the router.
Bytes Transmitted to Router	Bytes sent to the router
Pass-thru Packets sent to Router	Pass-through packets sent to the router.
Pass-thru Bytes sent to Router	Pass-through bytes sent to the router.
Redirect Packets sent to SN	Redirect packets sent to WAAS nodes (WNs) for optimization.
Redirect Bytes sent to SN	Redirect bytes sent to WNs.
Cummulative WCCP Stats	Cumulative statistics for all WCCP routers.
Total Packets Received from all Routers	Total packets received from all routers.
Total Bytes Received from all Routers	Total bytes received from all routers.
Total Packets Transmitted to all Routers	Total packets sent to all routers.
Total Bytes Transmitted to all Routers	Total bytes sent to all routers.

Table 3-123 Field Descriptions for the show statistics wccp Command on an ANC

Field	Description
Total Pass-thru Packets sent to all Routers	Total pass-through packets sent to all routers.
Total Pass-thru Bytes sent to all Routers	Total pass-through bytes sent to all routers.
Total Redirect Packets sent to SN	Total redirect packets sent to all WNs.
Total Redirect Bytes sent to SN	Total redirect bytes sent to all WNs.

Related Commands

(config) wccp access-list

(config) wccp router-list

(config) wccp router-list

(config) wccp shutdown

(config) wccp tcp-promiscuous service-pair

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 3-124 describes the fields shown in the **show statistics windows-domain** command display.

Table 3-124 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.

Table 3-124 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 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 3-125 describes the fields shown in the **show sysfs volumes** command display.

Table 3-125 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 3-126 describes the fields shown in the **show tacacs** command display.

Table 3-126 Field Descriptions for the show tacacs Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for authorization or configuration authentication.
TACACS+ Configuration	TACACS+ server parameters.
TACACS+ Authentication	Indicates whether TACACS+ authentication is enabled on the the WAAS device.
Key	Secret key that the WAE uses to communicate with the TACACS+ server. The maximum length of the TACACS+ key is 32 characters.
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.
Server	Hostname or IP address of the TACACS+ server.

Table 3-126 Field Descriptions for the show tacacs Command (continued)

Field	Description
Port	Port number 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 3-127 describes the fields shown in the **show tcp** command display. This command displays the settings configured with the **tcp** global configuration command.

Table 3-127 Field Descriptions for the show tcp Command

Field	Description
TCP Configuration	
TCP keepalive timeout XX sec	Length of time that the WAAS device is set to keep a connection open before disconnecting.
TCP keepalive probe count X	Number of times the WAAS device will retry a connection before the connection is considered unsuccessful.
TCP keepalive probe interval XX sec	Length of time (in seconds) that the WAAS device is set to keep an idle connection open.
TCP explicit congestion notification disabled	Configuration status of the TCP explicit congestion notification feature. Values are enabled or disabled.
TCP cwnd base value X	Value (in segments) of the send congestion window.
TCP initial slowstart threshold value X	Threshold (in segments) for slow start.
TCP increase (multiply) retransmit timer by X	Number of times set to increase the length of the retransmit timer base value.
TCP memory_limit	
Low water mark	Lower limit (in MB) of memory pressure mode, below which TCP enters into normal memory allocation mode.
High water mark (pressure)	Upper limit (in MB) of normal memory allocation mode, beyond which TCP enters into memory pressure mode.
High water mark (absolute)	Absolute limit (in MB) on TCP memory usage.

Related Commands

clear 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**]

Syntax Description

page	(Optional) Displays command output page by page.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show tech-support** 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 **(config) logging console** command.)

Examples

The following is sample output from the **show tech-support** command:

Note Because the **show tech-support** command output can be long, excerpts are shown in this example.

```
WAE# show tech-support
------------------ version and hardware --------------------

Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
...
Version: ce510-4.0.0.180

Compiled 18:08:17 Feb 16 2006 by cnbuild

System was restarted on Fri Feb 17 23:09:53 2006.
The system has been up for 5 weeks, 3 days, 2 hours, 9 minutes, 49 seconds.

CPU 0 is GenuineIntel Intel(R) Celeron(R) CPU 2.40GHz (rev 2) running at 2401MHz
.
Total 1 CPU.
512 Mbytes of Physical memory.
...
BIOS Information:
Vendor                             : IBM
Version                            : -[PLEC52AUS-C.52]-
Rel. Date                          : 05/19/03
...
```

```
List of all disk drives:
Physical disk information:

  disk00: Normal                (IDE disk)                 76324MB( 74.5GB)
  disk01: Normal                (IDE disk)                 76324MB( 74.5GB)


Mounted filesystems:

  MOUNT POINT       TYPE       DEVICE          SIZE    INUSE     FREE USE%
  /                 root       /dev/root       31MB     26MB      5MB  83%
  /sw               internal   /dev/md0       991MB    430MB    561MB  43%
  /swstore          internal   /dev/md1       991MB    287MB    704MB  28%
  /state            internal   /dev/md2      3967MB     61MB   3906MB   1%
  /disk00-04        CONTENT    /dev/md4     62539MB     32MB  62507MB   0%
  /local/local1     SYSFS      /dev/md5      3967MB    197MB   3770MB   4%
  .../local1/spool  PRINTSPOOL /dev/md6       991MB     16MB    975MB   1%


Software RAID devices:

  DEVICE NAME  TYPE     STATUS                PHYSICAL DEVICES AND STATUS
  /dev/md0     RAID-1   NORMAL OPERATION      disk00/00[GOOD]  disk01/00[GOOD]
  /dev/md1     RAID-1   NORMAL OPERATION      disk00/01[GOOD]  disk01/01[GOOD]
/dev/md0     RAID-1   NORMAL OPERATION      disk00/00[GOOD]  disk01/00[GOOD]
  /dev/md1     RAID-1   NORMAL OPERATION      disk00/01[GOOD]  disk01/01[GOOD]
  /dev/md2     RAID-1   NORMAL OPERATION      disk00/02[GOOD]  disk01/02[GOOD]
...
Currently content-filesystems RAID level is not configured to change.


------------------ running configuration -------------------

! WAAS version 4.0.0
!
!
...
------------------ processes --------------------

CPU average usage since last reboot:
   cpu: 0.00% User,  1.79% System,  3.21% User(nice),  95.00% Idle
--------------------------------------------------------------------
 PID  STATE PRI User T  SYS T        COMMAND
----- ----- --- ------ ------ --------------------
    1    S    0  20138  21906 (init)
    2    S    0      0      0 (migration/0)
    3    S   19      0      0 (ksoftirqd/0)
    4    S  -10      0      0 (events/0)
    5    S  -10      0      0 (khelper)
   17    S  -10      0      0 (kacpid)
   93    S  -10      0      0 (kblockd/0)
...
```

Related Commands

show version

show hardware

show disks details

show running-config

show processes

show processes memory

show memory

show interface

show cdp entry

show cdp neighbors

show statistics wccp

show alarms all

show statistics auto-discovery

show statistics ip

show statistics icmp

show statistics netstat

show statistics peer

show statistics tfo

show disks SMART-info

show disks SMART-info details

show disks failed-sectors

show telnet

To display Telnet services configuration for a WAAS device, use the **show telnet** EXEC command.

show telnet

Syntax Description

This command has no arguments or keywords.

Defaults

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

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 tfo tcp** command. It displays TCP buffer information for the WAE.

```
WAE# show tfo tcp
Maximum Segment Size:
   Configured:
         Optimized MSS                      : 1432 bytes
         Original MSS                       : 1432 bytes
   Default:
         Optimized MSS                      : 1432 bytes
         Original MSS                       : 1432 bytes

Buffer Sizing Status:
   Configured:
      Adaptive buffer sizing                : enabled
         Maximum receive buffer size        : 8192 KB
         Maximum orig side receive buf size : 256 KB (capped)
         Maximum send buffer size           : 8192 KB
      Fixed buffer sizing                   : disabled
         Optimized side receive buffer size : 2048 KB
         Optimized side send buffer size    : 2048 KB
         Original side receive buffer size  : 32 KB
         Original side send buffer size     : 32 KB
   Default:
      Adaptive buffer sizes                 :
         Maximum receive buffer size        : 8192 KB
         Maximum send buffer size           : 8192 KB
      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

TFO Status:
   Adaptive buffer sizing is enabled
```

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

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.

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
--------------------------------------------------------------
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

show user

To display user identification number and username information for a particular user of a WAAS device, use the **show user** EXEC command.

show user {**uid** *number* | **username** *name*}

Syntax Description

uid *number*	Displays user information based on the identification number of the user (0–65535).
username *name*	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 3-128 describes the fields shown in the **show user** command display.

Table 3-128 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**]

Syntax Description

administrative	Displays a list of users defined on the device.
history	(Optional) Displays a historical list of user log-ins.
locked-out	(Optional) Displays a list of locked out users.
logged-in	(Optional) Displays a list of users that are logged in.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-129 describes the fields shown in the **show users administrative history** command display.

Table 3-129 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. When windows domain authentication is enabled, a space in the windows domain username is replaced by the "+" symbol in the output.
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.
Loggin details	Day of the week, month, date, time, and whether or not the user is still logged in.

Table 3-130 describes the fields shown in the **show users administrative logged-in** command display.

Table 3-130 Field Descriptions for the show users administrative logged-in Command

Field	Description
Username	Users currently logged in to the appliance CLI. When windows domain authentication is enabled, a space in the windows domain username is replaced by the "+" symbol in the output.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that is logged in to this appliance.
Loginn 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**]

Syntax Description

last	(Optional) Displays the version information for the last saved image.
pending	(Optional) Displays the version information for the pending upgraded image.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-131 describes the fields shown in the **show version** command display.

Table 3-131 Field Descriptions for the show version Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) *year* by Cisco Systems, Inc. Cisco Wide Area Application Services (universal-k9) Software Release XXX (build b*XXX* month day year)	Software application, copyright, release, and build information. Displays universal-k9 for the full software image, accelerator-k9 for the accelerator only software image, and universal-npe-k9 or accelerator-npe-k9 for the NPE versions of those images. The NPE image versions have the disk encryption feature disabled for use in countries where disk encryption is not permitted.
Version	Version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Compiled information for the software build.
Device Id	Hardware device ID.
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	Length of time the system has been running since the last reboot.

show wccp

To display Web Cache Connection Protocol (WCCP) information for a WAE, use the **show wccp** EXEC command.

show wccp clients

show wccp egress

show wccp flows tcp-promiscuous [**summary**]

show wccp masks tcp-promiscuous

show wccp routers [**detail**]

show wccp services [**detail**]

show wccp statistics

show wccp status

Syntax Description

clients	Displays which WAEs are seen by which routers.
egress	Displays WCCP egress methods.
flows	Displays WCCP packet flows. This option is not available on ANCs
tcp-promiscuous	Displays TCP-promiscuous service information.
summary	(Optional) Displays summarized information about TCP-Promiscuous caching service packet flows.
masks	Displays WCCP mask assignments for a given service.
routers	Displays routers seen and not seen by this WAE.
services	Displays WCCP services configured.
detail	(Optional) Displays details of routers or services.
statistics	Displays WCCP generic routing encapsulation packet-related information.
status	Displays the enabled state of WCCP and the configured service IDs.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-132 describes the fields shown in the **show wccp statistics** command display.

Table 3-132 Field Descriptions for the show wccp statistics 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 non-WCCP packets received	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. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts on non-owned bucket	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.

Table 3-132 Field Descriptions for the show wccp statistics 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.
GRE packets sent to router (not bypass)	Number of GRE packets that are sent back from the WAE to the router from which the request was redirected, and are not bypass traffic.
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.

Table 3-132 Field Descriptions for the show wccp statistics Command (continued)

Field	Description
Connections bypassed during 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.
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.
L2 Bypass packets destined for loopback	Number of packets that were bypassed 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.
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 received on loopback	Number of packets that are dropped by the WAE because they were received on the loopback interface.
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).
Packets fragmented for bypass	Number of bypass GRE packets that do not contain enough data to hold an IP header.
Packets fragmented for egress	Number of egress 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.
WCCP Loop Packets detected	Number of WCCP loop packets detected.
WCCP Loop Packets dropped	Number of WCCP loop packets dropped.

The following is sample output from the **show wccp clients** command:

```
WAE# show wccp clients
Wide Area Engine List for Service: 61
Number of WAE's in the Cache farm: 2
        IP address = 10.75.152.131       Lead WAE = NO   Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226

        IP address = 10.75.152.130       Lead WAE = YES  Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226

Wide Area Engine List for Service: 62
Number of WAE's in the Cache farm: 2
        IP address = 10.75.152.131       Lead WAE = NO   Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226

        IP address = 10.75.152.130       Lead WAE = YES  Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226
```

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
        Webcache ID                        : 10.43.65.52
        Service Enabled                    : Yes
        Service Priority                   : 34
        Service Protocol                   : 6
        Service Flags (in Hex)             : 501
        Weight for this Web-CE             : 0
        Redirect method                    : GRE
        Assignment method                  : MASK
        Return method (Auto Negotiated)  :GRE
        Egress method                      : IP-Forwarding
        Negotiated HIA interval            : 2.00 second(s)
        Negotiated failure-detection timeout  : 30.00 second(s)
        Negotiated RA timeout              : 15.00 second(s)
        Values configured:
        Source IP mask (in Hex)            : f00
        Destination IP mask (in Hex)       : 0
        Last Received Assignment Key IP address: 0.0.0.0
        Last Received Assignment Key Change Number: 0
        Flow Protection Enabled: NO
        Flow Protection Timeout: 0 secs
        Join Alarm Raised for service: NO
        Mask Mismatch Alarm Raised for service: NO
        Missing Assignment Alarm Raised for service: NO
        Farm Incompatible Alarm Raised for service: NO


Service Details for TCP Promiscuous 62 Service
        Webcache ID                        : 10.43.65.52
        Service Enabled                    : Yes
        Service Priority                   : 34
        Service Protocol                   : 6
        Service Flags (in Hex)             : 502
        Weight for this Web-CE             : 0
        Redirect method                    : L2
        Assignment method                  : MASK
       Return method (Auto Negotiated)   : L2
        Egress method                      : L2
        Negotiated HIA interval            : 2.00 second(s)
        Negotiated failure-detection timeout  : 30.00 second(s)
        Negotiated RA timeout              : 15.00 second(s)
        Values configured:
        Source IP mask (in Hex)            : 0
        Destination IP mask (in Hex)       : f00
        Last Received Assignment Key IP address: 0.0.0.0
        Last Received Assignment Key Change Number: 0
        Flow Protection Enabled: NO
        Flow Protection Timeout: 0 secs
        Join Alarm Raised for service: NO
        Mask Mismatch Alarm Raised for service: NO
        Missing Assignment Alarm Raised for service: NO
        Farm Incompatible Alarm Raised for service: NO
```

The following is sample output from the **show wccp routers** command:

```
WAE# show wccp routers
Router Information for Service Id: 61
        Routers Seeing this Wide Area Engine(1)
        Router Id       Sent To
        10.43.228.165    10.43.228.65
        Routers not Seeing this Wide Area Engine
        10.10.10.45    -Redirect Method Mismatch-
        Routers Notified of from other WAE's
                -NONE-

Router Information for Service Id: 62
        Routers Seeing this Wide Area Engine(1)
        Router Id       Sent To
        10.43.228.165    10.43.228.65
        Routers not Seeing this Wide Area Engine
        10.10.10.45    -Redirect Method Mismatch
        Routers Notified of from other WAE's
                -None-
```

The following is sample output from the **show wccp routers detail** command:

```
WAE# show wccp routers detail
Router Information for Service Id: 61

        Routers Seeing this Wide Area Engine(1)

  Router Id         Sent To         Recv ID  KeyIP           KeyCN    MCN

  10.75.152.226      10.75.152.129    03456469 10.75.152.130    1        233
        Transmit timer (ms): 0/0        Timer Scale: (0/0),(0/0)
        Last ISU received: 1/19/2012 00:09:51
        Output Interface IP Address: 10.75.152.130       Interface State: UP
        MAC Addr: 00:24:97:7a:d0:30

        Routers not Seeing this Wide Area Engine
                -NONE-

        Routers Notified of from other WAE's
                -NONE-
```

```
Router Information for Service Id: 62

        Routers Seeing this Wide Area Engine(1)

  Router Id          Sent To          Recv ID  KeyIP           KeyCN    MCN

  10.75.152.226       10.75.152.129    03433645 10.75.152.130    1        229
        Transmit timer (ms): 0/0        Timer Scale: (0/0),(0/0)
        Last ISU received: 1/19/2012 00:09:51
        Output Interface IP Address: 10.75.152.130       Interface State: UP
        MAC Addr: 00:24:97:7a:d0:30

        Routers not Seeing this Wide Area Engine
                -NONE-

        Routers Notified of from other WAE's
                -NONE-
```

The following is sample output from the **show wccp status** command:

```
WAE# show wccp status
WCCP Interception :
Configured State :  Enabled
Operational State : Enabled

Services Enabled on this WAE:
        TCP Promiscuous 61
        TCP Promiscuous 62
```

The Configured State refers to the state configured. The Operational State refers to the actual system state, which could differ from the configured state. For example, if an ANC is converging due to a cluster change, the system disables WCCP until convergence is completed.

The following is sample output from the **show wccp egress** command:

```
WAE# show wccp egress

        TCP Promiscuous Service : 61
        Egress Method in Use: L2

        TCP Promiscuous Service : 62
        Egress Method in Use: L2
```

Related Commands

(config) wccp access-list

(config) wccp router-list

(config) wccp router-list

(config) wccp shutdown

(config) wccp tcp-promiscuous service-pair

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.

Device Modes

application-accelerator

central-manager

Examples

Table 3-133 describes the fields shown in the **show windows-domain** command display.

Table 3-133 Field Descriptions for the show windows-domain Command

Field	Description
Login Authentication for Console/Telnet Session:	Status of the primary login authentication method for the session: enabled or disabled.
Configuration Authentication for Console/Telnet Session: enabled (secondary)	Status of the secondary login authentication method for the session:enabled or disabled.
Windows domain Configuration:	Shows the Windows domain configuration settings.
Workgroup	Workgroup identification string.
Comment	Comment line.
Net BIOS	Windows NetBIOS name for the WAE.
Realm	Kerberos Realm (similar to the Windows domain name, except for Kerberos).
WINS Server	IP address of the WINS server.
Password Server	Kerberos server DNS name.
Security	Type of authentication configured, either “Domain” for NTLM or “ADS” for Kerberos.
Administrative groups	
Super user group	Active Directory(AD) group name. Users in this group have administrative rights.
Normal user group	AD group name. Users in this group have the normal/default privilege level in the WAE.

Related Commands

windows-domain

(config) windows-domain

show windows-domain encrypted services

To display Windows domain encrypted services information for a WAAS device, use the **show windows-domain encrypted services** EXEC command.

show windows-domain encrypted services { identity [detail] | blacklist identity | status | keylist user }

Syntax Description

identity	Identity tag of the encryption service.
identity detail	Identity details including identity tag, account type, account name, domain, realm, status, and match domains.
blacklist identity	Identity tag, blacklist reason, and domain name.
status	Service name, configuration state (enabled or disabled), and operational state (running or
keylist user	Number of keys, maximum retrieval time (in milliseconds), average retrieval time (in milliseconds), and domain name.

Defaults

No default behavior or values.

Device Modes

application-accelerator

central-manager

Related Commands

windows-domain

(config) windows-domain

shutdown

To shut down the WAAS device, use the **shutdown** EXEC command.

shutdown [**poweroff**]

Syntax Description

poweroff	(Optional) Turns off the power after closing all applications and operating system.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

A controlled shutdown refers to the process of properly shutting down a WAAS device without turning off the power on the device. With a controlled shutdown, all of the application activities and the operating system are properly stopped on a WAE, but the power remains on. Controlled shutdowns of a WAAS device can help you minimize the downtime when the WAAS device is being serviced.

Caution If a controlled shutdown is not performed, the WAAS file system can be corrupted. Rebooting the WAAS device takes longer if it was not properly shut down.

Note A WAAS device cannot be powered on again through the WAAS software after a software poweroff. You must press the power button once on a WAAS device to bring it back online.

The **shutdown** EXEC command facilitates a proper shutdown for WAAS device, and is supported on all WAE hardware models. The **shutdown poweroff** command is also supported by all of the WAE hardware models as they support the ACPI.

The **shutdown** command closes all applications and stops all system activities, but keeps the power on. The fans continue to run and the power LED is on, indicating that the device is still powered on. The device console displays the following menu after the shutdown process is completed:

```
================ SHUTDOWN SHELL ================
System has been shut down.


You can
0. Power down system by pressing and holding power button
1. Reload system by software
2. Power down system by software
[1-2]?
```

The **shutdown poweroff** command closes all applications and the operating system, stops all system activities, and turn off the power. The fans stop running and the power LED starts flashing, indicating that the device has been powered off.

Note If you use the **shutdown** or **shutdown poweroff** commands, the device does not perform a file system check when you power on and boot the device the next time.

Table 3-134 describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

Table 3-134 Description of the shutdown Command Operations

Activity	Process
User performs a shutdown operation on the WAE	Shutdown poweroff `WAE# shutdown poweroff`
User intervention to bring WAE back online	After a shutdown poweroff, you must press the power button once to bring the WAAS device back online.
File system check	Is *not* 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 2) to shut down a WAAS device.

To shut down 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.
```

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* [**management**]

Syntax Description

options	Options to use with the **ssh** EXEC command. Options include the following: • 3des-cbc • 3des • blowfish • aes128-cbc • aes192-cbc • aes256-cbc • blowfish • blowfish-cbc • des • arcfour • cast128-cbc For more information about SSH, see RFC 4254. For more information on SSH and ciphers, see RFC 4253.
management	Uses the designated management interface for the SSH operation.

Defaults

By default, the Secure Shell (SSH) feature is disabled on a WAAS device.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication. The SSH client accepts both IPv4 and IPv6 addresses.

Note The Telnet daemon can still be used with the WAAS device. SSH does not replace Telnet.

Examples

The following example shows how to log in to a WAAS device using the SSH client:

```
WAE# ssh 10.11.55.2
```

Related Commands

telnet

(config) sshd

(config) ssh-key-generate

tcpdump

To dump network traffic, use the **tcpdump** EXEC command.

tcpdump [*LINE*]

Syntax Description

LINE	(Optional) Dump options. For more information see the "Usage Guidelines" section.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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.

Note

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 [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
                [ -E algo:secret ] [ -F file ] [ -i interface ] [ -r file ]
                [ -s snaplen ] [ -T type ] [ -w file ] [ -y datalinktype ]
                [ expression ]
```

You can use either linux interface port names (for example, eth0) or WAAS port names (for example, GigabitEthernet 1/0 port 80, or InlinePort 1/0 lan) to designate the interface from which you want to capture packets. You cannot specify an inlineGroup.

Examples

The following example shows how to start a network traffic dump to a file named *tcpdump.txt*:

```
WAE# tcpdump -w tcpdump.txt
```

Related Commands

less

packet-capture

ping

tethereal

traceroute

telnet

To log in to a WAAS device using the Telnet client, use the **telnet** EXEC command.

telnet {*hostname* | *ip-address*} [*portnum*] [**management**]

Syntax Description

hostname	Hostname of the network device.
ip-address	IP address (IPv4 or IPv6) of the network device.
portnum	(Optional) Port number (1–65535). The default port number is 23.
management	Uses the designated management interface for the Telnet operation.

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 management
```

Related Commands

ssh

(config) telnet enable

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal** EXEC command.

terminal {**length** *length* | **monitor** [**disable**]}

Syntax Description

length *length*	Sets the length of the display on the terminal (0–512). Setting the length to 0 means there is no pausing.
monitor	Copies the debug output to the current terminal.
disable	(Optional) Disables monitoring at this specified terminal.

Defaults

The default is 24 lines.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

When 0 is entered as the *length* parameter, the output to the screen does not pause. For all nonzero values of *length*, the -More- prompt is displayed when the number of output lines matches the specified *length* number. The -More- prompt is considered a line of output. To view the next screen, press the **Spacebar**. To view one line at a time, press the **Enter** key.

The **terminal monitor** command allows a Telnet session to display the output of the **debug** commands that appear on the console. Monitoring continues until the Telnet session is terminated.

For proper display of the **setup** command, leave the terminal length set to the default value of 24 lines.

Examples

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
```

Related Commands

All **show** commands.

test

To perform authentication and diagnostic tests for the Radius/Tacacs/Windows users, use the **test** EXEC command.

test aaa {**radius** | **tacacs** | **windows**} *username password*

Syntax Description

aaa	Performs authentication tests for the users trying to access the WAAS Central Manager or WAE.
radius	Uses the RADIUS server for authentication purposes.
tacacs	Uses the TACACS server for authentication purposes.
windows	Uses the Windows domain for authentication purposes.
username	Username for authentication.
password	Password for authentication.

Defaults

No default behavior or values.

Command Modes

EXEC mode

Device Modes

application-accelerator

central-manager

tethereal

To analyze network traffic from the command line, use the **tethereal** EXEC command.

tethereal [*LINE*]

Syntax Description

LINE	(Optional) Options. For more information see the “Usage Guidelines” and “Examples” sections.

Defaults

No default behavior values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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.When using the **-a** option to print heavy traffic to the screen, it can take significantly longer than the autostop duration to display the information on the screen. Wait for the command to finish. Displaying output to the console can take significantly longer than through telnet or SSH, therefore console display is not recommended.

When using the **-f** option with the host or not host filter expression, the wrong traffic may be captured with WCCP GRE encapsulated or VLAN traffic. With WCCP GRE traffic, tethereal sees only the outermost IP address, not the original IP address inside the encapsulated packets. Add the **proto 47** keyword into the **-f** filter expression to capture the correct traffic (protocol 47 is GRE traffic). Additionally, for VLAN traffic, add the **vlan** keyword into the **-f** filter expression so that VLAN traffic is parsed correctly.

When using the **-a** filesize option together with the **-R** option, tethereal may stop unexpectedly and print the message "Memory limit is reached" before reaching the specified autostop file size. In this case, the maximum memory limit for the command was reached before the autostop file size limit.

You can use either Linux interface port names (for example, eth0) or WAAS port names (for example, GigabitEthernet 1/0 port 80, or InlinePort 1/0 lan) to designate the interface from which you want to capture packets. You cannot specify an inlineGroup.

Examples

The following example shows how to display the options available with the WAAS **tethereal** command:

```
WAE# tethereal -h
tethereal: Setting virtual memory limit to 209715200
TShark 1.0.0
Dump and analyze network traffic.
See http://www.wireshark.org for more information.
```

```
Copyright 1998-2008 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Usage: tshark [options] ...

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
Capture output:
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
                           filesize:NUM - switch to next file after NUM KB
                              files:NUM - ringbuffer: replace after NUM files
Input file:
  -r <infile>              set the filename to read from (no pipes or stdin!)

Processing:
  -R <read filter>         packet filter in Wireshark display filter syntax
  -n                       disable all name resolutions (def: all enabled)
  -N <name resolve flags>  enable specific name resolution(s): "mntC"
  -d <layer_type>==<selector>,<decode_as_protocol> ...
                           "Decode As", see the man page for details
                           Example: tcp.port==8888,http
Output:
  -w <outfile|->           set the output filename (or '-' for stdout)
  -C <config profile>      start with specified configuration profile
  -F <output file type>    set the output file type, default is libpcap
                           an empty "-F" option will list the file types
  -V                       add output of packet tree        (Packet Details)
  -S                       display packets even when writing to a file
  -x                       add output of hex and ASCII dump (Packet Bytes)
  -T pdml|ps|psml|text|fields
                           format of text output (def: text)
  -e <field>               field to print if -Tfields selected (e.g. tcp.port);
                           this option can be repeated to print multiple fields
  -E<fieldsoption>=<value> set options for output when -Tfields selected:
     header=y|n            switch headers on and off
     separator=/t|/s|<char> select tab, space, printable character as separator
     quote=d|s|n           select double, single, no quotes for values
  -t ad|a|r|d|dd|e         output format of time stamps (def: r: rel. to first)
  -l                       flush standard output after each packet
  -q                       be more quiet on stdout (e.g. when using statistics)
  -X <key>:<value>         eXtension options, see the man page for details
  -z <statistics>          various statistics, see the man page for details

Miscellaneous:
  -h                       display this help and exit
  -v                       display version info and exit
  -o <name>:<value> ...    override preference setting
```

Related Commands

packet-capture

tcpdump

top

To view the current top CPU activities, use the **top** EXEC command.

top -hv | -cisS -d *delay* **-n** *iterations* **[-u** *user* **| -U** *user***] -p** *pid* **[,***pid* **...]**

Syntax Description

-h	Prints help information and exits.
-v	Prints version information and exits.
-c	Displays the command line instead of the command name only.
-i	Suppresses the display of any idle or zombie processes.
-s	Tells top to run in secure mode. This option disables the potentially dangerous interactive commands.
-S	(Optional) Specifies cumulative mode, where each process is listed with the CPU time it has spent. It also lists the CPU time of the dead children for each process.
-d *delay*	Specifies the delay between screen updates.
-n *iterations*	Specifies the number of iterations. Update the display this number of times and then exit.
-u *user*	Monitors only processes with the specified effective UID or username.
-p *pid*	(Optional) Monitors only those processes with the given process id. This option can be given up to twenty times. This option is not available interactively.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **top** command is a system-defined alias for the Linux **top** command, which displays and updates information about the top CPU processes. It provides a real-time view of the processor activity. It lists the most CPU-intensive tasks on the system, and provides an interactive interface for manipulating processes. It can sort the tasks by CPU usage, memory usage, and runtime.

The command runs in an interactive environment and you can interact with the output by pressing various keys. Press h or ? to display the following help for interactive commands:

```
Help for Interactive Commands - procps version 3.2.5
Window 1:Def: Cumulative mode Off.  System: Delay 3.0 secs; Secure mode Off.

  Z,B       Global: 'Z' change color mappings; 'B' disable/enable bold
  l,t,m     Toggle Summaries: 'l' load avg; 't' task/cpu stats; 'm' mem info
  1,I       Toggle SMP view: '1' single/separate states; 'I' Irix/Solaris mode
  f,o     . Fields/Columns: 'f' add or remove; 'o' change display order
  F or O  . Select sort field
  <,>     . Move sort field: '<' next col left; '>' next col right
  R       . Toggle normal/reverse sort
  c,i,S   . Toggle: 'c' cmd name/line; 'i' idle tasks; 'S' cumulative time
  x,y     . Toggle highlights: 'x' sort field; 'y' running tasks
  z,b     . Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
  u       . Show specific user only
  n or #  . Set maximum tasks displayed

  k,r       Manipulate tasks: 'k' kill; 'r' renice
  d or s    Set update interval
  W         Write configuration file
  q         Quit
          ( commands shown with '.' require a visible task display window )
Press 'h' or '?' for help with Windows,
any other key to continue
```

Examples

The following example shows how to display the options available with the WAAS **top** command:

```
WAE# top -h
    top: procps version 3.2.5
usage:  top -hv | -bcisS -d delay -n iterations [-u user | -U user] -p pid [,pid ...]
```

Note The **-b** option is not supported.

The following example shows an example of the interactive command output:

```
WAE# top
top - 17:54:02 up 9 days,  6:09,  1 user,  load average: 0.05, 0.17, 0.19
Tasks: 992 total,   1 running, 991 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.7% us,  2.3% sy,  4.0% ni, 91.1% id,  1.7% wa,  0.0% hi,  0.3% si
Mem:   1939124k total,  1528440k used,   410684k free,   159720k buffers
Swap:  2037624k total,      812k used,  2036812k free,   554824k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
28359 admin     20   0  2544 1584  808 R  1.3  0.1   0:00.29 top
 7694 admin     30  10 1448m 105m  15m S  0.7  5.6  19:33.74 java
 9312 admin     30  10  494m 173m  20m S  0.7  9.2   2:47.23 java
 6950 admin     30  10  684m 204m 4876 S  0.3 10.8  28:31.64 so_dre
 7702 admin     30  10  955m 121m  18m S  0.3  6.4   3:07.97 java
 8782 admin     30  10 1448m 105m  15m S  0.3  5.6   3:32.04 java
 8802 admin     30  10 1448m 105m  15m S  0.3  5.6   0:49.17 java
    1 admin     20   0  1488  540  468 S  0.0  0.0   0:06.78 init
    2 admin     15  -5     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 admin     RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 admin     15  -5     0    0    0 S  0.0  0.0   0:09.07 ksoftirqd/0
    5 admin     RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
```

Related Commands

show processes

traceroute

To trace the route between a WAAS device to a remote host, use the **traceroute** EXEC command.

traceroute [**management**] {*hostname* | *ip-address*} [**tcp-syn**]

Syntax Description

management	(Optional) Uses the designated management interface for the traceroute.
hostname	Name of remote host.
ip-address	IP (v4) address of remote host.
tcp-syn	(Optional) Sends TCP-SYN packets for trace routing instead of UDP

Defaults

No default behavior or 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  * * *
 . . .
```

Related Commands

ping

ping6

traceroute6

waas-tcptrace

traceroute6

To trace the route between a WAAS device to a remote host with an IPv6 address, use the **traceroute6** EXEC command.

traceroute6 [**management**] {*hostname* | *ip-address*}

Syntax Description

management	(Optional) Uses the designated management interface for the traceroute.
hostname	Name of remote host.
ip-address	IP v6 address of remote host.

Defaults

No default behavior or 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 **traceroute6** to find the route to a remote host, when either the hostname or the IP address is known.

If a device’s management interface is used to trace the route between two end systems using **traceroute6** and the management interface goes down, the communication will still succeed if the end device’s address is reachable from any other interface.

Examples

The following example shows how to trace the route between the WAAS device and a device with an IP address of 2013:1:1:2::4:

```
WAE# traceroute6 2013:1:1:2::4
traceroute to 2013:1:1:2::4 (2013:1:1:2::4) from 2013:1:1:10::5, 30 hops max, 24 byte
packets
1  2013:1:1:10::1 (2013:1:1:10::1)  0.326 ms  0.341 ms  0.313 ms
2  2013:1:1:1::1 (2013:1:1:1::1)  0.461 ms  0.255 ms  0.277 ms
3  2013:1:1:2::4 (2013:1:1:2::4)  0.569 ms  0.59 ms  0.389 ms
```

Related Commands

ping

ping6

traceroute

waas-tcptrace

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**}

Syntax Description

archive	Forces the archiving of the transaction log file.
export	Forces the archived transaction log files to be exported.
flow	Forces the archiving or exporting of the Traffic Flow Optimization (TFO) transaction log file.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows how to force the archiving of the TFO transaction log file on the WAE:

```
WAE# transaction-log force archive flow
```

Related Commands

show transaction-logging

type

To display a file, use the **type** EXEC command.

type *filename*

Syntax Description

filename	Name of file.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **type** command to display the contents of a file within any file directory on a WAAS device. The **type** command may be used to monitor features such as transaction logging or system logging (syslog).

Examples

The following example shows how to display the contents of the *syslog.txt* file:

```
WAE# type /local1/syslog.txt
```

Related Commands

cpfile

dir

lls

ls

pwd

rename

type-tail

To view a specified number of lines of the end of a log file, to view the end of the file continuously as new lines are added to the file, to start at a particular line in the file, or to include or exclude specific lines in the file, use the **type-tail** EXEC command.

type-tail *filename* [*line* | **follow** | **|** {**begin** *LINE* | **exclude** *LINE* | **include** *LINE*}]

Syntax Description

filename	File to be examined.
line	(Optional) Number of lines from the end of the file to be displayed (1–65535).
follow	(Optional) Displays the end of the file continuously as new lines are added to the file.
|	(Optional) Displays contents of the file according to the **begin**, **exclude**, and **include** output modifiers.
begin *LINE*	Identifies the line at which to begin file display. Specifies a regular expression to match in the file.
exclude *LINE*	Indicates lines that are to be excluded from the file display. Specifies a regular expression to match in the file.
include *LINE*	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 looks for a list of log files in the */local1* directory and then displays the last ten lines of the *syslog.txt* file. In this example, the number of lines to display is not specified, so the default of ten lines is used:

```
WAE# ls /local1
actona
core_dir
crash
```

```
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed

WAE# type-tail /local1/syslog.txt
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get https
equest throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/ftp connection 5
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/ftp' from dataserver
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get ftp-ov
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-11java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/http/perf/throughput/requests/sum' from dataserver
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: unable to get http r
quest throughput stats(error 4)
Apr 17 00:23:20 edge-wae-11 java: %CE-TBD-3-100000: WCCP_COND_ACCEPT: TU
LE DELETE conditional accept tuple {Source IP [port] = 0.0.0.0 [0]   Destinatio
 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
```

vm

To initialize the virtual machine after the VMware cloning operation, or to configure the host clock sync setting, use the **vm** EXEC command.

vm {{**clock-sync** {**disable** | **enable** | **status**} | **init**}

Syntax Description

clock-sync	Manually changes the host clock sync setting.
disable	Disables VM clock sync to host.
enable	Enables VM clock sync to host.
status	Displays the status of the VM clock sync to host setting.
init	Initializes the VM after the VMware cloning operation.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **vm** for vWAAS virtual machine operations. To speed up vWAAS deployments, you can create a clone of the vWAAS virtual machine. However, since the clone is an exact copy of the original vWAAS VM, you must use the **vm init** command to remove the certificate hash and the device registration information before the new vWAAS VM will register with the Central Manager.

