Exec Mode Commands

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

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

The user EXEC mode is used by local and general system administrators, while the privileged EXEC mode is used by the root administrator. Use the **enable** and **disable** commands to switch between the two levels. Access to the user-level EXEC command line requires a valid password.

The user-level EXEC commands are a subset of the privileged-level EXEC commands. The user-level EXEC prompt is the hostname followed by a right angle bracket (>). The prompt for the privileged-level EXEC command line is the pound sign (#). To execute an EXEC command, enter the command at the EXEC system prompt and press the **Return** key.

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

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

```
WAE> enable
WAE#
```

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

```
WAE# exit
WAE>
```

cd

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

cd *directoryname*

Syntax Description

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

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

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

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

clear logging

clear statistics {**all** | **authentication** | **history** | **icmp** | **ip** | **radius** | **running** | **tacacs** | **tcp** | **udp** | **windows-domain**}

clear users administrative

clear windows-domain-log

Syntax Description

cdp	Resets the Cisco Discovery Protocol (CDP) statistical data.
counters	Clears the CDP counters.
table	Clears the CDP tables.
ip access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
acl-name	(Optional) Clears the counters for the specified access list, identified using an alphanumeric identifier of up to 30 characters, beginning with a letter.
acl-num	(Optional) Clears the counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
logging	Clears the syslog messages saved in the disk file.
statistics	Clears the statistics as specified.
all	Clears all statistics.
authentication	Clears the authentication statistics.
history	Clears the statistics history.
icmp	Clears the ICMP statistics.
ip	Clears the IP statistics.
radius	Clears the RADIUS statistics.
running	Clears the running statistics.
tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
udp	Clears the UDP statistics.
windows-domain	Clears the Windows domain statistics.
users	Clears the connections (login) of authenticated users.
administrative	Clears the connections of administrative users authenticated through a remote login service.
windows-domain-log	Clears the Samba, Kerberos, and Winbind log files.

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, as shown in the following example.

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

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

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

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

Examples

In the following example, all entries in the *syslog.txt* file are cleared on the WAAS device:

```
WAE# clear logging
```

In the following example, all authentication, RADIUS and TACACS+ information is cleared on the WAAS device:

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

In the following example, all entries in the Windows domain log file are cleared on the WAAS device:

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

Related Commands

show interface

show wccp

clock

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

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

Syntax Description

read-calendar	Reads the calendar and updates the system clock.
set	Sets the time and date.
time	Current time in hh:mm:ss format (hh: 00–23; mm: 00–59; ss: 00–59).
day	Day of the month (1–31).
month	Month of the year (January, February, March, April, May, June, July, August, September, October, November, December).
year	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 sets the software clock on the WAAS device:

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

Related Commands

show clock

cms

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Use the **cms config-sync** command to enable registered WAAS devices and standby WAAS Central Manager to contact the primary WAAS Central Manager immediately for a getUpdate (get configuration poll) request before the default polling interval of 5 minutes. For example, when a node is registered with the primary WAAS Central Manager and activated, it appears as Pending in the WAAS Central Manager GUI until it sends a getUpdate request. The **cms config-sync** command causes the registered node to send a getUpdate request at once, and the status of the node changes as Online.

Use the **cms database create** command to initialize the CMS database. Before a node can join a WAAS network, it must first be registered and then activated. The **cms enable** global configuration command automatically registers the node in the database management tables and enables the CMS. The node sends its attribute information to the WAAS Central Manager over the SSL protocol and then stores the new node information. The WAAS Central Manager accepts these node registration requests without admission control and replies with registration confirmation and other pertinent security information required for getting updates. Activate the node using the WAAS Central Manager GUI.

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

To back up the existing management database for the WAAS Central Manager, use the **cms database backup** command. For database backups, specify the following items:

- Location, password, and user ID
- Dump format in PostgreSQL plain text syntax

The naming convention for backup files includes the time stamp.

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

When you use the **cms recover identity** *word* command when recovering lost registration information, or replacing a failed node with a new node that has having the same registration information, you must specify the device recovery key that you configured in the Modifying Config Property, System.device.recovery.key window of the WAAS Central Manager GUI.

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

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

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

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

Examples

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

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

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

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

Related Commands

(config) cms

show cms

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

Usage Guidelines

Use this command to enter global configuration mode.

Examples

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

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

Related Commands

(config) end

(config) exit

show running-config

show startup-config

copy cdrom

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

copy cdrom install *filedir filename*

Syntax Description

cdrom	Copies a file from the CD-ROM.
install	Installs the software release file.
filedir	Directory location of the software release file.
filename	Filename of the software release file.

Defaults

No default behaviors or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy compactflash

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

copy compactflash install *filename*

Syntax Description

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

Defaults

No default behaviors or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy disk

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

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

Syntax Description

disk	Copies a local disk file.
ftp	Copies to a file on an FTP server.
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	Copies the configuration file from the disk to startup configuration (NVRAM).
filename	Name of the existing configuration file.

Defaults

No default behaviors or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **copy disk ftp** EXEC command copies files from a SYSFS partition to an FTP server. The **copy disk startup-config** EXEC command copies a startup configuration file to NVRAM.

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy ftp

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

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

Syntax Description

ftp	Copies a file from an FTP server.
central	Copies a file to the software upgrade image repository.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server where the image file to be copied is located.
remotefilename	Name of the file to be copied to the image repository.
slotnumber	Slot location (1–5) into which the upgrade image is to be copied.
username	(Optional) Specifies FTP authentication.
username	(Optional) Clear text of the username.
password	(Optional) Password for FTP authentication.
proxy	(Optional) Specifies proxy address.
hostname	(Optional) Hostname of the proxy server.
ip-address	(Optional) IP address of the proxy server.
proxy_portnum	(Optional) Port number on the proxy server.
username	(Optional) Specifies the proxy server authentication username.
username	(Optional) Clear text of the username.
password	(Optional) Password for proxy server authentication.
port	(Optional) Specifies port at which to connect to the FTP server.
port-num	(Optional) Port number on the FTP server.
md5	(Optional) Specifies MD5 signature of the file being copied.
md5sum	(Optional) MD5 signature.
disk	Copies a file to a local disk.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server where the file to be copied is located.
remotefilename	(Optional) Name of the file to be copied to the local disk.
localfilename	(Optional) Name of the copied file as it appears on the local disk.
install	(Optional) Copies the file from an FTP server and installs the software release file to the local device.
hostname	(Optional) Name of the FTP server.
ip-address	(Optional) IP 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 The **copy ftp disk** EXEC command copies a file from an FTP server to a SYSFS partition on the WAAS device.

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

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

Upgrading the BIOS

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

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

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

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

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

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

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

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

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

```
WAE# reload
```

The new BIOS takes effect after the system reboots.

Examples

The following example copies an image file from an FTP server and installs the file on the local device:

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

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

```
WAE-7326# copy ftp install upgradeserver /bios/update53/derived/ 7326_bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER myusername
upgradeserver.cisco.com FTP server (Version wu-2.6.1-18) ready.
```

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

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy http

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

copy http {**central** {*hostname* | *ip-address*} *remotefiledir remotefilename slotnumber* [**username** *username password* | **proxy** {*hostname* | *ip-address*} *proxy_portnum* [**username** *username password*] | **port** *port-num* | **md5** *md5sum*] | **install** {{*hostname* | *ip-address*} *remotefiledir remotefilename*}[**port** *port-num* [**proxy** {*hostname* | *ip-address*} | **username** *username password* [**proxy** {*hostname* | *ip-address*} *proxy_portnum*]] | **proxy** {*hostname* | *ip-address*} *proxy_portnum* | **username** *username password* [**proxy** {*hostname* | *ip-address*} *proxy_portnum*]]}

Syntax Description

http	Copies the file from an HTTP server.
central	Copies a file to the software upgrade image repository.
hostname	Hostname of the HTTP server.
ip-address	IP address of the HTTP server.
remotefiledir	Directory on the HTTP server where the image file to be copied is located.
remotefilename	Name of the file to be copied to the image repository.
slotnumber	Slot location (1–5) into which the upgrade image is to be copied.
username	(Optional) Specifies HTTP authentication.
username	(Optional) Clear text of the username.
password	(Optional) Password for HTTP authentication.
proxy	(Optional) Specifies proxy address.
hostname	(Optional) Hostname of the proxy server.
ip-address	(Optional) IP address of the proxy server.
proxy_portnum	(Optional) Port number on the proxy server.
username	(Optional) Specifies the proxy server authentication username.
username	(Optional) Clear text of the username.
password	(Optional) Password for proxy server authentication.
port	(Optional) Specifies port at which to connect to the HTTP server.
port-num	(Optional) Port number on the HTTP server.
md5	(Optional) Specifies MD5 signature of the file being copied.
md5sum	(Optional) MD5 signature.
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 address of the HTTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
port	(Optional) Port to connect to the HTTP server (default is 80).
port-num	(Optional) HTTP server port number (1–65535).
proxy	(Optional) Allows the request to be redirected to an HTTP proxy server.

hostname	(Optional) Name of the HTTP server.
ip-address	(Optional) IP address of the HTTP server.
proxy_portnum	(Optional) HTTP proxy server port number (1–65535).
username	Username to access the HTTP proxy server.
username	User login name.
password	Establishes password authentication.

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 disk and part goes to flash memory. Use the **copy http central** EXEC command to download a software image into the repository from an HTTP server.

You can also use the **copy http install** EXEC commands to redirect your transfer to a different location or HTTP proxy server, by specifying the **proxy** *hostname* | *ip-address* option. A username and a password have to be authenticated with a primary domain controller (PDC) before the transfer of the software release file to the WAAS device is allowed.