You must reload the device after running **vm init**.

Use the **vm clock-sync** command to manually change the host clock sync setting without configuring NTP.

Examples

The following example shows how to initialize the virtual machine after the VMware cloning operation:

```
WAE# vm init
This command performs the following actions:
 - remove any network interface IP addresses,
 - deregister this device from CM, and
 - delete the machine's unique certificate hash.

Reload is REQUIRED to generate a new certificate hash
Continue?  (yes|no) [no]? yes
Interface Virtual 1/0 -> no ip address 2.1.6.116 255.255.255.0
Init complete.Reload the device to generate new certificate hash.
WAE#
```

Related Commands

cms

waas-tcptrace

To list all the WAAS devices in the path to a destination host, use the **waas-tcptrace** EXEC command.

waas-tcptrace *ip-address port*

Syntax Description

ip-address	IP address of the destination host.
port	Port to connect to on the destination host.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use **waas-tcptrace** to list all the WAAS devices in the path between the device on which this command is run and the specified destination host. The path is traversed in both directions.

This command returns the configured application accelerators, system policy, and effective system policy for each WAAS device found in the path, as well as the overall system policy for the connection.

You can use this command to find the overall policy applied to the connection and to find asymmetric paths.

Examples

The following example shows how to trace the route between the WAAS device and a destination host with an IP address of 2.75.227.50 on port 80:

```
WAE# waas-tcptrace 2.75.227.50 80
Response recieved from 2.75.227.137 on path TO destination...
Response recieved from 2.75.227.137 on path FROM destination ....

******************************************************************************************
******************************
Number of WAAS devices on the path TO 2.75.227.50 = 1
------------------------------------------------------------------------------------------
------------------------------
 IP               MAC                 AD Ver  Packet    Position  Device  Configured AO
Configured TFO    Derived TFO
------------------------------------------------------------------------------------------
------------------------------
 2.75.227.137      0:21:5e:28:e1:34    4      Regular   1         SN      HTTP
Optimize Full     Optimize Full
------------------------------------------------------------------------------------------
------------------------------
Number of WAAS devices on the path FROM 2.75.227.50 = 1
------------------------------------------------------------------------------------------
------------------------------
```

```
 IP               MAC                 AD Ver  Packet    Position  Device  Configured AO
Configured TFO    Derived TFO
------------------------------------------------------------------------------------------
------------------------------
 2.75.227.137      0:21:5e:28:e1:34    4      Regular   1         SN      HTTP
Optimize Full     Optimize Full
------------------------------------------------------------------------------------------
------------------------------
The derived TFO policy for this connection is Passthrough (No Peer)
******************************************************************************************
******************************
```

Related Commands

traceroute

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 join or leave a Windows domain or access the Windows domain utilities on a WAAS device, use the **windows-domain** EXEC command.

windows-domain join domain-name *domain* **[organization-unit** *org_unit*] **user** *username* [**debug**]

windows-domain leave [**user** *username*]

windows-domain diagnostics {**domain-controller** {**list** | **status | time** [**domain-name** *domain_name*]} | **encryption-service** {**get-key** *fqdn domain_name*} | **getent** | **group** {**gid** *gid_no* | **groupname** *groupname* | **username** *username*} | **machine-account-info** | **user** [**sid** *sid_name* | **uid** *user_no* | **username** *username*] | **verify join**}

Syntax Description

join	Joins a Windows domain.
domain-name *domain*	Specifies the domain to join.
organization-unit *org_unit*	(Optional) Specifies the organization unit of the domain.
user *username*	Specifies a user that has the permission to create a machine account on the domain controller.
debug	(Optional) Logs the domain join operation to the following file: /local1/logs/windows_domain_join.log
leave	Leaves a Windows domain.
diagnostics	Enables the selection of Windows domain diagnostic utilities.
domain-controller	Displays domain controller status information.
list	Displays information about all available domain controllers.
status	Displays the status of the currently joined domain controller.
time	Displays the time of the currently joined domain controller.
domain-name *domain_name*	(Optional) Displays the time of the domain controller specified.
encryption-service	Displays encryption service status information.
get-key *fqdn domain_name*	Displays the key retrieval information of the fully qualified domain name (for example, *machine-name*.cisco.com) and domain name.
getent	Displays the utility to get unified list of local users, PDC users, and groups.
group	Displays the diagnostic information of all groups or a particular group on Active Directory. In the output, a space in the group name is replaced by the "+" symbol.
gid *gid_no*	Displays group-related diagnostics information that corresponds to the group ID number specified.
groupname *groupname*	Displays group-related diagnostic information of a particular group.
username *username*	Displays group-related diagnostics information of a user.
machine-account-info	Displays the machine account-related information.

user	Displays the diagnostic information of all users or a particular user on Active Directory. In the output, a space in the username is replaced by the "+" symbol.
sid *sid_name*	(Optional) Displays the diagnostic information of a user based on the SID of the user specified.
uid *user_no*	(Optional) Displays the diagnostic information of a user based on the UID specified.
username *username*	(Optional) Display the diagnostic information of a user on Active Directory based on the username.
verify join	Displays the domain join status.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **windows-domain** command to join or leave a Windows domain or activate the selected Windows domain diagnostic utility.

When you use the **windows-domain join** command, it automatically discovers the windows domain configuration parameters and prompts you to approve the changes. You can respond with **yes** to approve the changes, **quit** to do nothing and exit the command, or **no** to enter interactive edit mode where you can edit any of the parameters before submitting the change.

If you do not specify the password as part of the command, you are prompted for the password and it is not shown on the console when you enter it.

Note When you use the command windows-domain diagnostics encryption-service get-key user *username* domain-name *domain_name* to configure WAAS as an identity server, you must execute this command two times to ensure that the key retrieval process is complete.

As shown below, the first time you execute this command an in-progress message is displayed, and the second time a completion message is displayed.

```
WAE# windows-domain diagnostics encryption-service get-key user username domain-name domain_name
WAE# Key retrieval in progress.
WAE# windows-domain diagnostics encryption-service get-key user username domain-name domain_name
WAE# The key for the user username is now in the cache.
```

Examples

The following example shows how to join a Windows domain and includes the interactive output:

```
WAE# windows-domain join domain-name waaslab.com user Administrator
```

```
Joining to AD Domain: WAASLAB.COM
With Computer DNS Name: wae.waaslab.com

administrator@WAASLAB.COM's password:
SUCCESS
```

The following example shows how to leave a Windows domain:

```
WAE# windows-domain leave user myname
```

Note In version 5.1.1, although the **windows-domain leave** operation disables the machine account on Active Directory (AD), it does not delete it.

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
```

Related Commands **(config) windows-domain**

write

To save startup configurations on a WAAS device, use the **write** EXEC command.

write [**erase** | **memory** | **mib-data** | **terminal**]

Syntax Description

erase	(Optional) Erases startup configuration from NVRAM.
memory	(Optional) Writes the configuration to NVRAM. This is the default location for saving startup information.
mib-data	(Optional) Saves MIB persistent configuration data to disk.
terminal	(Optional) Writes the configuration to a terminal session.

Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC

Device Modes

application-accelerator

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

zzdebugshell

To enter debug shell mode, use the **zzdebugshell** EXEC command. To exit from the shell environment, use the **exit** command.

⚠ **Caution** The **zzdebugshell** command can only be used by Cisco support personnel during a live support session. The **zzdebugshell** command requires both administrative WAAS user credentials and a special authentication token from Cisco TAC personnel. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 23.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

As highlighted in the above Caution note, the **zzdebugshell** command can only be used by Cisco support personnel during a live support session. The **zzdebugshell** command requires both administrative WAAS user credentials and a special authentication token from Cisco TAC personnel. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 23.

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 cms enable tacacs+

no aaa accounting cms enable tacacs+

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**

Syntax Description

cms enable tacacs+	Enables accounting for all commands executed internally by the Central Manager. This feature is disabled by default.
commands	Configures accounting for all commands at the specified privilege level.
0	Specifies the user privilege level for a normal user.
15	Specifies the user privilege level for an administrative user.
default	Sets AAA accounting to use the default accounting list.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server.
stop-only	Sends a stop accounting notice at the end of the process requested by the user.
wait-start	Sends both a start and a stop accounting notice to the accounting server. However, the requested user service does not begin until the start accounting notice is acknowledged. The user cannot execute a CLI command or login until the user is on record. A stop accounting notice is also sent but does not need acknowledgement.
tacacs	Enables use of TACACS+ for accounting.
exec	Enables accounting for user EXEC processes (user shells). When enabled, the EXEC shell accounting reports EXEC terminal session (user shell) events and login and logout by an administrator to the EXEC shell.
system	Enables accounting for all system-level events not associated with users, such as reloads.

Defaults

AAA accounting is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Examples

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) aaa authorization commands

To authorize commands issued through the CLI by a user on a WAAS device, use the **aaa authorization commands** global configuration command. To disable command authorization, use the **no** form of this command.

aaa authorization commands *level* **default tacacs+**

no aaa authorization commands *level* **default tacacs+**

Syntax Description

level **default tacacs+**	Configures command authorization for commands issued by the CLI user. Commands at the specified privilege level (0 or 15) are authorized. Level 0 authorizes EXEC commands, level 15 authorizes both EXEC and global configuration commands.

Defaults

AAA command authorization is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Command authorization enforces authorization through an external AAA server for each command executed by the user. All commands executed by a CLI user are authorized before they are executed.

When command authorization is configured for level 0, only EXEC commands are authorized, regardless of user level (normal or super).

When command authorization is configured for level 15, EXEC and global configuration commands are authorized, regardless of user level (normal or super).

Once it is configured, command authorization configuration is displayed in the running config. When the running config is copied to the startup config, command authorization is configured as the last config so that during the reload, the startup config need not be authorized.

Only commands executed through the CLI interface are subject to command authorization.

Examples

The following example shows how to configure command authorization for level 15 (authorization for both EXEC and global configuration commands) on the WAAS device:

```
WAE(config)# aaa authorization commands 15 default tacacs+
```

Related Commands

show aaa authorization

(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 epm {**enable** | **exception** {**coredump** | **debug** | **no-coredump**}}

no accelerator epm {**enable** | **exception** {**coredump** | **debug** | **no-coredump**}}

Syntax Description

enable	(Optional) Enables the EPM application accelerator.
exception	(Optional) Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	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

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** | **dre-hints** {**access-list** *acl* | **enable**}| **exception** {**coredump** | **debug** | **no-coredump**} | **metadatacache** {**access-list** *acl* | **enable** | **conditional-response enable** | **filter-extension** *extension-list* | **redirect-response enable** | **request-ignore-no-cache enable** | **response-ignore-no-cache enable**| **unauthorized-response enable** | **max-age** *seconds* | **min-age** *seconds* | **filter-extension** *extension-list* | **https** {**access-list** *acl* | **enable**}} | **sharepoint-opt prefetch enable | suppress-server-encoding** {**access-list** *acl* | **enable**}}

no accelerator http {enable | dre-hints {**access-list** *acl* |**enable**}| **exception** {**coredump** | **debug** | **no-coredump**} | **metadatacache** {**access-list** *acl* | **enable** | **conditional-response enable** | **filter-extension** *extension-list* | **redirect-response enable** | **request-ignore-no-cache enable** | **response-ignore-no-cache enable**| **unauthorized-response enable** | **max-age** *seconds* | **min-age** *seconds* | **filter-extension** *extension-list* | **https {access-list** *acl* | **enable**}} | **sharepoint-opt prefetch enable** | **suppress-server-encoding** {**access-list** *acl* | **enable**}}

Syntax Description

enable	(Optional) Enables the HTTP application accelerator.
dre-hints	Configures HTTP and HTTPS DRE hints feature.
access-list *acl*	Configures the HTTP AO feature subnet to associate an access list to an HTTP AO feature. *acl* refers to an ACL that can be created by the *ip access-list* CLI. See (config) ip access-list, page -664.
exception	(Optional) Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	Restarts the accelerator and does not write a core file.
metadatacache	(Optional) Configures metadata caching.
enable	(Optional) Enables metadata caching.
conditional-response enable	(Optional) Enables caching of HTTP 304 messages.
redirect-response enable	(Optional) Enables caching of HTTP 301 messages.
request-ignore-no-cache enable	Configures the metadata cache to ignore cache-control on requests.
response-ignore-no-cache enable	Configures the metadata cache to ignore cache-control on responses.
unauthorized-response enable	(Optional) Enables caching of HTTP 401 messages.
max-age *seconds*	(Optional) Specifies the maximum number of seconds to retain HTTP header information in the cache. The default is 86400 seconds (24 hours). Valid time periods range from 5–2592000 seconds (30 days).
min-age *seconds*	(Optional) Specifies the minimum number of seconds to retain HTTP header information in the cache. The default is 60 seconds. Valid time periods range from 5–86400 seconds (24 hours).

filter-extension ***extension-list***	(Optional) String containing a comma-separated list of file extensions to which metadata caching is to be applied. Do not include the dot at the beginning of the file extension. You can specify a maximum of 20 file extensions.
https enable	(Optional) Enables metadata caching for HTTPS traffic.
sharepoint-opt prefetch enable	(Optional) Enables data to be prefetched from the SharePoint server and serve it from the cache to the client.
suppress-server-encoding enable	(Optional) Enables suppression of Accept-Encoding compress, gzip, and deflate request-headers between the client and the server for HTTP and HTTPS.

Defaults

The HTTP accelerator is enabled by default and will start automatically if the Enterprise license is installed. The default exception action is coredump.

The metadata caching feature is disabled by default for all response types. The default max-age is 86400 seconds (24 hours), the default min-age is 60 seconds, and the default filter extension list is empty (meaning that metadata caching is applied to all extension types).

The SharePoint optimization feature is disabled by default.

When suppress-server-encoding is enabled, it suppresses the server compression for both HTTP and HTTPS requests. The suppress server encoding feature is disabled by default.

The DRE hints feature applies to both HTTP and HTTPS requests. It is disabled by default.

The subnet feature is enabled after the subnet configuration is added.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **accelerator http enable** command to enable the acceleration of HTTP traffic.

You can enable or disable each of three metadata caches (conditional-response, redirect-response, and unauthorized-response) separately. By default they are all enabled when you enable HTTP metadata caching. If you disable the HTTP accelerator, metadata caching is also disabled.

When you enable the suppress-server-encoding feature, the WAE removes the Accept-Encoding header from HTTP requests, preventing the web server from compressing HTTP data that it sends to the client. This allows the WAE to apply its own compression to the HTTP data, typically resulting in much better compression than the web server.

Use the SharePoint optimization feature when you need to access Microsoft Office documents stored on a SharePoint server 2010, using a web browser. Enabling this feature will prefetch the data from the server and serve it from the cache, which reduces latency and improves the user experience.

The DRE hint feature improves DRE performance. This feature is not automatically enabled when metadata caching or the suppress server encoding feature is enabled.

The options **request-ignore-no-cache** and **response-ignore-no-cache** are disabled by default. Because the HTTP accelerator is conservative in caching client request metadata and server response metadata, deployments may want to test with these settings enabled to improve the HTTP metadata cache hit ratio to achieve less latency.

If an existing subnet configuration gets modified or removed, the new configuration applies to new connections only, and does not impact the existing HTTP sessions. The change takes effect only after the change is updated in the kernel. Only one ACL is associated with each feature and a new subnet configuration replaces the old one. Use the **no** command to remove the subnet configuration. If the HTTP AO feature is globally disabled, the feature is not applied to any session. If the HTTP AO feature is globally enabled, and if the acl lookup result for this session is permit, the feature applies to the session; otherwise, it does not apply. HTTP AO bypass-list takes precedence over this feature.

Examples

The following example shows how to enable the HTTP application accelerator:

```
WAE(config)# accelerator http enable
```

The following example shows how to enable and configure the metadata cache to operate only on specific file types:

```
WAE(config)# accelerator http metadatacache enable
WAE(config)# accelerator http metadatacache filter-extension html,css,jpg,gif
```

Related Commands

clear cache

show accelerator

show cache http-metadatacache

show statistics accelerator

(config) accelerator http object-cache enable

To turn on the CE (cache engine) for the WAE, use the **accelerator http object-cache enable** global configuration command. To disable the CE on the WAE, use the **no** form of this command.

accelerator http object-cache enable

no accelerator http object-cache enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

When accelerator http object cache is enabled, it turns on the CE.

Note Turning on the CE with **accelerator http object-cache enable** starts Transparent caching in Basic mode. After using this command, you can also specify the type of caching you want the CE to perform: transparent, transparent standard, transparent advanced, bypass, or OTT (Over the Top caching). Each of these is listed below in Related Commands.

Examples

The following example shows how to enable HTTP object cache:

```
DT-HTTP-AO-DC-W594-52-18(config)# accelerator http object-cache enable
```

Related

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache transparent enable

To enable transparent basic caching mode on the CE, use the **accelerator http object-cache transparent enable** global configuration command. To disable transparent basic caching mode on the CE, use the **no** form of this command.

accelerator http object-cache transparent enable

no accelerator http object-cache transparent enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is enabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

When transparent basic caching mode is enabled on the CE, the CE caches only responses marked explicitly as cacheable.

Examples

The following example shows how to enable transparent caching on the CE.

```
WAAS(config)# accelerator http object-cache transparent enable
```

Related

(config) accelerator http object-cache enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache transparent basic

To enable transparent basic caching mode on the CE, use the **accelerator http object-cache transparent standard** global configuration command. To disable transparent basic caching mode on the CE, use the **no** form of this command.

accelerator http object-cache transparent basic

no accelerator http object-cache transparent basic

Syntax Description

This command has no arguments or keywords.

Command Default

The default is enabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

In transparent basic caching mode (which follows the standards set in RFC-2616), the CE:

- caches responses marked explicitly as cacheable (as in transparent caching mode)
- caches objects with no explicit cache marker with a **last- modified** date
- ignores "reload" headers from clients

Use the sub-mode facility (prompt ">") to set transparent standard mode for all sites, or for a specified IPv4 address or hostname (domain):

- **no** - Turns off the command or resets it to its defaults.
- **default** - Sets the transparent basic cache mode as the default for all sites.
- **exit** - Exits the sub-mode options menu.
- **server** *parameter* - Specifies a particular server for transparent basic caching, either in octet format ("A.B.C.D."), or with the server name in FQDN format (with a maximum of 255 total characters based on RFC-1035, and a maximum of 63 characters per label/segment).

A maximum of 512 host entries is supported for transparent basic caching mode.

Examples

The following example shows how to configure transparent basic as the default caching mode for a specified site:

```
accelerator http object-cache transparent basic
server * cisco.com
exit
```

Related

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache transparent standard

To enable transparent standard caching mode on the CE, use the **accelerator http object-cache transparent standard** global configuration command. To disable transparent standard caching mode on the CE, use the **no** form of this command.

accelerator http object-cache transparent standard

no accelerator http object-cache transparent standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default is enabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

In transparent standard caching mode, the CE:

- caches responses marked explicitly as cacheable (for transparent caching mode)
- caches objects with no explicit cache marker and with a **last- modified** date
- ignores “reload” headers from clients

Use the sub-mode facility (prompt “>”) to set transparent standard mode for all sites, or for a specified IPv4 address or hostname (domain):

- **no** - Turns off the command or resets it to its defaults.
- **default** - Sets the transparent standard cache mode as the default for all sites.
- **exit** - Exits the sub-mode options menu.
- **server** *parameter* - Specifies a particular server for transparent standard caching, either in octet format (“A.B.C.D.”), or with the server name in FQDN format (with a maximum of 255 total characters based on RFC-1035, and a maximum of 63 characters per label/segment).

A maximum of 512 host entries is supported for transparent standard caching mode.

Examples

The following example shows how to configure transparent standard as the default caching mode for a specified site:

```
accelerator http object-cache transparent standard
default
server 7.2.2.7
server www.cnn.com
exit
```

Related

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache transparent advanced

To enable transparent advanced caching mode on the CE, use the **accelerator http object-cache transparent advanced** global configuration command. To disable transparent advanced caching mode on the CE, use the **no** form of this command.

accelerator http object-cache transparent advanced

no accelerator http object-cache transparent advanced

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

In transparent advanced mode, the CE caches media files by MIME type, more aggressively, and caches all objects for longer times (when there is no specified expiration time).

Use the sub-mode facility (prompt “>”) to set transparent advanced mode for all sites, or for a specified IPv4 address or hostname (domain):

- **no** - Turns off the command or resets it to its defaults.
- **default** - Sets the transparent advanced cache mode as the default for all sites.
- **exit** - Exits the sub-mode options menu.
- **server** *parameter* - Specifies a particular server for transparent standard caching, either in octet format (“A.B.C.D.”), or with the server name in FQDN format (with a maximum of 255 total characters based on RFC-1035, and a maximum of 63 characters per label/segment).

A maximum of 512 host entries is supported for transparent advanced caching mode.

Examples

The following example shows how to configure transparent advanced caching as the default caching mode for all sites:

```
accelerator http object-cache transparent advanced
default
exit
```

Related

(config) accelerator http object-cache enable

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache transparent bypass

To turn off caching for a configured site, use the **accelerator http object-cache transparent bypass** global configuration command. To turn on caching for a configured site, use the **no** form of this command.

accelerator http object-cache transparent bypass

no accelerator http object-cache transparent bypass

Syntax Description

This command has no arguments or keywords.

Command Default

The default is enabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use this command to turn off caching for all configured sites or for a specific site.

Enables the transparent bypass mode of the CE for all sites or for a specific site. In this mode, caching is turned off for all sites or for a specified site(s). Transparent bypass mode suppresses all caching so that individual hostname rules are successfully applied.

Use the sub-mode facility (prompt ">") to set transparent bypass mode for all configured sites or for a specified IPv4 address or hostname (domain):

- **no** - Turns off the command or resets it to its defaults.
- **default** - Sets the transparent bypass mode as the default for all sites.
- **exit** - Exits the sub-mode options menu.
- **server** *parameter* - Specifies a particular server for transparent advanced caching, either in octet format ("A.B.C.D."), or with the server name in FQDN format (with a maximum of 255 total characters based on RFC-1035, and a maximum of 63 characters per label/segment).

Note When you configure Bypass mode as the site-specific transparent caching policy, you must specify a complete server name or complete (FQDN) domain name. If you use a wildcard to specify sites for Bypass mode, the sites will still be optimized via Akamai Cache.

Examples

The following is an example of how to set transparent bypass mode for a specified site:

```
accelerator http object-cache transparent bypass
server 7.2.2.7
server www.cnn.com
exit
```

Related

(config) accelerator http object-cache enable

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache ott enable

In OTT (Over the Top caching) caching mode, the CE caches content of third-party websites, using a predefined set of rules. Use the **accelerator http object-cache ott enable** global configuration command to turn on OTT caching mode. To turn off OTT caching, use the **no** form of this command.

accelerator http object-cache ott enable

no accelerator http object-cache ott enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is enabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

OTT (Over the Top) Caching caches dynamic content by examining the URL related to a session and a site to determine if the object is identical to one previously stored in the CE cache.

OTT is used for streamed content, particularly video content, and for sites that use dynamic URLs based on session or authentication methods. Currently, the CE only uses OTT for one site, www.youtube.com.

⚠

Caution Though it is possible to enable OTT caching with this command, note that you must initially enable OTT from the WAAS CM, so that registration takes place and the activation file is loaded. Initially enabling OTT via the CLI would also invalidate the EULA.

Examples

The following example shows how to enable OTT caching:

```
WAAS(config)# accelerator http object-cache ott enable
```

Related

(config) accelerator http object-cache enable

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache connected enable

(config) accelerator http object-cache connected enable

To enable the CE to retrieve content from Akamai's CDNs (Content Data Networks), use the **accelerator http object-cache connected enable** global configuration command. This enables Connected Cache mode. To turn off Connected Cache mode, use the **no** form of this command.

accelerator http object-cache connected enable

no accelerator http object-cache connected enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The Connected Cache (CC) feature allows the CE to cache content that is delivered by an Edge server on the Akamai Intelligent Platform. Object caching is done on the client side WAAS device only. Prepositioning may be leveraged to cache HTTP websites delivered via the Akamai Intelligent Platform.

⚠ **Caution** Though it is possible to enable Connected Cache with this command, note that you must initially enable Connected Cache from the WAAS CM so that registration takes place and the activation file is loaded. Initially enabling Connected Cache via the CLI would also invalidate the EULA.

Examples

The following example shows how to enable the Connected Cache.

```
WAAS(config)# accelerator http object-cache connected enable
```

Related

(config) accelerator http object-cache enable

(config) accelerator http object-cache transparent enable

(config) accelerator http object-cache transparent basic

(config) accelerator http object-cache transparent standard

(config) accelerator http object-cache transparent advanced

(config) accelerator http object-cache transparent bypass

(config) accelerator http object-cache ott enable

(config) accelerator http object-cache cws-check enable

To enable the Cisco Cloud Web Security feature, use the **accelerator http object-cache cws-check enable** global configuration command. To turn off the Cisco Cloud Web Security feature, use the **no** form of this command.

accelerator http object-cache cws-check enable

no accelerator http object-cache cws-check enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The Cisco Cloud Web Security feature provides content scanning of HTTP and secure HTTP/S traffic and malware protection service to web traffic. Cisco Cloud Web Security servers scan the web traffic content and either allow or block the traffic based on the configured policies. Servers use credentials such as private IP addresses, usernames, and user groups to identify and authenticate users and redirect the traffic for content scanning.

This command enables the same feature that is displayed on the WAAS Central Manager Advanced Cache Settings screen, as the **Cisco Cloud Web Security present** check box.

Examples

The following example shows how to enable the Cisco Cloud Web Security feature.

```
WAAS(config)# accelerator http object-cache cws-check enable
```

Related

(config) accelerator http preposition proxy server

To configure a proxy that can be used by any HTTP/S preposition task, use the **accelerator http preposition proxy server** global configuration command. To disable command authorization, use the **no** form of this command.

accelerator http preposition proxy server *ip address* **port** *port*

no accelerator http preposition proxy server *ip address* **port** *port*

Syntax Description

server *ip address*	The specified server address, in FQDN format, for the proxy server.
port *port*	The specified server port number to connect to the proxy server. The port number is from 1 to 65535.

Defaults

No default behaviors or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **accelerator http preposition proxy server** command to configure a proxy server that can be used by an HTTP/S preposition task.

Related Commands

(config-preposition) accelerator http preposition task task-name

(config) accelerator http object-cache enable

(config) accelerator ica

To enable the ICA application accelerator, use the **accelerator ica** global configuration command. To disable the ICA application accelerator, use the **no** form of this command.

accelerator ica {**enable** | **exception** {**coredump** | **debug** | **no-coredump**} | **wansecure-mode** | **session-limit** *limit* {**always** | **none**}}

accelerator ica {**enable** | **exception** {**coredump** | **debug** | **no-coredump**} | **wansecure-mode** | **session-limit** *limit* {**always** | **none**}}

Syntax Description

enable	Enables the ICA traffic accelerator.
exception	Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	Restarts the accelerator and does not write a core file.
wansecure-mode	Configures the state of WAN Secure mode.
session-limit *limit*	Sets the session limit for the ICA AO. The maximum value that can be set is the device TFO (Transport Flow Optimization) limit.
always	Enables WAN Secure mode for ICA.
none	Disables WAN Secure mode for ICA (default).

Defaults

The ICA accelerator is enabled by default. The default exception action is coredump. The default WAN Secure mode state is none.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **accelerator ica enable** command to enable the acceleration of ICA (Independent Computing Architecture) traffic with the transparent ICA accelerator. The ICA application accelerator provides WAN optimization on a WAAS device for ICAtraffic which is used to access a virtual desktop infrastructure (VDI). This is done through a process that is both automatic and transparent to the client and server.

Use the **accelerator ica session-limit** *limit* command to limit the number of session for the ICA AO (application accelerator).

Warning

Make sure you have accurately measured the per ICA user bandwidth before changing the accelerator ica session-limit *limit* parameter. Failure to do so could lead to undesired overload scenarios.

Here are guidelines and limitations for the **accelerator session-limit** *limit* command:

- You must enter this command when the ICA AO is running.
- The new value takes effect only after the ICA AO is restarted.

  Before an ICA AO restart, the **show statistics accelerator** output includes old and pending values for session limits counters; after an ICA AO restart, the output includes only new session limit values. Here is how the session limit counters are displayed for **show statistics accelerator** for each scenario:

  - *Before ICA AO restart*—After you have entered a new session limit value, but before an ICA AO restart, the Connection Limit and Effective Limit counters will still show the old ICA session limit values. Another counter, New ICA Session Limit, shows the new (pending) value.
  - *After ICA AO restart*—After you have entered a new session limit value, and after an ICA AO restart, the Connection Limit and Effective Limit counters will show the new ICA session limit value. The New ICA Session Limit counter is no longer needed, and is not included in the output.
- The maximum value that can be set is the device TFO limit.
- After you have saved the entered value to the startup configuration, the value is persistent across device reboots.

Use the **accelerator ica wansecure-mode always** command to enable WAN Secure mode for ICA. The WAN Secure mode configuration in both of the peer WAEs must match in order for the ICA accelerator to optimize connections.

WAN Secure mode requires that the SSL application accelerator is enabled. Use the **accelerator ssl enable** global configuration command to enable the SSL accelerator.

Examples

The following example shows how to enable the ICA application accelerator:

```
WAE(config)# accelerator ica enable
```

The following example shows how to set a session limit for the ICA application accelerator:

```
WAE(config)# accelerator ica session limit ?
default Set default session limit
WORD Session count (integer value)

WAE(config)# accelerator ica session limit 33
Setting session limit to 33. Changes will take effect after you restart ICA AO.
WARNING: Make sure you have accurately measured the per ICA user bandwidth before changing
this parameter. Failure to do so could lead to undesired overload scenarios.
```

Related Commands

show accelerator

show statistics accelerator

(config) windows-domain

(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** | **encryption** | **read-opt** | **write-opt** | **reserved-pool-size maximum-percent** *max_percent* | **wansecure-mode** {**always** | **auto** | **none**} | **exception** {**coredump** | **debug** | **no-coredump**}}

no accelerator mapi {**enable** | **encryption** | **read-opt** | **write-opt** | **reserved-pool-size maximum-percent** *max_percent* | **wansecure-mode** {**always** | **auto** | **none**} | **exception** {**coredump** | **debug** | **no-coredump**}}

Syntax Description

enable	Enables the MAPI traffic accelerator.
encryption	Enables the acceleration of encrypted MAPI traffic.
read-opt	Enables the read-ahead optimization of the MAPI traffic for mail reading.
write-opt	Enables the asynchronous write optimization of the MAPI traffic for mail sending.
reserved-pool-size maximum-percent *max_percent*	Configures the maximum reserved connection pool percent, specified as the percent of the device TFO connection limit, to restrict the maximum connections reserved for MAPI optimization during TFO overload. Range is from 5 to 50. Default is 15.
wansecure-mode	Configures the state of WAN Secure mode.
always	Enables WAN Secure mode for encrypted MAPI acceleration.
auto	Enables WAN Secure mode for encrypted MAPI acceleration only if encrypted traffic is received.
none	Disables WAN Secure mode for encrypted MAPI acceleration.
exception	(Optional) Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	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. Encrypted MAPI traffic acceleration is not enabled by default. The read optimization (**read-opt**) and write optimization (**write-opt**) features are enabled by default when the MAPI accelerator is enabled. The default maximum reserved connection pool percent is 15. The default WAN secure mode is auto. 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.

Use the **reserved-pool-size** keyword to restrict the maximum number of connections reserved for MAPI optimization during TFO overload. It is specified as a percent of the TFO connection limit of the platform. Valid percent ranges from 5%-50%. The default is 15% which would reserve approximately 0.5 connection for each client-server Association Group (AG) optimized by MAPI accelerator.

The client maintains at least one AG per server it connects to with an average of about 3 connections per AG. For deployments that observe a greater average number of connections per AG, or where TFO overload is a frequent occurrence, a higher value for the reserved pool size maximum percent is recommended.

Reserved connections would remain unused when the device is not under TFO overload. Reserved connections are released when the AG terminates.

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

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

enable	(Optional) Enables the EPM application accelerator.
exception	(Optional) Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	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 object-cache enable

To enable a specified AO object cache, use the **accelerator** *ao-name* **object-cache enable** global configuration command.

accelerator *ao-name* **object-cache enable**

no accelerator *ao-name* **object-cache enable**

Syntax Description

accelerator *ao-name*	Name of application accelerator object cache: SMB or HTTP.

Command Default

The default is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **accelerator** *ao-name* **object-cache enable** command to enable a specified AO object cache.

Note To ensure that each AO object cache and the global object cache function successfully, note these guidelines:

- Each AO object cache can be enabled or disabled independent of whether or not the global object cache is enabled or disabled.
- You must disable all individual AO object caches *before* you use the **no object-cache enable** global configuration command to disable the global object cache.
- The **object-cache enable** global configuration command does not automatically enable individual AO object caches.
- You can enable or disable an individual AO object cache whether or not the associated AO is enabled or disabled.

Examples

The following example shows how to enable the MAPI object cache:

```
(config)# accelerator smb object-cache enable
```

Related

(config) object-cache enable

show cache object-cache

show object-cache

show statistics object-cache

(config) accelerator smb

To enable the SMB application accelerator, use the **accelerator smb** global configuration command. To disable the SMB application accelerator, use the **no** form of this command.

accelerator smb {{**alarm digital-signing enable** | **metadata-cache-max-limit enable } | batch-close-opt enable** | **change-notif size** *size* | **dir-opt** {**enable** | **aging** *seconds*} | **dre-hints dre enable** | **dynamic-share** *name* | **enable** } **exception** {**coredump** | **debug** | **no-coredump**} | **highest-dialect** {**ntlm0-12** | **smb2-002** | **smb2-1**} **exceed-action** {**handoff** | **mute**} | **invalid-fid-opt enable** | **iobuf size** *mb* | **load-bypass enable | max-pkt-size size** *kb* | **metadata-opt** {**enable** | **cache-size** *mb* [**force**]} | **namedpipe-opt** {**enable** | **cache-size** *kb* | **resp-cache lifetime** *seconds* | **sess-cache lifetime** *seconds*} | **nf-cache** {**enable** | **aging** *seconds* | **bypass-patterns** *regex* | **size** *mb*} | **object-cache enable | oplock-opt {client-patterns** *name* **| enable }** | **office-opt enable** | **optimization bypass-pattern** *regex* | **print-opt enable | read-ahead** {**enable** | **buffer-size** *mb* [**force**] | **exhaust-distance** *kb* | **extended-window** *kb* | **hit-threshold** *percentage* | **init-window** *kb* | **max-active** *div* | **wait-distance** *kb*} | **signing** {**enable** | **unwrap**} | **smb2-read-caching enable | smb2-write-opt {enable | smb2-quota-aging** *seconds* **| smb2-quota-threshold** *mb***} | wansecure-mode {always | none} | write-opt** {**enable** | **quota-aging** *seconds* | **quota-threshold** *mb*}}

no accelerator smb {**alarm digital-signing enable** | **batch-close-opt enable** | **change-notif size** *size* | **dir-opt** {**enable** | **aging** *seconds*} | **dre-hints dre enable** | **dynamic-share** *name* | **enable** } **exception** {**coredump** | **debug** | **no-coredump**} | **highest-dialect** {**ntlm0-12** | **smb2-002** | **smb2-1**} **exceed-action** {**handoff** | **mute**} | **invalid-fid-opt enable** | **iobuf size** *mb* | **load-bypass enable | max-pkt-size size** *kb* | **metadata-opt** {**enable** | **cache-size** *mb* [**force**]} | **namedpipe-opt** {**enable** | **cache-size** *kb* | **resp-cache lifetime** *seconds* | **sess-cache lifetime** *seconds*} | **nf-cache** {**enable** | **aging** *seconds* | **bypass-patterns** *regex* | **size** *mb*} | **object-cache enable | oplock-opt {client-patterns** *name* **| enable }** | **office-opt enable** | **optimization bypass-pattern** *regex* | **print-opt enable | read-ahead** {**enable** | **buffer-size** *mb* [**force**] | **exhaust-distance** *kb* | **extended-window** *kb* | **hit-threshold** *percentage* | **init-window** *kb* | **max-active** *div* | **wait-distance** *kb*} | **signing** {**enable** | **unwrap**} | **smb2-read-caching enable | smb2-write-opt {enable | smb2-quota-aging** *seconds* **| smb2-quota-threshold** *mb***} | | write-opt** {**enable** | **quota-aging** *seconds* | **quota-threshold** *mb*}}

Syntax Description

alarm digital-signing enable	Enables the digital-signing alarm.
alarm metadata-cache-max-limit enable	Enables alarm for metadata cache maximum limit
batch-close-opt enable	Enables asynchronous close optimization for SMB2 protocol.
change-notif size *size*	Sets the change notification table size. Valid values range from 1–2048 entries. The default is10.
dir-opt enable	Enables directory listing optimization.
aging *seconds*	Configures metadata directory list aging time to the specified number of seconds. If the age of a metadata directory list exceeds this time when the metadata is requested, the entry is considered stale and is updated by retrieving it from the file server.
dre-hints dre enable	Enables DRE and LZ hints.

dynamic-share *name*	Adds the specified share to the existing dynamic share configuration. The share name must use the format //server/share and must not exceed 256 characters.
enable	Enables the SMB traffic accelerator.
exception	(Optional) Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	Restarts the accelerator and does not write a core file.
highest-dialect	Configures the highest dialect to be optimized.
ntlm0-12	Configures NTLM version 0.12 to be the highest dialect.
smb2-002	Configures SMB version 2.002 to be the highest dialect.
smb2-1	Configures SMB version 2.1 to be the highest dialect.
exceed-action	Configures the action if a request uses a dialect higher than the configured highest dialect to be optimized.
handoff	The connection is handed off to the generic application accelerator.
mute	The connection is removed from the negotiate request.
invalid-fid-opt enable	Enables SMB2 invalid file ID optimization. The SMB accelerator issues a local response to files with invalid file ID values.
iobuf size *mb*	Configures the IOBUF buffer size, in MB, from 50 to 1000.
load-bypass enable	Enables SMB object-cache load bypass.
max-pkt-size *kb*	Configures the maximum SMB packet size, in KB, from 64 to 16384.
metadata-opt enable	Enables metadata optimization.
cache-size *mb*	Configures metadata cache size, in MB, from 50 to 360000.
force	Forces the metadata cache size setting.
namedpipe-opt enable	Enables named pipe optimization.
cache-size *kb*	Configures the size of the named pipe cache, in KB, from 128 to 150000.
resp-cache lifetime *seconds*	Configures the response cache lifetime, in seconds, from 0 to 1024.
sess-cache lifetime *seconds*	Configures the session cache lifetime, in seconds, from 0 to 1024.
nf-cache enable	Enables not-found metadata cache optimization.
aging *seconds*	Configures the length of time, in seconds, that not-found metadata cache entries are held in the cache, from 1 to 60 (the default is 30).
bypass-patterns *regex*	Configures a case-insensitive regular expression that matches filenames to be bypassed by the not-found metadata cache.
size *mb*	Configures the maximum size of the not-found metadata cache, in MB, from 1 to 256 (the default is 32).
object-cache enable	Enables SMB object-caching.
office-opt enable	Enables Microsoft Office optimization.
oplock-opt enable	Enables Oplock optimization.
client patterns	Configures client patterns where oplock optimization will be applied.

optimization bypass-pattern *regex*	Configures a case-insensitive regular expression that matches filenames to be bypassed for all optimizations. If regular expression uses backslash, then a double-backslash needs to be used. Additionally, it must be a single regular expression, using a pipe '|' symbol as a delimiter within the expression.
print opt enable	Enables SMB print optimization.
read-ahead enable	Enables read-ahead optimization.
buffer size *mb*	Configures read-ahead buffer size, in MB, from 50 to 10000.
force	Forces the read-ahead cache size setting.
exhaust-distance *kb*	Configures read-ahead window exhaust distance, in KB, from 128 to 1024 (the default is 196).
extended-window *kb*	Configures read-ahead window exhaust distance, in KB, from 256 to 3200 (the default is 640).
hit-threshold *percentage*	Configures read-ahead hit threshold, as a percentage from 10 to 100 (the default is 70).
init-window *kb*	Configures read-ahead initial window size, in KB, from 128 to 1024 (the default is 196).
max-active *div*	Configures read-ahead maximum active memory usage divisor, from 2 to 10 (the default is 4).
wait-distance *kb*	Configures read-ahead wait distance, in KB, from 128 to 3200 (the default is 512).
signing enable	Enables smb2 signing optimization. Should be enabled at the Edge WAE.
signing unwrap	Enable or disable signature verification (unwrap) of request packets at Edge WAE.
smb2-read-caching	Enables smb2 read caching optimization.
smb2-write enable	Enables smb2 asynchronous write optimization.
quota-aging *seconds*	Configures network share quota threshold aging time, in seconds, from 1 to 120 (the default is 60).
quota-threshold *mb*	Configure network share quota threshold, in MB, from 1 to 1024 (the default is 20).
wansecure-mode	Configures the state of WAN Secure mode.
always	Enables WAN Secure mode for signing optimization.
none	Disables WAN Secure mode for signing optimization.
write-opt enable	Enables asynchronous write optimization.

Defaults

The SMB accelerator is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The enterprise license is required to start the SMB accelerator.

The EXEC mode command **show running-config** displays non-default settings only. Therefore, the command **no accelerator smb enable** does not show up in the running configuration if the SMB accelerator is disabled, while the **accelerator smb enable** command does display if the SMB accelerator is enabled.

Use the **object-cache enable** command to enable disk caching of SMB traffic.

Use the **accelerator smb signing unwrap enable** command to verify signature of the signed request packets at the Edge WAE. This checks whether the packet is modified/tampered while coming over the LAN. However, since the packet usually travels in the LAN from the Client to the Edge WAE, chances of man-in-middle attacks are less likely and you may choose to disable Edge side signature verification for request packets.

Use the **accelerator smb wansecure-mode always** command to enable WAN Secure mode for optimizing signed SMBv2 traffic. The default is “always”. The WAN Secure mode configuration for both the EDGE WAE and Core WAEs must match (be set at “always”) in order for the SMB accelerator to optimize signed SMBv2 connections. Even if one side has “none” set, then the signed connections would be handed over for generic optimization.

Use the **accelerator smb wansecure-mode none** to disable the wansecure -mode.

WAN Secure mode requires that the SSL application accelerator is enabled. Use the **accelerator ssl enable** global configuration command to enable the SSL accelerator.

Examples

The following example shows how to enable the SMB application accelerator:

```
WAE(config)# accelerator smb enable
```

The following example shows how to configure a case-insensitive regular expression that matches filenames to be bypassed for all optimizations:

```
WAE(config)# accelerator smb optimization bypass-pattern \\.pst|\\.accd[betr]
```

This configuration would bypass files that contain .pst, .accdb, .accde, .accdt, and .accdr (Outlook PST files, and MS Access files).

Related Commands

show accelerator

show statistics accelerator

(config) accelerator smb preposition

To create a smb preposition directive, use the **accelerator smb preposition** global configuration command. To disable the SSL application accelerator, use the **no** form of this command.

accelerator smb preposition task-id{**credentials** | **duration**<*min*> **| enable | exit | max-cache <***percentage*> **| max-file-size** <*max-file-size*> **| min-file-size**<*min-file-size*> **| name <***directive name*> **| no | pattern {contains | ends-with | equals | starts with } | recursive | signing {kerberos | ntlm } | root** <*full path*>**| schedule {daily | date | monthly | now | weekly}| server** <*server name*> }

no accelerator smb preposition task{**enable** | **exception** {**coredump** | **debug** | **no-coredump**}}

Syntax Description

credentials	Sets user and password credentials. Use password 0 to use and show a password as a plaintext and password 1 to store and show a DES-encrypted password.
duration	Sets the maximum duration limit minutes that the task can run.
enable	Enables the directive (use no enable to disable).
exit	Exit from this submode.
max-cache	Sets the maximum percentage of the cache that the task can occupy.
max-file-size	Sets maximum file size (KB) limit.
min-file-size	Sets minimum file size (KB) limit.
name	Sets the name of the directive.
no	Negate a command or set its defaults.
pattern	Sets a string filter on the file names.
recursive	Defines if the preposition is recursive.
signing	Enables signing using NTLM or Kerberos [Support SMBv2 dialect]
root	Adds a preposition root. Multiple roots are supported.
schedule	Sets the schedule to start the task.
server	Sets server name for the directive. Only one server is allowed.

Defaults

The accelerator SMB preposition is enabled by default..

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the following guidelines when you create a smb preposition directive.

Root Directories

Special characters like ; | && || : * ? < > “ ` ! [ ] + = , are not allowed for top level shares. Additionally, when you create subdirectories inside the shares, the following special characters are not allowed: ; | && || : * ? < > “ ` !

Do not use the special character “;“ in files and directory names, else it will throw up errors. Additionally, we do not support extended Unicode characters in files and directories for release 6.2.1 and any such files or directories would be skipped and not prepositioned.

Pattern

Do not use a space or the following special characters when defining patterns:

; | && || : * ? < > \ / “ ` !

Username

The following characters are not allowed to be used as username ; | && || : \ / * ? < > + = , [ ] “ ` !.

Server Name

The following characters are not allowed to be used in server names ; | && || , ~ : ! ` @ # $ % ^ & ‘ { } ()_“

Domain Name

The following characters are not allowed to be used as domain names ; | && || : \ / * ? < > “ ` !.

Examples

The following example shows how to configure the accelerator SMB preposition directive:

```
WAE(config)# accelerator smb preposition 106
server "15.50.0.3"
credentials username "Administrator" domain "test" password 1/ zXnLZdloxuElwx3pDAWuQ==
root "/abcd#@ %^&/"
root "/abcd#@$%/"
root "/abcd#@$% 12/"
root "/abc/"
schedule now
pattern exclude equals "@#$%^&()-_==+ nbe{}[]''',..qwe12.txt"
enable
recursive
exit
```

Related Commands

show accelerator

show statistics accelerator

(config) accelerator smb preposition dre

To enable DRE for smb preposition tasks, use the **accelerator smb preposition dre** global configuration command. Use the no form of the command to disable it.

accelerator smb preposition dre enable

no accelerator smb preposition dre enable

Syntax Description

enable	Enables dre for smb preposition tasks.

Defaults

The SMB preposition dre is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **accelerator smb preposition dre** command if you want to cache files in both Object Cache and DRE cache. If you do not enable this, files are cached only in Object Cache.

Examples

The following example shows how to enable dre for the SMB preposition task:

```
WAE(config)# accelerator smb preposition dre 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

enable	(Optional) Enables the SSL application accelerator.
exception	(Optional) Configures the action to be taken if an exception occurs.
coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	Restarts accelerator and does not write a core file.

Defaults

The SSL 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 ssl enable** 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 **no** version of this command.

Examples

The following example shows how to enable the SSL application accelerator:

```
WAE(config)# accelerator ssl enable
```

Related Commands

show accelerator

show statistics accelerator

crypto delete

crypto export

crypto generate

crypto import

(config) crypto pki

(config) crypto ssl

(config-ca) ca-certificate

(config-ca) description

(config-ca) revocation-check

(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*]}

Syntax Description

clear *1-999*	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. **Note** The **alarm overload-detect clear** value must be less than the **alarm overload-detect raise** value.
raise *10-1000*	(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.
enable	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

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*

Syntax Description

tag *name*	Sets the asset tag name.

Defaults

No default behaviors or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Examples

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

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

(config) authentication 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

configuration	Sets the administrative login authorization (configuration) parameters for the WAAS device.
local	Selects the local database method for the WAAS device.
radius	Selects the RADIUS method for the WAAS device.
tacacs	Selects the TACACS+ method for the WAAS device.
windows-domain	Selects the Windows domain controller method for the WAAS device.
enable	Enables the specified methods for the WAAS device.
primary	(Optional) Specifies the first method that the WAAS device should use.
secondary	(Optional) Specifies the second method that the WAAS device should use.
tertiary	(Optional) Specifies the third method that the WAAS device should use if the primary and secondary methods fail.
quaternary	(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.

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure administrative login authentication and authorization for your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure administrative login authentication and authorization on a single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

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

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

The **authentication login tacacs** and **authentication configuration tacacs** commands use a remote TACACS+ server to determine the level of user access. 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.

You can configure multiple TACACS+ or RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+ or RADIUS farm, in order. If authentication fails for any reason other than a server is unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **authentication fail-over server-unreachable** command.

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. Secondary authentication servers are queried in order only if the primary server is unreachable. If authentication fails for any other reason, alternate servers are not queried.

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 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 enable

To configure “enable authentication” to use local "admin" user account password instead of using external authentication servers, use the **authentication enable** global configuration mode command. To disable this, use the **no** form of the command.

authentication enable local

no authentication enable local

Syntax Description

local	Selects the local admin user account password to enable authentication information for the WAAS device.

Defaults

When this command is configured, the local admin user account password is used for enable authentication by default.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

When a user who does not have privileged EXEC level types "enable" at the WAE>prompt, the request for enable access is not sent to the external authentication servers, but is processed on the WAE, using only the local admin user account password to verify the given password and provide access.

Note Critical commands (e.g. configuration and management) require that the user be at the privileged EXEC level. To change to the privileged EXEC level, type "enable" at the WAE> prompt.

Examples

The following example shows how to configure enable authentication by using local admin user account password.

```
WAE(config)# authentication enable local.
```

Related

(config) authentication configuration

show authentication

(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

Syntax Description

windows-domain-ctrl	Selects a Windows domain controller for domain server authentication.
disconnected-mode enable	Enables authentication in the disconnected mode.

Defaults

The local authentication method is enabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The **authentication** command configures both the authentication and authorization methods that govern login and configuration access to the WAAS device.

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure administrative login authentication and authorization for your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure administrative login authentication and authorization on a single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

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

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

The **authentication login tacacs** and **authentication configuration tacacs** commands use a remote TACACS+ server to determine the level of user access. 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.

You can configure multiple TACACS+ or RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+ or RADIUS farm, in order. If authentication fails for any reason other than a server is unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **authentication fail-over server-unreachable** command.

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. Secondary authentication servers are queried in order only if the primary server is unreachable. If authentication fails for any other reason, alternate servers are not queried.

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 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

To specify authentication failover if the primary authentication server is unreachable, use the **authentication fail-over** global configuration mode command. To disable this feature, use the **no** form of this command.

authentication fail-over server-unreachable

no authentication fail-over server-unreachable

Syntax Description

server-unreachable	Specifies that the WAAS device is to query the secondary authentication database only if the primary authentication server is unreachable.

Defaults

This feature is disabled by default. This means that the WAAS device tries the other authentication methods if the primary method fails for any reason, not just if the server is unreachable.

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.

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure administrative login authentication and authorization for your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure administrative login authentication and authorization on a single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

The **authentication 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.

You can configure multiple TACACS+ or RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+ or RADIUS farm, in order. If authentication fails for any reason other than a server is unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **authentication fail-over server-unreachable** command.

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.

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.

Related Commands

(config) radius-server

show authentication

show statistics radius

show statistics tacacs

(config) tacacs

windows-domain

(config) windows-domain

(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

local	Selects the local database method for the WAAS device.
radius	Selects the RADIUS method for the WAAS device.
tacacs	Selects the TACACS+ method for the WAAS device.
windows-domain	Selects the Windows domain controller method for the WAAS device.
enable	Enables the specified methods for the WAAS device.
primary	(Optional) Specifies the first method that the WAAS device should use.
secondary	(Optional) Specifies the second method that the WAAS device should use.
tertiary	(Optional) Specifies the third method that the WAAS device should use if the primary and secondary methods fail.
quaternary	(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.

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure administrative login authentication and authorization for your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure administrative login authentication and authorization on a single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

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

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

The **authentication login tacacs** and **authentication configuration tacacs** commands use a remote TACACS+ server to determine the level of user access. 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.

You can configure multiple TACACS+ or RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+ or RADIUS farm, in order. If authentication fails for any reason other than a server is unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **authentication fail-over server-unreachable** command.

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. Secondary authentication servers are queried in order only if the primary server is unreachable. If authentication fails for any other reason, alternate servers are not queried.

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 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 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 [**max-retry-attempts** *number*]

no authentication strict-password-policy [**max-retry-attempts** *number*]

Syntax Description

max-retry-attempts *number*	(Optional) Specifies the maximum number of failed login attempts allowed before the user is locked out. The range is 1–25; the default is 3.

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.
- The password cannot contain dictionary words.

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.

Examples

The following example shows how to enable the strong password policy:

```
WAE(config)# authentication strict-password-policy
```

The following example shows how to enable the strong password policy and set the maximum retry attempts to 5:

```
WAE(config)# authentication strict-password-policy max-retry-attempts 5
```

The following example shows how to disable the strong password policy:

```
WAE(config)# no authentication strict-password-policy
```

Related Commands

clear users

show authentication

(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 itps** | **hold-time** *minutes*}

no auto-discovery blacklist {**enable itps** | **hold-time** *minutes*}

Syntax Description

blacklist	Specifies the TFO auto-discovery blacklist server configuration.
enable	Enables the TFO auto-discovery blacklist operation.
itps	Configures interposer- ssl blacklist operation.
hold-time *minutes*	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.

Use the **auto-discovery blacklist enable itps** command to configure the interposer-ssl blacklist operation. Once enabled, depending on the nature of the error, the server or client ip is blacklisted.If blacklisted, any request sent to this particular server cannot use the SMART-SSL optimization for the next 60 minutes. Optimization requests to this server will be treated as pass through connections.

Similarly, if the client IP is blacklisted due to some error, the SMART-SSL accelerator will not accept any new connection requests from this client for the next 20 seconds. Optimization requests from this particular client will be treated as pass-through connections.

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

To enable the discovery of a 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* | **TenGigabitEthernet** *slot/port*]

no auto-register enable [**FastEthernet** *slot/port* | **GigabitEthernet** *slot/port* | **TenGigabitEthernet** *slot/port*] [**preserve-ip**]

Syntax Description

enable	Enables the automatic registration of devices using DHCP with the WAAS Central Manager.
FastEthernet *slot/port*	(Optional) Selects a Fast Ethernet interface for automatic registration using DHCP. Selects slot number and port number of the Fast Ethernet interface. Valid slot values depend on the hardware platform.
GigabitEthernet *slot/port*	(Optional) Selects a Gigabit Ethernet interface for automatic registration using DHCP. Selects slot number and port number of the Gigabit Ethernet interface. Valid slot values depend on the hardware platform.
TenGigabitEthernet *slot/port*	(Optional) Selects a TenGigabitEthernet interface for automatic registration using DHCP. Selects slot number and port number of the 10-Gigabit Ethernet interface. Valid slot values depend on the hardware platform.
preserve-ip	(Optional) Converts a dynamic IP address to a static IP address when you remove the automatic registration from an interface so that the interface remains configured with an IP address.

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 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.

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** command, you must first disable the automatic registration of devices through DHCP by using the **no auto-register enable** command. If you want to keep the dynamic IP address that had been assigned to the interface, use the **preserve-ip** option to convert it to a static IP address.

After the WAE configures its network settings from DHCP, it needs to know the Central Manager hostname so it can register with the Central Manager.

The WAE queries the DNS server to obtain the Central Manager hostname. For autoregistration to work, you must configure the DNS server with the Central Manager hostname by configuring a DNS SRV (Service Location) record. For more information about autoregistration and how to configure the DNS SRV record, see the section on autoregistration in the "Planning Your WAAS Network" chapter of the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to enable autoregistration on GigabitEthernet port 1/0:

```
WAE(config)# auto-register enable GigabitEthernet 1/0
```

The following example shows how to disable autoregistration on all configured interfaces on the WAE without losing any IP addresses assigned by autoregistration DHCP:

```
WAE(config)# no auto-register enable preserve-ip
```

Related Commands

show auto-register

show running-config

show startup-config

(config) banner

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

banner {**enable** | {{**exec** | **login** | **motd**} [**message** *text*]}}

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

Syntax Description

enable	Enables banner support on the WAE.
exec	Configures an EXEC banner.
login	Configures a login banner.
motd	Configures an MOTD banner.
message *text*	(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.

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.

Examples

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

```
WAE(config)# banner motd message This is a WAAS 4.0.7 device
```

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

```
WAE(config)# banner motd message "This is the motd message.
\nThis is a WAAS 4.0.7 device\n"
```

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

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

The following example shows how to enable banner support:

```
WAE(config)# banner enable
```

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

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

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

```
This is the motd banner.
This is a WAAS 4.0.7 device
This is login banner.
Use your password to login.

Cisco Wide Area Application Services Engine

admin@wae's password:
```

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

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

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

```
WAE#
```

Related Commands

show banner

(config) 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

enable	Enables CDP globally.
holdtime *seconds*	Sets the length of time in seconds (10–255) that a receiver keeps CDP packets before they are discarded. The default is 180 seconds.
timer *seconds*	Sets the interval between the CDP advertisements in seconds (5–254). The default is 60 seconds.

Defaults

holdtime: 180 seconds

timer: 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:

```
WAE(config)# cdp enable
WAE(config)# cdp holdtime 10
WAE(config)# cdp timer 15
```

Related Commands

(config-if) cdp

clear arp-cache

show cdp

(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

address	Specifies the hostname or IP address of the WAAS Central Manager with which the WAE should register.
hostname	Hostname of the WAAS Central Manager with which the WAE should register.
ip-address	IP address of the WAAS Central Manager with which the WAE should register.
role	Configures the WAAS Central Manager role to either primary or standby.
primary	Configures the WAAS Central Manager to be the primary WAAS Central Manager for the WAEs that are registered with it.
standby	Configures the WAAS Central Manager to be the standby WAAS Central Manager for the WAEs that are registered with it.
ui	Configures the WAAS Central Manager GUI port address.
port *port-num*	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.

Defaults

The WAAS Central Manager GUI is preconfigured to use port 8443.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Examples

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

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

timezone *timezone hoursoffset*	Configures the name of the standard time zone and hours offset from UTC (–23 to +23). See Table 3-1 in the “Usage Guidelines” section.
minutesoffset	(Optional) Minutes offset (see Table 3-1 in the “Usage Guidelines” section) from UTC (0–59).
summertime *timezone*	Configures the name of the summer or daylight saving time zone.
date	Configures the absolute summer time.
startday	Date (1–31) to start.
startmonth	Month (January through December) to start.
startyear	Year (1993–2032) to start.
starthour	Hour (0–23) to start in hour:minute (hh:mm) format.
endday	Date (1–31) to end.
endmonth	Month (January through December) to end.
endyear	Year (1993–2032) to end.
endhour	Hour (0–23) to end in hour:minute (hh:mm) format.
offset	Minutes offset from UTC (0–1439). The summer time offset specifies the number of minutes that the system clock moves forward at the specified start time and backward at the end time.
recurring	Configures the recurring summer time.
1-4	Configures the starting week number 1–4.
startweekday	Day of the week (Monday–Friday) to start.
endweekday	Weekday (Monday–Friday) to end.
first	Configures the summer time to recur beginning the first week of the month.
last	Configures the summer time to recur beginning the last week of the month.

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 *0 0* is the offset (ahead or behind) UTC is in hours and minutes. (UTC was formerly known as Greenwich mean time [GMT]).

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

Note The time zone entry is case sensitive and must be specified in the exact notation listed in Table 3-1. 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

Table 3-1 Time Zone—Offsets from UTC (continued)

Time Zone	Offset from UTC
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	–4
Canada/Newfoundland	–3.30
Canada/Saskatchewan	–6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0

Table 3-1 Time Zone—Offsets from UTC (continued)

Time Zone	Offset from UTC
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	–12
Pacific/Samoa	–11
US/Alaska	–9
US/Central	–6
US/Eastern	–5
US/East-Indiana	–5
US/Hawaii	–10
US/Mountain	–7
US/Pacific	–8

Examples

The following example 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

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

database maintenance	Configures the embedded database clean or reindex maintenance routine.
full	Configures the full maintenance routine and cleans the embedded database tables.
enable	Enables the specified routine or process to be performed on the embedded database tables.
schedule *weekday*	Sets the schedule for performing the maintenance routine to a day of the week. every-day Every day Mon every Monday Tue every Tuesday Wed every Wednesday Thu every Thursday Fri every Friday Sat every Saturday Sun every Sunday
at *time*	Sets the maintenance schedule time of day to start the maintenance routine (0–23:0–59) (hh:mm). at Maintenance time of day Mon every Monday Tue every Tuesday Wed every Wednesday Thu every Thursday Fri every Friday Sat every Saturday Sun every Sunday
regular	Configures the regular maintenance routine and reindexes the embedded database tables.
rpc timeout	Configures the timeout values for remote procedure call connections.
connection *5-1800*	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.

incoming-wait *10-600*	Specifies the maximum time to wait for a client response. The timeout period is in seconds. The default is 30 seconds.
transfer *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.

Tip If you are trying to register a device that had previously been registered with a WAAS Central Manager and the **cms enable** global configuration command fails, use the **cms deregister force** command. If you get an error saying that the management service is not enabled when you use the **cms deregister force** command, delete the device from the WAAS Central Manager.

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
```

Related Commands

cms

show cms

(config) crypto encryption-service

To configure encryption services on a WAAS device, use the **crypto encryption service** global configuration command. To disable a **crypto encryption-service**, use the **no** form of the command.

crypto encryption-service enable

Syntax Description

enable	Enables the encryption service

Defaults

This is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the command to enable the encryption service and to configure the interposer.

Examples

The following example shows how to enable an encrypted service on a WAAS device.

```
WAE(config)# crypto encryption-service enable
```

Related Commands

show statistics encryption-services

(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*}

crypto pki global-settings [**ocsp url** *url* | **revocation-check** {**ocsp-cert-url** [**none**] | **ocsp-url** [**none**] }]

Syntax Description

ca *certificate-authority-name*	Configures encryption certificate authority information. Using this command enables certificate authority configuration mode. See PKI Certificate Authority Configuration Mode Commands, page -839.
global-settings	Configures PKI encryption global settings. Using this command enables PKI global settings configuration mode. See PKI Certificate Authority Configuration Mode Commands, page -839.
ocsp url *url*	(Optional) Configures an OCSP URL.
revocation-check	(Optional) Configures certificate revocation methods.
ocsp-cert-url	Specifies to use the URL from the certificate.
none	(Optional) Specifies a null method that returns revocation success.
ocsp-url	Specifies to use the URL from the global OCSP setting.

Defaults

No default behavior or values.

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

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 {**accelerated-service** *service-name* | **global-settings** | **host-service peering**}}

no crypto ssl {**cipher-list** *cipher-list-name* | **management-service** |
services {**accelerated-service** *service-name* | **global-settings** | **host-service peering**}}

Syntax Description

cipher-list *cipher-list-name*	Configures the SSL cipher suite list. Using this command enables SSL cipher list configuration mode. See the SSL Cipher List Configuration Mode Commands chapter.
management-service	Configures SSL management services. Using this command enables SSL management service configuration mode. See the SSL Management Service Configuration Mode Commands chapter.
services	Configures other SSL services (accelerated, global, and host peering).
accelerated-service *service-name*	Configures SSL accelerated services. Using this command enables SSL accelerated service configuration mode. See the SSL Accelerated Service Configuration Mode Commands chapter.
global-settings	Configures SSL service global settings. Using this command enables SSL service global configuration mode. See the SSL Global Service Configuration Mode Commands chapter.
host-service peering	Configures SSL host peering services. Using this command enables SSL host peering service configuration mode. See the SSL Host Peering Service Configuration Mode Commands chapter.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **crypto ssl** global configuration command to enter SSL cipher list configuration mode, SSL management service configuration mode, SSL accelerated service configuration mode, SSL service global configuration mode, or SSL host peering service 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)#
```

The following example puts the WAAS device into SSL management service configuration mode. The mode change is indicated by the system prompt:

```
WAE(config)# crypto ssl management-service
WAE(config-ssl-mgmt)#
```

The following example puts the WAAS device into SSL accelerated service configuration mode, editing the myservice accelerated service. The mode change is indicated by the system prompt:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)#
```

The following example puts the WAAS device into SSL global service configuration mode. The mode change is indicated by the system prompt:

```
WAE(config)# crypto ssl services global-settings
WAE(config-ssl-global)#
```

The following example puts the WAAS device into SSL host peering service configuration mode. The mode change is indicated by the system prompt:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)#
```

Related Commands

(config) crypto pki

(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** | **application-accelerator profile branch** | **central-manager** }

no device mode {**application-accelerator** | **application-accelerator profile branch** | **central-manager** |}

Syntax Description

application-accelerator	Configures the WAAS device to function as a WAAS Accelerator. All of the branch and data center WAEs that are doing traffic optimization must be operating in this mode.
application-accelerator profile branch	For use with WAVE-7541, WAVE-7571 and WAVE-8541, which enables the device to function as a branch device, to configure resource pre-allocation resources for various WAAS services to be branch traffic scenario and branch services. The branch profile-enabled connection count used for computing memory for pre-allocation is 3/4 of the TFO limit for WAVE-7571 and WAVE-8541.
central-manager	Configures the WAAS device to function as a WAAS Central Manager.

Defaults

The default device operation mode is application-accelerator.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

application-accelerator profile branch

Usage Guidelines

If the WAAS device is operating with an Accelerator only image, you will not be able to convert it to central-manager mode until after you update it with a Full image and reboot. You can use the **show version** EXEC command to check the type of software image the WAE is running.

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. 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) 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

diskxx	Name of the disk (disk00-disk05).
shutdown	Disables the disk for maintenance.
force	(Optional) Forces a disk to be reenabled when used with the **no** form of this command. 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

You can replace a failed disk or perform a scheduled disk maintenance on the WAE-612. Use the **disk disk-name** *diskxx* **shutdown** global configuration command to manually shut down a disk for a scheduled disk maintenance. (For the schedule disk maintenance procedure, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 14.)

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 object-cache extend

disk

show disks

(config) disk cache

To configure Akamai cache and Object cache partitions, use the **disk cache** global configuration command. If disk configuration is not required, use the default option or use the **restore factory-default preserve basic-config** EXEC command.

disk cache {default | Akamai-OC-equal | Akamai-weight1 | OC-weight1 | Akamai-weight2 | OC-weight2}{force}

Syntax Description

default	Sets the available partition to predefined values for Akamai cache and Object cache.
Akamai-OC-equal	Sets the available partition size to 50% each for both Akamai cache and Object cache.
Akamai-weight1	Sets size of partition to 60% for Akamai cache and 40% for Object cache.
OC-weight1	Sets size of partition to 60% for Object cache and 40% for Akamai cache.
Akamai-weight2	Sets size of partition to 80% for Akamai cache and 20% for Object cache.
OC-weight2	Sets size of partition to 80% for Object cache and 20% for Akamai cache.
force	Changes the mode to the user defined configuration, without warning the user that existing cache data will be lost.

Command Default

The “default” configuration for disk cache management sets the available partition to predefined values for Akamai cache and Object cache.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Upgrading 294,594,694:

When you upgrade to software version 6.1.1, and configure the device/s for data cache management for the first time and perform a reload, all the data-cache is lost on reload.

Upgrading vWAAS/ISR-WAAS/SM-SRE:

When you upgrade to software version 6.1.1, and configure the device/s for data cache management for the first time and perform a reload, both data and system partitions are re-created. Logs and Data Cache are cleaned up, but software version and CM registration information is preserved.

Fresh deployment in all models:

When you do a fresh deployment of 6.1.1, and configure the device/s for data cache management for the first time and perform a reload, only Akamai and object-cache data is lost.

Second/Subsequent configuration in all models:

Configuring DCM for second/subsequent times cleans only the Akamai and object cache partitions. All other partitions are retained.

The status of data cache can be displayed using the **show disk cache-details** EXEC mode command. If data-cache is enabled, the show running configuration will display the config.

Data Cache Management is not supported on the following hardware platforms.

- 7541, 7571 and 8541, vWAAS 6K and 12K.

Examples

The following example shows how to set the available partition size equally among Akamai cache and Object cache:

```
WAE(config)# disk cache Akamai-Oc-equal
```

Related Commands

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

SyntaxDescription

enable	Enables disk encryption.

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.

Note If you are using a No Payload Encryption (NPE) image, the disk encryption feature has been disabled for use in countries where disk encryption is not permitted.

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

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

Syntax Description

remap	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**]

Syntax Description

force	(Optional) Forces RAID Logical drive to be reenabled when used with the **no** form of this command.

Defaults

The RAID-5 array is configured by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

This command is supported on WAE-7541, WAE-7571, and WAE-8541 models only.

Use this command to operate the WAE in diskless mode. In diskless mode, the partitions and disks are not mounted and cannot be used.

You must reload the device for this command to take effect.

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 **no disk logical shutdown force** command, then reload the WAE.

Examples

The following example shows how shutdown the RAID-5 logical disk drive using the **disk logical shutdown** command:

```
WAE(config)# disk logical shutdown
```

Related Commands

(config) disk disk-name

(config) disk object-cache extend

To enable extended object cache, use the **disk object-cache extend** global configuration command. To disable this feature, use the **no** form of this command.

disk object-cache extend

no disk object-cache extend

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Extended Object Cache is supported only on 674-4G, 674-8G and 694 models.
When extended object cache is enabled, the object cache space is increased only after saving the configuration and performing a reload.

The status of extended object cache can be displayed using the **show disk details** EXEC mode command. The output of this command states whether extended object cache is enabled or disabled.

This feature is supported only on WAE-674-4G, and WAE-674-8G models.

When a device is changed to AppNav mode, a warning message tells the user that changing the Device mode to AppNav Controller, will forcefully disable disk object-cache extend.The new configuration will take effect after a reload. If the user confirms, the system proceeds with reloading the system configuration and the extended object cache is disabled.

Examples

The following example shows how to enable extended object cache:

```
WAE(config)# disk object-cache extend
Cumulative disk space for all VBs will be reduced to 30GB.
Are you sure want to enable [yes/no]?
```

Related Commands

(config) disk object-cache extend

(config) dre

To enable and configure DRE (Data Redundancy Elimination) auto bypass and load monitor settings, use the **dre** global configuration command. To disable DRE settings, use the **no** form of this command.

dre {**auto-bypass** {**cache-percent** [*percent_no*] | **comp-threshold** [*comp_threshold*] | **enable**} | **load-monitor** {**report** | **disk-max-latency** [*disk-mask-latency*] | **threshold** [*threshold*] }}

no dre {**auto-bypass** {**cache-percent** | **comp-threshold** | **enable**} | **load-monitor** {**report** | | **disk-max-latency** | **threshold**}}

Syntax Description

auto-bypass	Configures DRE auto bypass settings.
cache-percent *percent_no*	Sets the cache size percent threshold for bypass trigger (1-99).
comp-threshold *comp_threshold*	Sets the DRE compression ratio threshold for bypass trigger (1-50).
enable	Enables DRE auto bypass.
load-monitor	Configures load monitor settings.
report	Enables load report.
disk-max-latency *disk-max-latency*	Sets the disk latency maximum (1-1000). Default is 5.
threshold *threshold*	Sets the DRE load threshold (50-99). Default is 95.

Defaults

Enabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **dre auto-bypass** global configuration command to generate an alarm and automatically DRE bypass application traffic.

Examples

The following example shows how to enable DRE auto bypass using the **dre** command:

```
WAE(config)# dre auto-bypass enable
```

Related Commands

(config) dre

(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

timeout	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

central-manager

Usage Guidelines

A Telnet session or Secure Shell (SSH) session with the WAAS device can remain open and inactive for the interval of time specified by the **exec-timeout** command. When the **exec-timeout** interval elapses, the WAAS device automatically closes the Telnet or SSH session.

Examples

The following example 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

(config) telnet enable

(config) exit

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

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

All modes

Device Modes

application-accelerator

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 exporter

To configure the collector server destination for the exported information, use the **flow exporter** global configuration command.

flow exporter *exporter name* {**description** | **destination** *ip_address*| **exit | export-protocol { ipfix | netflowv9} | no | transport }**

Syntax Description

description	Provides a description for the exporter.
destination	Specifies the destination for the flow records
exit	Exits from this submode
export-protocol	Specifies the export protocol for the flow records - IPFIX or Netflow-v9 (default).
no	Negates a command or set its defaults
transport	Specifies the transport protocol for the flow records. The default port is 2055.
enable	Enables flow monitoring.
host *ip_address*	Specifies the IP address of the collection control agent.

Defaults

No default behavior or values.

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.

Examples

The following example shows how to enable flow monitoring using the **flow exporter** command:

```
WAE(config)# flow exporter exporter name
WAE(config-flow_exporter)# destination 2.2.2.2
WAE(config-flow_exporter)# description descriptive name
WAE(config-flow_exporter)# export-protocol ?
  IPFIX       IPFIX export protocol
  netflow-v9  Netflow v9 export protocol (default)
WAE(config-flow_exporter)# export-protocol ipFIX
WAE(config-flow_exporter)# transport udp ?
  <1-65535>  Specify the UDP port number (default is 2055)
WAE(config-flow_exporter)# transport udp 12000
WAE(config-flow_exporter)# exit
```

Related Commands

debug flow

(config) flow record

To configure WAAS-specific flow information to be sent to the collector, use the **flow record** global configuration command.

flow record *record name* {**collect** | **exit | no}**

Syntax Description

collect	Collects flow information.
exit	Exits from this submode.
no	Negates a command or sets its defaults.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

For information about how to configure a flow record for flow monitoring on the WAE, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 15.

Examples

The following example shows how to create a flow record using the **flow record** command:

```
WAE(config)# flow record waas all
WAE(config)# collect waas
WAE(config)# exit
```

Related Commands

(config) flow monitor

(config) flow exporter

(config) flow monitor

To enable network traffic flow monitoring and to register the WAE with the tcpstat-v1 collector for traffic analysis (in case of NetQoS), 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*}

flow monitor *monitor name* {**description** | **enable** | **exporter** | **record** | **rename** }

Syntax Description

tcpstat-v1	Sets the tcpstat-v1 collector configuration.
enable	Enables flow monitoring.
host *ip_address*	Specifies the IP address of the collection control agent.
description	Provides a description for the monitor.
exporter	Specifies the exporter.
record	Specifies the record to be exporter.
rename	Renames this monitor.

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.

Examples

The following example shows how to enable flow monitoring (for NetQos) using the **flow monitor** command :

```
WAE(config)# flow monitor tcpstat-v1 enable
```

For Netflowv9, the following example shows how to specify which flow record should go to which flow exporter using the **flow monitor** command :

```
WAE(config)# flow monitor MonitorName
WAE(config-flow_monitor)# exporter ExporterName
WAE(config-flow_monitor)# record RecordName
WAE(config-flow_monitor)# enable
```

Related Commands

debug flow

(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
  tcp-promiscuous   TCP promiscuous mode service
```

The following example shows how to use partial help to determine the syntax of a WCCP argument:

```
WAE(config)# wccp tcp ?
  service-pair Pair of TCP promiscuous services
```

Related Commands

show running-config

(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*

Syntax Description

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

Defaults

The default hostname is the model number of the WAAS device (for example WAE-612).

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this command to configure the hostname for the WAAS device. The hostname is used for the command prompts and default configuration filenames. This name is also used for routing, so it conforms to the following rules:

- It can use only alphanumeric characters and hyphens (-).
- The maximum length is 30 characters.
- The following characters are considered illegal and cannot be used when naming a device: @, #, $,%, ^, &, *, (), |, \””/, <>.

Examples

The following example shows how to change the hostname of the WAAS device to *sandbox*:

```
WAE(config)# hostname sandbox
Sandbox(config)#
```

The following example shows how to remove the hostname:

```
Sandbox(config)# no hostname
WAE(config)#
```

Related Commands

dnslookup

(config) ip

(config-if) ip

show hosts

(config) inetd

To enable FTP 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**}

no inetd enable {**ftp** }

Syntax Description

enable	Enables services.
ftp	Enables FTP services.

Defaults

FTP is enabled..

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** 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 InlineGroup

(config) interface GigabitEthernet

(config) interface TenGigabitEthernet

(config-if) encapsulation dot1Q

(config) interception

To configure traffic interception with an access list, use the **interception** global configuration command. To disable the interception access list, use the **no** form of this command.

interception access-list {*acl-num* | *acl_name*}

no interception access-list {*acl-num* | *acl_name*}

Syntax Description

acl_num	Numeric identifier that identifies the ACL to apply to traffic interception. For standard ACLs, the valid range is 1–99; for extended ACLs, the valid range is 100–199.
acl_name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to traffic interception.

Defaults

No default behaviors or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **interception** command to apply an access list (ACL) to traffic interception. Packets permitted by the ACL are intercepted for WAAS optimization (on an application accelerator device) or for distribution (on an ANC). Packets denied by the ACL are passed through by WAAS. You can define ACLs by using the **ip access-list standard** or **ip access-list extended** configuration commands.

Note On an ANC the `tcp ... established` extended ACL rule type is not supported.

If you specify an interception ACL that is not defined, it is considered to be a "permit any" ACL and all traffic is intercepted.

An interception ACL works both with WCCP and inline interception modes.

When used with interface ACLs and WCCP ACLs, the interface ACL is applied first, the WCCP ACL is applied second, and then the interception ACL is applied last.

Examples

The following example shows how to define and apply an ACL that intercepts all traffic except WWW traffic from a particular client:

```
dc-wae(config)# ip access-list extended iacl
```

```
dc-wae(config-ext-nacl)# deny tcp host 10.74.2.132 any eq www
dc-wae(config-ext-nacl)# permit ip any any
dc-wae(config-ext-nacl)# exit

dc-wae(config)# interception access-list iacl
```

Related Commands

(config) ip access-list

show ip access-list

(config) interception-method

To configure the traffic interception method, use the **interception-method** global configuration command. To disable the interception method, use the **no** form of this command.

interception-method {**inline** | **appnav-controller** | **wccp** }[**force**]

no interception-method {**inline** | **appnav-controller** | **wccp** }[**force**]

Syntax Description

inline	Enables inline traffic interception. For vWAAS with WAAS Version 6.2.1 and later, this parameter is also available for vWAAS.
appnav-controller	Enables a WAAS node to receive traffic for optimization from an AppNav Controller in an AppNav deployment. (Available only on devices in application-accelerator device mode.)
wccp	Enables WCCP traffic interception.
force	Forces the configuration without prompting.

Defaults

No default behaviors or values.

Command Modes

global configuration

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

You must use the **interception-method** command to enable a traffic interception method before configuring other traffic interception settings. Other settings that are specific to a particular traffic interception method are not available until after you use this command to enable the method.

When you are changing the traffic interception method, all configuration settings for the current method are removed before the new method is enabled. You are prompted to confirm before the command proceeds.

Examples

The following example shows how to enable WCCP interception:

```
dc-wae(config)# interception-method wccp
Inline interception method will be removed. Proceed?[yes]: yes
```

Related Commands

(config) bridge

(config) inline

(config) interface InlineGroup

(config) wccp tcp-promiscuous service-pair

show interception-method

(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 *index* | **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*]}} |
ipv6 {address [autoconfig | dhcp | use-link-local-only | ip_address] | nd [dad-transmits *range*]} |
load-interval *seconds* **|** **mtu** *mtusize* | **shutdown** | **standby** *group-index* [**primary**]]

no interface GigabitEthernet *slot/port* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **cdp enable** |
channel-group *index* | **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*]}} |
ipv6 {address [autoconfig| dhcp | use-link-local-only| ip_address] | nd [secondary]} |
load-interval *seconds* **|** **mtu** *mtusize* | **shutdown** | **standby** *group-index* [**primary**]

Syntax Description

GigabitEthernet *slot/port*	Selects a Gigabit Ethernet interface to configure (slot and port number). The slot number and port number are separated with a forward slash character (/). Valid slot and port values depend on the hardware platform.
autosense	(Optional) Sets the GigabitEthernet interface to automatically sense the interface speed.
bandwidth	(Optional) Sets the bandwidth of the specified interface.
10	Sets the bandwidth of the interface to 10 megabits per second (Mbps).
100	Sets the bandwidth of the interface to 100 Mbps.
1000	Sets the bandwidth of the interface to 1000 Mbps. This option is not available on all ports and is the same as autosense.
cdp enable	(Optional) Enables Cisco Discovery Protocol (CDP) on the specified interface.
channel-group *index*	(Optional) Assigns the interface to the EtherChannel with the specified index (1-7).
description *text*	Enters a description of the interface.
full-duplex	(Optional) Sets the interface to full-duplex operation.
half-duplex	(Optional) Sets the interface to half-duplex operation. **Note** We strongly recommend that you do not use half duplex on the WAE, routers, switches, or other devices.
ip	(Optional) Enables IP configuration commands for the interface.
access-group	Configures access control for IP packets on this interface using access control list (ACL).
acl_num	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.
acl_name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.

in	Applies the specified ACL to inbound packets on the current interface.
out	Applies the specified ACL to outbound packets on the current interface.
address *ip-address netmask*	Sets the interface IP address and netmask.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
dhcp	(Optional) Sets the IP address to the address that is negotiated over Dynamic Host Configuration Protocol (DHCP).
client-id *id*	(Optional) Specifies the client identifier.
hostname *name*	(Optional) Specifies the hostname.
ipv6	(Optional) Enables IPv6 configuration commands for the interface.
address	Sets the interface IPv6 address
autoconfig	Obtain IPv6 address using auto configuration.
dhcp	Sets the IP address to the address that is negotiated over DHCP.
use-link-local-only	Enable IPv6 on interface using single link-local address.
ipv6 address	Specify IPv6 address in X:X:X:X: : X/0-128 format.
nd	Sets neighbor discovery parameters for the interface.
secondary	(Optional) Specifies that the configured address is a secondary IPv6 address. If this keyword is omitted, the configured address is the primary IPv6 address.
load-interval *seconds*	(Optional) Sets the interval at which to poll the interface for statistics and calculate throughput. Ranges from 30 to 600 seconds. The default is 30 seconds.
mtu *mtusize*	(Optional) Sets the interface Maximum Transmission Unit (MTU) size in bytes (576–1500).
shutdown	(Optional) Shuts down this interface.
standby *group-index*	(Optional) Sets the standby group number to *group-index*.
primary	(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). Using this option automatically enables autosense on the interface.

Note Changing the interface bandwidth, duplex mode, or MTU can cause network disruption for up to 30 seconds. The best practice is to make such changes when traffic interception is disabled or at an off-peak time when traffic disruption is acceptable.

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.

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** *id* **hostname** *name* 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, 10 Gigabit Ethernet, port-channel and standby 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** *group-index* interface configuration command. To make an interface the active interface in a standby group, use the **standby** *group-index* **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.

If a device has only two interfaces, you cannot assign an IP address to both a standby group and a port channel. On such a device, 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
```

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 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
```

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.
```

The following example shows how to assign an IPv6 global address on a Gigabit Ethernet interface:

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# ipv6 address 2001:db8::8:800:200c:417a/64
```

Related Commands

(config) interface InlineGroup

(config) interface PortChannel

(config) interface standby

(config) interface TenGigabitEthernet

(config) interface virtual

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**} | **cdp enable** | **encapsulation dot1q** *VLAN* | **full-duplex** | **half-duplex** | **inline** [**vlan** {**all** | **native** | *vlan_list*}] | **ip** {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} | **load-interval** *seconds* | **shutdown**]

no interface InlineGroup *slot/grpnumber* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **cdp enable** | **encapsulation dot1q** *VLAN* | **full-duplex** | **half-duplex** | **inline** [**vlan** {**all** | **native** | *vlan_list*}] | **ip** {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} | **load-interval** *seconds* | **shutdown**]

Syntax Description

slot/grpnumber	Slot and inline group number for the selected interface. The slot and inline group number are separated with a forward slash character (/). Valid slot and inline group values depend on the hardware platform.
autosense	(Optional) Sets the Gigabit Ethernet interface to automatically sense the interface speed.
bandwidth	(Optional) Sets the bandwidth of the specified interface.
10	Sets the bandwidth of the interface to 10 megabits per second (Mbps).
100	Sets the bandwidth of the interface to 100 Mbps.
1000	Sets the bandwidth of the interface to 1000 Mbps. This option is not available on all ports and is the same as autosense.
cdp enable	(Optional) Enables Cisco Discovery Protocol (CDP) on the specified interface.
encapsulation dot1q *VLAN*	(Optional) Sets the 802.1Q VLAN ID to be assigned to traffic leaving the WAE through this interface. The VLAN ID can range from 1–4094.
full-duplex	(Optional) Sets the interface to full duplex.
half-duplex	(Optional) Sets the interface to half duplex. **Note** We strongly recommend that you do not use half duplex on the WAE, routers, switches, or other devices.
inline	(Optional) Enables inline interception for an InlineGroup of interfaces.
vlan	(Optional) Modifies the VLAN list parameters.
all	Applies the command to all tagged and untagged packets.
native	Specifies untagged packets.
vlan_list	Comma-separated list of VLAN IDs. Restricts the inline feature to the specified set of VLANs.
ip	(Optional) Enables IP configuration commands for the interface.
access-group	Configures access control for IP packets on this interface using access control list (ACL).
acl_num	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.
acl_name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.

in	Applies the specified ACL to inbound packets on the current interface.
out	Applies the specified ACL to outbound packets on the current interface.
load-interval *seconds*	(Optional) Sets the interval at which to poll the interface for statistics and calculate throughput. Ranges from 30 to 600 seconds. The default is 30 seconds.
shutdown	(Optional) Shuts down this interface.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

An InlineGroup interface is a logical grouping of a pair of Ethernet ports that are physically contained on the optional Cisco WAE Inline Network Adapter or Cisco Interface Module. .

You can have multiple InlineGroup interfaces, which allows for multiple 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 If the VLAN ID that you set with the **encapsulation dot1q** option 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.

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

(config) interface GigabitEthernet

(config) interface PortChannel

(config) interface standby

(config) interface TenGigabitEthernet

(config) interface virtual

show interface

show running-config

show startup-config

(config) interface PortChannel

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

interface PortChannel *index* [**description** *text* | **ip** {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} | **address** *ip-address netmask*} | **ipv6** {**address** {**autoconfig** | **use-link-local only** | **ipv6 address**} | **nd** dad-tansmits *range*} | **load-interval** *seconds* **| shutdown** | **standby** *index*]

no interface PortChannel *index* [**description** *text* | **ip** {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} | **address** *ip-address netmask*} | **ipv6** {**address** {**autoconfig** | **use-link-local only** | **ipv6 address**} | **nd** dad-tansmits *range*} | **load-interval** *seconds* **| shutdown** | **standby** *index*]

Syntax Description

PortChannel *index*	Configures an EtherChannel with an interface number of 1–7.
description *text*	(Optional) Enters a description of the interface.
ip	(Optional) Enables IP configuration commands for the interface.
access-group	Configures access control for IP packets on this interface using an access control list (ACL).
acl_num	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.
acl_name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
in	Applies the specified ACL to inbound packets on the current interface.
out	Applies the specified ACL to outbound packets on the current interface.
address *ip-address netmask*	Sets the interface IP address and netmask.
ipv6	(Optional) Enables IPv6 configuration commands for the interface.
address	Sets the ipv6 address of the interface.
autoconfig	Obtain IPv6 address using auto configuration.
use-link-local only	Enable IPv6 on interface using single link-local address.
ipv6 address	Specify IPv6 address in X:X:X:X: : X/0-128 format
nd	Sets neighbor discovery parameters of the interface.
dad-transmits *range*	Number of attempts by which duplicate address should be detected.
load-interval *seconds*	(Optional) Sets the interval at which to poll the interface for statistics and calculate throughput. Ranges from 30 to 600 seconds. The default is 30 seconds.
shutdown	(Optional) Shuts down this interface.
standby *index*	(Optional) Includes the port-channel interface in the specified standby group (1-3).

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Port channels (EtherChannels) for the WAAS software support the grouping of multiple same-speed network interfaces into one virtual interface. This configuration allows you to set or remove a virtual interface that consists of up to four physical interfaces . Port channels also provide interoperability with Cisco routers, switches, and other networking devices or hosts that support port channels, load balancing, and automatic failure detection and recovery based on the current link status of each interface. You must configure port channels on the switch or router if you configure it on the WAE.

You cannot add an interface that already has a configured IP address, or is configured as primary or secondary, to a port channel.

You cannot remove a port-channel interface that is configured as the primary interface on a WAE.

Note You cannot use the inline Ethernet interfaces that are located on the Cisco WAE Inline Network Adapter to form a port-channel interface. However, you can use the interfaces on a Cisco Interface Module to form a port-channel interface.

Note No two interfaces can have IP addresses in the same subnet.

Examples

The following example shows how to create a port-channel interface. 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 a port-channel interface:

```
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

(config) interface GigabitEthernet

(config) interface InlineGroup

(config) interface standby

(config) interface TenGigabitEthernet

(config) interface virtual

(config) port-channel

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 *group-index* {**description** *text* | **ip address** *ip_address netmask* | **ipv6** {**address** {**autoconfig** | **use-link-local only** | **ipv6 address**} | **nd** dad-tansmits *range*} | **load-interval** *seconds* **| shutdown** }

no interface standby *group-index* {**description** *text* | **ip address** *ip_address netmask* | **ipv6** {**address** {**autoconfig** | **use-link-local only** | **ipv6 address**} | **nd** dad-tansmits *range*} | **load-interval** *seconds* **| shutdown** }

Syntax Description

group-index	Standby group interface. Specify a group index of 1–3, depending on the platform.
description *text*	Enters a description of the interface.
ip address *ip_address netmask*	Specifies the IP address and netmask of the interface.
ipv6	(Optional) Enables IPv6 configuration commands for the interface.
address	Sets the ipv6 address of the interface.
autoconfig	Obtain IPv6 address using auto configuration.
use-link-local only	Enable IPv6 on interface using single link-local address.
ipv6 address	Specify IPv6 address in X:X:X:X: : X/0-128 format
nd	Sets neighbor discovery parameters of the interface.
dad-transmits *range*	Number of attempts by which duplicate address should be detected.
load-interval *seconds*	(Optional) Sets the interval at which to poll the interface for statistics and calculate throughput. Ranges from 30 to 600 seconds. The default is 30 seconds.
shutdown	Shuts down this interface.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

WAVE-294/594/694/7541/7571/8541 devices support up to two standby groups. .

A standby group cannot be removed if it is configured as the system primary interface.

A standby group can have up to two member interfaces.

Note No two interfaces can have IP addresses in the same subnet.

Related Commands

(config) interface GigabitEthernet

(config) interface InlineGroup

(config) interface PortChannel

(config) interface TenGigabitEthernet

(config) interface virtual

show interface

show running-config

show startup-config

(config) interface TenGigabitEthernet

To configure a TenGigabitEthernet 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 TenGigabitEthernet *slot/port* [**cdp enable** | **channel-group** *index* | **description** *text* |
ip {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} |
address {*ip_address netmask* [**secondary**] | **ipv6 {address {autoconfig | use-link-local only |**
ipv6 address} | nd dad-tansmits range} | **dhcp** [**client-id** *id*][**hostname** *name*]}} |
load-interval *seconds* **| mtu** *mtusize* | **shutdown** | **standby** *group-index* [**primary**]]

no interface TenGigabitEthernet *slot/port* [**cdp enable** | **channel-group** *index* | **description** *text* |
ip {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} |
address {*ip_address netmask* [**secondary**] | **ipv6 {address {autoconfig | use-link-local only |**
ipv6 address} | nd dad-tansmits range} | **dhcp** [**client-id** *id*][**hostname** *name*]}} |
load-interval *seconds* **| mtu** *mtusize* | **shutdown** | **standby** *group-index* [**primary**]]

Syntax Description

slot/port	TenGigabitEthernet interface to configure (slot and port number). The slot number and port number are separated with a forward slash character (/). Valid slot and port values depend on the hardware platform.
cdp enable	(Optional) Enables Cisco Discovery Protocol (CDP) on the specified interface.
channel-group *index*	(Optional) Assigns the interface to the EtherChannel with the specified index (1–7).
description *text*	Enters a description of the interface.
ip	(Optional) Enables IP configuration commands for the interface.
access-group	Configures access control for IP packets on this interface using access control list (ACL).
acl_num	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.
acl_name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
in	Applies the specified ACL to inbound packets on the current interface.
out	Applies the specified ACL to outbound packets on the current interface.
address *ip-address netmask*	Sets the interface IP address and netmask.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
dhcp	(Optional) Sets the IP address to the address that is negotiated over Dynamic Host Configuration Protocol (DHCP).
client-id *id*	(Optional) Specifies the client identifier.
hostname *name*	(Optional) Specifies the hostname.
ipv6	(Optional) Enables IPv6 configuration commands for the interface.
address	Sets the ipv6 address of the interface.

autoconfig	Obtain IPv6 address using auto configuration.
use-link-local only	Enable IPv6 on interface using single link-local address.
ipv6 address	Specify IPv6 address in X:X:X:X: : X/0-128 format
nd	Sets neighbor discovery parameters of the interface.
dad-transmits *range*	Number of attempts by which duplicate address should be detected.
load-interval *seconds*	(Optional) Sets the interval at which to poll the interface for statistics and calculate throughput. Ranges from 30 to 600 seconds. The default is 30 seconds.
mtu *mtusize*	(Optional) Sets the interface Maximum Transmission Unit (MTU) size in bytes (576–1500).
shutdown	(Optional) Shuts down this interface.
standby *group-index*	(Optional) Sets the standby group number to *group-index*.
primary	(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.

Note Changing the MTU can cause network disruption for up to 30 seconds. The best practice is to make such changes when traffic interception is disabled or at an off-peak time when traffic disruption is acceptable.

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 TenGigabitEthernet 1/0), use the **show running-config** or **show startup-config** commands. The **ip** and **shutdown** commands are listed separately in this command reference.

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** *id* **hostname** *name* 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, 10 Gigabit Ethernet, port-channel and standby 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** *group-index* interface configuration command. To make an interface the active interface in a standby group, use the **standby** *group-index* **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, and 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.

If a device has only two interfaces, you cannot assign an IP address to both a standby group and a port channel. On such a device, 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 TenGigabitEthernet 1/0 ip access-group 1 in
```

The following example shows that an interface can be configured in a sequence of CLI commands:

```
WAE(config)# interface TenGigabitEthernet 1/0
WAE(config-if)# ip access-group 1 in
WAE(config-if)# exit
```

The following example shows how to enable a shut down interface:

```
WAE(config)# no interface TenGigabitEthernet 1/0 shutdown
```

The following example shows how to add an interface to a channel group:

```
WAE# configure
WAE(config)# interface TenGigabitEthernet 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 TenGigabitEthernet 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 TenGigabitEthernet interface:

```
WAE# configure
WAE(config)# interface TenGigabitEthernet 1/0
WAE(config-if)# ip address 10.10.10.10 255.0.0.0 secondary
```

The following example shows how to configure a description for a TenGigabitEthernet interface:

```
WAE(config)# interface TenGigabitEthernet 1/0
WAE(config-if)# description This is a TenGigabitEthernet interface.
```

Related Commands

(config) interface GigabitEthernet

(config) interface InlineGroup

(config) interface PortChannel

(config) interface standby

(config) interface virtual

show interface

show running-config

show startup-config

(config) interface virtual

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

interface virtual *slot/port* {**cdp enable** | **description** *text* |
ip {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} | **address** {*ip_address netmask* [**secondary**]
| **ipv6** {**address** {**autoconfig** | **use-link-local only** | **ipv6 address**} | **nd** dad-tansmits *range*} |
load-interval *seconds* | | **mtu** *mtusize* | **shutdown** }

no interface virtual *slot/port* (**cdp enable** | **description** *text* |
ip {**access-group** {*acl-num* | *acl_name*} {**in** | **out**} | **address** {*ip_address netmask* [**secondary**]
| **ipv6** {**address** {**autoconfig** | **use-link-local only** | **ipv6 address**} | **nd** dad-tansmits *range*} |
load-interval *seconds* | | **mtu** *mtusize* | **shutdown** }

Syntax Description

slot/port	vWAAS interface to configure (slot and port number). The slot range is 1–2; the port range is 0. The slot number and port number are separated with a forward slash character (/).
cdp enable	(Optional) Enables Cisco Discovery Protocol (CDP) on the specified interface.
description *text*	Enters a description of the interface.
ip	(Optional) Enables IP configuration commands for the interface.
access-group	Configures access control for IP packets on this interface using access control list (ACL).
acl_num	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.
acl_name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
in	Applies the specified ACL to inbound packets on the current interface.
out	Applies the specified ACL to outbound packets on the current interface.
address *ip-address netmask*	Sets the interface IP address and netmask.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
dhcp	(Optional) Sets the IP address to the address that is negotiated over Dynamic Host Configuration Protocol (DHCP).
client-id *id*	(Optional) Specifies the client identifier.
hostname *name*	(Optional) Specifies the hostname.
ipv6 address	Specify IPv6 address in X:X:X:X: : X/0-128 format
nd	Sets neighbor discovery parameters of the interface.
dad-transmits *range*	Number of attempts by which duplicate address should be detected.

mtu *mtusize*	(Optional) Sets the interface Maximum Transmission Unit (MTU) size in bytes (576–1500).
shutdown	(Optional) Shuts down this interface.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

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 virtual 1/0), use the **show running-config** or **show startup-config** commands.

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 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** *id* **hostname** *name* 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.

After you define the description for an interface, use the **show** EXEC commands to display the defined interface descriptions. Enter the **show interface virtual** EXEC command to display the defined description for a virtual interface on the WAE.

Examples

The following example shows how to assign a secondary IP address on a virtual interface on a vWAAS device:

```
WAE# configure
WAE(config)# interface virtual 1/0
WAE(config-if)# ip address 10.10.10.10 255.0.0.0 secondary
```

The following example shows how to configure a description for a virtual interface:

```
WAE(config)# interface virtual 1/0
WAE(config-if)# description This is a virtual interface.
```

Related Commands

(config) interface GigabitEthernet

(config) interface InlineGroup

(config) interface PortChannel

(config) interface standby

(config) interface TenGigabitEthernet

show interface

show running-config

show startup-config

(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 {**access list** |**default-gateway** [**management**] *ip-address* | **domain-name** *name1 name2 name3* | **ftp management** | **host** *hostname ip-address* | **icmp** | **name-server {interface** | *ip-addresses* }| **ntp** | **radius management** | **tacacs management** | **path-mtu-discovery enable** | **route** [**management**] *dest_addrs net_addrs gateway_addrs* | **tftp management** | **unreachable**}

no ip {**default-gateway** [**management**] *ip-address* | **domain-name** *name1 name2 name3* | **ftp management** | **host** *hostname ip-address* | **name-server** *ip-addresses* | **radius management** | **tacacs management** | **path-mtu-discovery enable** | **route** [**management**] *dest_addrs net_addrs [gateway_addrs]* | **tftp management**}

Syntax Description

access list	Specifies the access lists on a WAAS device.
default-gateway *ip-address*	Specifies the IP address of the default gateway (if not routing IP).
management	Specifies that the default gateway or net route is for the management interface.
domain-name *name1 name2 name3*	Specifies domain names (up to three can be specified).
ftp management, management-v6	Configures the device to use the management interface(IPv4 or IPv6) for FTP traffic.
host *hostname ip-address*	Adds an entry to the /etc/hosts file on the device, mapping the specified hostname to the specified IP address of the host.
icmp	Configures ICMP options.
name-server interface management, management-v6	Configures the device to use the management interface (IPv4 or IPv6)for name-server queries.
ip-addresses	Specifies the address of the name server and IP addresses of the name servers (IPv4 or IPv6 address up to a maximum of three).
ntp management, management-v6	Configures the device to use the management interface (IPv4 or IPv6)for NTP.
radius management, management-v6	Configures the device to use the management interface for radius traffic.
tacacs management, management-v6	Configures the device to use the management interface (IPv4 or IPv6) for tacacs traffic.
path-mtu-discovery enable	Enables RFC 1191 Path Maximum Transmission Unit (MTU) discovery.
route *dest_addrs net_addrs gateway_addrs*	Specifies the net route (destination route address, netmask address, and gateway address).

tftp management, management-v6	Configures the device to use the management interface (IPv4 or IPv6) for TFTP traffic.
unreachable	Enables ICMP destination unreachable messages.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager. (Management interface commands are not available when device is on central manager mode)

Usage Guidelines

To define a default gateway, use the **ip default-gateway** command. If you have designated a management interface, you can configure a different default gateway for the management interface by using the **management** keyword. 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 three 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 disabled because the WAE does not receive ICMP packets. 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 default gateway for the management interface on the WAAS device, if it is different from the standard default gateway:

```
WAE(config)# ip default-gateway management 192.168.10.35
```

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

To create and modify access lists on a WAAS device for controlling access to interfaces or applications, and to define subnets, use the **ip access-list** global configuration command. To disable an access list, use the **no** form of this command.

ip access-list {**standard** {*acl-name* | *acl-num*} | **extended** {*acl-name* | *acl-num*} | **logging**}

no ip access-list {**standard** {*acl-name* | *acl-num*} | **extended** {*acl-name* | *acl-num*} | **logging**}

Syntax Description

standard	Enables standard ACL configuration mode. The CLI enters the standard ACL configuration mode in which all subsequent commands apply to the current standard access list. The (config-std-nacl) prompt appears: WAE(config-std-nacl)# See the "Standard ACL Configuration Mode Commands" section for details about working with entries in a standard access list and the commands available from the standard ACL configuration mode (config-std-nacl)#.
extended	Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. The (config-ext-nacl) prompt appears: `WAE(config-ext-nacl)#` See the "Extended ACL Configuration Mode Commands" section for details about working with entries in an extended access list and the commands available from the extended ACL configuration mode (config-ext-nacl)#.
acl-name	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
acl-num	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
logging	Enables logging for all IP access lists.

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)#
```

To define a subnet, use either a standard or an extended ACL. In an HTTP AO subnet configuration, the **access-list** option must have at least one condition statement in it for it to exist. The list is terminated by an implicit **deny any** (standard access list) or **deny ip any any** (extended access list) condition statement. This statement applies to HTTP AO optimizations unless the ACL has an explicit **permit all** statement in it. If an *acl name* or *acl number* does not exist (if no condition statements exist in the access list), it is considered as an implicit **permit any** (standard access list) or **permit ip any any**(extended access list) condition statement. We recommend that you explicitly add **permit any** or **deny any** at the end of the ACL to make all the conditions clear for the subnet feature.

Use the **ip access-list logging** command to log denied packets.

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
 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
. . .
```

The following example shows how to configure an ACL to define a subnet:

```
WAE(config)# ip access-list extended md_acl
WAE(config-ext-nacl)# permit ip 2.57.34.0 0.0.0.255 2.57.34.0 0.0.0.255
WAE(config-ext-nacl)# exit
WAE(config)# ip access-list standard 10
WAE(config-std-nacl)# deny 1.1.1.0 0.0.0.255
WAE(config-std-nacl)# permit any
WAE(config-std-nacl)# exit
```

(config) ip icmp rate-limit unreachable

To limit the rate at which Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **ip icmp rate-limit unreachable** command in global configuration mode. To remove the rate limit, use the no form of this command.

ip icmp rate-limit unreachable df *microseconds*

no ip icmp rate-limit unreachable df *microseconds*

Syntax Description

df	Limits the rate ICMP destination unreachable messages are sent when Type 3 code 4, destination unreachable, don't fragment (DF) bit sent and fragmentation required, is specified in the IP header of the ICMP destination unreachable message.
microseconds	Time limit (in microseconds) in which one ICMP destination unreachable message is sent. The range is 250 microseconds to 1000000 microseconds.

Defaults

The default value is one ICMP destination unreachable message per 500 microseconds.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

This feature is enabled by default. The no ip icmp rate-limit unreachable df command turns off the previously configured rate limit.

The software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the df option is not configured, the ip icmp rate-limit unreachable command sets the time values for DF destination unreachable messages. If the df option is configured, its time values remain independent from those of general destination unreachable messages.

Examples

The following example sets the rate of the ICMP destination unreachable message to one message every 10 microseconds:

```
WAE(config)# ip icmp rate-limit unreachable df 10
```

The following example turns off the previously configured rate limit:

```
WAE(config)# no ip icmp rate-limit unreachable df
```

Related Commands

clear arp-cache

(config-if) ip access-group

show ip access-list

(config) ip unreachables df

(config) ip unreachables df

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the ip unreachables df command in global configuration mode. To disable this function, use the no form of this command.

ip unreachables df

no ip unreachables df

SyntaxDescription

df	Limits the rate ICMP destination unreachable messages are sent when Type 3 code 4, destination unreachable, don't fragment (DF) bit sent and fragmentation required, is specified in the IP header of the ICMP destination unreachable message.

Defaults

The default value is one ICMP destination unreachable message per 500 microseconds.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

If the software receives a nonbroadcast packet destined for itself that uses an unknown protocol, it sends an ICMP protocol unreachable message back to the source. Similarly, if the software receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address, it sends an ICMP host unreachable message to the source. This feature is enabled by default.

ExamplesExamples

The following example enables the generation of ICMP unreachable messages, as appropriate, on an interface:

```
WAE(config)# interface ethernet 0
WAE(config)# ip unreachables df
```

Related Commands

clear arp-cache

(config-if) ip access-group

show ip access-list

(config) ip icmp rate-limit unreachable

(config) ipv6

To change the initial network device configuration settings, use the **ipv6** global configuration command. To delete or disable these settings, use the **no** form of this command.

ipv6 {**default-gateway** [**management**] *ip-v6 address* | **route** [**management**] *ip-v6 address*}

no ipv6 {**default-gateway** [**management**] *ip-v6 address* | **route** [**management**] *ip-v6 address*}

Syntax Description

default-gateway *ip-address*	Specifies the IPv6 address of the default gateway, in the X:X:X:X format.
route *ip-v6 address*	Specifies the net route and the IPv6 address.
management	Specifies that the default gateway or net route is for the management interface.

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.If you have designated a management interface, you can configure a different default gateway for the management interface by using the **management** keyword. The WAAS device uses the default gateway to route IP packets when there is no specific route found to the destination. To remove the IP default gateway, use the **no** form of this command.

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.If you have designated a management interface, you can configure a different ip route for the management interface by using the **management** keyword.

To configure static IP routing, use the **ip route** command. To remove the route, use the **no** form of this command.

Examples

The following example shows how to configure a default gateway for the WAAS device:

```
WAE(config)# ipv6 default-gateway 2013:1:1:10::1
```

The following example shows how to configure a default gateway for the management interface on the WAAS device, if it is different from the standard default gateway:

```
WAE(config)# ipv6 default-gateway management 2013:1:2:10::1
```

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

```
WAE(config)# ipv6 route 2000:2:3:4::6/128 2013:1:1:10::1
```

Related Commands

(config) ip

show ip routes

(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 {**dns**}

no kerberos {**dns**}

Syntax Description

dns	Enables or disables DNS lookup for Kerberos.

Defaults

kerberos-realm: NULL string

port-number: 88

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

All Windows 2000 domains are also Kerberos realms. Because the Windows 2000 domain name is also a DNS domain name, the Kerberos realm name for the Windows 2000 domain name is always in uppercase letters. This capitalization follows the recommendation for using DNS names as realm names in the Kerberos Version 5 protocol document (RFC-1510) and affects only interoperability with other Kerberos-based environments.

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

Syntax Description

This command has no arguments or keywords.

Defaults

The kernel debugger is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

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**. On a vWAAS device, kdb can be enabled by pressing the **Esc** key and typing **kdb**.

The WAAS device is often unattended at many sites, and it is desirable for the WAAS device to automatically reboot after generating a core dump instead of requiring user intervention. Disabling the kernel debugger allows automatic recovery.

Examples

The following example shows how to enable, and then disable, access to the kernel debugger:

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

Related Commands

(config) kernel kdump enable

(config) kernel kdump enable

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 kernal crash dump file is stored in the following disk location: /local/local1/crash/*timestamp*/vmcore

The analysis of the kernal 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

Syntax Description

console	Configures the console terminal line settings.
carrier-detect	Sets the device to check the carrier detect signal before writing to the console.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Examples

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

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

enable	Enables system logging.
priority *loglevel*	Sets which priority level messages to send. Use one of the following keywords or you can specify the numeric priority: • **alert**—Immediate action needed. Priority 1. • **critical**—Immediate action needed. Priority 2. • **debug**—Debugging messages. Priority 7. • **emergency**—System is unusable. Priority 0. • **error**—Error conditions. Priority 3. • **information**—Informational messages. Priority 6. • **notice**—Normal but significant conditions. Priority 5. • **warning—**Warning conditions. Priority 4.

Defaults

Logging: on

Priority of message for console: warning (4)

Log file: /local1/syslog.txt

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **logging** command to set specific parameters of the system log file.

You can configure logging to send various levels of messages to the console using the **logging console priority** option.

Examples

The following example shows how to send messages that have a priority code of “error” (Level 3) to the console:

```
WAE(config)# logging console priority error
```

The following example shows how 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

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

enable	Enables system logging.
filename *filename*	Sets the name of the syslog file.
priority *loglevel*	Sets which priority level messages to send. Use one of the following keywords or you can specify the numeric priority: • **alert**—Immediate action needed. Priority 1. • **critical**—Immediate action needed. Priority 2. • **debug**—Debugging messages. Priority 7. • **emergency**—System is unusable. Priority 0. • **error**—Error conditions. Priority 3. • **information**—Informational messages. Priority 6. • **notice**—Normal but significant conditions. Priority 5. • **warning—**Warning conditions. Priority 4.
recycle *size*	Overwrites *syslog.txt* when it surpasses the recycle size (1000000–50000000 bytes).