Upgrading the BIOS

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

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

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

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

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

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

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

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

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

```
WAE# reload
```

The new BIOS takes effect after the system reboots.

Examples

The following example copies an image file from an HTTP server and installs 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 dependant files that are downloaded from Cisco.com for the BIOS upgrade are automatically deleted from the WAAS device after the BIOS upgrade procedure has been completed.

```
WAE-7326# copy ftp install upgradeserver /bios/update53/derived/ 7326_bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER myusername
upgradeserver.cisco.com FTP server (Version wu-2.6.1-18) ready.
Password required for myusername.
Sending:PASS ********
Please read the file README_dotfiles
 it was last modified on Wed Feb 19 16:10:26 2005- 94 days ago
Please read the file README_first
 it was last modified on Wed Feb 19 16:05:29 2005- 94 days ago
User myusername logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,240,57,37)
Sending:CWD /bios/update53/derived/
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,240,146,117)
Sending:RETR 7326_bios.bin
Opening BINARY mode data connection for 7326_bios.bin (834689 bytes).
Fri Jan  7 15:29:07 UTC 2005
BIOS installer running!
Do not turnoff the system till BIOS installation is complete.
Flash chipset:Macronix 29LV320B
0055000.FLS:280000 [80000]
Erasing block 2f:280000 - 28ffff
Erasing block 30:290000 - 29ffff
Erasing block 31:2a0000 - 2affff
Erasing block 32:2b0000 - 2bffff
Erasing block 33:2c0000 - 2cffff
Erasing block 34:2d0000 - 2dffff
Erasing block 35:2e0000 - 2effff
Erasing block 36:2f0000 - 2fffff
Programming block 2f:280000 - 28ffff
Programming block 30:290000 - 29ffff
Programming block 31:2a0000 - 2affff
Programming block 32:2b0000 - 2bffff
Programming block 33:2c0000 - 2cffff
Programming block 34:2d0000 - 2dffff
Programming block 35:2e0000 - 2effff
Programming block 36:2f0000 - 2fffff
SCSIROM.BIN:260000 [20000]
Erasing block 2d:260000 - 26ffff
Erasing block 2e:270000 - 27ffff
Programming block 2d:260000 - 26ffff
Programming block 2e:270000 - 27ffff
PXEROM.BIN:250000 [10000]
Erasing block 2c:250000 - 25ffff
Programming block 2c:250000 - 25ffff
```

```
Primary BIOS flashed successfully
Cleanup BIOS related files that were downloaded....
The new software will run after you reload.
```

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy running-config

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

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

Syntax Description

running-config	Copies the current system configuration.
disk	Copies the current system configuration to a disk file.
filename	Name of the file to be created on disk.
startup-config	Copies the running configuration to startup configuration (NVRAM).
tftp	Copies the running configuration to a file on a TFTP server.
hostname	Hostname of the TFTP server.
ip-address	IP 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 WAAS device's running system configuration to a SYSFS partition, flash memory, or TFTP server. The **copy running-config startup-config** EXEC command is equivalent to the **write memory** EXEC command.

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy startup-config

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

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

Syntax Description

startup-config	Copies the startup configuration.
disk	Copies the startup configuration to a disk file.
filename	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 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

The **copy startup-config** EXEC command copies the startup configuration file to a TFTP server or to a SYSFS partition.

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy sysreport

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

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

Syntax Description

sysreport	Generates and saves a report containing WAAS system information in a file.
disk	Copies system information to a disk file.
filename	Name of the file to be created on disk. Note that .tar.gz is appended to the filename that you specify.
ftp	Copies system information to a FTP server.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotedirectory	Remote directory where the system information file is to be created on the FTP server.
remotefilename	Remote filename of the system information file to be created on the FTP server.
tftp	Copies system information to a TFTP server.
hostname	Hostname of the TFTP server.
ip-address	IP address of the TFTP server.
remotefilename	Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.
start-date	Start date of 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	End date of information in the generated system report. If omitted, this date defaults to today's date. The report includes files through the end of this day.
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).

Defaults

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

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example copies system information to the file mysysinfo on the local WAAS device:

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

The following example copies system information by FTP to the file foo in the root directory of the FTP server named myserver:

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

Related Commands

show running-config

show startup-config

wafs

copy system-status

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

copy system-status disk *filename*

Syntax Description

system-status disk	Copies the system status to a disk file.
filename	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

The **copy system-status** EXEC command creates a file on a SYSFS partition containing hardware and software status information.

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy tech-support

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

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

Syntax Description

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

Defaults

No default behaviors or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **copy tech-support tftp** EXEC command can copy technical support information to a TFTP server or to a SYSFS partition.

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy tftp

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

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

Syntax Description

tftp	Copies an image from a TFTP server.
disk	Copies an image from a TFTP server to a disk file.
hostname	Hostname of the TFTP server.
ip-address	IP 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.
hostname	Hostname of the TFTP server.
ip-address	IP address of the TFTP server.
remotefilename	Name of the remote image file to be copied from the TFTP server. Use the complete pathname.
startup-config	Copies an image from a TFTP server to the startup configuration.
hostname	Hostname of the TFTP server.
ip-address	IP address of the TFTP server.
remotefilename	Name of the remote image file to be copied from the TFTP server. Use the complete pathname.

Defaults

No default behaviors or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **copy tftp disk** EXEC command copies a file from a TFTP server to disk.

Related Commands

- install
- reload
- show running-config
- show startup-config
- wafs
- write

cpfile

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

cpfile *oldfilename newfilename*

Syntax Description

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

Use this EXEC command to create a copy of a file. Only SYSFS files can be copied.

Examples

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

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

Related Commands

deltree

dir

lls

ls

mkdir

pwd

rename

debug

To monitor and record the WAAS application acceleration and the CIFS caching application functions, use the **debug** EXEC command. Use the **no** form of the command to disable debugging.

debug [*option*]

Note We recommend that you use the **debug** command only at the direction of Cisco TAC. (For more information, see the "Obtaining Technical Assistance" section on page xvii.) The performance of the WAAS device degrades when you use the **debug** command.

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Note The following **debug** command options are supported in the application-accelerator device mode only: **dre**, **epm**, **print-spooler**, **tfo**, **wafs**, and **wccp**.

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 Technical Assistance" section on page xvii.

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

Valid values for the *option* argument are as follows:

aaa accounting	Records AAA accounting actions.
all	Enables all debugging options.
authentication	Debugs authentication.
print-services	Debugs print services authentication.
user	Debugs the user login against the system authentication.

buf	Debugs the buffer manager.
all	Debugs all buffer manager functions.
dmbuf	Debugs the buffer manager dmbuf.
dmsg	Debugs the buffer manager dmsg.
cdp	Records CDP information and actions.
adjacency	Records the CDP neighbor.
events	Records the CDP events.
ip	Records CDP IP.
packets	Records the packet-related CDP.
cli	Debugs the CLI command.
all	Debugs all CLI commands.
bin	Debugs the CLI command binary program.
parser	Debugs the CLI command parser.
cms	Debugs the CMS.
dataserver	Debugs the data server.
all	Debuts all data server functions.
clientlib	Debugs the data server client library module.
server	Debugs the data server module.
dhcp	Debugs the DHCP.
dre	Enables DRE debugging.
aggregation	Enables DRE chunk-aggregation debugging.
all	Enables the debugging of all DRE commands.
cache	Enables DRE cache debugging.
connection	Enables DRE connection debugging.
aggregation *acl*	Enables DRE chunk-aggregation debugging for a specified connection.
cache *acl*	Enables DRE cache debugging for a specified connection.
core *acl*	Enables DRE core debugging for a specified connection.
message *acl*	Enables DRE message debugging for a specified connection.
misc *acl*	Enables DRE other debugging for a specified connection.
core	Enables DRE core debugging.
message	Enables DRE message debugging.
misc	Enables DRE other debugging.
emdb	Debugs the embedded database.
level *debug-level*	(Optional) Specifies the debug level (0 through 16).
logging	Debugs logging.
all	Debugs all logging functions.
ntp	Debugs NTP.

print-spooler	Debugs the print spooler feature.
all	(Optional) Debug the print spooler using all debug features.
brief	(Optional) Debug the print spooler using only brief debug messages.
errors	(Optional) Debug the print spooler using only the error conditions.
warnings	(Optional) Debug the print spooler using only the warning conditions.
rpc	Displays the remote procedure calls (RPC) logs.
detail	Displays the RPC logs of priority "detail" level or higher.
trace	Displays the RPC logs of priority "trace" level or higher.
stats	Debugs the statistics.
all	Debugs all statistics functions.
collection	Debugs the statistics collection.
computation	Debugs the statistics computation.
history	Debugs the statistics history.
tfo	Enables TFO debugging.
buffer-mgr	Enables TFO buffer manager debugging.
connection	Enables TFO connection debugging.
auto-discovery *acl*	Enables TFO connection debugging for the auto-discovery module.
comp-mgr *acl*	Enables TFO connection debugging for the compression module.
conn-mgr *acl*	Enables TFO connection debugging for the connection manager.
filtering *acl*	Enables TFO connection debugging for filtering module.
netio-engine *acl*	Enables TFO connection debugging for network input/output module.
policy-engine *acl*	Enables TFO connection debugging of application policies.
stat-mgr	Enables TFO statistics manager debugging.
translog	Enables TFO transaction log debugging.
wafs	Sets the notification level (debug, info, warn, error) at which messages from the WAAS software component and utilities are logged.
all	Sets the logging level for all software components and utilities at once.
core-fe	Sets the logging level for the WAE that is acting as a core file engine.
edge-fe	Sets the logging level for WAE that is acting as an edge file engine.
manager	Sets the logging level for the Device Manager.
utilities	Sets the logging level for WAAS utilities.

wccp	Debugs the WCCP information.
all	Debugs all WCCP functions.
detail	Debugs the WCCP details.
error	Debugs the WCCP errors.
events	Debugs the WCCP events.
keepalive	Debugs the WCCP keepalives that are sent to the applications.
packets	Debugs the WCCP packet-related information.
slowstart	Debugs the WCCP slow start.

Examples

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

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

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

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

Note If the watchdog utility is not running, the message "WAAS is not running" appears.

Related Commands

no debug

show debugging

undebug

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

Examples

The following example deletes a temporary file from the */local1* directory using an absolute path.

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

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

deltree

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

deltree *directory*

Syntax Description

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

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

Examples

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

Examples

The following example displays 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 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
```

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

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

```
WAE> enable
Password:
```

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

Examples

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

```
WAE# disable
WAE>
```

Related Commands

enable

disk

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

disk delete-partitions *diskname*

disk mark *diskname* {**bad** | **good**}

disk reformat *diskname*

disk scan-errors *diskname*

delete-partitions	Deletes data on the specified disk drive. After using this command, the WAAS software treats the specified disk drive as blank. All previous data on the drive is inaccessible.
diskname	Name of the disk from which to delete partitions (disk00, disk01).
mark	Marks a disk drive as good or bad.
diskname	Name of the disk to be marked (disk00, disk01).
bad	Marks the specified disk drive as bad. Using this command makes data on this disk inaccessible. If later this disk is marked good, WAAS software treats it as a blank drive.
good	Marks the specified disk drive as good.
reformat	Performs a low-level reformatting of a SCSI disk drive and remaps bad sectors. **Caution** Use this command with extreme caution to avoid loss of data.
diskname	Name of the disk to be reformatted (disk00, disk01).
scan-errors	Scans SCSI or IDE disks for errors and remaps the bad sectors, if they are unused.
diskname	Name of the disk to be scanned for errors (disk00, disk01).

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

A WAAS device can use two disk drives for either storage capacity increase or for increased reliability. This is known as Redundant Array of Independent Disks (RAID) and is implemented in WAAS as a software feature.

RAID-1 is automatically applied to any WAAS device that is running the WAAS software and that have two or more disk drives. RAID-1 provides disk mirroring (data is written redundantly to two or more drives). The goal is higher reliability through redundancy. With RAID-1, file system write performance may be affected because each disk write must be executed against two disk drives.

RAID-1 (mirroring) is used for all file systems on the device. This setup ensures reliable execution of the software in all cases.

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

Manually Marking and Unmarking WAE Disk Drives

A disk drive on a WAAS device can be marked as a good drive, one that is operating properly and being used, or as a bad drive, one that is not operating properly and will not be used after a **reload** command is executed.

The following scenario shows how to mark disk01 as bad, reload the WAAS device, and then mark disk01 as good so that it can be used again.

1. Mark disk01 as bad by entering the **disk mark** EXEC command as follows:

```
WAE# disk mark disk01 bad
disk01 is marked as bad.
It will be not used after reload.
```

2. Display the details about the disks by entering the **show disks details** EXEC command. Disk01 is now shown with an asterisk (*) because it was marked after the WAAS device was booted. Notice that Disk01 is reported as "Normal" (currently being used).

```
WAE# show disks details
Physical disk information:

  disk00: Normal                (h00 c00 i00 l00 - DAS)     76324MB( 74.5GB)
  disk01: Normal                (h01 c00 i00 l00 - DAS)     76324MB( 74.5GB) (*)

(*) Disk drive won't be used after reload.

Mounted filesystems:

  MOUNT POINT       TYPE       DEVICE           SIZE    INUSE     FREE USE%
  /                 root       /dev/root        34MB     28MB      6MB  82%
...
```

3. Reload the WAAS device by entering the **reload** EXEC command. When asked, press **Enter** to proceed with the reload. After the WAAS device is reloaded, Disk01, which is marked as a bad disk drive, will not be used.

```
WAE# reload
Proceed with reload?[confirm]
...
```

4. After the reload is completed, display the details about the disks by entering the **show disks details** EXEC command. Disk01 is now shown as "Not used (*)" because Disk01 was detected as bad after the WAE was rebooted.

```
WAE# show disks details
Physical disk information:

  disk00: Normal                (h00 c00 i00 l00 - DAS)     76324MB( 74.5GB)
  disk01: Not used

(*) Disk drive won't be used after reload.
...
```

5. Mark disk01 as good by entering the **disk mark** EXEC command.

```
WAE# disk mark disk01 good
disk01 is marked as good.
It will be used after reload.
```

6. Verify that Disk01 is now marked as "Not used" by entering the **show disks details** EXEC command. Reload the WAAS device by entering the **reload** EXEC command. When asked, press **Enter** to proceed with the reload. After the WAAS device is reloaded, Disk01, which is marked as a good disk drive, will be used again. Use the **show disks details** EXEC command to verify the disk is operating normally.

```
WAE# show disks details
Physical disk information:

disk00: Normal                (h00 c00 i00 l00 - DAS)     76324MB( 74.5GB)
disk01: Not used
...

WAE# reload
Proceed with reload?[confirm]
...
WAE# show disks details

Physical disk information:

  disk00: Normal                (h00 c00 i00 l00 - DAS)     76324MB( 74.5GB)
  disk01: Normal                (h01 c00 i00 l00 - DAS)     76324MB( 74.5GB)
...
```

Reformatting a SCSI Disk Drive

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

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

Note This command is only available on systems with SCSI drives: WAE-611 and WAE-7326.

The following scenario shows how to reformat a SCSI drive:

1. Mark the SCSI drive as bad. In this example, it is disk01.

```
WAE# disk mark disk01 bad
```

2. Reboot the WAAS device so that the bad disk is not in use.

```
WAE# reload
```

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

```
WAE# disk reformat disk01
```

4. Reboot the WAAS device. Normal software RAID recovery is performed and the reformatted disk is prepared for use.

```
WAE# reload
```

Removing All Disk Partitions on a Single Disk Drive

Use the **disk delete-partitions** EXEC command to remove all disk partitions on a single disk drive on WAAS device.

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

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

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

Related Commands

(config) disk

show disks

dnslookup

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

dnslookup {*hostname* | *domainname*}

Syntax Description

hostname	Name of DNS server on the network.
domainname	Name of domain.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

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

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

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

enable

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

enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

```
WAE> enable
Password:
```

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

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

Examples

The following example shows how to access privileged EXEC mode:

```
WAE> enable
WAE#
```

Related Commands

disable

exit

exit

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

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

All modes

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example terminates privileged-level EXEC mode and returns to the user-level EXEC mode:

```
WAE# exit
WAE>
```

find-pattern

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example searches 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 searches a file for a pattern and prints 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 searches a file for a pattern and prints 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 the output of the **help** EXEC command:

```
WAE# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered.
```

install

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

install *imagefilename*

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.

Syntax Description

imagefilename	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 components of the optional software to the software file system (swfs) partition.

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

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

Examples

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

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

Related Commands

copy disk

reload

less

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

less *file_name*

Syntax Description

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

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

Examples

To display the text of the *syslog.txt* file using the LESS application, enter the following command:

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

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

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

Examples

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

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

Related Commands

dir

lls

ls

ls

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

ls [*directory*]

Syntax Description

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

To list the filenames and subdirectories within a particular directory, use the **ls** *directory* command; to list the filenames and subdirectories of the current working directory, use the **ls** command. To view the present working directory, use the **pwd** command.

Examples

The following example lists the files and subdirectories within the root directory:

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

Related Commands

dir

lls

pwd

mkdir

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

mkdir *directory*

Syntax Description		
	directory	Name of the directory to create.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example creates 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 you want to create.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example creates 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 a NTP server, use the **ntpdate** EXEC command.

ntpdate {*hostname* | *ip-address*}

Syntax Description

hostname	NTP hostname.
ip-address	NTP server IP address.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example sets the software clock on the WAAS device using a NTP server:

```
WAE# ntpdate 10.11.23.40
```

Related Commands

clock

(config) clock

show clock

show ntp

no debug

To disable the display of debugging information on a WAAS device, use the **no** form of a **debug** command.

no debug *command*

Note The following **no debug** command options are supported in the application-accelerator device mode only: **dre**, **epm**, **print-spooler**, **tfo**, **wafs**, and **wccp**.

Syntax Description

aaa accounting	Disables debugging of AAA accounting actions.
all	Disables all debugging options.
authentication	Disables authentication debugging.
print-services	Disables debugging of WAAS print services authentication.
user	Disables debugging of the user login against the system authentication.
buf	Disables buffer manager debugging.
all	Disables debugging for all buffer manager functions.
dmbuf	Disables the buffer manager dmbuf debugging.
dmsg	Debugs the buffer manager dmsg.
cdp	Disables the debugging of CDP information and actions.
adjacency	Disables debugging of CDP neighbor adjacency.
events	Disables debugging of the CDP events.
ip	Disables debugging of CDP IP.
packets	Disables debugging of packet-related CDP.
cli	Disables CLI command debugging.
all	Disables debugging of all CLI commands.
bin	Disables debugging of the CLI command binary program.
parser	Disables debugging of the CLI command parser.
cms	Disables the debugging of CMS.
dataserver	Disables the debugging of the data server.
all	Disables the debugging of all data server functions.
clientlib	Disables the debugging of the data server client library module.
server	Disables the debugging of the data server module.
dhcp	Disables the debugging of DHCP.

dre	Disables DRE debugging.
aggregation	Disables the debugging of DRE chunk-aggregation debugging.
all	Disables the debugging of all DRE commands.
cache	Disables DRE cache debugging.
connection	Disables DRE connection debugging.
aggregation *acl*	Disables DRE chunk-aggregation debugging for a specified connection.
cache *acl*	Disables DRE cache debugging for a specified connection.
core *acl*	Disables DRE core debugging for a specified connection.
message *acl*	Disables DRE message debugging for a specified connection.
misc *acl*	Disables DRE other debugging for a specified connection.
core	Disables DRE core debugging.
message	Disables DRE message debugging.
misc	Disables DRE other debugging.
emdb	Disables the debugging of the embedded database.
logging	Disables the debugging of logging.
all	Disables the debugging of all logging functions.
ntp	Disables the debugging of NTP.
print-spooler	Disables the debugging of the print spooler feature.
all	(Optional) Disables the debugging of the print spooler using all debug features.
brief	(Optional) Disables the debugging of the print spooler using only brief debug messages.
errors	(Optional) Disables the debugging of the print spooler using only the error conditions.
warnings	(Optional) Disables the debugging of the print spooler using only the warning conditions.
rpc	Disables the debugging of the remote procedure calls (RPC) logs.
detail	Disables the debugging of the RPC logs of priority "detail" level or higher.
trace	Disables the debugging of the RPC logs of priority "trace" level or higher.
stats	Disables the debugging of the statistics.
all	Disables the debugging of all statistics functions.
collection	Disables the debugging of the statistics collection.
computation	Disables the debugging of the statistics computation.
history	Disables the debugging of the statistics history.

tfo	Disables TFO debugging.
buffer-mgr	Disables TFO buffer manager debugging.
connection	Disables TFO connection debugging.
auto-discovery *acl*	Disables TFO connection debugging for the auto-discovery module.
comp-mgr *acl*	Disables TFO connection debugging for the compression module.
conn-mgr *acl*	Disables TFO connection debugging for the connection manager.
filtering *acl*	Disables TFO connection debugging for filtering module.
netio-engine *acl*	Disables TFO connection debugging for network input/output module.
policy-engine *acl*	Disables TFO connection debugging of application policies.
stat-mgr	Disables TFO statistics manager debugging.
translog	Disables TFO transaction log debugging.
wafs	Sets the notification level (debug, info, warn, error) at which messages from the WAAS software component and utilities are logged.
all	Sets the logging level for all software components and utilities at once.
core-fe	Sets the logging level for WAEs acting as a core file engine.
edge-fe	Sets the logging level for WAEs acting as an edge file engine.
manager	Sets the logging level for the Device Manager.
utilities	Sets the logging level for WAAS utilities.
wccp	Disables the debugging of WCCP.
all	Disables the debugging of all WCCP functions.
detail	Disables the debugging of the WCCP details.
error	Disables the debugging of the WCCP errors.
events	Disables the debugging of the WCCP events.
keepalive	Disables the debugging of the WCCP keepalives that are sent to the applications.
packets	Disables the debugging of the WCCP packet-related information.
slowstart	Disables the debugging of the WCCP slow start.

Defaults

No default behavior or values

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Examples

The following example disables monitoring of user authentication:

```
WAE# no debug authentication user
```

ping

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

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

Syntax Description

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

Examples

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

```
WAE# ping 172.19.131.189
PING 172.19.131.189 (172.19.131.189) from 10.1.1.21 : 56(84) bytes of
data.
64 bytes from 172.19.131.189: icmp_seq=0 ttl=249 time=613 usec
64 bytes from 172.19.131.189: icmp_seq=1 ttl=249 time=485 usec
64 bytes from 172.19.131.189: icmp_seq=2 ttl=249 time=494 usec
64 bytes from 172.19.131.189: icmp_seq=3 ttl=249 time=510 usec
64 bytes from 172.19.131.189: icmp_seq=4 ttl=249 time=493 usec

--- 172.19.131.189 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.485/0.519/0.613/0.047 ms
WAE#
```

pwd

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

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example displays the current working directory:

```
WAE# pwd
/local1
```

Related Commands

cd

dir

lls

ls

reload

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

reload [**force**]

Syntax Description

force	(Optional) Forces a reboot without further prompting.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

To reboot a WAAS device, use the **reload** command. If no configurations are saved to flash memory, you are prompted to enter configuration parameters upon restart. Any open connections are dropped after you issue this command, and the file system is reformatted upon restart.

To save any file system contents to disk from memory before a restart, use the **cache synchronize** command.

Examples

The following example halts operation of the WAAS device and reboots it with the configuration saved in flash memory. You are not prompted for confirmations during the process.

```
WAE# reload force
```

Related Commands

write

rename

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

rename *oldfilename newfilename*

Syntax Description

oldfilename	Original filename.
newfilename	New filename.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following example renames the *errlog.txt* file to *old_errlog.txt*:

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

Related Commands

cpfile

restore

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Backing up the Central Manager Database

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

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

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

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

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

Rolling Back the Configuration

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

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

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

Examples

The following two examples illustrate the results of using the **restore factory-default** and **restore factory-default preserve basic-config** commands. Because configuration parameters and data are lost, prompts are given before initiating the restore operation to ensure that you want to proceed.

```
WAE# restore factory-default
This command will wipe out all of data on the disks
and wipe out WAAS CLI configurations you have ever made.
If the box is in evaluation period of certain product,
the evaluation process will not be affected though.

It is highly recommended that you stop all active services
before this command is run.

Are you sure you want to go ahead?[yes/no]

WAE# restore factory-default preserve basic-config
This command will wipe out all of data on the disks
and all of WAAS CLI configurations except basic network
configurations for keeping the device online.
The to-be-preserved configurations are network interfaces,
default gateway, domain name, name server and hostname.
If the box is in evaluation period of certain product,
the evaluation process will not be affected.

It is highly recommended that you stop all active services
before this command is run.

Are you sure you want to go ahead?[yes/no]
```

Note You can enter basic configuration parameters (such as IP address, hostname, and name server) at this point, or later through entries in the command-line interface.

In the following example, entering the **show disks details** command after the **restore** command is used verifies that the **restore** command has removed data from the partitioned file systems: SYSFS, WAAS, and PRINTSPOOLFS.

```
WAE# show disks details

Physical disk information:

  disk00: Normal                (h00 c00 i00 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 first example below, version Y of the software is installed (using the **copy** command), but the administrator has not switched over to it yet, so the current version is still version X. The system is then reloaded (using the **reload** command), and it verifies that version Y is the current version running.

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

```
WAE# copy ftp install server path waas.versionY.bin
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.0 (build b340 Mar 25 2
006)
Version: fe611-4.0.0.340

Compiled 17:26:17 Mar 25 2006 by cnbuild

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

WAE# show version last
    Nothing is displayed.
WAE# show version pending
WAAS 4.0.1 Version Y
WAE# reload
...... reloading ......
```

```
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
...
WAE# restore rollback
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 this EXEC command to remove any directory from the WAAS file system. The **rmdir** command only removes empty directories.

Examples

The following example deletes 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. This command uses SSH for transferring data between hosts.

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

Syntax Description

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

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

setup

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

setup

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

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

Enter choice:

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

show aaa accounting

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

show aaa accounting

This command displays configuration information for the following AAA accounting types:

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Examples

The following example displays the current AAA configuration:

```
WAE# show aaa accounting
Accounting Type   Record event(s)  Protocol
-------------------------------------------------
Exec shell        start-stop       tacacs
Command level  0  stop-only        tacacs
Command level 15  disabled
System            start-stop       tacacs
```

Related Commands

(config) aaa accounting

show alarms

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

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 (for example, the CIFS service) 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."

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

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

The three levels of alarms in WAAS software are:

- Critical—Alarms that affect the existing traffic through the WAE, and are considered fatal (the WAE cannot recover and continue to process traffic).
- Major—Alarms which indicate a major service (for example, the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted.
- Minor—Alarms which indicate that a condition that will not affect a service has occurred, but that corrective action is required to prevent a serious fault from occurring.

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

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

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

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

Examples

The following sample output for the **show alarm history** command displays all major alarms generated on the WAAS device since the last software reload:

```
WAE# show alarms history
     Op Sev Alarm ID             Module/Submodule     Instance
     -- --- -------------------- -------------------- --------------------
   1 C  Ma  tfo_accl_wellness    sysmon               accl=CIFS
   2 C  Cr  wafs_edge_down       wafs
   3 R  Ma  tfo_accl_wellness    sysmon               accl=CIFS
   4 R  Cr  wafs_edge_down       wafs
   5 R  Ma  core_dump            sysmon               core

Op - Operation: R-Raised, C-Cleared
Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor
```

The following sample output of the **show alarm history** command displays the complete details of alarms 1 through 3 in the alarm history event record:

```
WAE# show alarms history 1 3 detail support
     Op Sev Alarm ID             Module/Submodule     Instance
     -- --- -------------------- -------------------- --------------------
   1 C  Ma  tfo_accl_wellness    sysmon               accl=CIFS
     Apr 12 20:25:58.119 UTC, Processing Error Alarm, #000003, 1000:445005
     The CIFS TFO Accelerator application has had a keepalive failure.
     Its wellness is in question.