Defaults

Logging: on

Priority of message for disk log file: debug (7)

Log file: /local1/syslog.txt

Log file recycle size: 10,000,000 bytes

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **logging** 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

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*

Syntax Description

facility	Facility parameter for syslog messages. Use one of the following keywords: • **auth**—Authorization system • **daemon—**System daemons • **kernel**—Kernel • **local0**—Local use • **local1**—Local use • **local2**—Local use • **local3**—Local use • **local4**—Local use • **local5**—Local use • **local6**—Local use • **local7**—Local use • **mail—**Mail system • **news—**USENET news • **syslog—**Syslog itself • **user—**User process • **uucp—**UUCP system

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

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

hostname	Hostname of the remote syslog host. Specify up to four remote syslog hosts. **Note** To specify more than one syslog host, use multiple command lines; specify one host per command.
ip-address	IP (IPV4/IPv6) address of the remote syslog host. Specify up to four remote syslog hosts. **Note** To specify more than one syslog host, use multiple command lines; specify one host per command.
port *port_num*	(Optional) Specifies the port to be used when logging to a host. The default port is 514.
priority *loglevel*	(Optional) Sets which priority level messages to send. Use one of the following keywords or you can specify the numeric priority: • **alert**—Immediate action needed. Priority 1. • **critical**—Immediate action needed. Priority 2. • **debug**—Debugging messages. Priority 7. • **emergency**—System is unusable. Priority 0. • **error**—Error conditions. Priority 3. • **information**—Informational messages. Priority 6. • **notice**—Normal but significant conditions. Priority 5. • **warning**—Warning conditions. Priority 4.
rate-limit *message_rate*	(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.

Defaults

Logging: on

Priority of message for a host: warning (4)

Command Modes

global configuration

Device Modes

application-accelerator

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

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** *key-num* [**md5** *authentication-key*] |
server {*ip-address* | *hostname*} [*ip-addresses* | *hostnames*] |
server-with-authentication {*ip-address* **|** *hostname*} **key** *key-num*]

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** *key-num* [**md5** *authentication-key*] |
server {*ip-address* | *hostname*} [*ip-addresses* | *hostnames*] |
server-with-authentication {*ip-address* **|** *hostname*} **key** *key-num*]

Syntax Description

authenticate	(Optional) Authenticates the NTP server.
authentication-key *key-num*	(Optional) Sets the ID of the NTP authentication key. Maximum of 4 authentication keys can be configured. The ID must be a positive integer.
md5 *authentication-key*	(Optional) Sets the value for the NTP authentication key (type MD5). The key value must be from 0 to 4294967295.
server	(Optional) Sets the NTP server IP address for the WAAS device.
ip-address	NTP server IPv4 or IPv6 address (maximum of 4).
hostname	NTP server hostname (maximum of 4).
ip-addresses	(Optional) IP address of the time server that provides the clock synchronization (maximum of 4).
hostnames	(Optional) Hostname of the time server that provides the clock synchronization (maximum of 4).
server-with-authentication	(Optional) Sets the authentication NTP server IP address for the WAAS device.
key *key-num*	(Optional) Sets the NTP authentication key ID for the authentication NTP server.

Defaults

The default NTP version number is 3.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Note 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
OR
WAE(config)# ntp 2012:3:3:3::8
WAE(config)# ntp 2012:3:3:3::8
```

clock

(config) clock

show clock

show ntp

(config) object-cache enable

To confirm repurposing of SMB resources if the disk has not already been partitioned for object cache, use the **object-cache enable** global configuration command. To disable this function, use the "no" form of the command.

object-cache enable

no object-cache enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

When object cache is enabled, you are prompted to confirm the repurposing of SMB resources if the disk has not already been partitioned for object cache.

If this is the first time disk resources are being assigned to object cache, the **object-cache enable** command will prompt you to reboot the device, since the disk partitioning only takes effect on the next reboot. The configuration is then saved, and the object cache does not have to be re-enabled on the next reboot.

Note To ensure success of the **object-cache enable** command, verify the following two conditions:

- Disk assignments have been made to object cache *before* you use this command.
- Use this command *before* you use the **accelerator smb** global configuration command.

Examples

The following example shows how to enable object cache:

```
(config)# object-cache enable
```

Related

(config) accelerator object-cache enable

show cache object-cache

show object-cache

show statistics object-cache

(config) peer

To enable peer optimization, use the **peer** global configuration command. To disable peer optimization, use the **no** form of this command.

peer device-id *deviceid* [**description** *description*] **optimization enable**

no peer device-id *deviceid* [**description** *description*] **optimization enable**

Syntax Description

device-id *deviceid*	Configures the device ID of the peer device with which to enable or disable optimization.
description *hostname*	(Optional) Configures a string that is the device description of the peer device. You should use the hostname of the peer WAE for the description.
optimization enable	Enables optimization with the specified peer.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **no peer** command to disable optimization between peer devices in a serial cluster.

Use the **peer** command to reenable optimization between peer devices if it has been disabled previously.

The *deviceid* is a hexadecimal string (for example, d4:65:01:40:40:8a) that you can obtain with the **show device-id** or **show hardware** EXEC commands.

You can configure optimization for only one peer device with this command.

Examples

The following example shows how to disable optimization with a serial peer device:

```
WAE(config)# no peer device-id d4:65:01:40:40:8a description wae-sj-dc2 optimization
enable
```

Related Commands

show device-id

show hardware

(config) interception

(config) policy-map

To configure an optimization policy map, use the **policy-map** global configuration command. To unconfigure settings, use the **no** form of this command.

policy-map type { **waas**} *policymap-name* [**rename** *new-name*]

no policy-map type { **waas**} *policymap-name*

Syntax Description

waas	Configures a WAAS optimization policy map.
policymap-name	Policy map name (up to 40 alpha-numeric characters and hyphen, beginning with a letter).
rename *new-name*	(Optional) Renames the policy map with the specified new name.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **policy-map** command to add or modify policy maps that associate policy actions with class maps. This command invokes the Policy Map configuration mode, which is indicated by a different prompt **(**config-pmap**)**. For more information on Policy Class Map configuration mode commands, see the "Policy Map Configuration Mode Commands" section. To return to global configuration mode, enter the **exit** command.

You can delete a policy map by using the **no** form of this command.

The WAAS software comes with many class maps and policy rules that help your WAAS system classify and optimize some of the most common traffic on your network. Before you create a new class map or policy rule, we recommend that you review the default class map and policy rules and modify them as appropriate. It is usually easier to modify an existing class map or policy rule than to create a new one. For a list of the default applications, class maps, and policy rules, see the *Cisco Wide Area Application Services Configuration Guide*.

Note We strongly recommend that you use the WAAS Central Manager GUI to centrally configure policy maps for your WAAS devices. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to configure a WAAS optimization policy map:

```
wae(config)# policy-map type waas myPolicy
wae(config-pmap)# description My optimization policy
wae(config-pmap)# class httpx
wae(config-pmap-c)# optimize full accelerate http application Web
```

Related Commands

(config) class-map

(config) service-policy

(config) port-channel

To configure port channel load-balancing 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** | **src-dst-ip-port**}

no port-channel load-balance {**src-dst-ip** | **src-dst-ip-port**}

Syntax Description

load-balance	Configures the load-balancing method.
src-dst-ip	Specifies the load-balancing method based on a combination of source and destination IP addresses.
src-dst-ip-port	Specifies the load-balancing method based on a combination of source and destination IP addresses/ports.

Defaults

src-dst-ip-port is the default load-balancing method.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to configure src-dst-ip load balancing on a port channel and then disable it:

```
WAE(config)# port-channel load-balance src-dst-ip
WAE(config)# no port-channel load-balance src-dst-ip
```

Related Commands

(config) interface PortChannel

(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** slot/*port* | **PortChannel** *index* | **Standby** *group-index* | **TenGigabitEthernet** slot/*port*} {**IPv4** | **IPv6**}[**management**]

no primary-interface {**GigabitEthernet** *slot*/*port* | **PortChannel** *index* | **Standby** *group-index* | **TenGigabitEthernet** slot/*port*} {**IPv4** | **IPv6**}[**management**]

primary-interface virtual *slot/port* {**IPv4** | **IPv6**}[**management**]

no primary-interface virtual *slot/port* {**IPv4** | **IPv6**}[**management**]

Syntax Description

GigabitEthernet *slot/port*	Selects a Gigabit Ethernet interface as the primary interface of the WAAS device. Valid slot and port values depend on the hardware platform.
PortChannel *index*	Selects a port channel interface as the primary interface of the WAAS device. Specify the port channel index number (1–4).
Standby *group-index*	Selects a standby group as the primary interface of the WAAS device. Specify the standby group number (1–3).
TenGigabitEthernet *slot/port*	Selects a TenGigabitEthernet interface as the primary interface of the WAAS device. Valid slot and port values depend on the hardware platform.
IPv4	Configures interface for IPv4 traffic.
IPv6	Configures interface or IPv6 traffic.
management	Designates the specified interface for management traffic.
virtual	Selects the virtual interface as the primary interface. Specify the slot range (1–2) and the port range as 0.

Defaults

The default primary interface is the Gigabit Ethernet 0/0 or 1/0 interface, depending on the hardware platform. 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, for IPv6 traffic, on a WAAS device:

```
WAE(config)# primary-interface GigabitEthernet 1/0 IPv6
```

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 IPv6
```

The following example shows how to specify port channel interface 1 as the primary interface on a WAAS device:

```
WAE(config)# primary-interface portchannel 1 IPv6
```

The following example shows how to specify the Gigabit Ethernet slot 1, port 0 as the primary interface, for IPv6 traffic, on a WAAS device and designate it to be used for management traffic:

```
WAE(config)# primary-interface GigabitEthernet 1/0 IPv6 management
```

To configure a primary interface to be used as a management interface, you should have configured it with an ip and default-gateway address.

Related Commands

(config) interface GigabitEthernet

(config) interface TenGigabitEthernet

(config) radius-server

To configure a set of RADIUS authentication server settings on the WAAS device, use the r**adius-server** global configuration command. To disable RADIUS authentication server settings, use the **no** form of this command.

radius-server {**host** *hostname* | ip-addr | ipv6 {ipv6-address} [**primary**] | **key** *keyword* | **retransmit** *retries* | **timeout** *seconds*}

no radius-server {**host** *hostname* | *hostipaddr* | ipv6 {ipv6-address} [**primary**] | **key** *keyword* | **retransmit** *retries* | **timeout** *seconds*}

Syntax Description

host *hostname*	Specifies a RADIUS server. You can have a maximum of 5 servers.
ip-address	IPv4 address of the RADIUS server.
ipv6	IPv6 address of the RADIUS server.
primary	(Optional) Sets the server as the primary server.
key *keyword*	Specifies the encryption key shared with the RADIUS servers. You can have a maximum of 15 characters.
retransmit *retries*	Specifies the number of transmission attempts (1–3) to an active server for a transaction. The default is 2.
timeout *seconds*	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

retransmit *retries*: 2

timeout *seconds*: 5

Command Modes

global configuration

Device Modes

application-accelerator

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 **(config) authentication configuration** command.)

You can configure multiple RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the RADIUS farm, in the order in which they were configured. If authentication fails for any reason other than a server is unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **authentication fail-over server-unreachable** 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 **show radius-server** command.

```
WAE(config)# radius-server host 172.16.90.121
WAE(config)# radius-server key myradiuskey
WAE# show radius-server
Radius Configuration:
---------------------
Radius Authentication is on
    Timeout       = 5
    Retransmit    = 3
    Key           = ****
    Servers
    -------
```

Related Commands

show radius-server

(config) service-policy

To configure optimization service policy, use the **service-policy** global configuration command. To unconfigure settings, use the **no** form of this command.

service-policy {**optimize** *policy-map-name* | **type** {**waas** {**config** {**remove-all** | **restore-predefined**}| **set ip dscp** *dscp-marking*}}

no service-policy {**optimize** *policy-map-name* | **type** { **waas** {**config** {**remove-all** | **restore-predefined**}| **set ip dscp** *dscp-marking*}}

Syntax Description

optimize *policy-map-name*	Specifies the active optimization policy map.
type	Specifies an operation on optimization policies.
waas	Specifies an operation on optimization policies.
set ip dscp *dscp-marking*	Specifies the default DSCP marking value, as shown in Table 3-2.

Defaults

The default DSCP marking value is copy.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

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.

A DSCP value is assigned in a policy rule and applies to all traffic associated with a class 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.

Table 3-2 lists the valid DSCP marking values that you can specify.

Table 3-2 DSCP Marking Values

DSCP Code	Description
0 - 63	Marks packets with a numeric dscp from 0 to 63.
af11	Marks packets with AF11 dscp (001010).
af12	Marks packets with AF11 dscp (001100).
af13	Marks packets with AF13 dscp (001110).
af21	Marks packets with AF21 dscp (010010).
af22	Marks packets with AF22 dscp (010100).

Table 3-2 DSCP Marking Values (continued)

DSCP Code	Description
af23	Marks packets with AF23 dscp (010110).
af31	Marks packets with AF31 dscp (011010).
af32	Marks packets with AF32 dscp (011100).
af33	Marks packets with AF33 dscp (011110).
af41	Marks packets with AF41 dscp (100010).
af42	Marks packets with AF42 dscp (100100).
af43	Marks packets with AF43 dscp (100110).
cs1	Marks packets with CS1 (precedence 1) dscp (001000).
cs2	Marks packets with CS2 (precedence 2) dscp (010000).
cs3	Marks packets with CS3 (precedence 3) dscp (011000).
cs4	Marks packets with CS4 (precedence 4) dscp (100000).
cs5	Marks packets with CS5 (precedence 5) dscp (101000).
cs6	Marks packets with CS6 (precedence 6) dscp (110000).
cs7	Marks packets with CS7 (precedence 7) dscp (111000).
copy	Copies the DSCP value from the incoming packet to the outgoing packet. (default)
default	Marks packets with default dscp (000000).
ef	Marks packets with EF dscp (101110).

Examples

The following example shows how to set the default DSCP marking value to copy:

```
WAE(config)# service-policy type waas set ip dscp copy
```

The following example shows how to restore optimization policies:

```
WAE(config)# service-policy type waas config restore-predefined
```

Related Commands

show service-policy

(config) class-map

(config) policy-map

(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**} **name** *attr-name* **value** *attr-value*

no smb-conf section {**global**} **name** *attr-name* **value** *attr-value*

Syntax Description

global	Specifies one of the global print parameters.
name *attr-name*	Specifies the name of the parameter in the specified section that you want to manually configure (up to 80 characters).
value *attr-value*	Specifies the value of the parameter (up to 255 characters).

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

Legacy print services are no longer supported in WAAS 4.4.x and later. We recommend using the Windows print accelerator (see the (config) accelerator windows-print command).

The *smb.conf* file contains a variety of samba Configuration 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.

Table 3-3 Samba Configuration Parameters

Parameter Name	Default Value	Parameter Description
global parameters		
idmap uid	70000-200000	Range of user IDs allocated for mapping UNIX users to NT user SIDs.
idmap gid	70000-200000	Range of group IDs allocated for mapping UNIX groups to NT group SIDs.

Table 3-3 Samba Configuration Parameters (continued)

Parameter Name	Default Value	Parameter Description
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.
lpq cache time	0	Cache time for the results of the **lpq** command.
log file	/local/local1/errorlog/samba.log	Location where print-related errors are logged.
max log size	50	Maximum number of errors the log file can contain. After 50 errors, for each new error logged, the oldest error is removed.

socket options	TCP_NODELAY
	SO_RCVBUF=8192
	SO_SNDBUF=8192
		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 *nmbd* to be a local master browser on a subnet.
domain master	no	Parameter that sets *nmbd* to be a domain master browser for its given workgroup.
preferred master	no	Parameter that sets *nmbd* 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 **windows-domain comment** command.
netbios name	MYFILEENGINE	Name of the Samba server hosting print services. This parameter can also be set by the **windows-domain netbios-name** command.
realm	CISCO	Active Directory domain name. Always uppercase. This parameter can also be set by the **windows-domain realm** command.
wins server	10.10.10.1	IP address of the Windows domain server used to authenticate user access to print services. This parameter can also be set by the **windows-domain wins-server** command.
password server	10.10.10.10	Optional IP address of the password server used for authentication of users. This parameter can also be set by the **windows-domain password-server** command.

Table 3-3 Samba Configuration Parameters (continued)

Parameter Name	Default Value	Parameter Description
security	domain	Use Windows domain server for authentication. This parameter can also be set by the **windows-domain security** command.
client schannel	no	Secure channel indicator used for Windows domain server authentication.
ldap ssl	none	Defines whether or not Samba should use SSL when connecting to the LDAP server. The default is unconfigured. If set to “off,” SSL is never used when querying the directory server. To enable the LDAPv3 StartTLS extended operation (RFC2830), set to “yes”.

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 LDAP server signing:

```
WAE# smb-conf global name “ldap ssl” value “yes”
```

Related Commands

show smb-conf

windows-domain

(config) accelerator windows-print

(config) windows-domain

(config) snmp-server access-list

To configure a standard access control list on a WAAS device to allow access through an SNMP agent, use the **snmp-server access-list** global configuration command. To remove a standard access control list, use the **no** form of this command.

snmp-server access-list {*num* | *name*}

no snmp-server access-list {*num* | *name*}

Syntax Description

num	Standard access list number (1–99).
name	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

Usage Guidelines

If you are using an SNMP server ACL, you must permit the loopback interface.

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
```

Note You must first create access list 12 using the **ip access-list standard** global configuration command.

Related Commands

(config) ip access-list

show running-config

(config) snmp-server community

To enable the SNMP agent on a WAAS device and to set up the community access string to permit access to the SNMP agent, use the **snmp-server community** global configuration command. To disable the SNMP agent and remove the previously configured community string, use the **no** form of this command.

snmp-server community *string* [**group** *groupname* | **rw**]

no snmp-server community *string* [**group** *groupname* | **rw**]

Syntax Description

string	Community string that acts like a password and permits access to the SNMP agent. You can use up to a maximum of 64 characters.
group *groupname*	(Optional) Specifies the group name to which the community string belongs. You can use a maximum of 64 characters.
rw	(Optional) Enables read-write access to this community string.

Defaults

The SNMP agent is disabled and a community string is not configured. When configured, an SNMP community string by default permits read-only access to all objects.

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 notify inform

(config) snmp-server user

(config) snmp-server view

ssh

(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*

Syntax Description

contact *line*	Specifies the text for MIB-II object *sysContact*. This is the identification of the contact person for this managed node.

Defaults

No system contact string is set.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

The system contact string is the value stored in the MIB-II system group *sysContact* object.

Examples

The following example shows how to set a system contact string and then remove it:

```
WAE(config)# snmp-server contact Dial System Operator at beeper # 27345

WAE(config)# no snmp-server contact
```

Related Commands

(config) snmp-server community

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

ssh

(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** | **linkdown** | **linkup**]

Syntax Description

alarm	(Optional) Enables WAAS alarm traps.
clear-critical	(Optional) Enables clear-critical alarm traps.
clear-major	(Optional) Enables clear-major alarm traps.
clear-minor	(Optional) Enables clear-minor alarm traps.
raise-critical	(Optional) Enables raise-critical alarm traps.
raise-major	(Optional) Enables raise-major alarm traps.
raise-minor	(Optional) Enables raise-minor alarm traps.
config	Enables CiscoConfigManEvent traps.
entity	Enables SNMP entity traps.
event	Enables Event MIB traps.
content-engine	Enables SNMP WAAS traps.
disk-fail	(Optional) Enables disk failure error traps.
disk-read	(Optional) Enables disk read error traps.
disk-write	(Optional) Enables disk write error traps.
overload-bypass	(Optional) Enables WCCP overload bypass error traps.
transaction-log	(Optional) Enables transaction log write error traps.
snmp	Enables SNMP-specific traps.
authentication	(Optional) Enables authentication trap.
cold-start	(Optional) Enables cold start trap.
linkdown	(Optional) Enables link down trap.
linkup	(Optional) Enables link up trap.

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
```

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

ssh

(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*]}}

Syntax Description

group *name*	Specifies the SNMP group. You can enter a maximum of 64 characters.
v1	Specifies the group using the Version 1 Security Model.
notify *name*	(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.
read *name*	(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.
write	(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.
v2c	Specifies the group using the Version 2c Security Model.
v3	Specifies the group using the User Security Model (SNMPv3).
auth	Specifies the group using the AuthNoPriv Security Level.
noauth	Specifies the group using the noAuthNoPriv Security Level.
priv	Specifies the group using the AuthPriv Security Level.

Defaults

The default is that no user security model group is defined.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

The maximum number of SNMP groups that can be created is 10.

Select one of three SNMP security model groups: Version 1 (**v1**) Security Model, Version 2c (**v2c**) Security Model, or the User Security Model (**v3** or SNMPv3). Optionally, you then specify a notify, read, or write view for the group for the particular security model chosen. The **v3** option allows you to specify the group using one of three security levels: **auth** (AuthNoPriv Security Level), **noauth** (noAuthNoPriv Security Level), or **priv** (AuthPriv Security Level).

Examples

The following example 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

ssh

(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* | *ipv-4address/ipv6-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

hostname	Hostname of the SNMP trap host that will be sent in the SNMP trap messages from the WAAS device.
ipv4-address/ipv6-address	IPv4/IPv6 address of the SNMP trap host that will be sent in the SNMP trap messages from the WAAS device.
communitystring	Password-like community string sent in the SNMP trap messages from the WAE. You can enter a maximum of 64 characters.
v2c	(Optional) Specifies the Version 2c Security Model.
retry *number*	(Optional) Sets the count for the number of retries (1–10) for the inform request. (The default is 2 tries.)
timeout *seconds*	(Optional) Sets the timeout for the inform request (1–1000 seconds). The default is 15 seconds.
v3	(Optional) Specifies the User Security Model (SNMPv3).
auth	Sends a notification using the AuthNoPriv Security Level.
noauth	Sends a notification using the noAuthNoPriv Security Level.
priv	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

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

ssh

(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*

Syntax Description

location *line*	Specifies the text for MIB-II object *sysLocation*. This string describes the physical location of this node.

Defaults

No system location string is set.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

The system location string is the value stored in the MIB-II system group system location object. You can see the system location string with the **show snmp** EXEC command.

Examples

The following example shows how configure a system location string:

```
WAE(config)# snmp-server location Building 3/Room 214
```

Related Commands

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server mib

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

ssh

(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

Syntax Description

persist	Configures MIB persistence.
event	Enables MIB persistence for the Event MIB.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

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

ssh

(config) snmp-server monitor user

To specify the user to be used for active monitoring of triggers, use the **snmp-server monitor-user** global configuration command. To disable the user from monitoring, use the **no** form of this command.

snmp-server monitor-user *existing snmpv3 user*

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

Using the **snmp-server monitor-user** global configuration command, you can specify the user that will be used for active monitoring of triggers. Any SNMP V3 user can be configured as a Monitor User. This user should have sufficient permission to run a query on the objects specified in triggers. No priv key should be associated with this user, because this user monitors triggers internally.

Examples

The following example shows how to specify the user that is to be used for active monitoring of triggers:

```
WAE(config)# snmp-server monitor-user acme admin
```

Related Commands

(config) snmp-server user

(config) snmp-server trigger

(config) snmp-server trap-source

(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

ssh

(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** *index* | **Standby** *grpnumber* | **TenGigabitEthernet** *slot/port*}

no snmp-server trap-source {**GigabitEthernet** *slot/port* | **PortChannel** *index* | **Standby** *grpnumber* | **TenGigabitEthernet** *slot/port*}

Syntax Description

GigabitEthernet *slot/port*	Selects a Gigabit Ethernet interface to configure as the trap source. The slot number and port number are separated with a forward slash character (/). Valid slot and port values depend on the hardware platform.
PortChannel *index*	Selects a port channel (1–4) to configure as the trap source.
Standby *grpnumber*	Selects a standby group (1–3) to configure as the trap source.
TenGigabitEthernet *slot/port*	Selects a TenGigabitEthernet interface to configure as the trap source. The slot number and port number are separated with a forward slash character (/). Valid slot and port values depend on the hardware platform.

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

(config) snmp-server trigger

(config) snmp-server trigger

To configure thresholds for a user-selected MIB object for monitoring purposes on a WAAS device, use the **snmp-server trigger** global configuration command. To remove access, use the **no** form of this command.

snmp-server trigger {*trigger name* | *mib varname* [wildcard] | *wait-time*
[**absent** [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*]
[*LINE*] |
equal [**absolute** *threshold value* **|** **delta** *threshold value*] **|**
greater-than [**absolute** *threshold value* **|** **delta** *threshold value*] **|**
less-than [**absolute** *threshold value* **|** **delta** *threshold value*] **|**
on- change [*LINE* **| mibvar1***mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*]
[*LINE*] |
present [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*]
[*LINE*] |
threshold *lower threshold value* |
]}

no snmp-server trigger {*trigger name* | *mib varname* [wildcard] | *wait-time*
[**absent** [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*]
[*LINE*] |
equal [**absolute** *threshold value* **|** **delta** *threshold value*] **|**
greater-than [**absolute** *threshold value* **|** **delta** *threshold value*] **|**
less-than [**absolute** *threshold value* **|** **delta** *threshold value*] **|**
on- change [*LINE* **| mibvar1***mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*]
[*LINE*] |
present [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*]
[*LINE*] |
threshold *lower threshold value* |
]}

Syntax Description

trigger name	Configures a custom defined name for the notification trigger that you want to monitor.
mibvar	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.
wildcard	(Optional) Treats the specified MIB variable name as having a wildcard.
wait-time	(Optional) Number of seconds, 60–600, to wait between trigger samples.
absent	(Optional) Applies the absent existence test.
LINE	(Optional) Description of the threshold being created.
mibvar1 *mibvar1*	(Optional) Adds a MIB object to the notification.
mibvar2 *mibvar2*	(Optional) Adds a MIB object to the notification.
mibvar3 *mibvar3*	(Optional) Adds a MIB object to the notification.
equal	Applies the equality threshold test.
absolute *value*	(Optional) Specifies an absolute value sample type.

delta *value*	Specifies a delta sample type.
greater-than	Applies the greater-than threshold test.
less-than	Applies the less-than threshold test.
on-change	Applies the changed existence test.
present	(Optional) Applies the present test.
threshold	Configures a maximum and minimum threshold for a MIB object.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Using the **snmp-server trigger** global configuration command, you can define additional SNMP traps for other MIB objects of interest to your particular configuration. You can select any MIB object from any of the support MIBs for your trap. The trap can be triggered based on a variety of tests:

- absent—A specified MIB object that was present at the last sampling is no longer present as of the current sampling.
- equal—The value of the specified MIB object is equal to the specified threshold.
- 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.
- threshold- Min value and Max values specifying the lower and upper thresholds.

The threshold value can be based on an *absolute* sample type or on a *delta* sample type. An absolute sample type is one in which the test is evaluated against a fixed integer value between zero and 4294967295. A delta sample type is one in which the test is evaluated against the change in the MIB object value between the current sampling and the previous sampling.

After you configure SNMP traps, you must use the **snmp-server enable traps event** global configuration command for the event traps you just created to be generated. To save the MIB data using the **write mib-data** EXEC command.

Note You can create valid triggers only on read-write and read-only MIB objects. If you try to create a trigger on a read-create MIB object, you receive an error message.

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(config)# snmp-server trigName esConTabIsConnected ?
  <60-600>  The number of seconds to wait between trigger sample
  wildcard  Option to treat the MIB variable as wildcarded
WAE(config)# snmp-server trigName esConTabIsConnected wildcard 600 ?
  absent        Absent existence test
  equal         Equality threshold test
  greater-than  Greater-than threshold test
  less-than     Less-than threshold test
  on-change     Changed existence test
  present       Present present test
  threshold     Threshold test
WAE(config)# snmp-server trigName esConTabIsConnected wildcard 600 less-than?
  absolute Absolute sample type
  delta   Delta sample type
WAE(config)# snmp-server trigName esConTabIsConnected wildcard 600 less-than absolute ?
  <0-4294967295>  Less-than threshold value
WAE(config)# snmp-server trigName esConTabIsConnected wildcard 600 less-than absolute 1 ?
  LINE     Trigger-comment
  mibvar1  Optional mib object to add to the notification
WAE(config)# snmp-server trigName esConTabIsConnected wildcard 600 less-than absolute 1
"Lost the connection with the core server."
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 trigName 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

(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 nmp-server user *name group*
[**auth** {**md5** *password* [**priv** *password*] |
sha *password* [**priv** *password*]} |
remote *octetstring* [**auth** {**md5** *password* [**priv** *password*] |
sha *password* [**priv** *password*]}]]

Syntax Description

name group	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 32 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.
auth	(Optional) Configures user authentication parameters.
md5 *password*	Configures HMAC MD5 user authentication password.
priv *password*	(Optional) Alphanumeric string (256 characters maximum) that configures the authentication HMAC-MD5 user private password. The following special characters are not supported: space, backwards single quote (`), double quote ("), pipe (|), or question mark (?). **Note** For SNMPv3 users using WAAS Software Version 6.x and later, the private password must be a minimum of 8 alphanumeric characters and a maximum of 256 alphanumeric characters.
sha *password*	Configures the HMAC-SHA authentication password. You can enter a maximum of 256 characters.
remote *octetstring*	(Optional) Specifies the globally unique identifier (engineID) for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users (10 to 64 characters, not counting colons). 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. (Colons will be removed in the show running-config command output.)

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

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

(config) snmp-server monitor user

ssh

(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**}

Syntax Description

viewname MIBfamily	Name of this family of view subtrees and a subtree of the MIB. You can enter a maximum of 64 characters.
excluded	Excludes the MIB family from the view.
included	Includes the MIB family 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

ssh

(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* }

no sshd {**allow-non-admin-users** | **enable** | **password-guesses** *number* | **timeout** *seconds* }

Syntax Description

allow-non-admin-users	Allows nonadministrative users to gain SSH access to the chosen device (or device group). By default, this option is disabled. **Note** Nonadministrative users are 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.
enable	Enables the SSH daemon on a WAAS device.
password-guesses *number*	Specifies the maximum number of allowable password guesses per connection (1–3). The default is 3.
timeout *seconds*	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. 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.

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: ssh version 2 protocol is enabled

Note The SSH version 1 protocol is no longer supported. Only the SSH version 2 protocol is supported by the WAAS device.

Command Modes

global configuration

Device Modes

application-accelerator

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.

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 timeout 20
```

Related Commands

(config) ssh-key-generate

(config) ssh-key-generate

To generate the SSH host key for a WAAS device, use the **ssh-key-generate** global configuration command. To remove the SSH key, use the **no** form of this command.

ssh-key-generate [**key-length** *length*]

no ssh-key-generate [**key-length** *length*]

Syntax Description

key-length *length*	(Optional) Configures the length of the SSH key. The number of bits is 768–2048.

Defaults

key-length *length*: 1024 bits

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Before you enter the **sshd enable** command, enter the **ssh-key-generate** command to generate a private and a public host key, which the client programs use to verify a server 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.

Examples

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 key-length 860
Ssh host key generated successfully
Saving the host key to box ...
Host key saved successfully
WAE(config)# sshd enable
Starting ssh daemon ...
Ssh daemon started successfully
```

Related Commands

(config) sshd

(config) stats-collector logging

To configure the statistics collector for the SMB accelerator, use the **stats-collector logging** global configuration command. To unconfigure the statistics collector, use the **no** form of this command.

stats-collector logging {**enable** | **rate** {**10** | **30**}}

no stats-collector logging {**enable** | **rate** {**10** | **30**}}

Syntax Description

enable	Enables the statistics collector.
rate {**10** | **30**}	Configures the collection interval to 10 or 30 seconds.

Defaults

The statistics collector is disabled. The collection interval is set to 30 seconds.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

This command configures periodic statistics logging for the SMB application accelerator. After enabling logging, you can disable it with the **no** form of the command. Statistics for the most recent 14 days are saved.

Examples

The following example shows how to enable statistics collection:

```
WAE(config)# stats-collector logging enable
```

The following example shows how to disable statistics collection:

```
WAE(config)# no stats-collector logging enable
```

Related Commands

copy monitoring-log

(config) system jumbomtu

To configure a jumbo MTU on all devices interfaces, use the **system jumbomtu** global configuration command. To remove the jumbo MTU, use the **no** form of this command.

system jumbomtu *size*

no system jumbomtu *size*

Syntax Description

size	Configures the size of the MTU (576–9000 or 9216 bytes, depending on platform).

Defaults

MTU size is 1500 bytes.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

This command is available only on the following platforms: WAVE-294/594/694/7541/7571/8541, and vWAAS. This command changes the MTU setting for all interfaces on the device, including logical interfaces with at least one physical member, and may cause current active connections to time out. After you change the MTU using this command, you cannot change the MTU of individual interfaces.

Examples

The following example shows how to configure a jumbo MTU:

```
WAE(config)# system jumbomtu 9000
Changing system mtu setting will change the MTU values on all the interfaces. This may
cause the current active connections in the device to timeout.
Are you sure you want to do this? (y/n) [n]y
```

Related Commands

show interface

(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*| *ipv6 {ipv6-address}*} [**primary** | **port** *number*] | **key** *keyword* | **password ascii** | **retransmit** *retries* | **timeout** *seconds*}

no tacacs {**host** {*hostname* | *ip-address* | *ipv6 {ipv6-address}*} [**primary** | **port** *number*] | **key** *keyword* | **password ascii** | **retransmit** *retries* | **timeout** *seconds*}

Syntax Description

host	Specifies a server address.
hostname	Hostname of the TACACS+ server.
ip-address	IP address of the TACACS+ server.
ipv6	IPv6 address of the TACACS+ server.
primary	(Optional) Sets the server as the primary server.
port *number*	Sets the port number of the TACACS+ server. If not specified, the default port 49 is used.
key *keyword*	Sets the security word. An empty string is the default.
password ascii	Specifies ASCII as the TACACS+ password type.
retransmit *retries*	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.
timeout *seconds*	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

port *number*: 49

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.)

Note When AAA Command Authorization is enabled for a device through the Central Manager GUI, TACACS+ CLI configuration changes are not allowed and **tacacs** commands will fail.

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 must not exceed 32 printable ASCII characters. An empty key string is the default. All leading spaces are ignored; spaces within and at the end of the key string are not ignored. Double quotes are not required even if there are spaces in the key.

Note If you configure a TACACS+ key on the WAAS device (the TACACS+ client), make sure that you configure an identical key on the external TACACS+ server. Do not use the following characters: backwards single quote (`), double quote ("), pipe (|), closing bracket (]), number sign (#), or backslash (\).

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.

If you do not use the **primary** keyword to specify the primary server, the primary server is the first one configured. If you remove the primary server by using the **no tacacs host** command, the first configured server (other than the removed server) becomes the primary server.

You can configure multiple TACACS+ servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+, in the order in which they were configured. If authentication fails for any reason other than a server is unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **authentication fail-over server-unreachable** command.

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

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

cwnd-base *segments*	Sets initial send congestion window in segments (1–10).
ecn enable	Enables TCP explicit congestion notification.
increase-xmit-timer-value *value*	Specifies the factor (1-3) used to modify the length of the retransmit timer by 1 to 3 times the base value determined by the TCP algorithm. **Note** 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.
init-ss-threshold *value*	Sets initial slow-start threshold value (2-10).
keepalive-probe-cnt *count*	Specifies the length of time that the WAAS device keeps an idle connection open. The number of probe counts is 1–10.
keepalive-probe-interval *seconds*	Specifies the number of times that the WAAS device retries a connection. The keepalive probe interval is in seconds (1–300).
keepalive-timeout *seconds*	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: 2 segments

tcp keepalive-probe-cnt: 4

tcp keepalive-probe-interval: 75 seconds

tcp keepalive-timeout: 90 seconds

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

The following are the usage guidelines for this command:

Caution 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

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

coredump	Writes a core file (default).
debug	Hangs the system until it is explicitly restarted.
no-coredump	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 exeption handling to a core file using the **tfo exception** command:

```
WAE(config)# tfo exception coredump
```

Related Commands

(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

DRE	Configures TFO optimization with or without Data Redundancy Elimination (DRE).
yes	Enables DRE.
no	Disables DRE.
compression	Configures TFO optimization with or without generic compression.
LZ	Configures TFO optimization with Lempel-Ziv (LZ) compression.
none	Configures TFO optimization with no compression.
full	Configures TFO optimization with DRE and LZ compression. Using this keyword is the same as specifying the **tfo optimize DRE yes compression LZ** command.

Defaults

The default TFO optimization on a WAAS device is **tfo optimize full**.

Command Modes

global configuration

Device Modes

application-accelerator

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

enable	Enables TCP adaptive buffer sizing.
receive-buffer-max *size*	Sets the maximum size of the receive buffer. Valid values range from 1 to 32768 KB.
send-buffer-max *size*	Sets the maximum size of the send buffer. Valid values range from 1 to 32768 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

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*

Syntax Description

segment-size	Optimized side TCP max segment size (512–9216).

Defaults

The default value of the segment size is 1432 bytes. If a jumbo MTU is configured, the default segment size is the jumbo MTU value – 68 bytes.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

This command sets the TCP maximum segment size on TFO optimized sockets (the connection between two peer WAEs).