     /alm/maj/sysmon/accl=XXXX/tfo_accl_wellness:

         A TFO Accelerator application has had a keepalive failure.
```

```
    Explanation:
        The System Monitor issues this to indicate that one of the
        TFO Accelerators is failing to perform a wellness update
        within the allotted time. The implications are that some
        connections may not be optimized properly by TFO and thus
        optimization performance may be reduced.

    Action:
        Examine the status of the specified accelerator to verify it
        is still operating properly and make adjustments to return
        it to full health if necessary.



  2 C  Cr  wafs_edge_down       wafs
    Apr 12 20:25:30.756 UTC, Processing Error Alarm, #000002, 10000:1000001
    WAFS Edge is down.

    /alm/crit/wafs/wafs_edge_down:

        WAFS Edge is down.

    Explanation:
        This alarm is used to check if the Edge is working.

    Action:
        Please reactivate the Edge component on the device.



  3 R  Ma  tfo_accl_wellness    sysmon              accl=CIFS
    Apr 12 20:24:43.127 UTC, Processing Error Alarm, #000003, 1000:445005
    The CIFS TFO Accelerator application has had a keepalive failure.
    Its wellness is in question.

    /alm/maj/sysmon/accl=XXXX/tfo_accl_wellness:

        A TFO Accelerator application has had a keepalive failure.

    Explanation:
        The System Monitor issues this to indicate that one of the
        TFO Accelerators is failing to perform a wellness update
        within the allotted time. The implications are that some
        connections may not be optimized properly by TFO and thus
        optimization performance may be reduced.

    Action:
        Examine the status of the specified accelerator to verify it
        is still operating properly and make adjustments to return
        it to full health if necessary.



Op - Operation: R-Raised, C-Cleared
Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor
```

This sample output for the **show alarm status** command displays the status of critical, major, and minor alarms and the alarm overload status and alarm overload configuration on the WAAS device.

```
WAE# show alarms status
Critical Alarms :          0
Major Alarms    :          1
Minor Alarms    :          0

Overall Alarm Status : Major
Device is NOT in alarm overload state.

Device enters alarm overload state @   10 alarms/sec.
Device exits alarm overload state  @    1 alarms/sec.
Overload detection is ENABLED.
```

Related Commands

(config) alarm overload-detect

(config) snmp-server enable traps

show arp

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

show arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows the ARP table:

```
WAE# show arp
Protocol  Address          Flags      Hardware Addr     Type  Interface
Internet  10.56.40.17      Adj        00:06:5B:FE:4D:05 ARPA  GigabitEthernet1/0
Internet  10.56.40.2       Adj        00:0F:F8:A0:9F:8A ARPA  GigabitEthernet1/0
Internet  10.56.40.1       Adj        00:00:0C:07:AC:01 ARPA  GigabitEthernet1/0
```

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

The following table describes the fields shown in the **show arp** display.

Field	Description
Protocol	Type of protocol.
Address	IP address of the host name.
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 {**print-services** | **user** | **content-request**}

Syntax Descriptions

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The WAAS software supports print service request authentication through the Windows domain server. A print service request authenticates the domain and password of a user with a preconfigured Windows domain server before allowing requests from the user to be served by the WAAS device. To display the authentication for a print services request, use the **show authentication print-services** EXEC command. To view user authorization for print services, use the **show print-services admin-group** EXEC command.

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.

Examples

To display the current administrative login authentication and authorization (authentication configuration) on a WAAS device, use the **show authentication user** EXEC command. The sample output shows the authentication and authorization schemes (for example, local, RADIUS, TACACS+, or Windows domain) that the WAAS device is configured to use to authenticate and authorize administrative login requests.

```
WAE# show authentication user
Login Authentication:         Console/Telnet/Ftp/SSH Session
----------------------------- -----------------------------
local                         enabled (primary)
Windows domain                disabled
Radius                        disabled
Tacacs+                       disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
----------------------------- -----------------------------
local                         enabled (primary)
Windows domain                disabled
Radius                        disabled
Tacacs+                       disabled
```

The following example displays the authentication and authorization information for WAAS print services:

```
WAE# show authentication print-services
    Windows domain server authenticates the Print Services
WAE# show print-services admin-group
    There is no configured administrator group for print-services.
```

The following example displays the content request authentication configuration information in the disconnected mode:

```
WAE# show authentication content-request
The content request authentication in disconnected mode is disabled
```

Related Commands

(config) authentication

clear

show statistics authentication

show auto-register

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

show auto-register

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays the status of the automatic registration feature of a WAE:

```
WAE# show auto-register
Auto registration is disabled.
```

Related Commands

(config) auto-register

show bypass

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

show bypass list

Syntax Description

list	Bypass list entries. Maximum of 50.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The maximum number of static bypass entries is 50.

Examples

The following example displays a list of entries in the bypass list:

```
WAE# show bypass list

          Client                Server        Entry type
          ------                ------        ----------
    172.16.11.11:0          any-server:0     static-config
      any-client:0        172.31.23.23:0     static-config
```

Related Commands

(config) bypass

show cdp

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

show cdp [**entry** *neighbor* [**protocol** | **version** [**protocol**]] | **holdtime** | **interface** [**FastEthernet** *slot/port* | **GigabitEthernet** *slot/port*] | **neighbors** [**detail** | **FastEthernet** *slot/port* [**detail**] | **GigabitEthernet** *slot/port* [**detail**]] | **run** | **timer** | **traffic**]

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following examples display CDP information regarding how frequently CDP packets are resent to neighbors, the length of time that CDP packets are held by neighbors, the disabled status of CDP Version 2 multicast advertisements, CDP Ethernet interface ports, and general CDP traffic information:

```
WAE# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is not enabled

WAE# show cdp holdtime
180 seconds

WAE# show cdp interface gigabitethernet 1/0
GigabitEthernet1/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

WAE# show cdp neighbors gigabitethernet 1/0 detail
Device ID: actona-core1-6513(L)
Entry address(es):
  IP address: 10.10.40.3
Platform: cisco WS-C6513,  Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0,  Port ID (outgoing port): GigabitEthernet5/30
Holdtime : 124 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-PS-M), Version 12.1(26)E, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 24-Dec-04 08:02

advertisement version: 2
VTP Management Domain: 'actona'
Native VLAN: 1

WAE# show cdp traffic
CDP counters :
        Total packets Output: 188242, Input: 186151
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements Output: 188242, Input: 93072
        CDP version 2 advertisements Output: 0, Input: 93079
```

Related Commands

(config) cdp

(config-if) cdp

clear

show clock

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

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

Syntax Description

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

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 US/Eastern time zone that includes summer time information for the system clock to adjust automatically every April and October. There are about 1500 "standard" time zone names.

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

The **show clock standard-timezones all** EXEC command enables you to browse through all standard timezones and choose from these predefined time zones. This enables you to choose a customized name that does not conflict with the predefined names of the standard time zones. Most predefined names of the standard time zones have two components, a region name and a zone name. You can list time zones by several criteria, such as regions and zones.

Examples

The following example shows date and time information, such as day of the week, month, time (hh:mm:ss), and year in local time relative to Israeli Standard Time (UTC plus two hours):

```
WAE# show clock
Local time: Wed Apr  6 20:03:56 IST 2005
```

The following example shows optional detailed date and time information, including local time relative to UTC. In addition to the information shown in the previous example, **show clock detail** provides the UTC offset, and the local time zone.

```
WAE# show clock detail
Local time: Wed Apr  6 20:10:40 IST 2005

  UTC time: Wed Apr  6 18:10:40 UTC 2005

Epoch: 1112811040 seconds
UTC offset: 7200 seconds (2 hours 0 minutes)
```

The following example shows an excerpt of the output from the **show clock standard-timezones all** EXEC command. A partial list is shown. Each time zone is listed on a separate line.

```
WAE # show clock standard-timezones all
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
.
.
.
```

The following example shows an excerpt of the output from the **show clock standard-timezones region** EXEC command. As the example shows, all first level time zone names or directories are listed. All 1500 time zones are organized into directories by region.

```
WAE # show clock standard-timezones regions
Africa/
America/
Antarctica/
Arctic/
Asia/
Atlantic/
Australia/
Brazil/
CET
.
.
.
US/
UTC
Universal
```

```
W-SU
WET
Zulu
```

The following example shows an excerpt of the output from the **show clock standard-timezones zones** EXEC command. As the following example shows, this command lists the name of every time zone that is within the specified region (for example, the US region).

```
WAE # show clock standard-timezones zones US
Zones within region US
======================

US/Alaska
US/Aleutian
US/Arizona
US/Central
US/East-Indiana
US/Eastern
US/Hawaii
US/Indiana-Starke
US/Michigan
US/Mountain
US/Pacific
US/Samoa
```

The following sample shows an excerpt of the output from the **show clock standard-timezones details** EXEC command. The time zone is case-sensitive. As the following example shows, this command shows details about the specified time zone (for example, the US/Eastern time zone). The command output also includes the standard offset from the GMT.

```
WAE # show clock standard-timezones details US/Eastern
US/Eastern is standard timezone.
Getting offset information (may take a while) ...
Standard offset from GMT is -300 minutes (-5 hour(s)).
It has built-in summertime.
Summer offset from GMT is -240 minutes. (-4 hour(s)).
```

Related Commands

clock

(config) clock

show cms

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following two examples show the result of using the **show cms info** command on a WAAS device:

```
WAE# show cms info
CDN information :
Model                           = CDM4630
Node Id                         = 91
Device Mode                     = cdm
Current CDM role                = Primary

CMS services information :
Service cms_httpd is running
Service cms_cdm is running
```

The following example shows the CMS application processes:

```
WAE# show cms processes
Service cms_httpd running
Service cms_cdm running
```

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

```
WAE# show cms database content text
Database content can be found in /local1/cms-db-12-12-2002-17:06:08:070.txt.
```

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

```
WAE# show cms database content xml
Database content can be found in /local1/cms-db-12-12-2002-17:07:11:629.xml.
```

Related Commands

cms

(config) cms

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.

Usage Guidelines

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

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

In the following 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:

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

Related Commands

debug

undebug

show device-mode

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

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

Syntax Description

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

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

In the WAAS software release and later releases, you must deploy the WAAS Central Manager on a dedicated appliance. The device mode feature allows you to deploy a WAAS device as either a WAAS Central Manager or a WAE. Because you must deploy a WAAS Central Manager on a dedicated appliance, a WAAS device can only operate in one device mode; either in central-manager mode or application-acclerator mode.

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

Examples

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

```
WAE# show device mode
```

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

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

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

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

Related Commands

(config) device mode

show disks

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

show disks {**details** | **failed-sectors** [*disk_name*] | **SMART-info** [**details**]}

Syntax Description

details	Displays currently effective configurations with more details.
failed-sectors	Displays a list of failed sectors on all disks.
disk_name	(Optional) Name of the disk for which failed sectors are displayed (disk00 or disk01).
SMART-info	Displays hard drive diagnostic information and information about impending disk failures.
details	(Optional) Displays more detailed SMART disk monitoring information.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

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

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

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

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

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

Proactively Monitoring Disk Health with SMART

The ability to proactively monitor the health of disks is available using SMART. SMART provides you with hard drive diagnostic information and information about impending disk failures.

SMART is supported by most disk vendors and is a standard method used to determine how healthy a disk is. SMART attributes include several read-only attributes (for example, the power on hours attribute, the load and unload count attribute) that provide the WAAS software with information regarding the operating and environmental conditions that may indicate an impending disk failure.

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

Even though SMART attributes are vendor dependent there is a common way of interpreting most SMART attributes. Each SMART attribute has a normalized current value and a threshold value. When the current value exceeds the threshold value, the disk is considered to have "failed." The WAAS software monitors the SMART attributes and reports any impending failure through syslog messages, SNMP traps, and alarms.

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

Examples

In the following example, enter the **show disks details** EXEC command to display detailed information about the current disk configuration on the WAAS device:

```
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 the output of the **show disks SMART-info** EXEC command:

```
WAEA# show disks SMART-info
=== disk00 ===
Device: IBM-ESXS ST3146707LW   FN Version: B26B
Serial number: 3KS2YL00000000000CM3
Device type: disk
Transport protocol: Parallel SCSI (SPI-4)
Local Time is: Fri Mar 31 13:06:08 2006 UTC
Device supports SMART and is Enabled
Temperature Warning Enabled
SMART Health Status: OK

=== disk01 ===
Device: IBM-ESXS ST3146707LW   FN Version: B26B
Serial number: 3KS1ZTRH00000000CK61
Device type: disk
Transport protocol: Parallel SCSI (SPI-4)
Local Time is: Fri Mar 31 13:06:08 2006 UTC
Device supports SMART and is Enabled
Temperature Warning Enabled
SMART Health Status: OK
```

The following example displays more detailed SMART output from the **show disks SMART-info details** EXEC command:

```
WAE# show disks SMART-info details
=== disk00 ===
Device: IBM-ESXS ST3146707LW   FN Version: B26B
Serial number: 3KS2YL94000000000CM3
Device type: disk
Transport protocol: Parallel SCSI (SPI-4)
Local Time is: Fri Mar 31 13:06:53 2006 UTC
Device supports SMART and is Enabled
Temperature Warning Enabled
SMART Health Status: OK

Current Drive Temperature:     33 C
Drive Trip Temperature:        65 C
Vendor (Seagate) cache information
  Blocks sent to initiator = 4048936465
  Blocks received from initiator = 100130496
  Blocks read from cache and sent to initiator = 56503638
  Number of read and write commands whose size <= segment size = 10124024
  Number of read and write commands whose size > segment size = 0

Error counter log:
          Errors Corrected    Total      Total   Correction     Gigabytes    Tot
al
              delay:       [rereads/    errors   algorithm      processed    unc
```

Related Commands

disk

(config) disk

show tech-support

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

The following example displays flash memory information. Note that a new software image has been downloaded, but not yet deployed.

```
WAE# show flash
WAAS software version (disk-based code): WAAS-4.0.0-b340

System image on flash:
Version: 4.0.0.340

System flash directory:
System image: 107 sectors
Bootloader, rescue image, and other reserved areas: 24 sectors
256 sectors total, 125 sectors free.
```

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

Examples

The following example 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:

```
WAE# show hardware
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.0 (build b340 Mar 25 2
006)
Version: fe611-4.0.0.340

Compiled 17:26:17 Mar 25 2006 by cnbuild

System was restarted on Mon Mar 27 15:25:01 2006.
The system has been up for 3 days, 21 hours, 15 minutes, 13 seconds.

CPU 0 is GenuineIntel Intel(R) Pentium(R) 4 CPU 3.00GHz (rev 4) running at 3002M
Hz.
Total 1 CPU.
2048 Mbytes of Physical memory.
1 CD ROM drive (HL-DT-ST GCR-8240N)
2 GigabitEthernet interfaces
1 Console interface

Manufactured As: WAE-611-K9  [8836PBN]

BIOS Information:
Vendor                              : IBM
...
```

Related Commands

show hardware

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

Examples

The following **show hosts** example lists the name servers and their corresponding IP addresses. It also lists the host names, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary:

```
WAE# show hosts
Domain names:
------------


Name Server(s):
-------------

Host Table:
hostname                 inet address         aliases
--------                 ------------         -------

Edge-WAE1                10.10.10.32
```

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 status for the tftp service, but you can ignore this line because tftp is not supported on WAAS.

Examples

The following example displays the enabled or disabled status of TCP/IP services on the WAAS device:

```
WAE# show inetd
Inetd service configurations:
ftp             enable
rcp             disabled
tftp            disabled
```

Related Commands

(config) inetd

show interface

To display the hardware interface information for a WAAS device, use the **show interface** EXEC command.

show interface {**GigabitEthernet** *slot/port* | **ide** *control_num* | **PortChannel** *port-num* | **scsi** *device_num* | **Standby** *group_num* | **usb**}

Syntax Description

GigabitEthernet	Displays the Gigabit Ethernet interface device information (only on suitably equipped systems).
slot/port	Slot and port number for the Gigabit Ethernet interface. The slot range is 0–3; the port range is 0–3. The slot number and port number are separated with a forward slash character (/).
ide	Displays the IDE interface device information.
control_num	IDE controller number (0–1).
PortChannel	Displays the port channel interface device information.
port-num	Port number for the port channel interface (1–2).
scsi	Displays the SCSI interface device information.
device_num	SCSI device number (0–7).
Standby	Displays the standby group information.
group_num	Standby group number (1–4).
usb	Displays the USB interface device information.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays information for the Gigabit Ethernet interface slot 1/port 0 configured on the WAAS device:

```
WAE# show interface GigabitEthernet 1/0
Type:Ethernet
Ethernet address:00:0D:60:84:30:84
Internet address:10.56.41.180
Broadcast address:10.56.43.255
Netmask:255.255.252.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 49288883
Input Errors: 0
Input Packets Dropped: 0
```

```
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 547899
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:1000
Collisions: 0
Interrupts:18
Base address:0x2000
Flags:UP BROADCAST RUNNING MULTICAST
Mode: autoselect, full-duplex, 1000baseTX
```

The following example displays information for the port channel interface configured on the WAAS device:

```
waas-cm# show interface PortChannel 1
Interface PortChannel 1 (0 physical interface(s)):
--------------------
Type:Ethernet
Ethernet address:00:00:00:00:00:00
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 0
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 0
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:0
Collisions: 0
Flags:BROADCAST MASTER MULTICAST
```

The following example displays information for the SCSI interface configured on the WAAS device:

```
waas-cm# show interface scsi 1
SCSI interface 0: LSI Chip sym00c000, device id 0xc, revision id 0x2
```

The following example displays information for the standby interface on the WAAS device:

```
WAE# show interface Standby 4
Standby Group: 4
        Description: This is an interface that acts as a backup
        IP address: 10.10.10.4, netmask: 255.0.0.0
        Member interfaces: none
        Active interface: none
```

Related Commands

(config) interface

show running-config

show startup-config

show inventory

To display the system inventory information for a WAAS device, use the **show inventory** EXEC command.

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show inventory** EXEC command allows you to view the UDI for a WAAS device. Typically, a WAAS device contains the following three identification items, which make up the UDI:

- Product ID (PID)
- Version ID (VID)
- Serial number (SN)

This identity information is stored in the WAAS device's nonvolatile memory.

The UDI is electronically accessed by the product operating system or network management application to enable identification of unique hardware devices. The data integrity of the UDI is vital to customers. The UDI that is programmed into the WAAS device's nonvolatile memory is equivalent to the UDI that is printed on the product label and on the carton label. This UDI is also equivalent to the UDI that can be viewed through any electronic means and in all customer-facing systems and tools. Currently, there is only CLI access to the UDI; there is no SNMP access to the UDI information.

You can also use the **show tech-support** EXEC command to display the WAAS device's UDI.