Examples

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 **tfo tcp optimized-mss** command:

```
WAE(config)# tfo tcp optimized-mss 512
```

Related Commands

(config) tfo tcp keepalive

(config) tfo tcp optimized-receive-buffer

(config) tfo tcp optimized-send-buffer

(config) tfo tcp original-mss

(config) tfo tcp original-receive-buffer

(config) tfo tcp original-send-buffer

(config) tfo tcp optimized-receive-buffer

To configure a WAE for Traffic Flow Optimization (TFO) 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*

Syntax Description

buffer-size	Receive buffer size in kilobytes. Valid values range from 1 to 32768 KB.

Defaults

32 KB

Command Modes

global configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a WAE for Traffic Flow Optimization with a 32 KB optimized-side receive buffer using the **tfo tcp optimized-receive-buffer** command:

```
WAE(config)# tfo tcp optimized-receive-buffer 32
```

Related Commands

(config) tfo tcp keepalive

(config) tfo tcp optimized-mss

(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-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*

Syntax Description

buffer-size	Send buffer size in kilobytes. Valid values range from 1 to 32768 KB.

Defaults

32 KB

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The buffer should be equal to or greater than twice 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 Mbps * 0.15 sec = 6.75 Mb, or 0.844 MB (844 KB). In this case, you could set the buffer size to 2000 KB.

Examples

The following example shows how to configure a WAE for Traffic Flow Optimization with a 32 KB optimized-side send buffer using the **tfo tcp optimized-send-buffer** command:

```
WAE(config)# tfo tcp optimized-send-buffer 32
```

Related Commands

(config) tfo tcp keepalive

(config) tfo tcp optimized-mss

(config) tfo tcp optimized-receive-buffer

(config) tfo tcp original-mss

(config) tfo tcp original-receive-buffer

(config) tfo tcp original-send-buffer

(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*

Syntax Description

segment-size	Original (end-point) side TCP max segment size (512–9216).

Defaults

The default value of the segment size is 1432 bytes. If a jumbo MTU is configured, the default segment size is the jumbo MTU value – 68 bytes.

Command Modes

global configuration

Device Modes

application-accelerator

Examples

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 **tfo tcp original-mss** command:

```
WAE(config)# tfo tcp original-mss 1432
```

Related Commands

(config) tfo tcp keepalive

(config) tfo tcp optimized-mss

(config) tfo tcp optimized-receive-buffer

(config) tfo tcp optimized-send-buffer

(config) tfo tcp original-receive-buffer

(config) tfo tcp original-send-buffer

(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*

Syntax Description

buffer-size	Receive buffer size in kilobytes. Valid values range from 1 to 32768 KB.

Defaults

32 KB

Command Modes

global configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a WAE for Traffic Flow Optimization with a 32 KB unoptimized-side receive buffer using the **tfo tcp original-receive-buffer** command:

```
WAE(config)# tfo tcp original-receive-buffer 32
```

Related Commands

(config) tfo tcp keepalive

(config) tfo tcp optimized-mss

(config) tfo tcp optimized-receive-buffer

(config) tfo tcp optimized-send-buffer

(config) tfo tcp original-mss

(config) tfo tcp original-send-buffer

(config) tfo tcp original-send-buffer

To configure a WAE for Traffic Flow Optimization (TFO) 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*

Syntax Description

buffer-size	Send buffer size in kilobytes. Valid values range from 1 to 32768 KB.

Defaults

32 KB

Command Modes

global configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a WAE for Traffic Flow Optimization with a 32 KB unoptimized-side receive buffer using the **tfo tcp original-send-buffer** command:

```
WAE(config)# tfo tcp original-send-buffer 32
```

Related Commands

(config) tfo tcp keepalive

(config) tfo tcp optimized-mss

(config) tfo tcp optimized-receive-buffer

(config) tfo tcp optimized-send-buffer

(config) tfo tcp original-mss

(config) tfo tcp original-receive-buffer

(config) threshold-monitor

To configure monitoring thresholds, use the **threshold-monitor** global configuration command. To restore default settings, use the **no** form of this command.

threshold-monitor {**system {load {** *load monitoring threshold percent* **} | cpu {** *higher threshold percentage* **|** *lower threshold percentage* **| win size** *size* **| sampling intervals** *interval*} **| enable** }}

no threshold-monitor {**system {load** *load monitoring threshold percent* | **cpu {***higher threshold percentage* **|** *lower threshold percentage* **| win size** *size* **| sampling intervals** *interval*} **| enable** }}

Syntax Description

system load	Sets the system load threshold to the specified percentage (80–100) of rated connection capacity.
cpu	Configures the threshold value for CPU load monitoring.
cpu utilization higher threshold percent	Sets the high threshold percentage (80-100) above which the system goes into the overloaded state when it is normal. But in the overloaded state, it doesn't go back to the normal state until the CPU utilization goes below the low threshold. The default CPU high threshold is 95 percent.
cpu utilization lower threshold percent	Sets the low threshold percentage (80-100) below which the system goes into the normal state when it is overloaded. This value has to be lower than the high threshold. The default CPU lower threshold is 90 percent.
win-size *size*	Configures the sampling window size for the moving average. It is the number of the most recent CPU utilization samples taken in calculating the latest CPU utilization percentage. The result is the average of the given number of samples.
sampling-intervals *interval*	Configures the sampling rate for the normal state and the overloaded state.
enable	Enables CPU load monitoring.

Defaults

The system load percentage is 95 percent of rated connection capacity for the device.

The CPU load percentage is 95 percent of the total CPU usage.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The system load percentage threshold refers to the percentage of connection capacity used for application accelerators and TFO connections on a WAE. If the configured load threshold for any application accelerator or TFO connections is exceeded on a WAE, the connection threshold exceeded alarm is raised. This alarm is cleared when the connection count falls to 10 percent less than the configured threshold (85 percent by default).

The CPU load threshold refers to the CPU load utilization on a WAE. When the average CPU utilization on the device exceeds the set threshold for 2 minutes, the device stops accepting new connections and passes any new connections through. When the average CPU utilization falls below the threshold for 2 minutes, the device resumes accepting optimized connections. You can disable CPU load monitoring by using the no form of the CPU enable command.

Examples

The following example shows how to configure a system load threshold of 90 percent:

```
WAE(config)# threshold-monitor system load 90
```

Related Commands

show statistics accelerator

show statistics connection

show statistics tfo

(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* {**passwd** | **privilege** {**0** | **15**}}

no username *name* {**passwd** | **privilege** {**0** | **15**}}

Syntax Description

name	Username.
passwd	Configures the password interactively.
privilege	Sets the user privilege level.
0	Specifies the user privilege level for the normal user.
15	Specifies the user privilege level for the superuser.

Defaults

The default administrator account is as follows:

- Username: admin
- Password: default
- Privilege: superuser (15)

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure passwords and privilege levels for users on your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure and administer users on 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(config)# username bwhidney passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager.  Please use the central manager to configure
user accounts.
New WAAS password:
Retype new WAAS password:

WAE(config)# username abeddoe privilege 15
Warning: User configuration performed via CLI may be overwritten
by the central manager.  Please use the central manager to configure
```

```
user accounts.
```

Related Commands

show user

(config) wccp access-list

To configure an IP access list on a WAE for inbound WCCP GRE encapsulated traffic, use the **wccp access-list** global configuration command. 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*}

Syntax Description

acl-number	Standard IP access list number (1–99).
ext-acl-number	Extended IP access list number (100–199).
acl-name	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. WCCP commands are available only after the interception method is set to WCCP by the **interception-method** command.

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
```

Related Commands

show ip access-list

show wccp

(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*

Syntax Description

number	Router list number (1–7).
ip-address	IP address of the router to add to the list. You can specify up to 32 IP addresses, each separated by the space character.

Defaults

Disabled

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Each router list can contain up to 32 routers and you can have up to 8 router lists.

Note The WAAS Central Manager uses router list number 8 for a default router list that contains the default gateway.

Note The **ip wccp** global configuration command must be used to enable WCCP on each router that is included on the router list.

WCCP works only with IPv4 networks. WCCP commands are available only after the interception method is set to WCCP by the **interception-method** command.

Examples

The following example shows that router list number 2 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 2 192.168.68.98
```

The following example shows how to delete the router list number 2 created in the previous example:

```
WAE(config)# no wccp router-list 2 192.168.68.98
```

The following example shows how to create a router list (router list 1) with two routers 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 10.10.10.3
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# router-list-num 1
WAE(config-wccp-service)# enable
```

Related Commands

(config) wccp tcp-promiscuous service-pair

(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*

Syntax Description

max-wait *seconds*	Sets the clean shutdown time interval. The time is in seconds (0–86400). The default is 120 seconds

Defaults

The maximum time interval before a clean shutdown is 120 seconds.

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** command or disable WCCP. 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. WCCP commands are available only after the interception method is set to WCCP by the **interception-method** command.

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 enable** WCCP command. After you enter this command, the WAE waits 1000 seconds before it shuts down WCCP Version 2.

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# no enable
```

A countdown message appears, indicating how many seconds remain before WCCP will be shut down on the WAE:

```
WCCP clean shutdown initiated
Waiting for shutdown ok (999 seconds) . Press ^C to skip waiting
WCCP clean shutdown wait time expired
```

Related Commands

(config) wccp tcp-promiscuous service-pair

(config) wccp tcp-promiscuous service-pair

To configure the Web Cache Coordination Protocol (WCCP) Version 2 TCP promiscuous mode service, use the **wccp tcp-promiscuous service-pair** global configuration command. To negate these actions, use the **no** form of this command.

wccp tcp-promiscuous {**service-pair** *serviceID serviceID+1* | *serviceID*}

no wccp tcp-promiscuous {**service-pair** *serviceID serviceID+1* | *serviceID*}

Syntax Description

service-pair *serviceID serviceID+1*	Specifies a pair of IDs for the WCCP service on devices configured as application accelerators. Valid values are two consecutive numbers from 1-100, inclusive.
serviceID	Specifies one ID for the WCCP service. A valid value is from 1-100, inclusive.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **wccp tcp-promiscuous service-pair** command to configure and enable the WCCP interception method. This command initiates the WCCP configuration mode as indicated by the **(**config-wccp-service**)** prompt. For more information on WCCP configuration mode commands, see the "WCCP Configuration Mode Commands" section.

Within WCCP configuration mode, you can use the various commands (**egress-method**, **failure-detection**, and so on) to define WCCP settings. To return to global configuration mode, enter the **exit** command.

You must use the **enable** WCCP configuration command to enable the WCCP service.

You must configure two WCCP service IDs on WAEs operating in application-acceleration mode.

Note WCCP works only with IPv4 networks. WCCP commands are available only after the interception method is set to WCCP by the **interception-method** global configuration command.

Examples

The following example shows how to configure WCCP service IDs 61 and 62 and put a WAE into WCCP configuration mode:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)#
```

Related Commands

(config) wccp router-list

(config) wccp shutdown

show wccp

(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* | **encryption-service** {**enable** | **identity** *name* [**default** | **enable** | **machine-account** | **match** | **password** | **user-account**]} | **ldap-sign-and-seal enable** | **machine-account-password lifespan** *duration* **| 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* | **encryption-service** {**enable** | **identity** *name*} | **ldap-sign-and-seal enable** | **machine-account-password lifespan** *duration* **| netbios-name | password-server** {*hostname* | *ipaddress*} | **realm** *kerberos-realm* | **wins-server** {*hostname* | *ipaddress*} | **workgroup** *name* | **security ADS**}

Syntax Description

administrative	Sets administrative options.
group	Sets an administrative group name.
normal-user	Sets the administrative group name for the normal user (privilege 0).
super-user	Sets the administrative group name for the superuser (privilege 15).
groupname	Name of the administrative group.
comment *string*	Specifies a comment for the Windows domain server. This is a text string.
encryption-service	Configures encrypted service.
enable	Enables encrypted service.
identity *name*	Specifies the encrypted service identity to manage. The name is the WAAS tag-name identifier.
default	Sets the identity as the default match.
machine-account	Specifies machine account identity.
match	Specifies a match.
password	Specifies the password for the identity.
user-account *name*	Defines and edits the user account identity.
ldap-sign-and-seal	Configures the LDAP sign and seal service.
enable	Enables the LSAP sign and seal service. This service is disabled by default.
machine-account-password	Configures the password settings.
lifespan *duration*	Configures the lifespan duration in seconds. The minimum is 1 hour, the maximum is 60 days, and the default is 30 days.
netbios-name *name*	Specifies the NetBIOS name of the WAE. The NetBIOS name must not consist of only numbers; it must include some letters.
password-server	Specifies the password server used to verify a client password.
hostname	Hostname of the password server.
ipaddress	IP address of the password server.

realm *kerberos-realm*	Specifies the Kerberos realm to use for authentication. The realm is used as the Active Directory Service (ADS) equivalent of the NT4 domain. This argument is valid only when Kerberos ADS mode is used. 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. Example: kerberos-realm = MYBOX.MYCOMPANY.COM
wins-server	Specifies the Windows Internet Naming Service (WINS) server.
hostname	Hostname of the WINS server.
ipaddress	IP address of the WINS server.
workgroup *name*	Specifies the name of the workgroup (or domain) in which the WAAS device resides.
security	Sets Kerberos authentication.
ADS	Specifies the Active Directory Service.

Defaults

Windows domain options are disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this global configuration command to set the Windows domain server parameters for a WAAS device.

Note For the windows domain encryption service identity to be configured successfully when you use **windows-domain encryption-service identity** *name*, the identity name must be the same as the machine identity (command parameter: **machine-account**) that was generated when joining the domain.

When you enable Kerberos authentication, the default **realm** is DOMAIN.COM and the **security** is ADS. If you disable Kerberos authentication, the **security** is domain.

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 configure the Windows domain server at 10.10.24.1 for a WAAS device with a NetBIOS name of myWaasDevice in the ABC domain. It also identifies the password server:

```
WAE(config)# windows-domain wins-server 10.10.24.1
WAE(config)# windows-domain password-server 10.10.100.4
WAE(config)# windows-domain netbios-name myWaasDevice
WAE(config)# windows-domain workgroup ABC
```

The following example shows how to configure the windows domain server when Kerberos authentication is enabled using the **kerberos** command:

```
WAE(config)# windows-domain realm ABC.COM
WAE(config)# windows-domain 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: MYWAASDEVICE
    Realm: ABC
    WINS Server: 10.10.10.1
    Password Server: 10.10.10.10
    Security: ADS
```

Related Commands

(config) kerberos

show windows-domain

windows-domain

Interface Configuration Mode Commands

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** *index* | **Standby** *group-index* | **TenGigabitEthernet** *slot/port* }

Syntax Description

GigabitEthernet *slot/port*	Selects a Gigabit Ethernet interface to configure.
InlineGroup *slot/group*	Selects an inline group interface to configure.
PortChannel *index*	Selects the port channel interface to configure.
Standby *group-index*	Selects the standby group to configure.
TenGigabitEthernet *slot/port*	Selects a 10-Gigabit Ethernet interface to configure.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Within interface configuration mode, you can use the interface commands (**autosense**, **bandwidth**, **cdp**, and so on) to configure the specified interface.

To return to global configuration mode, use the **exit** command at the interface configuration mode prompt.

Examples

The following example shows how to enter interface configuration mode:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)#
```

Related Commands

(config) interface InlineGroup

(config) interface PortChannel

(config) interface standby

(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

(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**}

Syntax Description

10	Sets the link speed to 10 megabits per second (Mbps).
100	Sets the link speed to 100 Mbps.
1000	Sets the link speed to 1000 Mbps. This option is not available on all ports and is the same as autosense.

Defaults

No default behaviors or values.

Command Modes

interface configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

To configure the link speed of a network interface on a WAAS device, use the **bandwidth** interface configuration command. The speed is specified in megabits per second (Mbps). The WAAS software automatically enables autosense if the speed is set to 1000 Mbps.

Note Changing the interface bandwidth, duplex mode, or MTU can cause network disruption for up to 10 seconds. The best practice is to make such changes when traffic interception is disabled or at an off-peak time when traffic disruption is acceptable.

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.

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

Syntax Description

enable	Enables CDP on an interface.

Defaults

No default behavior or values.

Command Modes

interface configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Using the **cdp enable** command in global configuration mode enables CDP globally on all the interfaces of the WAAS device. If you want to control CDP behavior per interface, then use the **cdp enable** command in interface configuration mode.

Note Enabling CDP at the interface level overrides the global control. However, you must enable CDP globally on the WAAS device before you enable CDP on an interface. Otherwise, the following message is displayed in the command output:

```
WAE(config-if)# cdp enable
Cannot enable CDP on this interface, CDP Global is disabled
```

Examples

The following example 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
```

Related Commands

(config) cdp

show cdp

show interface

(config-if) channel-group

To configure the port-channel group for a network interface, use the **channel-group** interface configuration command. To restore default values, use the **no** form of this command.

channel-group *index*

no channel-group *index*

Syntax Description

index	Assigns the interface to the port channel with the specified index 1–7.

Defaults

No default behaviors or values.

Command Modes

interface configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to configure an interface with a channel group:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# channel-group 1
```

Related Commands

(config) interface GigabitEthernet

(config-if) description

To configure the description for a network interface, use the **description** interface configuration command. To remove the description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	Interface description.

Defaults

No default behaviors or values.

Command Modes

interface configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to configure an interface with a description:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# description interception interface 1
```

Related Commands

(config) interface GigabitEthernet

(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*

Syntax Description

VLAN	VLAN ID from 1–4094.

Defaults

No default behavior or values.

Command Modes

interface configuration

Device Modes

application-accelerator

Usage Guidelines

The **encapsulation dot1Q** command is available only for the inlineGroup interface.

Note 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 or module 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.

Examples

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
```

Related Commands

(config) interface GigabitEthernet

(config-if) ip

(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) 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.

Note Changing the interface bandwidth, duplex mode, or MTU can cause network disruption for up to 10 seconds. The best practice is to make such changes when traffic interception is disabled or at an off-peak time when traffic disruption is acceptable.

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

(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.

Note Changing the interface bandwidth, duplex mode, or MTU can cause network disruption for up to 10 seconds. The best practice is to make such changes when traffic interception is disabled or at an off-peak time when traffic disruption is acceptable.

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

(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

vlan	(Optional) Modifies the VLAN list parameters.
all	Applies the command to all tagged and untagged packets.
native	Specifies untagged packets.
vlan_list	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 packets on VLANs 5, 10, 11, 12, 13, 14, and 15.

```
(config)# interface inlineGroup 1/0
(config-if)# no inline vlan 5,10-15
(config-if)# exit
```

The following example shows how to enable inline interception for all untagged traffic and traffic only on VLANs 0 through 100 on the ports in group 1 in slot 2:

```
(config)# interface inlineGroup 2/1
(config-if)# no inline vlan 101-4095
(config-if)# exit
```

The following example shows how to enable inline interception for traffic only on VLAN 395 on the ports in group 1 in slot 2. Because the default behavior is to enable traffic on all VLANs, you must first disable all VLANs, 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

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*]}

no ip address {*ip-address ip-subnet* [**secondary**] | **dhcp** [**client-id** *id*][**hostname** *name*]}

Syntax Description

address	Sets the IP address of an interface.
ip-address	IP address.
ip-subnet	IP subnet mask.
secondary	(Optional) Makes this IP address a secondary address.
dhcp	Sets the IP address negotiated over DHCP.
client-id *id*	(Optional) Specifies the client identifier.
hostname *name*	(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 inline module. The change in the IP address takes place immediately.

The **ip address** interface configuration command allows configuration of secondary IP addresses for a specified interface as follows:

```
WAE(config-if)# ip address ip_address netmask secondary
```

Up to four secondary IP addresses can be specified for each interface. The same IP address cannot be assigned to more than one interface. The secondary IP address becomes active only after a primary IP address is configured. The following command configures the primary IP address:

```
WAE(config-if)# ip address ip_address netmask
```

The secondary IP addresses are disabled when the interface is shut down and are enabled when the interface is brought up.

Use the **no** form of the command to disable a specific IP address:

```
WAE(config-if)# no ip address ip_address netmask
```

Note No two interfaces can have IP addresses in the same subnet.

Use the **ip-address dhcp** command to negotiate a reusable IP address from DHCP.

Examples

The following example shows how to configure the port-channel interface with an IP address of 10.10.10.10 and a netmask of 255.0.0.0:

```
WAE# configure
WAE(config)# interface PortChannel 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

(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**}

Syntax Description

acl-name	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
acl-num	Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
in	Applies the specified access list to inbound packets on the current interface.
out	Applies the specified access list to outbound packets on the current interface.

Defaults

No default behavior or values.

Command Modes

interface configuration

Device Modes

application-accelerator

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) load-interval

To configure the interval at which to poll the network interface for statistics, use the **load-interval** interface configuration command. To remove the configuration, use the **no** form of this command.

load-interval *seconds*

no load-interval *seconds*

Syntax Description

seconds	Sets the interval at which to poll the interface for statistics and calculate throughput. Ranges from 30 to 600 seconds. The default is 30 seconds.

Defaults

30 seconds.

Command Modes

interface configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to configure the load interval for an interface:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# load-interval 60
```

Related Commands

(config) interface GigabitEthernet

(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*

Syntax Description

mtusize	MTU packet size in bytes (88–1500).

Defaults

No default behavior or values.

Command Modes

interface configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

The MTU is the largest size of IP datagram that can be transferred using a specific data link connection. Use the **mtu** command to set the maximum packet size in bytes.

The MTU field is not editable if the interface is assigned to a standby or port channel group.

Note Changing the interface bandwidth, duplex mode, or MTU can cause network disruption for up to 10 seconds. The best practice is to make such changes when traffic interception is disabled or at an off-peak time when traffic disruption is acceptable.

Examples

The following example shows how to set the MTU to 1500 bytes and then remove that setting:

```
WAE(config-if)# mtu 1500
WAE(config-if)# no mtu 1500
```

Related Commands

show interface

show running-config

(config-if) shutdown

To shut down a specific hardware interface on a WAAS device, use the **shutdown** interface configuration command. To restore an interface to operation, use the **no** form of this command.

shutdown

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

(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 *group-index* [**primary**] {**description** *text* | **ip** *ip-address netmask* | **shutdown** }

no standby *group-index* [**primary**] {**description** *text* | **ip** *ip-address netmask* | **shutdown** }

Syntax Description

group-index	Standby group.
primary	(Optional) Defines the active interface in the standby group. By default, the first attached interface is active.
description *text*	(Optional) Sets the description for the specified interface. The maximum length of the description text is 240 characters.
ip *ip-address netmask*	Sets the IP address and the netmask for the specified standby group. The group IP address and netmask of a standby group must be configured on all of the member interfaces.
shutdown	(Optional) Shuts down the specified standby group. You can shut down a standby group even if you have not configured a group IP address for the standby group. **Note** When a standby group is shut down, all of the alarms previously raised by this standby group are cleared.

Defaults

There are no standby interfaces by default.

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** interface configuration command. To make an interface the active interface in a standby group, use the **standby** *group-index* **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** *group-index* command and 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.

```
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

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*}

Syntax Description

standard	Enables standard ACL configuration mode. The CLI enters the standard ACL configuration mode in which all subsequent commands apply to the current standard access list. The (config-std-nacl) prompt appears: `WAE(config-std-nacl)#`
acl-name	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
acl-num	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For standard access lists, the valid range is 1 to 99.

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

To delete a line from the standard IP ACL, use the **delete** standard ACL configuration command.

delete *line-num*

Syntax Description

line-num	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

insert *line-num*	(Optional) Inserts the conditions following the specified line number into the access list.
deny	Causes packets that match the specified conditions to be dropped.
source-ip	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).
wildcard	(Optional) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1. **Note** For standard IP ACLs, the *wildcard* parameter of the **ip access-list** command is always optional. If the **host** keyword is specified for a standard IP ACL, then the *wildcard* parameter is not allowed.
host *source-ip*	Matches the following IP address.
any	Matches any IP address.

Defaults

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

Command Modes

standard ACL configuration mode

Device Modes

application-accelerator

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 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

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

start-line-num	(Optional) Line number from which the list begins.
end-line-num	(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

old-line-num	Line number of the entry to move.
new-line-num	New position of the entry. The existing entry is moved to the following position in the access list.

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

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

insert *line-num*	(Optional) Inserts the conditions following the specified line number into the access list.
source-ip	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).
wildcard	(Optional) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1. **Note** For standard IP ACLs, the *wildcard* parameter of the **ip access-list** command is always optional. If the **host** keyword is specified for a standard IP ACL, then the *wildcard* parameter is not allowed.
host *source-ip*	Matches the following IP address.
any	Matches any IP address.

Defaults

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

Command Modes

standard ACL configuration mode

Device Modes

application-accelerator

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

extended	Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. The (config-ext-nacl) prompt appears: `WAE(config-ext-nacl)#`
acl-name	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
acl-num	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

line-num	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

central-manager

Examples

The following example shows how to delete line 10 from the extended ACL testextacl:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# delete 10
```

Related Commands

(config-ext-nacl) list

(config-ext-nacl) move

(config-ext-nacl) deny

To add a line to an extended access list that specifies the type of packets that you want the WAAS device to drop, use the **deny** 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

insert *line-num*	(Optional) Specifies to insert the conditions following the specified line number into the access list.
gre	Specifies to match packets using the Generic Routing Encapsulation protocol.
icmp	Specifies to match ICMP packets.
tcp	Specifies to match packets using the TCP protocol.
udp	Specifies to match packets using the UDP protocol.
ip	Specifies to match all IP packets.
proto-num	IP protocol number.
source-ip	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).

wildcard	(Optional) Wildcard. The notation is in 4-digit, dotted-decimal format. Tge 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 *wildcard* parameter of the **ip access-list** command is always optional. If the **host** keyword is specified for a extended IP ACL, then the *wildcard* parameter is not allowed.
host *source-ip*	Specifies to match the following IP address.
any	Specifies to match any IP address.
dest-ip	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).
operator port	(Optional) Operator to use with specified ports, where **lt** = less than, **gt** = greater than, **eq** = equal to, **neq** = not equal to, and **range** = an inclusive range. The port value is a number (0–65535) or a keyword; two port numbers are required with the **range** keyword. See the “Usage Guidelines” section for a listing of the UDP and TCP keywords.
established	(Optional) Specifies to match TCP packets with the acknowledgment or reset bits set.
icmp-type	(Optional) Match with ICMP message type (0–255).
code	(Optional) Code type is 0–255.
icmp-msg	(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

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
cmm	Cluster Membership Manager service	5787
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
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
ssh	Secure Shell login	22
tacacs	Terminal Access Controller Access Control System	49

Table 3-2 TCP Keywords for Extended Access Lists (continued)

CLI TCP Keyword	Description	TCP Port Number
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:

```
...
!
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

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

start-line-num	(Optional) Line number from which the list begins.
end-line-num	(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

old-line-num	Line number of the entry to move.
new-line-num	New position of the entry. The existing entry is moved to the following position in the access list.

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

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

insert *line-num*	(Optional) Specifies to insert the conditions following the specified line number into the access list.
gre	Specifies to match packets using the Generic Routing Encapsulation protocol.
icmp	Specifies to match ICMP packets.
tcp	Specifies to match packets using the TCP protocol.
udp	Specifies to match packets using the UDP protocol.
ip	Specifies to match all IP packets.
proto-num	IP protocol number.
source-ip	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).

wildcard	(Optional) Wildcard. The notation is in 4-digit, dotted-decimal format. Tge 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 *wildcard* parameter of the **ip access-list** command is always optional. If the **host** keyword is specified for a extended IP ACL, then the *wildcard* parameter is not allowed.
host *source-ip*	Specifies to match the following IP address.
any	Specifies to match any IP address.
dest-ip	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).
operator port	(Optional) Operator to use with specified ports, where **lt** = less than, **gt** = greater than, **eq** = equal to, **neq** = not equal to, and **range** = an inclusive range. The port value is a number (0–65535) or a keyword; two port numbers are required with the **range** keyword. See the "Usage Guidelines" section for a listing of the UDP and TCP keywords.
established	(Optional) Specifies to match TCP packets with the acknowledgment or reset bits set.
icmp-type	(Optional) Match with ICMP message type (0–255).
code	(Optional) Code type is 0–255.
icmp-msg	(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

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
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
ssh	Secure Shell login	22
tacacs	Terminal Access Controller Access Control System	49

Table 3-5 TCP Keywords for Extended Access Lists (continued)

CLI TCP Keyword	Description	TCP Port Number
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:

```
...
!
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

Use preposition configuration mode for configuring preposition tasks and related parameters. To enter this mode, enter the specified preposition command from the global configuration mode. The prompt for preposition configuration mode consists of the hostname of the WAE followed by (config-preposition) and the pound sign (#). You must be in preposition configuration mode to enter preposition configuration commands.

(config-preposition) accelerator http preposition dre enable

To enable DRE (DDUP feature) for preposition connections, use the **accelerator http preposition dre enable** preposition configuration command. To disable DRE for preposition connections, use the **no** form of this command.

accelerator http preposition dre enable

no accelerator http preposition dre enable

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

preposition configuration

Device Modes

application-accelerator

Usage Guidelines

<need info here>

Examples

The following example shows how to enable DRE for preposition connection.

```
WAAS(config-preposition)# accelerator http preposition dre enable
```

Related

(config-preposition) accelerator http preposition task task-name

(config-preposition) accelerator http preposition task *task-name*

To configure a preposition task for one or more sites, use the **accelerator http preposition task task-name** preposition configuration command. To disable the specified preposition task, use the **no** form of this command.

accelerator http preposition task *task-name* **duration | enable | pattern | rate | recursion | schedule | url**

no accelerator http preposition task *task-name* **duration | enable | pattern | rate | recursion | schedule | url**

task-name	The name of the preposition task. Preposition task name is an alphanumeric identifier up to 47 characters. Special characters like ‘/\{}()?”<>[]&*” are not allowed. Note the following when specifying a task • You can configure up to 10 URLs per task. • You can configure up to 10 schedules per task. • You can configure up to 50 tasks per device/device group.
pattern exclude *pattern*	The object type(s) to exclude from caching, such as .jsp or .asp, each separated by a comma or a space. The list of object name patterns to be excluded has a total pattern field limit of 47 characters.
pattern include *pattern*	The object type(s) to include in caching, such as .jsp or .asp, each separated by a comma or a space. The list of object name patterns to be included has a total pattern field limit of 47 characters.
schedule	The time for the preposition task to run, include start date and time and recurring dates and times. (no) schedule daily *hour:minute* (no) schedule yearly *day-of-month:month hour:minute* (no) schedule monthly date *list-of-day-of-month* time *hour:minute* (no) schedule weekly *list-of-day-of-week* time *hour:minute*
duration *minutes*	The maximum amount of time, in minutes, a preposition task can run before it is halted. You can set the duration to ensure that preposition tasks do not overlap with each other, or with times of high traffic. The range is 1 to 2,147,483,647 minutes.

depth	The depth of the link level at which the content is retrieved. Recursion depth is active only if you check the **Recursive Task** check box. Select 1, 2, 3, 5, 8, 13, or 21 from the drop-down list, or enter any custom value between 1-1000. The default is 1. **Note** A greater number of specified levels of links means a greater amount of data stored in the cache, sometimes exponentially more. If the amount of requested pre-fetched data becomes larger than the cache, the newly requested data will flush all previously stored data, and may slow down other operations that attempt to use the cache.
url	The base URL(s) for prepositioning. The maximum length for the URL is 900 characters. Characters not allowed in the URL are space, double quotes (“). ASCII characters are allowed in the range of ASCII 33 through ASCII 125. • Use a space to separate multiple URLs. • You can configure up to 10 URLs per task.
rate	The maximum download rate, in KBps. The range is 0 to 10,000,000. The default is 20. Zero indicates no enforced rate limiting.
recursive	The prepositioning should travel from the base URLs according to the specified **depth**.
recursion delay *seconds*	The amount of time, in seconds, between requests during recursive download.This simulates user wait time. Recursive delay time is necessary because some servers use the lack of time between requests to detect and restrict web spiders. Use a value between 0 and 600 seconds. A value of zero provides the best performance when there are no web spider restrictions.
recursion include domain *domain-suffix*	The list of server domain suffixes for which recursive spidering is permitted. If the list is empty, then spidering is only permitted within the same domain as the specified URL. You can configure up to ten servers: • The server name is up to 255 characters. • Server names are separated by comma or space.
enable	Enable the task to run. For the task to run, it must be enabled with at least URL and one schedule.

Command Default

The default is disabled.

Command Modes

preposition configuration

Device Modes

application-accelerator

Usage Guidelines

Use the sub-mode facility (prompt “>”) to configure a preposition task:

- **no** - Turns off the command or resets it to its defaults.
- **exit** - Exits the sub-mode options menu.

Examples

The following example shows the preposition task “test1,” which runs daily at 14:30. The task length is ten minutes; there is a recursion delay of two seconds between requests. The task URL is www.cisco.com. This task excludes .jsp files, and includes any objects to “www.sampletestdomain.com” if www.cisco.com references it. The task has a maximum download rate of 1000, and the recursion depth is four.

```
accelerator http preposition task test1
recursion depth 4
rate 1000
recursive
recursion delay 2
recursion include domain www.sampletestdomain.com
duration 10
pattern exclude .jsp
url www.cisco.com
schedule daily 14:30
enable
```

Related

(config-preposition) accelerator http preposition dre enable

(config-preposition) credentials

To set the username and password credentials for a file server in a preposition directive, use the **credentials** preposition configuration command.

credentials username *username* **password** {**0** | **1**} *password*}

Syntax Description

username *username*	Specifies the username.
password {**0** | **1**} *password*	Specifies the password. To indicate that the password string is unencrypted, specify **0**. To indicate that the password string is encrypted, specify **1**.

Defaults

No default behavior or values.

Command Modes

preposition configuration mode

Device Modes

application-accelerator

Examples

Related Commands

(config-preposition) server

(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

value	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

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.

For details on the valid DSCP marking values, see Table 3-2, “DSCP Marking Values” for the **service-policy** global configuration command.

Examples

Related Commands

(config) service-policy

(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		
	minutes	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

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

Usage Guidelines

You must use this command to enable a preposition directive after you define it and schedule it.

Examples

Related Commands

(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

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

percentage	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

Related Commands

(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

size_in_kb	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

Related Commands

(config-preposition) max-cache

(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

size_in_kb	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

Related Commands

(config-preposition) max-file-size

(config-preposition) name

To set the display name of a preposition directive, use the **name** preposition configuration command.

name *name*

Syntax Description

name	Name of a preposition directive.

Defaults

The default name is New preposition directive *n*.

Command Modes

preposition configuration mode

Device Modes

application-accelerator

Examples

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

equals	Specifies to limit the selected files to those filenames that are equal to the specified text.
starts-with	Specifies to limit the selected files to those filenames that start with the specified text.
ends-with	Specifies to limit the selected files to those filenames that end with the specified text.
contains	Specifies to limit the selected files to those filenames that contain the specified text.
text	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

Related Commands

(config-preposition) root

(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

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

path	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

Related Commands

(config-preposition) pattern

(config-preposition) recursive

(config-preposition) scan-type

(config-preposition) server

(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

full	Specifies to copy all files to the Edge WAE cache.
since last	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. 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.
since *period units*	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 **min**, **hour**, **day**, or **week**.

Defaults

Full

Command Modes

preposition configuration mode

Device Modes

application-accelerator

Examples

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

now	Specifies that prepositioning occurs within a few minutes of submitting the schedule.
daily *time*	Specifies that prepositioning occurs daily at the defined time at which to run the prepositioning task, in the following format: *hh*:*mm*, where *hh* is the hour (00–23) and *mm* is the minutes (00–59). Hours are in 24-hour format, as in the following example: 23:01
date *date time*	Specifies that prepositioning occurs at the defined time and date at which to run the prepositioning task, in the following format: *DD*:*MM*:*YYYY*, where *DD* is the day (01–31), *MM* is the month (01–12), and *YYYY* is the year (1993–2035). The time is in the following format: *hh*:*mm*, where *hh* is the hour (00–23) and *mm* is the minutes (00–59). Example: 28:09:2008 23:01
weekly *dayname*	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
time *time*	Specifies the time to run the preposition task on the specified days.
monthly	Specifies that prepositioning occurs on the selected days or dates of the month at the defined time.
week-day *dayname weeknumber*	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.
day *day*	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.

Defaults

now

Command Modes

preposition configuration mode

Device Modes

application-accelerator

Examples

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

name	Server name.

Defaults

No default behavior or values.

Command Modes

preposition configuration mode

Device Modes

application-accelerator

Examples

Related Commands

(config-preposition) credentials

(config-preposition) root

(config-preposition) use-proxy

To enable the proxy use by a specific preposition task, use the **use-proxy** global configuration command. To disable proxy use by a specific preposition task, the **no** form of this command.

use-proxy

no use-proxy

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

preposition configuration

Device Modes

application-accelerator

Usage Guidelines

For WAAS Version 6.2.1 and later, you can preposition external content in the case of a deployment with proxy. Consider the following when configuring HTTP/S preposition proxy for Akamai Connect:

- IPv4 proxy is supported for HTTP/S prepositioning.
- The HTTP preposition proxy feature is a feature independent of the WAAS CM and external HTTP proxy.
- Specific IP address-based proxy configuration is supported for HTTP/S preposition proxy. File-based and auto-detected configurations are not supported for HTTP/S preposition proxy.

Examples

Related

(config-preposition) accelerator http preposition task task-name

(config-preposition) user-agent

To create a user agent to display information about the client browsers and operating systems used to access the URLs specified for a preposition task, use the **user-agent** global configuration command. To not use a specified user agent, use the **no** form of this command.

user-agent *user-agent-string*

no user-agent *user-agent-string*

Syntax Description

user-agent *user-agent-string*	String for the user agent. Use only letters, numbers, hyphen, and underscore, up to a maximum of 256 characters.

Defaults

No default behavior or values.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

preposition configuration

Device Modes

application-accelerator

Usage Guidelines

The user agent displays information about the client browsers and operating systems used to access the URLs specified for a particular preposition task. The server populates the cache with content that is dependent in part on the type of user agent used for the specified cache prepositioning task.

Examples

Related

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*

Syntax Description

certificate_authority_name	Name of the certificate authority (CA). The CA name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the command to add and configure a certificate authority. This command initiates the certificate authority configuration mode, indicated by the **(config-ca)** prompt.

Within certificate authority configuration mode, you can use the various commands (**ca-certificate**, **description**, **revocation check**, and so on) to define an encryption certificate authority. To return to global configuration mode, enter **exit** at the certificate authority configuration mode prompt.

Examples

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 **crypto pki ca** command edits it. If the certificate authority does not exist, the **crypto pki ca** command creates it.

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# description This-is-my-CA-description
WAE(config-ca)# exit
WAE(config)#
```

Related Commands

(config-ca) ca-certificate

(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*

Syntax Description

filename.ca	Filename of the certificate authority. The filename must end in .ca and be no longer than 32 characters.