Examples

The following example shows the inventory information for a WAE model WAE-511:

```
WAE# show inventory

PID: WAE-511-K9 VID: 0 SN: serial_number
```

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

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) Displays information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl-num	(Optional) Displays 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. Unless you identify a specific access list by name or number, the system displays information about all the defined access lists, including the following sections:

- Available space for new lists and conditions
- Defined access lists
- References by interface and application

Examples

The following example shows sample output from the **show ip access-list** command:

```
WAE# show ip access-list
Space available:
    47 access lists
   492 access list conditions

Standard IP access list 1
  1 permit 10.1.1.2
  2 deny   10.1.2.1
    (implicit deny any: 2 matches)
  total invocations: 2
Extended IP access list 100
  1 permit tcp host 10.1.1.1 any
  2 permit tcp host 10.1.1.2 any
  3 permit tcp host 10.1.1.3 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
```

```
  total invocations: 0
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
    (implicit deny: 2 matches)
  total invocations: 12

Interface access list references:
  GigabitEthernet 1/0  inbound   100

Application access list references:
  tftp_server                    standard  1
    UDP ports:    69
```

The following shows sample output from the **show ip access-list** command for the access list named *test*:

```
WAE# show ip access-list test
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
    (implicit deny: 2 matches)
  total invocations: 12
```

Note The system displays the number of packets that have matched a condition statement only if the number is greater than zero.

Related Commands

clear

(config) ip access-list

show ip routes

To display the IP routing table for a WAAS device, use the **show ip routes** EXEC command.

show ip routes

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the IP routing table:

```
WAE# show ip routes
Destination      Gateway          Netmask
---------------- ---------------- ----------------
10.56.41.180     0.0.0.0          255.255.255.255
192.168.12.180   0.0.0.0          255.255.255.255
192.168.12.0     0.0.0.0          255.255.255.0
10.56.40.0       0.0.0.0          255.255.252.0
0.0.0.0          10.56.40.1       0.0.0.0


Number of route cache entries: 183
```

Related Commands

(config) ip

(config-if) ip

show kerberos

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

show kerberos

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

You can use the system message log to view information about events that have occurred on a WAAS device. The *syslog.txt* file is contained in the */local1* directory.

Examples

The following example displays the Kerberos authentication configuration on a WAAS device:

```
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: 0.0.0.0
    Port: 88
```

Related Commands

clear

(config) logging

show logging

To display the system message log configuration for a WAAS device, use the **show logging** EXEC command.

show logging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

You can use the system message log to view information about events that have occurred on a WAAS device. The *syslog.txt* file is contained in the */local1* directory.

Examples

The following example displays the syslog host configuration on a WAAS device:

```
WAE# show logging
Syslog to host is disabled
Priority for host logging is set to:  warning

Syslog to console is disabled
Priority for console logging is set to:  warning

Syslog to disk is enabled
Priority for disk logging is set to:  notice
Filename for disk logging is set to:  /local1/syslog.txt

Syslog facility is set to *

Syslog disk file recycle size is set to 1000000
```

Related Commands

clear

(config) logging

show sysfs

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

The following example displays information about the blocks in memory:

```
WAE# show memory
Total physical memory    :     510164 KB
Total free memory        :      43220 KB
Total memory shared      :          0 KB
Total buffer memory      :      12768 KB
Total cached memory      :     344472 KB
Total swap               :     509940 KB
Total free swap          :     509940 KB
```

show ntp

To display the NTP parameters for a WAAS device, use the **show ntp** EXEC command.

show ntp status

Syntax Description

status	Displays NTP status.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the current NTP parameters for a WAAS device. With the first attempt, it is determined that NTP has not been configured. After configuring NTP, the parameters are then displayed.

```
WAE# show ntp status
ntp disabled
server list:

WAE(config)# ntp server 172.16.10.80 172.16.10.150
WAE(config)# exit
WAE(config)# show ntp status
ntp enabled
server list: 172.16.10.80 172.16.10.50
     remote           refid      st t when poll reach   delay   offset jitter
==============================================================================
 ntp-sj1.abc.c 0.0.0.0         16 u    -   64    0    0.000    0.000 4000.00
 ntp-sj2.abc.c 0.0.0.0         16 u    -   64    0    0.000    0.000 4000.00
```

The following table describes the fields shown in the **show ntp status** display.

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.

Field	Description
-	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.
offset	Clock offset relative to the server.
jitter	Clock jitter.

Related Commands

clock

(config) clock

(config) ntp

show policy-engine application

To display application policy information for a WAE, use the **show policy-engine application** EXEC command.

show policy-engine application {**classifier** [*app-classifier*] | **dynamic** | **name**}

Syntax Description

classifier	Displays information about the specified application classifier. If no classifier is specified, this command displays information about all classifiers. Every application classifier with a single match is displayed in one line.
app-classifier	(Optional) The name of an application classifier. The name should not exceed 30 characters.
dynamic	Shows the application dynamic match information.
name	Shows the application names list.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays information about the specified application classifier Oracle for a WAE:

```
WEA# show policy-engine application classifier Oracle
Oracle                          (0)
match (0, id=0) dst port eq 66
match (1, id=1) dst port eq 1521
match (2, id=2) dst port eq 1525
```

The following example displays application dynamic match information:

```
WEA# show policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 8192  In Use: 0  Max In Use: 0  Allocations: 0

Individual Dynamic Match Information:
  --No Application Dynamic Matches are currently active.--
```

The following example displays the application names list:

```
WEA# show policy-engine application name
Number of Applications: 12
  1) Authentication                  (15)
  2) Backup                          (18)
  3) Call-Management                 (17)
  4) Conferencing                    (8)
  5) Console                         (4)
  6) Content-Management              (21)
  7) Directory-Services              (6)
  8) Email-and-Messaging             (12)
  9) Enterprise-Applications         (13)
 10) File-System                     (2)
 11) File-Transfer                   (16)
 12) Instant-Messaging               (22)
```

Related Commands

(config) policy-engine application classifier

(config) policy-engine application map adaptor EPM

(config) policy-engine application map adaptor WAFS accept

(config) policy-engine application map adaptor WAFS transport

(config) policy-engine application map basic delete

(config) policy-engine application map basic disable

(config) policy-engine application map basic insert

(config) policy-engine application map basic list

(config) policy-engine application map basic move

(config) policy-engine application map basic name

(config) policy-engine application map other optimize DRE

(config) policy-engine application map other optimize full

(config) policy-engine application map other pass-through

(config) policy-engine application name

(config) policy-engine config

show policy-engine status

To display high-level information about a WAE's policy engine, use the **show policy-engine status** EXEC command. This information includes the usage of the available resources, which include application names, classifiers, and conditions.

show policy-engine status

Command Modes

EXEC

Device Modes

application-accelerator

Examples

To display high-level information about a WAE's policy engine:

```
WEA# show policy-engine status
policy-engine resources usage:
                  Total    Used   Available
                  -----    ----   ---------
Application names   256      28     228
Classifiers         512     146     366
Conditions         1024     321     703
```

Related Commands

(config) policy-engine application classifier

(config) policy-engine application map adaptor EPM

(config) policy-engine application map adaptor WAFS accept

(config) policy-engine application map adaptor WAFS transport

(config) policy-engine application map basic delete

(config) policy-engine application map basic disable

(config) policy-engine application map basic insert

(config) policy-engine application map basic list

(config) policy-engine application map basic move

(config) policy-engine application map basic name

(config) policy-engine application map other optimize DRE

(config) policy-engine application map other optimize full

(config) policy-engine application map other pass-through

(config) policy-engine application name

(config) policy-engine config

show print-services

To display administrative users who have access to configuration privileges, print services, or print service processes on a WAAS device, use the **show print-services** EXEC command.

show print-services {**admin-group** | **drivers user** *username* | **process**}

Syntax Description

admin-group	Displays print services administrator group information.
process	Displays information about the print server and print spooler.
drivers	Displays printer drivers on this print server.
user *username*	Specifies a username that belongs to the print admin group.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

To view print service configuration information by administrative group:

```
WAE# show print-services admin-group
Administrator Group for print-services is : cupsAdmin
```

If there is no administrative group set, the output looks like this:

```
WAE# show print-services admin-group
There is no configured administrator group for print-services.
```

To view print service configuration information by the print service process:

```
WAE# show print-services process
Print server is not running.
Print spooler is not running.
```

Related Commands

(config) authentication

(config) print-services

show authentication

windows-domain

(config) windows-domain

show processes

To display CPU or memory processes for a WAAS device, use the **show processes** EXEC command.

show processes [**cpu** | **debug** *pid* | **memory** | **system** [**delay** *1-60* | **count** *1-100*]]

Syntax Description

cpu	(Optional) Displays CPU utilization.
debug	(Optional) Prints the system call and signal traces for a specified process identifier to display system progress.
pid	Process identifier.
memory	(Optional) Displays memory allocation processes.
system	(Optional) Displays system load information in terms of updates.
delay	(Optional) Specifies the delay between updates, in seconds (1–60).
count	(Optional) Specifies the number of updates that are displayed (1–100).

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the EXEC commands shown in this section to track and analyze system CPU utilization.

The **show processes debug** command displays extensive internal system call information and a detailed account of each system call (along with arguments) made by each process and the signals it has received.

Use the **show processes system** command to display system load information in terms of updates. The **delay** option specifies the delay between updates, in seconds. The **count** option specifies the number of updates that are displayed. This command displays these items:

- A list of all processes in wide format.
- Two tables listing the processes that utilize CPU resources. The first table displays the list of processes in descending order of utilization of CPU resources based on a snapshot taken after the processes system (ps) output is displayed. The second table displays the same processes based on a snapshot taken 5 seconds after the first snapshot.
- Virtual memory used by the corresponding processes in a series of five snapshots, each separated by 1 second.