Defaults

No default behavior or values.

Command Modes

certification authority configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Before you can assign a certification authority file using the **ca-certificate** command, the certification authority file must be imported using the **crypto import ca-certificate** EXEC command. See the crypto import command.

Examples

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
```

Related Commands

(config-ca) description

(config-ca) revocation-check

(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*

Syntax Description

description-text	Test to briefly describe the certification authority being used. The description text must not exceed 128 characters.

Defaults

No default behavior or values.

Command Modes

certification authority configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to define the descriptive text for the certification authority:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# description This is my CA description
```

Related Commands

(config-ca) ca-certificate

(config-ca) revocation-check

(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

none	No revocation checking is used.
ocsp-cert-url	Enables Online Certificate Status Protocol (OCSP) revocation status checking using the CA server URL defined in the CA certificate.
ocsp-url	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

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 PKI global settings configuration mode, you can use PKI global settings commands to define PKI settings. To return to global configuration mode, enter **exit** at the PKI 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) ocsp

(config-pki-global-settings) revocation-check

(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** global settings configurations mode command.

ocsp url http://*address*

Syntax Description

url http://*address*	URL to be used for OCSP revocation status checking.

Defaults

No default behavior or values.

Command Modes

PKI global settings configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to define the OCSP URL as www.myocspurl.com:

```
WAE(config)# crypto pki global-settings
WAE(config-pki-global-settings)# ocsp url http://www.myocspurl.com
```

Related Commands

(config-pki-global-settings) revocation-check

(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**]

Syntax Description

ocsp-cert-url	Enables Online Certificate Status Protocol (OCSP) revocation status checking using the CA server URL defined in the CA certificate.
ocsp-url	Enables OCSP revocation status checking using the URL defined for the global OCSP settings.
none or null	Specifies a revocation check null method that returns revocation.

Defaults

No default behavior or values.

Command Modes

PKI global settings configuration

Device Modes

application-accelerator

central-manager

Examples

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
```

Related Commands

(config-pki-global-settings) ocsp

SSL Accelerated Service Configuration Mode Commands

SSL accelerated services lets you enable and configure SSL acceleration on your WAAS system, and define services to be accelerated on the SSL path. To configure secure socket layer (SSL) encryption accelerated services on a WAAS device, use the **crypto ssl services accelerated-service** global configuration command. To delete a parameter use the **no** form of the command.

crypto ssl service accelerated-service <*service-name*> match sni

no crypto ssl service accelerated-service <*service-name*> match sni

Syntax Description

service-name	Name of the accelerated service that you want to create or edit. The service list name may contain up to 128 characters.
match sni	Matches SSL Server Name Indication(SNI) with Subject Alternate Names(SAN) in the configured SSL certificate.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **crypto ssl services accelerated-service** command to add and configure an accelerated service. The **crypto ssl services accelerated-service** command initiates accelerated service configuration mode, as indicated by the following prompt:

```
WAE(config-ssl-accelerated)#
```

Within SSL accelerated service configuration mode, you can use SSL accelerated service configuration commands. To return to global configuration mode, enter **exit** at the accelerated service configuration mode prompt.

Examples

The following example shows how to create or edit an accelerated service called myservice. If the service is already established on the WAAS device, the **crypto ssl services accelerated-service** command edits it. If the service does not exist, the **crypto ssl services accelerated-service** command creates it:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# exit
WAE(config)#
```

Related Commands

(config-ssl-accelerated) cipher-list

(config-ssl-accelerated) client-cert-key

(config-ssl-accelerated) client-cert-verify

(config-ssl-accelerated) client-version-rollback-check

(config-ssl-accelerated) description

(config-ssl-accelerated) inservice

(config-ssl-accelerated) server-cert-key

(config-ssl-accelerated) server-cert-verify

(config-ssl-accelerated) server-domain

(config-ssl-accelerated) server-ip

(config-ssl-accelerated) server-name

(config-ssl-accelerated) version

(config-ssl-accelerated) cipher-list

To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **cipher-list** command. To delete a cipher list use the **no** form of the command.

cipher-list *cipher-list-name*

no cipher-list *cipher-list-name*

Syntax Description

cipher-list-name	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

A cipher list is customer list of cipher suites that you assign to an SSL connection. (See the SSL Cipher List Configuration Mode Commands chapter for more information.)

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **cipher-list** command edits it. If the cipher list does not exist, the **cipher-list** command creates it:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# cipher-list myciphers
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) client-cert-key

To configure a certificate and private key, use the **client-cert-key** command.

client-cert-key *filename*

Syntax Description

filename	Filename of the certificate and key. Must be in PKCS#12 and have a ".p12" extension.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then import a certificate and key:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# client-cert-key cert.p12
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) client-cert-verify

To enable verification of client certificates, use the **client-cert-verify** command.

client-cert-verify [**revocation-check none**]

Syntax Description

revocation-check none	(Optional) Specifies a revocation check null method that returns revocation success.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

If the server and client devices are using self-signed certificates and certificate verification is enabled, WAAS devices will not be able to accelerate SSL traffic.

To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# client-cert-verify revocation-check none
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) client-version-rollback-check

To disable the client SSL version rollback check, use the **client-version-rollback-check** command.

client-version-rollback-check disable

Syntax Description

disable	Disables the client SSL version rollback check.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

If a non-RFC 2246 compliant client passes the incorrect client version in the SSL message, a bad record MAC SSL handshake failure may occur. The SSL accelerator terminates such connections. In this case, you can disable the client version rollback check which allows these connections to be optimized.

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then disable the client SSL version rollback check:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# client-version-rollback-check disable
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) description

To add a description of the SSL accelerated service, use the **description** command.

description *description*

Syntax Description

description	String that is the description of the SSL accelerated service.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then a description of the accelerated service:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# description SSL accelerated service
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) inservice

To enable the accelerated service, use the **inservice** command.

inservice

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then enable the accelerated service:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# inservice
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) protocol-chaining enable

To enable the accelerated service, use the **protocol-chaining enable** command. To disable this accelerated service, use the **no** form of this command.

protocol-chaining enable

Syntax Description

This command has no arguments or keywords.

Defaults

By default, protocol chaining is enabled.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then enable the protocol chaining:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# protocol-chaining enable
```

(config-ssl-accelerated) server-cert-key

To configure a certificate and private key, use the **server-cert-key** command.

server-cert-key *filename*

Syntax Description

filename	Filename of the certificate and key. Must be in PKCS#12 and have a ".p12" extension.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then import a certificate and key:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-cert-key cert.p12
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) server-cert-verify

To enable verification of server certificates, use the **server-cert-verify** command.

server-cert-verify [**revocation-check none**]

Syntax Description

revocation-check none	(Optional) Specifies a revocation check null method that returns revocation success.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

If the server and client devices are using self-signed certificates and certificate verification is enabled, WAAS devices will not be able to accelerate SSL traffic.

To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-cert-verify revocation-check none
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) server-domain

To configure the accelerated server domain and TCP port, use the **server-domain** command.

server-domain *srv-domain* {**port** *port-no*}

Syntax Description

server-domain *srv-domain*	Specifies the domain name of the accelerated server starting with the characters "*.". 255 alphanumeric characters maximum, 63 characters per label/segment.
port *port-no*	Specifies the port number of the accelerated server. Range is 1 to 65535.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the accelerated server domain name and port:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-domain 2.2.2.2 port 1
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) server-ip

To configure the accelerated server IP address and TCP port, use the **server-ip** command.

server-ip *ip-address* {**port** *port-no*}

Syntax Description

server-ip *ip-address*	Specifies the IP address of the accelerated server.
port *port-no*	Specifies the port number of the accelerated server. Range is 1 to 65535.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the accelerated server IP address and port:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-ip 2.2.2.2 port 1
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) server-name

To configure the accelerated server hostname and TCP port, use the **server-name** command.

server-name *hostname* {**port** *port-no*}

Syntax Description

server-name *hostname*	Specifies the hostname of the accelerated server. 255 alphanumeric characters max, 63 characters per label/segment.
port *port-no*	Specifies the port number of the accelerated server. Range is 1 to 65535.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the accelerated server name and port:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# server-name acc_server port 1
```

Related Commands

(config) crypto ssl

(config-ssl-accelerated) version

To specify the type of SSL protocol to use for accelerated services, use the **version** command.

version {**all** | **ssl3** | **tls1**}

Syntax Description

version {**all** | **ssl3** | **tls1**}	Specifies SSL3 for the SSL version 3 protocol, TLS1 for the Transport Layer Security version 1 protocol, or All to use both SSL3 and TLS1 SSL protocols.

Defaults

No default behavior or values.

Command Modes

SSL accelerated service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL accelerated service configuration mode, and then set the protocol to SSL version 3:

```
WAE(config)# crypto ssl services accelerated-service myservice
WAE(config-ssl-accelerated)# version SSL3
```

Related Commands

(config) crypto ssl

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*

Syntax Description

cipher-list-name	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **crypto ssl cipher-list** command to add and configure a cipher list. The **crypto ssl cipher-list** command initiates 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.

Examples

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 **crypto ssl cipher-list** command edits it. If the cipher list does not exist, the **crypto ssl cipher-list** 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)#
```

Related Commands

(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*]

Syntax Description

cipher-suite-name	Name of the cipher suite you want to add or reprioritize. Type any of the following strings: **dhe-rsa-with-3des-ede-cbc-sha** **dhe-rsa-with-aes-128-cbc-sha** **dhe-rsa-with-aes-256-cbc-sha** **dhe-rsa-with-des-cbc-sha** **rsa-with-3des-ede-cbc-sha** **rsa-with-aes-128-cbc-sha** **rsa-with-aes-256-cbc-sha** **rsa-with-des-cbc-sha** **rsa-with-rc4-128-md5** **rsa-with-rc4-128-sha** If you are establishing an SSL connection to a Microsoft IIS server, do not select a DHE-based cipher suite.
priority *value*	(Optional specifies)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

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

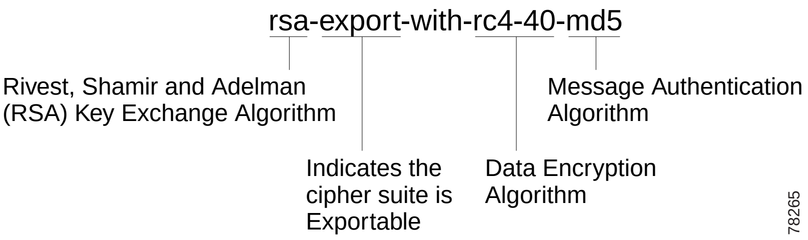

rsa-export-with-rc4-40-md5
Rivest, Shamir and Adelman (RSA) Key Exchange Algorithm
Message Authentication Algorithm
Indicates the cipher suite is Exportable
Data Encryption Algorithm
78265

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

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
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
WAE(config-cipher-list)# cipher rsa-with-3des-ede-cbc-sha priority 1
```

Related Commands

(config) crypto ssl

SSL Global Service Configuration Mode Commands

SSL global service lets you enable and configure basic SSL acceleration settings on your WAAS system. To configure global services on a WAAS device, use the **crypto ssl services global-settings** global configuration command. To delete a parameter use the **no** form of the command.

crypto ssl services global-settings

no crypto ssl services 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

central-manager

Usage Guidelines

Use the **crypto ssl services global-settings** command to configure basic SSL acceleration settings. The **crypto ssl services global-settings** command initiates SSL global service configuration mode, as indicated by the following prompt:

```
WAE(config-ssl-global)#
```

Within SSL global service configuration mode, you can use SSL global service configuration commands. To return to global configuration mode, enter **exit** at the SSL global service configuration mode prompt.

Examples

The following example shows how to enter SSL global service configuration mode:

```
WAE(config)# crypto ssl services global-settings
WAE(config-ssl-global)# exit
WAE(config)#
```

Related Commands

(config-ssl-global) cipher-list

(config-ssl-global) machine-cert-key

(config-ssl-global) version

(config-ssl-global) cipher-list

To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **cipher-list** command. To delete a cipher list use the **no** form of the command.

cipher-list *cipher-list-name*

no cipher-list *cipher-list-name*

Syntax Description

cipher-list-name	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

SSL global service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

A cipher list is customer list of cipher suites that you assign to an SSL connection. (See the SSL Cipher List Configuration Mode Commands chapter for more information.)

Examples

The following example shows how to enter SSL global service configuration mode, and then create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **cipher-list** command edits it. If the cipher list does not exist, the **cipher-list** command creates it:

```
WAE(config)# crypto ssl services management-service
WAE(config-ssl-global)# cipher-list myciphers
```

Related Commands

(config) crypto ssl

(config-ssl-global) machine-cert-key

To configure a certificate and private key, use the **machine-cert-key** command.

machine-cert-key *filename*

Syntax Description

filename	Filename of the certificate and key. Must be in PKCS#12 and have a ".p12" extension.

Defaults

No default behavior or values.

Command Modes

SSL global service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL global service configuration mode, and then import a certificate and key:

```
WAE(config)# crypto ssl services global-settings
WAE(config-ssl-global)# machine-cert-key cert.p12
```

Related Commands

(config) crypto ssl

(config-ssl-global) version

To specify the type of SSL protocol to use for global services, use the **version** command.

version {**all** | **ssl3** | **tls1**}

Syntax Description

version {**all** | **ssl3** | **tls1**}	Specifies SSL3 for the SSL version 3 protocol, TLS1 for the Transport Layer Security version 1 protocol, or All to use both SSL3 and TLS1 SSL protocols.

Defaults

No default behavior or values.

Command Modes

SSL global service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL global service configuration mode, and then set the protocol to SSL version 3:

```
WAE(config)# crypto ssl global-settings
WAE(config-ssl-global)# version SSL3
```

Related Commands

(config) crypto ssl

SSL Host Peering Service Configuration Mode Commands

SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections. To configure secure socket layer (SSL) encryption peering services on a WAAS device, use the **crypto ssl services host-service peering** global configuration command. To delete a parameter use the **no** form of the command.

crypto ssl services host-service peering

no crypto ssl services host-service peering

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 **crypto ssl services host-service** command to configure SSL peering service parameters. The **crypto ssl services host-service** command initiates SSL host peering service configuration mode, as indicated by the following prompt:

```
WAE(config-ssl-peering)#
```

Within SSL host peering service configuration mode, you can use SSL host peering service configuration commands. To return to global configuration mode, enter **exit** at the SSL host peering service configuration mode prompt.

Examples

The following example shows how to enter SSL host peering service configuration mode:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)# exit
WAE(config)#
```

Related Commands

(config-ssl-peering) cipher-list

(config-ssl-peering) peer-cert-verify

(config-ssl-peering) version

(config-ssl-peering) cipher-list

To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **cipher-list** command. To delete a cipher list use the **no** form of the command.

cipher-list *cipher-list-name*

no cipher-list *cipher-list-name*

Syntax Description

cipher-list-name	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

SSL host peering service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

A cipher list is customer list of cipher suites that you assign to an SSL connection. (See the SSL Cipher List Configuration Mode Commands chapter for more information.)

Examples

The following example shows how to enter SSL host peering service configuration mode, and then create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **cipher-list** command edits it. If the cipher list does not exist, the **cipher-list** command creates it:

```
WAE(config)# crypto ssl services management-service
WAE(config-ssl-peering)# cipher-list myciphers
```

Related Commands

(config) crypto ssl

(config-ssl-peering) peer-cert-verify

To enable verification of peer certificates, use the **peer-cert-verify** command.

peer-cert-verify [**revocation-check none**]

Syntax Description

revocation-check none	(optional) Specifies a revocation check null method that returns revocation success.

Defaults

No default behavior or values.

Command Modes

SSL host peering service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections.

If peer certificate verification is enabled, WAAS devices that use self-signed certificates will not be able to establish peering connections to each other and, thus, not be able to accelerate SSL traffic.

To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples

The following example shows how to enter SSL host peering service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)# peer-cert-verify revocation-check none
```

Related Commands

(config) crypto ssl

(config-ssl-peering) version

To specify the type of SSL protocol to use for management services, use the **version** command.

version {**all** | **ssl3** | **tls1**}

Syntax Description

version {**all** | **ssl3** | **tls1**}	Specifies SSL3 for the SSL version 3 protocol, TLS1 for the Transport Layer Security version 1 protocol, or All to use both SSL3 and TLS1 SSL protocols.

Defaults

No default behavior or values.

Command Modes

SSL host peering service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL host peering service configuration mode, and then set the protocol to SSL version 3:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)# version SSL3
```

Related Commands

(config) crypto ssl

SSL Management Service Configuration Mode Commands

SSL management services lets you configure SSL parameters used for secure communications between the Central Manager and the WAE devices. To configure secure socket layer (SSL) encryption management service parameters on a WAAS device, use the **crypto ssl management-service** global configuration command. To delete a parameter use the **no** form of the command.

crypto ssl management-service

no crypto ssl management-service

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 **crypto ssl management-service** command to configure management services. The **crypto ssl management-service** command initiates SSL management service configuration mode, as indicated by the following prompt:

```
WAE(config-ssl-mgmt)#
```

Within SSL management service configuration mode, you can use the SSL management service configuration commands. To return to global configuration mode, enter **exit** at the SSL management service configuration mode prompt.

Examples

The following example shows how to enter SSL management service configuration mode:

```
WAE(config)# crypto ssl management-service
WAE(config-ssl-mgmt)# exit
WAE(config)#
```

Related Commands

(config-ssl-mgmt) cipher-list

(config-ssl-mgmt) peer-cert-verify

(config-ssl-mgmt) version

(config-ssl-mgmt) cipher-list

To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **cipher-list** command. To delete a cipher list use the **no** form of the command.

cipher-list *cipher-list-name*

no cipher-list *cipher-list-name*

Syntax Description

cipher-list-name	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

SSL management service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

A cipher list is customer list of cipher suites that you assign to an SSL connection. (See the SSL Cipher List Configuration Mode Commands chapter for more information.)

Examples

The following example shows how to enter SSL management service configuration mode, and then create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **cipher-list** command edits it. If the cipher list does not exist, the **cipher-list** command creates it:

```
WAE(config)# crypto ssl services management-service
WAE(config-ssl-mgmt)# cipher-list myciphers
```

Related Commands

(config) crypto ssl

(config-ssl-mgmt) peer-cert-verify

To enable verification of peer certificates, use the **peer-cert-verify** command.

peer-cert-verify [**revocation-check none**]

Syntax Description

revocation-check none	(Optional) Specifies a revocation check null method that returns revocation success.

Defaults

No default behavior or values.

Command Modes

SSL management service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections.

If peer certificate verification is enabled, WAAS devices that use self-signed certificates will not be able to establish peering connections to each other and not be able to accelerate SSL traffic.

To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples

The following example shows how to enter SSL management service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl management-service
WAE(config-ssl-mgmt)# peer-cert-verify revocation-check none
```

Related Commands

(config) crypto ssl

(config-ssl-mgmt) version

To specify the type of SSL protocol to use for management services, use the **version** command.

version {**all** | **ssl3** | **tls1**}

Syntax Description

version tls1	Specifies TLS1 for the SSL version 3 protocol.
version ssl3	Specifies SSL3 for the Transport Layer Security version 1 protocol.
version all	Specifies ALL to use both SSL3 and TLS1 SSL protocols.

Defaults

No default behavior or values.

Command Modes

SSL management service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL management service configuration mode, and then set the protocol to SSL version 3:

```
WAE(config)# crypto ssl management-service
WAE(config-ssl-mgmt)# version SSL3
```

Related Commands

(config) crypto ssl

WCCP Configuration Mode Commands

To configure the Web Cache Coordination Protocol (WCCP) Version 2 TCP promiscuous mode service, use the **wccp tcp-promiscuous service-pair** global configuration command. To negate these actions, use the **no** form of this command.

wccp tcp-promiscuous {**service-pair** *serviceID serviceID+1* | *serviceID*}

no wccp tcp-promiscuous {**service-pair** *serviceID serviceID+1* | *serviceID*}

Syntax Description

service-pair *serviceID serviceID+1*	Specifies a pair of IDs for the WCCP service on devices configured as application accelerators. Valid values are two consecutive numbers from 1-100, inclusive.
serviceID	Specifies one ID for the WCCP service. A valid value is from 1-100, inclusive.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **wccp tcp-promiscuous service-pair** command to configure and enable the WCCP interception method. This command initiates the WCCP configuration mode as indicated by the **(**config-wccp-service**)** prompt.

Within WCCP configuration mode, you can use the various commands (**egress-method**, **failure-detection**, and so on) to define WCCP settings. To return to global configuration mode, enter the **exit** command.

You must use the **enable** WCCP configuration command to enable the WCCP service.

You must configure two WCCP service IDs on WAEs operating in application-acceleration mode.

Configurable WCCP service IDs allows a router to support multiple WCCP farms because the WAEs in different farms can use different service IDs. In WAAS versions earlier than 5.0, the default WCCP service IDs were 61 and 62.

The router service priority varies inversely with the service ID. The service priority of the service IDs 61/62 is 34. If you specify a lower service ID, the service priority is higher than 34 and if you specify a higher service ID, the service priority is lower than 34.

Note WCCP works only with IPv4 networks. WCCP commands are available only after the interception method is set to WCCP by the **interception-method** global configuration command.

Examples

The following example shows how to configure WCCP service IDs 61 and 62 and put a WAE into WCCP configuration mode:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)#
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) assignment-method

To configure the WCCP assignment method, hash type, or mask, use the **assignment-method** WCCP configuration command. To unconfigure the hash or mask setting, use the **no** form of this command.

assignment-method {**hash** {**hash-destination-ip** | **hash-source-ip**} | **mask** {**dst-ip-mask** *mask* | **src-ip-mask** *mask*}}

no assignment-method {**hash** {**hash-destination-ip** | **hash-source-ip**} | **mask** {**dst-ip-mask** *mask* | **src-ip-mask** *mask*}}

Syntax Description

hash	Specifies that the load-balancing assignment method is hash. Not supported on ANCs.
hash-destination-ip	Specifies that the load-balancing hash method should make use of the destination IP address. You can specify both the **hash-destination-ip** option and **the hash-source-ip** option.
hash-source-ip	Specifies that the load-balancing hash method should make use of the source IP address.
mask	Specifies that the load-balancing assignment method is mask.
dst-ip-mask *mask*	Specifies the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x0000000–0xFE000000.
src-ip-mask *mask*	Specifies the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000.

Defaults

The default load-balancing assignment method is mask. The default destination IP address mask is 0. The default source IP address mask for application accelerators is 0xF00 and for ANCs it is 0xF.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Usage Guidelines

In a service farm where the WAEs have different masks, the first WAE to establish two-way communication with the router(s) determines the farm's mask. All other WAEs cannot join the farm unless they are configured with the same mask.

The hash assignment method is not supported on ANCs.

Examples

The following example shows how to set a TCP promiscuous mode service mask on the source IP address:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# assignment-method mask src-ip-mask 0xFC0
```

Related Commands

show wccp

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) egress-method

To configure the WCCP egress method, use the **egress-method** WCCP configuration command. To unconfigure the egress method setting, use the **no** form of this command.

egress-method {**ip-forwarding** | **generic-gre** | **L2** | **wccp-gre**}

no egress-method {**ip-forwarding** | **generic-gre** | **L2** | **wccp-gre**}

Syntax Description

ip-forwarding	Configures the IP forwarding egress method.
generic-gre	Configures the generic GRE egress method.
L2	Configures the L2 egress method.
wccp-gre	Configures the WCCP GRE egress method.

Defaults

The default egress method is L2.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Usage Guidelines

The egress methods available on an application accelerator depend on the configured redirect method. If the redirect method is L2, the available egress methods include ip-forwarding and L2. If the redirect method is GRE, the available egress methods include ip-forwarding, generic-gre, and wccp-gre.

If you choose the L2 egress method, the WAE must be connected to a router or switch to which it has a Layer 2 connection and the router or switch must be configured for Layer 2 redirection.

On ANCs the egress method is not configurable and is set to match the redirect method.

Examples

The following example shows how to configure the egress method for WCCP GRE packet return:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# egress-method wccp-gre
```

The following example shows how to configure the egress method for IP forwarding:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# egress-method ip-forwarding
```

The following example shows how to configure the egress method for generic GRE 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)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# router-list-num 1
WAE(config-wccp-service)# egress-method generic-gre
```

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 wccp egress** EXEC command or the **show statistics connection egress-methods** EXEC command.

To view information about the generic GRE egress method, use the **show statistics generic-gre** EXEC command. To clear statistics information for the generic GRE egress method, use the **clear statistics generic-gre** EXEC command.

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) enable

To enable the WCCP service, use the **enable** WCCP configuration command. To disable the WCCP service, use the **no** form of this command.

enable

no enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure and enable WCCP:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# enable
WCCP configuration for TCP Promiscuous service 61 and 62 succeeded. Please remember to
configure WCCP service 61 and 62 on the corresponding router.
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) exit

To terminate WCCP configuration mode and return to the global configuration mode, use the **exit** WCCP configuration command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Examples

The following example shows how to terminate WCCP configuration mode:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# enable
WCCP configuration for TCP Promiscuous service 61 and 62 succeeded. Please remember to
configure WCCP service 61 and 62 on the corresponding router.
WAE(config-wccp-service)# exit
WAE(config)#
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) failure-detection

To configure the WCCP failure detection timeout, use the **failure-detection** WCCP configuration command. To unconfigure the failure detection setting, use the **no** form of this command.

failure-detection {**3** | **6** | **9** | **15** | **30**}

no failure-detection {**3** | **6** | **9** | **15** | **30**}

Syntax Description

{**3** | **6** | **9** | **15** | **30**}	Specifies the failure detection timeout in seconds. The 3 and 6 second values are valid only on ANCs .

Defaults

The default failure detection timeout is 30 seconds.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Usage Guidelines

The failure detection timeout value is negotiated with the router and takes effect only if the router also has the variable timeout capability. If the router has a fixed timeout of 30 seconds and you have configured a failure detection value on the WAE other than the default 30 seconds, the WAE is not able to join the farm and an alarm is raised (“Router unusable” with a reason of “Timer interval mismatch with router”).

Examples

The following example shows how to configure the failure detection timeout for 9 seconds:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# failure-detection 9
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) password

To configure the WCCP service password, use the **password** WCCP configuration command. To unconfigure the password, use the **no** form of this command.

password *password*

no password *password*

Syntax Description

password	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.

Defaults

No default behavior or values.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a WCCP service password:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# password mypass
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) redirect-method

To configure the WCCP redirect method, use the **redirect-method** WCCP configuration command. To unconfigure the redirect method setting, use the **no** form of this command.

redirect-method {**gre** | **L2**}

no redirect-method {**gre** | **L2**}

Syntax Description

gre	Configures the WAE to use Layer 3 GRE packet redirection.
L2	Configures the WAE to receive transparently redirected traffic from a WCCP Version 2-enabled switch or router if the WAE has a Layer 2 connection with the device and the device is configured for Layer 2 redirection.

Defaults

The default redirect method is L2.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Usage Guidelines

The redirect method configures how the WAE is to receive packets redirected by the switch or router.

The return method used to return nonoptimized (bypassed) packets to the router is automatically set the same as the configured redirect method.

The L2 redirect method is supported only if the WAE has a Layer 2 connection with the switch or router and the switch or router is configured for Layer 2 redirection. Because L2 redirection is implemented in hardware, it is more efficient and faster than GRE redirection.

Examples

The following example shows how to configure the redirect method for GRE:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# redirect-method gre
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) router-list-num

(config-wccp-service) weight

(config-wccp-service) router-list-num

To associate a configured router list with the WCCP service on a WAE, use the **router-list-num** WCCP configuration command. To unassociate the router list, use the **no** form of this command.

router-list-num *number*

no router-list-num *number*

Syntax Description

number	Number of the WCCP router list (1–7) that should be associated with the TCP promiscuous mode service. (These WCCP Version 2-enabled routers will transparently redirect TCP traffic to the WAE.)

Defaults

No default behavior or values.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Usage Guidelines

A WCCP router list must be configured on a WAE for WCCP traffic redirection to operate.

Using the **no router-list-num** WCCP configuration command removes the WAE from the cache farm of the routers in the list.

Examples

The following example shows how to configure a WCCP router list:

```
WAE(config)# wccp router-list 1 10.10.10.2
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# router-list-num 1
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) weight

(config-wccp-service) weight

To configure the weight assigned to a WAE, use the **weight** WCCP configuration command. To unconfigure the weight, use the **no** form of this command.

weight *number*

no weight *number*

Syntax Description

weight	A weight value from 1-10000. The way this number is interpreted depends on the total of the weight values of all WAEs in the service group. See the Usage Guidelines section for details.

Defaults

Weights are not assigned and the traffic load is distributed evenly between the WAEs in a service group.

Command Modes

WCCP configuration

Device Modes

application-accelerator

Usage Guidelines

This command specifies the weight value that is used for load balancing. The weight value ranges from 0 to 10000. If the total of all the weight values of the WAEs in a service group is less than or equal to 100, then the weight value represents a literal percentage of the total load redirected to the device for load-balancing purposes. For example, a WAE with a weight of 10 receives 10 percent of the total load in a service group where the total of all weight values is 50. If a WAE in such a service group fails, the other WAEs still receive the same load percentages as before the failure; they will not receive the load allocated to the failed WAE.

If the total of all the weight values of the WAEs in a service group is between 101 and 10000, then the weight value is treated as a fraction of the total weight of all the active WAEs in the service group. For example, a WAE with a weight of 200 receives 25 percent of the total load in a service group where the total of all the weight values is 800. If a WAE in such a service group fails, the other WAEs will receive the load previously allocated to the failed WAE. The failover handling is different than if the total weights are less than or equal to 100.

Examples

The following example shows how to configure the weight for WCCP load balancing:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# weight 250
```

Related Commands

show wccp

(config-wccp-service) assignment-method

(config-wccp-service) egress-method

(config-wccp-service) enable

(config-wccp-service) exit

(config-wccp-service) failure-detection

(config-wccp-service) password

(config-wccp-service) redirect-method

(config-wccp-service) router-list-num

Service Node Configuration Mode Commands

To configure a WAAS Node (WN) that is part of an AppNav Cluster, use the **service-insertion service-node** global configuration command. To unconfigure settings, use the **no** form of this command.

service-insertion service-node {**authentication sha1 key** *authkey* | **description** *description* | **enable** | **node-discovery enable** | **shutdown max-wait** *seconds*}

no service-insertion service-node {**authentication sha1 key** *authkey* | **description** *description* | **enable** | **node-discovery enable** | **shutdown max-wait** *seconds*}

Syntax Description

authentication sha1 key *authkey*	(Optional) Enables authentication between the WN and other devices in the AppNav Cluster and specifies an authentication key of up to 64 alphanumeric characters. This key must match the key configured in the service context.
description *description*	(Optional) Specifies a description of the node with up to 200 alphanumeric and space characters.
enable	(Optional) Enables the participation of the node in the AppNav Cluster.
node-discovery enable	(Optional) Specifies service-node discovery parameters and enables service-node discovery.
shutdown max-wait *seconds*	(Optional) Specifies the number of seconds that the node should wait for all connections to terminate when shutting down. Valid values range from 0-3600 seconds. The default is 120 seconds.

Defaults

There is no authentication key and no description configured. The shutdown waiting time is 120 seconds. The node is disabled.

Command Modes

global configuration

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Use the **service-insertion service-node** command to configure a WN that is part of an AppNav Cluster. When used without options, this command initiates the service node configuration mode, which is indicated by a different prompt **(**config-sn**)**. To return to global configuration mode, enter the **exit** command.

Each WN (and ANC acting as a WN) in the AppNav Cluster must be configured with WN settings by using the **service-insertion service-node** command. To begin using the node in the cluster, you must use the **enable** option.

Examples

The following example shows how to configure and enable a WN:

```
WAE(config)# service-insertion service-node
WAE(config-sn)# description London branch node 1
WAE(config-sn)# authentication sha1 key myauthkey
WAE(config-sn)# shutdown max-wait 120
WAE(config-sn)# enable
```

Related Commands

(config-sn) authentication

(config-sn) description

(config-sn) enable

(config-sn) node-discovery enable

(config-sn) shutdown

(config) service-policy

show service-insertion

(config-sn) authentication

To configure the WN authentication key, use the **authentication** service node configuration command. To unconfigure the authentication key, use the **no** form of this command.

authentication sha1 key *authkey*

no authentication sha1 key

Syntax Description

sha1 key *authkey*	Enables authentication between the WN and other devices in the AppNav Cluster and specifies an authentication key of up to 64 alphanumeric characters.

Defaults

No key is defined and authentication is not enabled.

Command Modes

Service node configuration

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The specified key must match the key configured in the service context.

Examples

The following example shows how to configure an authentication key:

```
WAE(config)# service-insertion service-node
WAE(config-sn)# authentication sha1 key myauthkey
```

Related Commands

(config-sn) description

(config-sn) enable

(config-sn) node-discovery enable

(config-sn) shutdown

(config) service-policy

show service-insertion

(config-sn) description

To configure the WN description, use the **description** service node configuration command. To unconfigure the description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	Specifies a description of the node with up to 200 alphanumeric and space characters.

Defaults

No default behavior or values.

Command Modes

Service node configuration

Device Modes

application-accelerator

appnav-controller

Examples

The following example shows how to configure a description:

```
WAE(config)# service-insertion service-node
WAE(config-sn)# description London branch node 1
```

Related Commands

(config-sn) authentication

(config-sn) enable

(config-sn) node-discovery enable

(config-sn) shutdown

(config) service-policy

show service-insertion

(config-sn) enable

To enable the participation of the WN in the AppNav Cluster, use the **enable** service node configuration command. To disable the node, use the **no** form of this command.

enable

no enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Service node configuration

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

A WN must be enabled before it can actively particpate in an AppNav Cluster and receive traffic for optimization.

Examples

The following example shows how to enable a WN for participation in an AppNav Cluster:

```
WAE(config)# service-insertion service-node
WAE(config-sn)# enable
```

Related Commands

(config-sn) authentication

(config-sn) description

(config-sn) node-discovery enable

(config-sn) shutdown

(config) service-policy

show service-insertion

(config-sn) node-discovery enable

To enable the node discovery of the Service Node(SN) in the AppNav Cluster, use the **node-discovery enable** service node configuration command. To disable the service node, use the **no** form of this command.

node-discovery enable{**bvi** *bridge_group_number* | **GigabitEthernet** *interface_slot* | **portchannel** *etherchannel_index* | **standby** *standby_index*}

no node-discovery enable

SyntaxDescription

bvi *bridge_group_number*	Select a bridge virtual interface for node-discovery.
GigabitEthernet *interface_slot*	Selects a gigabit ethernet interface for node discovery.
portchannel *etherchannel_ index*	Selects an ethernet channel interface for node discovery.
standby *standby_index*	Selects a standby group for node discovery.

Defaults

When service node is enabled, node discovery is enabled by default on eth0 interface.

Command Modes

Service node configuration

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Use the **node-discovery enable command** to configure the service node in the L2 proximity of any participating AppNav Controller so that it is automatically added to the cluster and can participate in WAN optimization. The node discovery configuration for a Service Node cannot be changed when the SN is enabled. To make changes on the node discovery configuration for a SN, the SN should be first disabled. For e.g. if you want to enable/disable the node discovery or change the node discovery interface, you can do so only when the SN is disabled.

Examples

The following example shows how to enable the node discovery of a SN for participation in an AppNav Cluster:

```
WAE(config)# service-insertion service-node
WAE(config-sn)# node-discovery enable ?
WAE(config-sn)# bvi 1
WAE(config-sn)# GigabitEthernet 1
WAE(config-sn)# portchannel 2
WAE(config-sn)# standby 1
```

Related Commands

(config-sn) authentication

(config-sn) description

(config-sn) shutdown

(config) service-policy

show service-insertion

(config-sn) shutdown

To configure the WN shutdown timeout, use the **shutdown** service node configuration command. To unconfigure the shutdown timeout, use the **no** form of this command.

shutdown max-wait *seconds*

no shutdown max-wait

Syntax Description

max-wait *seconds*	Specifies the number of seconds that the node should wait for all connections to terminate when shutting down. Valid values range from 0-3600 seconds. The default is 120 seconds.

Defaults

The shutdown waiting time is 120 seconds.

Command Modes

Service node configuration

Device Modes

application-accelerator

appnav-controller

Examples

The following example shows how to configure the shutdown timeout for two minutes:

```
WAE(config)# service-insertion service-node
WAE(config-sn)# shutdown max-wait 120
```

Related Commands

(config-sn) authentication

(config-sn) description

(config-sn) enable

(config-sn) node-discovery enable

(config) service-policy

show service-insertion

Service Context Configuration Mode Commands

To configure a service context for an AppNav Cluster, use the **service-insertion service-context** global configuration command. To unconfigure settings, use the **no** form of this command.

service-insertion service-context *contextname* {**authentication sha1 key** *authkey* | **description** *description* | **enable** [**graceful**] | **appnav-controller-group** *ancgroupname* | **service-node-group** *sngroupname* | **service-policy** *policyname*}

no service-insertion service-context *contextname* {**authentication sha1 key** *authkey* | **description** *description* | **enable** | **appnav-controller-group** *ancgroupname* | **service-node-group** *sngroupname* | **service-policy** *policyname*}

Syntax Description

contextname	Specifies the service context name to configure and enters service context group configuration mode to configure service context settings. If the service context does not exist, this command creates it.
authentication sha1 key *authkey*	(Optional) Enables authentication between devices in the AppNav Cluster and specifies an authentication key of up to 64 alphanumeric characters. This key must match the key configured on the WNs in the cluster.
description *description*	(Optional) Specifies a description of the service context with up to 200 alphanumeric and space characters.
enable	(Optional) Enables the service context for operation immediately.
graceful	(Optional) Enables the service context for operation in a graceful way that does not enable interception on this device until all cluster devices have agreed that this device has joined the cluster.
appnav-controller-group *ancgroupname*	Specifies the name of the ANCG to add to the service context. The ANCG must have been previously configured by the **service-insertion appnav-controller-group** command.
service-node-group *sngroupname*	Specifies the name of a WNG to add to the service context. The WNG must have been previously configured by the **service-insertion service-node-group** command.
service-policy *policyname*	Specifies the name of the AppNav policy to add to the service context. The policy must have been previously configured.

Defaults

There is no authentication key and no other settings are configured.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **service-insertion service-context** command to configure a service context for an AppNav Cluster. This command initiates the service context configuration mode, which is indicated by a different prompt **(**config-scxt**)**. To return to global configuration mode, enter the **exit** command.

Each ANC in the AppNav Cluster must be configured with the settings for the service context by using the **service-insertion service-context** command.

An AppNav Cluster can have up to 32 member WNGs and a maximum of 32 WNs.

Examples

The following example shows how to configure and enable a service context:

```
WAE(config)# service-insertion service-context mycontext
WAE(config-scxt)# description My service context
WAE(config-scxt)# authentication sha1 key myauthkey
WAE(config-scxt)# appnav-controller-group myControllerGroup
WAE(config-scxt)# service-node-group LondonNodeGroup
WAE(config-scxt)# service-node-group ChicagoNodeGroup
WAE(config-scxt)# service-policy myAppNavPolicy
WAE(config-scxt)# enable
```

Related Commands

(config-scxt) authentication

(config-scxt) description

(config-scxt) enable

(config-scxt) service-node-group

(config-scxt) service-policy

(config) service-policy

show service-insertion

Class Map Configuration Mode Commands

To configure an optimization class map, use the **class-map** global configuration command. To unconfigure settings, use the **no** form of this command.

class-map type {**waas**} [**match-all** | **match-any**] *classmap-name* [**rename** *new-name*]

no class-map type { **waas**} [**match-all** | **match-any**] *classmap-name*

Syntax Description

waas	Configures a WAAS optimization class map.
match-all	(Optional) Specifies that all match conditions must be satisfied to consider the class map matched (logical AND). Valid only on AppNav class maps.
match-any	(Optional) Specifies that any match condition must be satisfied to consider the class map matched (logical OR).
classmap-name	Class map name (up to 40 alpha-numeric characters and hyphen, beginning with a letter).
rename *new-name*	(Optional) Renames the class map with the specified new name.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **class-map** command to add or modify class maps and match conditions to identify specific types of traffic for use in policies. This command invokes the Class Map configuration mode, which is indicated by a different prompt **(**config-cmap**)**. To return to global configuration mode, enter the **exit** command.

You can delete a class map by using the **no** form of this command. You cannot delete a class map if any policies are using it.

When creating a new class map, you must add at least one condition. If any of the conditions specified match an already existing condition in the class-map, no action is taken.

Note You cannot have more than 512 different class maps and 1024 total match conditions.

The WAAS software comes with many class maps and policy rules that help your WAAS system classify and optimize some of the most common traffic on your network. Before you create a new class map or policy rule, we recommend that you review the default class map and policy rules and modify them as appropriate. It is usually easier to modify an existing class map or policy rule than to create a new one. For a list of the default applications, class maps, and policy rules, see the *Cisco Wide Area Application Services Configuration Guide*.

Note We strongly recommend that you use the WAAS Central Manager GUI to centrally configure class maps for your WAAS devices. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to configure a WAAS optimization class map:

```
wae(config)# class-map type waas myclass1
wae(config-cmap)# description My class number one
wae(config-cmap)# match protocol mapi tcp source ip 10.10.10.35
wae(config-cmap)# exit
```

Related Commands

(config-cmap) description

(config-cmap) match peer

(config-cmap) match protocol

(config-cmap) match tcp

(config-cmap) description

To configure the class map description, use the **description** class map configuration command. To unconfigure the description, use the **no** form of this command.

description *description*

no description *description*

Syntax Description

description	Specifies a description of the class map with up to 200 alphanumeric and space characters.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a class map description:

```
wae(config)# class-map type waas myclass1
wae(config-cmap)# description My class number one
```

Related Commands

(config-cmap) match protocol

(config-cmap) match tcp

(config-cmap) match protocol

To configure a match condition based on layer 7 protocol for the class map, use the **match protocol** class map configuration command. To unconfigure a match condition, use the **no** form of this command. The options for this command differ depending on what type of class map you are configuring.

For a WAAS optimization class map:

match protocol {**epm-uuid** *uuid* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**} [**tcp source** [**ip** *ip_address* [*wildcard_mask*]] [**port** *begin* [*end*]]

no match protocol {**epm-uuid** *uuid* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**} [**tcp source** [**ip** *ip_address* [*wildcard_mask*]] [**port** *begin* [*end*]]

Syntax Description

epm-uuid *uuid*	Specifies a custom EndPoint Mapper (EPM) service by its Universal Unique ID (UUID). Available only for WAAS optimization class maps. **Note** If you try to create a class map with an EPM UUID match condition that is already being used, an error message is displayed and the new class map is not created.
	Microsoft RPC application keywords:
mapi	Microsoft Exchange MAPI (Exchange Server Store EMSMDB),
ms-ad-rep	Microsoft Active Directory Replication (drsuapi),
ms-exch-nspi	Microsoft Active Directory Name Service Provider (NSP),
ms-frs	Microsoft File Replication Services (FRS),
ms-frs-api	Microsoft File Replication API,
ms-rfr	Microsoft Exchange Directory RFR interface,
ms-sql	Microsoft SQL,
msn-messenger	Microsoft Messenger Service,
netlogon	Netlogon RPC
tcp source	Specifies the criteria for matching source TCP packets.
ip *ip_address*	Specifies the IP address of the system that is the source of the traffic.
wildcard_mask	A wildcard subnet mask, which matches a range of source IP addresses. Use dotted decimal notation (such as 0.0.0.255 for /24).
port *begin* [*end*]	Specifies the criteria for identifying the port or ports used by the source host. Specify a single port or a begin and end port for a range. Available only for WAAS optimization class maps.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a protocol match condition for a class map:

```
wae(config)# class-map type waas myclass1
wae(config-cmap)# match protocol mapi tcp source ip 10.10.10.35
```

Related Commands

(config-cmap) description

(config-cmap) match tcp

(config-cmap) match tcp

To configure a match condition based on source and/or destination IP address and port for the class map, use the **match tcp** class map configuration command. To unconfigure a match condition, use the **no** form of this command. The options for this command differ depending on what type of class map you are configuring.

For a WAAS optimization class map:

match tcp {**any** |
destination [**ip** *ip_address* [*wildcard_mask*]] [**port** *begin* [*end*]] [**source ip** *ip_address* [*wildcard_mask*] [**port** *begin* [*end*]] |
source [**ip** *ip_address* [*wildcard_mask*]] [**port** *begin* [*end*]] [**destination ip** *ip_address* [*wildcard_mask*] [**port** *begin* [*end*]] [**protocol** {**epm-uuid** *uuid* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**}]}

no match tcp {**any** |
destination [**ip** *ip_address* [*wildcard_mask*]] [**port** *begin* [*end*]] [**source ip** *ip_address* [*wildcard_mask*] [**port** *begin* [*end*]] |
source [**ip** *ip_address* [*wildcard_mask*]] [**port** *begin* [*end*]] [**destination ip** *ip_address* [*wildcard_mask*] [**port** *begin* [*end*]] [**protocol** {**epm-uuid** *uuid* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**}]}

Syntax Description

any	Matches any TCP packets.
destination	Specifies the destination criteria for matching TCP packets.
ip *ip_address*	Specifies the IP address of the system that is the source or destination of the traffic.
wildcard_mask	A wildcard subnet mask, which matches a range of IP addresses. Use dotted decimal notation (such as 0.0.0.255 for /24).
port *begin* [*end*]	Specifies the criteria for identifying the port or ports used by the source or destination host. Specify a single port or a begin and end port for a range.
source	Specifies the source criteria for matching TCP packets.
protocol	Specifies the criteria for matching TCP packets based on layer 7 protocol.
epm-uuid *uuid*	Specifies a custom EndPoint Mapper (EPM) service by its Universal Unique ID (UUID). Available only for WAAS optimization class maps.
 mapi **ms-ad-rep** **ms-exch-nspi** **ms-frs** **ms-frs-api** **ms-rfr** **ms-sql** **msn-messenger** **netlogon**	Microsoft RPC application keywords: Microsoft Exchange MAPI (Exchange Server Store EMSMDB), Microsoft Active Directory Replication (drsuapi), Microsoft Active Directory Name Service Provider (NSP), Microsoft File Replication Services (FRS), Microsoft File Replication API, Microsoft Exchange Directory RFR interface, Microsoft SQL, Microsoft Messenger Service, Netlogon RPC

Defaults

No default behavior or values.

Command Modes

Class map configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a TCP match condition for a class map:

```
wae(config)# class-map type appnav myclass2
wae(config-cmap)# match tcp source port 4000 4004 destination ip 10.10.20.50
```

Related Commands

(config-cmap) description

(config-cmap) match protocol

Policy Map Configuration Mode Commands

To configure an optimization policy map, use the **policy-map** global configuration command. To unconfigure settings, use the **no** form of this command.

policy-map type { **waas**} *policymap-name* [**rename** *new-name*]

no policy-map type {**waas**} *policymap-name*

Syntax Description

waas	Configures a WAAS optimization policy map.
policymap-name	Policy map name (up to 40 alpha-numeric characters and hyphen, beginning with a letter).
rename *new-name*	(Optional) Renames the policy map with the specified new name.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **policy-map** command to add or modify policy maps that associate policy actions with class maps. This command invokes the Policy Map configuration mode, which is indicated by a different prompt **(**config-pmap**)**. To return to global configuration mode, enter the **exit** command.

You can delete a policy map by using the **no** form of this command.

The WAAS software comes with many class maps and policy rules that help your WAAS system classify and optimize some of the most common traffic on your network. Before you create a new class map or policy rule, we recommend that you review the default class map and policy rules and modify them as appropriate. It is usually easier to modify an existing class map or policy rule than to create a new one. For a list of the default applications, class maps, and policy rules, see the *Cisco Wide Area Application Services Configuration Guide*.

Note We strongly recommend that you use the WAAS Central Manager GUI to centrally configure policy maps for your WAAS devices. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to configure a WAAS optimization policy map:

```
wae(config)# policy-map type waas myPolicy
wae(config-pmap)# description My optimization policy
wae(config-pmap)# class httpx
wae(config-pmap-c)# optimize full accelerate http application Web
```

Related Commands

(config-pmap) class

(config-pmap) description

(config-pmap) class

To configure the service policy for a class map, use the **class** policy map configuration command. To unconfigure the service policy, use the **no** form of this command.

class *classmap-name* [**insert-before** [*existing_class*]]

no class *classmap-name* [**insert-before** [*existing_class*]]

Syntax Description

classmap-name	Class map name (up to 40 alpha-numeric characters and hyphen, beginning with a letter).
insert-before *existing_class*	Inserts a new class, or moves an existing class, before the specified class. If you do not specify an existing class name, the class is moved to the last position in the policy map.

Defaults

No default behavior or values.

Command Modes

Policy map configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **class** command to add or modify a service policy (policy rule) for traffic identified by a class map. This command invokes the Policy Map Class configuration mode, which is indicated by a different prompt **(**config-pmap-c**)**. For more information on Policy Class Map configuration mode commands, see the "Policy Map Class Configuration Mode Commands" section. To return to global configuration mode, enter the **exit** command.

You can delete a policy rule by using the **no** form of this command.

Examples

The following example shows how to configure a policy rule in an optimization policy map:

```
wae(config)# policy-map waas WAAS-GLOBAL
wae(config-pmap)# class httpx
wae(config-pmap-c)# optimize full accelerate http application Web
```

Related Commands

(config-pmap) description

(config-pmap) description

To configure the policy map description, use the **description** policy map configuration command. To unconfigure the description, use the **no** form of this command.

description *description*

no description *description*

Syntax Description

description	Specifies a description of the policy map with up to 200 alphanumeric and space characters.

Defaults

No default behavior or values.

Command Modes

Policy map configuration

Device Modes

application-accelerator

Examples

The following example shows how to configure a policy map description:

```
wae(config)# policy-map type waas myPolicy
wae(config-pmap)# description My optimization policy
```

Related Commands

(config-pmap) class

Policy Map Class Configuration Mode Commands

To configure a service policy in an optimization policy map, use the **class** policy map configuration command. To unconfigure settings, use the **no** form of this command.

class *classmap-name* [**insert-before** [*existing_class*]]

no class *classmap-name* [**insert-before** [*existing_class*]]

Syntax Description

classmap-name	Class map name (up to 40 alpha-numeric characters and hyphen, beginning with a letter).
insert-before *existing_class*	Inserts a new class, or moves an existing class, before the specified class. If you do not specify an existing class name, the class is moved to the last position in the policy map.

Defaults

No default behavior or values.

Command Modes

Policy map configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **class** command to add or modify a service policy (policy rule) for traffic identified by a class map. This command invokes the Policy Map Class configuration mode, which is indicated by a different prompt **(**config-pmap-c**)**. To return to global configuration mode, enter the **exit** command.

You can delete a policy rule by using the **no** form of this command.

The WAAS software comes with many class maps and policy rules that help your WAAS system classify and optimize some of the most common traffic on your network. Before you create a new class map or policy rule, we recommend that you review the default class map and policy rules and modify them as appropriate. It is usually easier to modify an existing class map or policy rule than to create a new one. For a list of the default applications, class maps, and policy rules, see the *Cisco Wide Area Application Services Configuration Guide*.

Note We strongly recommend that you use the WAAS Central Manager GUI to centrally configure policy maps for your WAAS devices. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to configure a policy rule in an optimization policy map:

```
wae(config)# policy-map waas WAAS-GLOBAL
wae(config-pmap)# class httpx
wae(config-pmap-c)# optimize full accelerate http application Web
```

Related Commands

(config-pmap-c) optimize

(config-pmap-c) optimize

(config-pmap-c) optimize

(config-pmap-c) pass-through

(config-pmap-c) set ip dscp

(config-pmap-c) set ip dscp

(config-pmap-c) optimize

To configure optimization actions in a WAAS optimization policy, use the **optimize** policy class map configuration command. To unconfigure optimization actions, use the **no** form of this command.

optimize {**tfo-only** | {[**DRE** {**bidirectional** | **adaptive** | **unidirectional**}] [**LZ**] | **full**} [**accelerate** {**cifs** | **http** | **ica** | **mapi** | **MS-port-mapper** | **ssl** | **video**}] [**application** *app-name*]

no optimize {**tfo-only** | {[**DRE** {**bidirectional** | **adaptive** | **unidirectional**}] [**LZ**] | **full**} [**accelerate** {**cifs** | **http** | **ica** | **mapi** | **MS-port-mapper** | **ssl** | **video**}] [**application** *app-name*]

Syntax Description

tfo-only	Optimize with transport flow optimizations (TFO) and not data redundancy elimination (DRE) or Lempel-Ziv (LZ) compression.
DRE	Optimize with DRE of the specified type.
bidirectional	Optimize with bidirectional caching DRE.
adaptive	Optimize with adaptive caching DRE.
unidirectional	Optimize with unidirectional caching DRE.
LZ	Apply LZ compression.
full	Apply full Layer 4 optimization; this keyword is equivalent to **DRE bidirectional LZ**.
accelerate {**cifs** | **http** | **ica** | **mapi** | **MS-port-mapper** | **ssl** | **video**}	Accelerate the traffic using the specified application accelerator, as follows: • **cifs**—CIFS or SMB accelerator • **http**—HTTP accelerator • **ica**—ICA accelerator • **mapi**—MAPI accelerator • **MS-port-mapper**—EPM accelerator • **ssl**—SSL accelerator • **video**—Video accelerator
application *app-name*	Assign the specified application identifier to connections matching the class for statistics collection.

Defaults

No default behavior or values.

Command Modes

Policy map class configuration

Device Modes

application-accelerator

Usage Guidelines

This command configures the optimization actions in a WAAS optimization policy.

You may specify only a single **optimize** or **pass-through** action for a particular class. If one of these actions is already present and you specify a new action, the new action replaces the existing action. If neither of these actions is specified, the default is **pass-through**.

The following DRE caching modes are supported:

- Bidirectional—The peer WAEs maintain identical caches for inbound and outbound traffic. This caching mode is best suited where a significant portion of the traffic seen in one direction between the peers is also seen in the reverse direction.
- Unidirectional—The peer WAEs maintain different caches for inbound and outbound traffic. This caching mode is best suited where a significant portion of the traffic seen in one direction between the peers is not seen in the reverse direction.
- Adaptive—The peer WAEs negotiate either bidirectional or unidirectional caching based on the characteristics of the traffic seen between the peers.

Examples

The following example shows how to configure the optimization action in a policy:

```
wae(config)# policy-map waas WAAS-GLOBAL
wae(config-pmap)# class httpx
wae(config-pmap-c)# optimize full accelerate http application Web
```

Related Commands

(config-pmap-c) pass-through

(config-pmap-c) set ip dscp

(config-pmap-c) pass-through

To configure the pass-through action in an optimization policy rule, use the **pass-through** policy class map configuration command. To unconfigure the pass-through action, use the **no** form of this command.

pass-through [**application** *app-name*]

no pass-through [**application** *app-name*]

Syntax Description

application *app-name*	(Optional) Assign the specified application identifier to connections matching the class for statistics collection. Available only for WAAS optimization class maps.

Defaults

No default behavior or values.

Command Modes

Policy map class configuration

Device Modes

application-accelerator

Usage Guidelines

In an optimization policy, this command prevents the traffic in the class from being optimized and instead the traffic is passed through unoptimized. You can optionally specify an application name with which to associate the traffic in the class for statistics collection purposes.

You may specify only a single **optimize** or **pass-through** action for a particular class. If one of these actions is already present and you specify a new action, the new action replaces the existing action. If neither of these actions is specified, the default is **pass-through**.

In an AppNav policy rule, this command prevents the traffic in the class from being distributed to WAAS nodes and instead the traffic is passed through unoptimized.

This command is useful in a nested policy to override a distribute action specified in the parent policy.

If you specify the pass-through action in a policy, any distribute or monitor-load actions are removed.

Examples

The following example shows how to configure the pass-through action in an optimization policy:

```
wae(config)# policy-map waas WAAS-GLOBAL
wae(config-pmap)# class httpx
wae(config-pmap-c)# pass-through
```

Related Commands

(config-pmap-c) optimize

(config-pmap-c) optimize

(config-pmap-c) optimize

(config-pmap-c) set ip dscp

(config-pmap-c) set ip dscp

(config-pmap-c) set ip dscp

To configure the DSCP marking in a WAAS optimization policy, use the **set ip dscp** policy class map configuration command. To unconfigure DSCP marking, use the **no** form of this command.

set ip dscp *dscp-marking*

no set ip dscp *dscp-marking*

Syntax Description

dscp-marking	Assign the specified DSCP marking value (Table 3-2) to the connections in the class.

Defaults

The default DSCP marking value is copy.

Command Modes

Policy map class configuration

Device Modes

application-accelerator

Usage Guidelines

This command overrides the global default DSCP marking value, which is set to copy by default.

If you do not specify the **set ip dscp** command, the class uses the global default DSCP marking, which is set by the **service-policy type waas set ip dscp** command.

You can specify the **set ip dscp** command only when the **optimize** action has been configured for a class.

Examples

The following example shows how to configure the DSCP marking value for connections in the class:

```
wae(config)# policy-map waas WAAS-GLOBAL
wae(config-pmap)# class httpx
wae(config-pmap-c)# optimize full accelerate http application Web
wae(config-pmap-c)# set ip dscp 10
```

Related Commands

(config-pmap-c) optimize

(config-pmap-c) pass-through

(config) service-policy

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
CLI	command-line interface
CM	Central Manager
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
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
TDB	Trivial DataBase

Table A-1 List of Acronyms and Abbreviations (continued)

Acronym	Expansion
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
WAFS	Wide Area File 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 3-532

(config) aaa authorization commands 3-535

(config) accelerator epm 3-536

(config) accelerator http 3-537, 3-548, 3-550, 3-552, 3-553

(config)accelerator http preposition proxy server 3-554

(config) accelerator ica 3-555

(config) accelerator mapi 3-557

(config) accelerator object-cache enable 3-560

(config) accelerator smb 3-562

(config) accelerator smb preposition 3-566

(config) accelerator smb preposition dre 3-568

(config) accelerator ssl 3-569

(config) alarm overload-detect 3-571

(config) asset 3-573

(config) authentication configuration 3-574

(config) authentication content-request 3-580

(config) authentication enable 3-579

(config) authentication fail-over 3-584

(config) authentication login 3-586

(config) auto-discovery 3-593

(config) auto-register 3-595

(config) banner 3-597

(config) cdp 3-599

(config) central-manager 3-600

(config) clock 3-602

(config) cms 3-606

(config) crypto encryption-service 3-609

(config) crypto pki 3-610

(config) crypto ssl 3-612

(config) device mode 3-614

(config) disk cache 3-617

(config) disk disk-name 3-616

(config) disk encrypt 3-619

(config) disk error-handling 3-620

(config) disk logical shutdown 3-621

(config) disk object-cache extend 3-622

(config) dre 3-623

(config) end 3-624

(config) exec-timeout 3-625

(config) exit 3-626

(config) flow exporter 3-627

(config) flow monitor 3-630

(config) flow record 3-629

(config) help 3-631

(config) hostname 3-633

(config) inetd 3-635

(config) inline vlan-id-connection-check 3-636

(config) interception 3-637

(config) interception-method 3-639

(config) interface GigabitEthernet 3-641

(config) interface InlineGroup 3-646

(config) interface PortChannel 3-649

(config) interface standby 3-652

(config) interface TenGigabitEthernet 3-654

(config) interface virtual 3-658

(config) ip 3-661

(config) ip access-list 3-664

(config)ip icmp rate-limit unreachable 3-667

(config)ip unreachables df 3-669

(config) ipv6 3-670

(config) kerberos 3-672

(config) kernel kdb 3-674

(config) kernel kdump 3-676

(config) line 3-677

(config) logging console 3-678

(config) logging disk 3-680

(config) logging facility 3-682

(config) logging host 3-684

(config) ntp 3-686

(config) object-cache enable 3-688

(config) peer 3-689

(config) policy-map 3-690

(config) port-channel 3-692

(config) primary-interface 3-693

(config) radius-server 3-695

(config) service-policy 3-697

(config) smb-conf 3-699

(config) snmp-server access-list 3-702

(config) snmp-server community 3-703

(config) snmp-server contact 3-705

(config) snmp-server enable traps 3-706

(config) snmp-server group 3-709

(config) snmp-server host 3-711

(config) snmp-server location 3-713

(config) snmp-server mib 3-714

(config) snmp-server notify inform 3-717

(config) snmp-server trap-source 3-718

(config) snmp-server user 3-723

(config) snmp-server view 3-725

(config) sshd 3-726

(config) ssh-key-generate 3-728

(config) stats-collector logging 3-729

(config) system jumbomtu 3-730

(config) tacacs 3-731

(config) tcp 3-734

(config) telnet enable 3-736

(config) tfo exception 3-737

(config) tfo optimize 3-738

(config) tfo tcp adaptive-buffer-sizing 3-739

(config) tfo tcp keepalive 3-740

(config) tfo tcp optimized-mss 3-741

(config) tfo tcp optimized-receive-buffer 3-742

(config) tfo tcp optimized-send-buffer 3-743

(config) tfo tcp original-mss 3-744

(config) tfo tcp original-receive-buffer 3-745

(config) tfo tcp original-send-buffer 3-746

(config) threshold-monitor 3-747

(config) username 3-749

(config) wccp access-list 3-751

(config) wccp router-list 3-753

(config) wccp shutdown 3-755

(config) wccp tcp-promiscuous service-pair 3-757

(config) windows-domain 3-759

snmp-server trigger 3-720

snmp-server user 3-716

EXEC Mode Commands

authentication strict-password-policy 3-591

cd 3-4

clear arp-cache 3-5

clear bmc 3-6

clear cache 3-7

clear cdp 3-10

clear connection 3-11

clear dre 3-12

clear ip 3-13

clear ipv6 3-14

clear license 3-15

clear logging 3-16

clear object-cache 3-17

clear service-policy 3-19

clear statistics 3-20

clear statistics accelerator 3-22

clear statistics connection 3-24

clear statistics object-cache 3-26

clear transaction-log 3-27

clear users 3-28

clear windows-domain 3-30

clear windows-domain-log 3-31

clock 3-32

cms 3-33

cms secure-store 3-36

configure 3-39

copy cdrom 3-40

copy compactflash 3-41

copy disk 3-42

copy ftp 3-43

copy http 3-45

copy monitoring-log 3-47

copy running-config 3-48

copy scp 3-49

copy startup-config 3-51

copy sysreport 3-52

copy system-status 3-55

copy tech-support 3-56

copy tftp 3-58

cpfile 3-59

crypto delete 3-60

crypto export 3-61

crypto generate 3-63

crypto import 3-65

crypto pki 3-67, 3-79, 3-80, 3-81, 3-136, 3-137, 3-138, 3-139, 3-140

debug aaa accounting 3-68, 3-530

debug accelerator 3-72

debug accelerator mapi rpchttp-layer 3-78

debug all 3-82

debug authentication 3-84

debug auto-discovery 3-86

debug buf 3-88

debug cdp 3-90

debug cli 3-92

debug cmm 3-94

debug cms 3-96

debug connection 3-98

debug dataserver 3-100

debug dhcp 3-102

debug dre 3-104

debug egress-method 3-106

debug encryption-service 3-108

debug fda 3-110

debug fdm 3-112

debug filtering 3-114

debug flow 3-116

debug generic-gre 3-118

debug hw-raid 3-120

debug imd 3-122

debug inline 3-124

debug logging 3-128

debug monapi 3-126, 3-130

debug nplogd 3-132

debug ntp 3-134

debug rbcp 3-141

debug rmd 3-143

debug rpc 3-145

debug service-insertion 3-147

debug service-policy 3-149

debug snmp 3-151

debug standby 3-153

debug statistics 3-155

debug tfo 3-157

debug translog 3-159

debug wafs 3-161

debug wccp 3-163

delfile 3-165

deltree 3-166

dir 3-167

disable 3-169

disk 3-170

dnslookup 3-173

enable 3-174

exit 3-175

find-pattern 3-176

help 3-178

install 3-179

less 3-181

license add 3-182

lls 3-183
ls 3-184
lsusb 3-186
mkdir 3-187
mkfile 3-188
ntpdate 3-189
packet-capture 3-190
ping 3-192
ping6 3-193
pwd 3-195
reload 3-196
rename 3-197
restore 3-198
rmdir 3-202
scp 3-203
script 3-205
setup 3-206
show aaa accounting 3-207
show aaa authorization 3-209
show accelerator 3-210
show alarms 3-215
show arp 3-218
show authentication 3-220
show auto-discovery 3-222
show auto-register 3-223
show banner 3-224
show bmc 3-225
show cache http-metadatacache 3-227
show cache object-cache 3-229
show cdp 3-231
show class-map 3-237
show clock 3-238
show cms 3-240
show cms secure-store 3-243
show crypto 3-245
show debugging 3-247
show device-id 3-248
show device-mode 3-249
show disks 3-251
show dre 3-259
show filtering list 3-260
show flash 3-262
show flow record 3-263
show hardware 3-264
show hosts 3-267
show inetd 3-268
show interception-method 3-269
show interface 3-270
show inventory 3-274
show ip access-list 3-275
show ip routes 3-277
show ipv6 3-278
show kdump 3-280
show kerberos 3-281
show key-manager 3-282
show license 3-283
show logging 3-284
show memory 3-285
show ntp 3-286
show object-cache 3-288
show peer optimization 3-289
show policy-map 3-290
show processes 3-291
show radius-server 3-293
show reload 3-295
show running-config 3-296
show service-insertion 3-298
show service-policy 3-304
show services 3-307
show smb-conf 3-308
show snmp 3-310
show ssh 3-316
show startup-config 3-317
show statistics accelerator 3-319
show statistics aoim 3-374
show statistics application 3-378
show statistics authentication 3-381
show statistics auto-discovery 3-382

show statistics class-default 3-385

show statistics class-map 3-386

show statistics connection 3-387

show statistics connection auto-discovery 3-391

show statistics connection closed 3-393

show statistics connection conn-id 3-395

show statistics connection egress-methods 3-398

show statistics connection optimized 3-402

show statistics connection pass-through 3-405

show statistics crypto ssl ciphers 3-407

show statistics datamover 3-408

show statistics dre 3-410

show statistics encryption-services 3-414

show statistics filtering 3-420

show statistics flow 3-423

show statistics generic-gre 3-426

show statistics icmp 3-427

show statistics icmp6 3-429

show statistics ip 3-432

show statistics ipv6 3-435

show statistics netstat 3-438

show statistics pass-through 3-441

show statistics peer 3-443

show statistics radius 3-446

show statistics service-insertion 3-448

show statistics services 3-449

show statistics sessions 3-450

show statistics snmp 3-451

show statistics system cpu 3-453

show statistics tacacs 3-455

show statistics tcp 3-457

show statistics tfo 3-461

show statistics udp 3-465

show statistics wccp 3-466

show statistics windows-domain 3-471

show sysfs volumes 3-473

show tacacs 3-474

show tcp 3-476

show tech-support 3-478

show telnet 3-481

show tfo tcp 3-482

show transaction-logging 3-484

show user 3-485

show users administrative 3-486

show version 3-488

show wccp 3-489

show windows-domain 3-496, 3-498

shutdown 3-499

ssh 3-502

tcpdump 3-504

telnet 3-506

terminal 3-507

test 3-508

tethereal 3-509

top 3-512

traceroute 3-514

traceroute6 3-516

transaction-log 3-517

type 3-518

type-tail 3-519

vm 3-521

waas-tcptrace 3-523

whoami 3-525

windows-domain 3-526

write 3-529

Extended ACL Configuration Mode Commands

(config-ext-nacl) delete 3-800

(config-ext-nacl) deny 3-801

(config-ext-nacl) exit 3-806

(config-ext-nacl) list 3-807

(config-ext-nacl) move 3-808

(config-ext-nacl) permit 3-809

Interface Configuration Mode Commands

(config-if) autosense 3-764

(config-if) bandwidth 3-765

(config-if) cdp 3-767

(config-if) channel-group 3-768

(config-if) description 3-769

(config-if) encapsulation dot1Q 3-770

(config-if) exit 3-771

(config-if) full-duplex 3-772

(config-if) half-duplex 3-774

(config-if) inline 3-776

(config-if) ip 3-778

(config-if) ip access-group 3-780

(config-if) load-interval 3-781

(config-if) mtu 3-782

(config-if) shutdown 3-783

(config-if) standby 3-784

PKI Certificate Authority Configuration Mode Commands

(config-ca) ca-certificate 3-841

(config-ca) description 3-842

(config-ca) revocation-check 3-843

PKI Global Settings Configuration Mode Commands

(config-pki-global-settings) ocsp 3-846

(config-pki-global-settings) revocation-check 3-847

Policy Map Class Configuration Mode Commands

(config-pmap-c) optimize 3-927

(config-pmap-c) pass-through 3-929

(config-pmap-c) set ip dscp 3-931

Policy Map Configuration Mode Commands

(config-pmap) class 3-923

(config-pmap) description 3-924

Preposition Configuration Mode Commands

(config-preposition) credentials 3-820

(config-preposition) dscp 3-821

(config-preposition) duration 3-822

(config-preposition) enable 3-823

(config-preposition) ignore-hidden-dir 3-824

(config-preposition) max-cache 3-825

(config-preposition) max-file-size 3-826

(config-preposition) min-file-size 3-827

(config-preposition) name 3-828

(config-preposition) recursive 3-830

(config-preposition) root 3-831

(config-preposition) scan-type 3-829, 3-832

(config-preposition) schedule 3-833

(config-preposition) server 3-835

(config-preposition) user-agent 3-837

(config-preposition) user-proxy 3-836

Service Node Configuration Mode Commands

(config-sn) authentication 3-905

(config-sn) description 3-906

(config-sn) enable 3-907

(config-sn) node-discovery 3-908

(config-sn) shutdown 3-910

SSL Accelerated Service Configuration Mode Commands

(config-ssl-accelerated) cipher-list 3-851

(config-ssl-accelerated) client-cert-key 3-852

(config-ssl-accelerated) client-cert-verify 3-853

(config-ssl-accelerated) client-version-rollback-check 3-854
(config-ssl-accelerated) description 3-855
(config-ssl-accelerated) inservice 3-856
(config-ssl-accelerated) server-cert-key 3-858
(config-ssl-accelerated) server-cert-verify 3-859
(config-ssl-accelerated) server-domain 3-860
(config-ssl-accelerated) server-ip 3-861
(config-ssl-accelerated) server-name 3-862
(config-ssl-accelerated) version 3-863

SSL Cipher List Configuration Mode Commands

(config-cipher-list) cipher 3-866

SSL Global Service Configuration Mode Commands

(config-ssl-global) cipher-list 3-871
(config-ssl-global) machine-cert-key 3-872
(config-ssl-global) version 3-873

SSL Host Peering Service Configuration Mode Commands

(config-ssl-peering) cipher-list 3-877
(config-ssl-peering) peer-cert-verify 3-878
(config-ssl-peering) version 3-879

SSL Management Service Configuration Mode Commands

(config-ssl-mgmt) cipher-list 3-883
(config-ssl-mgmt) peer-cert-verify 3-884
(config-ssl-mgmt) version 3-885

Standard ACL Configuration Mode Commands

(config-std-nacl) delete 3-789
(config-std-nacl) deny 3-790
(config-std-nacl) exit 3-792
(config-std-nacl) list 3-793
(config-std-nacl) move 3-794
(config-std-nacl) permit 3-795

WCCP Configuration Mode Commands

(config-wccp-service) assignment-method 3-889
(config-wccp-service) egress-method 3-891
(config-wccp-service) enable 3-893
(config-wccp-service) exit 3-894
(config-wccp-service) failure-detection 3-895
(config-wccp-service) password 3-896
(config-wccp-service) redirect-method 3-897
(config-wccp-service) router-list-num 3-899
(config-wccp-service) weight 3-900