Note CPU utilization and system performance are severely affected when you use these commands. We therefore recommend that you avoid using these commands, especially the **show processes debug** command, unless it is absolutely necessary.

Examples

The following example displays information about overall system utilization:

```
WAE# show processes cpu
CPU average usage since last reboot:
   cpu: 0.20% User,  0.47% System,  1.41% User(nice),  97.92% Idle
------------------------------------------------------------------------
 PID  STATE PRI User T  SYS T        COMMAND
----- ----- --- ------ ------ --------------------
    1     S   0    350     94 (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)
```

The following example displays information about memory utilization:

```
WAE# show processes memory
Total       Used       Free     Shared    Buffers     Cached
2120081408  786411520 1333669888          0   56590336  614592512

Swap Total       Used       Free
2107498496          0 2107498496

   PID State    TTY  %MEM    VM Size RSS (pages) Name
------ ----- ------ ----- ---------- ----------- ----
     1     S      0  0.0    1445888         135 (init)
     2     S      0  0.0          0           0 (migration/0)
     3     S      0  0.0          0           0 (ksoftirqd/0)
     4     S      0  0.0          0           0 (events/0)
```

The following table describes the fields shown in the **show processes** displays.

Field	Description
CPU Usage	CPU utilization as a percentage for user, system overhead, and idle.
PID	Process identifier.
STATE	Current state of corresponding processes. R = running S = sleeping in an interruptible wait D = sleeping in an uninterruptible wait or swapping Z = zombie T = traced or stopped on a signal
PRI	Priority of processes.
User T	User time utilization in seconds.
Sys T	System time utilization in seconds.
COMMAND	Process command.
Total	Total available memory in bytes.
Used	Memory currently used in bytes.
Free	Free memory available in bytes.
Shared	Shared memory currently used in bytes.
Buffers	Buffer memory currently used in bytes.
Cached	Cache memory currently used in bytes.
SwapTotal	Total available memory in bytes for swap purposes.

show radius-server

To display RADIUS configuration information for a WAAS device, use the **show radius-server** EXEC command.

show radius-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the RADIUS configuration information for the WAAS:

```
WAE# show radius-server
Radius Configuration:
---------------------
Radius Authentication is on
    Timeout       = 5
    Retransmit    = 3
    Key           = ****
    Servers
    -------
```

The following table describes the fields shown in the **show radius-server** display.

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.

Field	Description
Timeout	Number of seconds that the WAAS device waits for a response from the specified RADIUS authentication server before declaring a timeout.
Servers	RADIUS servers that the WAAS device is to use for RADIUS authentication.
IP	Hostname or IP address of the RADIUS server.
Port	Port number on which the RADIUS server is listening.

Related Commands (config) radius-server

show running-config

To display a WAAS device's current running configuration information on the terminal, use the **show running-config** EXEC command. This command replaces the **write terminal** command.

show running-config

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this EXEC command in conjunction with the **show startup-config** command to compare the information in running memory to the startup configuration used during bootup.

Examples

The following example displays the currently running configuration of a WAAS device:

```
WAE# show running-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname waas-cm
!
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
...
```

Related Commands

configure

copy running-config

copy startup-config

show services

To display services-related information for a WAAS device, use the **show services** EXEC command.

show services {**ports** [*port-num*] | **summary**}

Syntax Description

ports	Displays services by port number.
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 example displays a summary of the services:

```
WAE# show services summary

Service        Ports
-----------------------------------------------------
                CMS          1100  5256
                NLM          4045
               WAFS          1099
               emdb          5432
              MOUNT          3058
         MgmtAgent           5252
       WAFS_tunnel           4050
     CMS_db_vacuum           5257
```

show smb-conf

To view a WAAS device's current values of the Samba configuration file, *smb.conf*, use the **show smb-conf** EXEC command.

show smb-conf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

This command displays the global, print$, and printers parameters values of the *smb.conf* file for troubleshooting purposes. For a description of these parameters and their values, see "(config) smb-conf" command.

Examples

The following example displays all of the parameter values for the current configuration:

```
WAE# show smb-conf

Current smb-conf configurations -->

smb-conf section "global" name "ldap ssl" value "start_tls"
smb-conf section "printers" name "printer admin" value "root"

Output of current smb.conf file on disk -->


================================================

# File automatically generated


[global]
idmap uid = 70000-200000
idmap gid = 70000-200000
winbind enum users = no
winbind enum groups = no
winbind cache time = 10
winbind use default domain = yes
printcap name = cups
load printers = yes
printing = cups
cups options = "raw"
```

```
force printername = yes
lpq cache time = 0
log file = /local/local1/errorlog/samba.log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
smb ports = 50139
local master = no
domain master = no
preferred master = no
dns proxy = no
template homedir = /local/local1/
template shell = /admin-shell
ldap ssl = start_tls
comment = Comment:
netbios name = MYFILEENGINE
realm = ABC
wins server = 10.10.10.1
password server = 10.10.10.10
security = domain

[print$]
path = /state/samba/printers
guest ok = yes
browseable = yes
read only = yes
write list = root


[printers]
path = /local/local1/spool/samba
browseable = no
guest ok = yes
writable = no
printable = yes
printer admin = root

================================================
```

Related Commands

(config) smb-conf

windows-domain

(config) windows-domain

show snmp

To check the status of SNMP communications for a WAAS device, use the **show snmp** EXEC command.

show snmp {**alarm-history** | **engine ID** | **event** | **group** | **stats** | **user**}

Syntax Description

alarm-history	Displays SNMP alarm history information.
engineID	Displays local SNMP engine identifier.
event	Displays events configured through the Event MIB.
group	Displays SNMP groups.
stats	Displays SNMP statistics.
user	Displays SNMP users.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

This EXEC command provides information on various SNMP variables and statistics on SNMP operations.

Examples

The following example displays the SNMP alarm history information:

```
WAE# show snmp alarm-history
Index     Type Sev  Alarm ID ModuleID Category Descr
-----     ---- ---  -------- -------- -------- -----
1          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The rtspg service
died.
2          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The mediacache
service died.
3          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The sshdaemon
service died.
4          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The cache service
died.
5          R    Ma   330003   2000     3        Raise-Alarm: nodemgr: The ntpd service
died.
6          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The mediacache
service died.
7          R    Ma   445001   1000     3        Raise-Alarm: Kernel Crash files and / or
User Core files detected
8          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The cache service
died.
9          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The mediacache
service died.
```

```
10          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The rpc_httpd
service died.
11          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The rpc_httpd
service died.
12          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The cache service
died.
13          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The mediacache
service died.
14          R    Ma   330003   2000     3        Raise-Alarm: nodemgr: The ntpd service
died.
15          R    Ma   330003   2000     3        Raise-Alarm: nodemgr: The ntpd service
died.
16          R    Mi   330004   2000     3        Raise-Alarm: nodemgr: The mediacache
service died.
WAE#
```

The following table describes the fields shown in the **show snmp alarm-history** display.

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.

The following table summarizes the mapping of module names to modules IDs.

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

The following table summarizes the mapping of category names to category IDs.

Category Name	Category ID
Communications	1
Service Quality	2
Processing Error	3
Equipment	4
Environment	5
Content	6

The following examples display the SNMP engine ID and SNMP statistical data:

```
WAE# show snmp engineID
Local SNMP Engine ID: 00000009000000A11A3829CE

WAE# show snmp stats
Contact: username, system admin, user@cisco.com 555-1111
Location: Building 2, Floor 1, LabA
146 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    120 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    120 Set-request PDUs
146 SNMP packets output
    0 Too big errors
    2048 Maximum packet size
    0 No such name errors
    0 Bad values errors
    0 General errors
    146 Response PDUs
    0 Trap PDUs
```

The following table describes the fields shown in the **show snmp stats** display.

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.

Field	Description
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.

The following example displays information about the SNMP events set using the "snmp trigger" command:

```
WAE# show snmp event

 Mgmt Triggers:
 (1): Owner: CLI
   (1): 01 , Comment: isValid == 0, Sample: Abs, Freq: 120
         Test:  Boolean
         ObjectOwner: CLI, Object: CLI1
      Boolean Entry:
         Value: 0, Cmp: 2, Start: 1
         ObjOwn: , Obj: , EveOwn: CLI, Eve: CLI_EVENT

      Delta Value Table:
   (0): Thresh: , Exis: 1, Read: 0, OID: isValid.0 , val: 1
   (2): 02 , Comment: daysLeft, Sample: Abs, Freq: 120
         Test:  Boolean
         ObjectOwner: CLI, Object: CLI2
      Boolean Entry:
         Value: 10, Cmp: 3, Start: 1
         ObjOwn: , Obj: , EveOwn: CLI, Eve: CLI_EVENT

      Delta Value Table:
   (0): Thresh: , Exis: 1, Read: 0, OID: daysLeft.0 , val: 99999
(3): 03 , Comment: esConTabIsConnected, Sample: Abs, Freq: 60
         Test:  Boolean
         ObjectOwner: CLI, Object: CLI3
      Boolean Entry:
         Value: 0, Cmp: 2, Start: 1
         ObjOwn: , Obj: , EveOwn: CLI, Eve: CLI_EVENT

      Delta Value Table:
   (4): 04 , Comment: esConnectedSessionCount, Sample: Abs, Freq: 120
         Test:  Boolean
         ObjectOwner: CLI, Object: CLI4
      Boolean Entry:
         Value: 80, Cmp: 5, Start: 1
         ObjOwn: , Obj: , EveOwn: CLI, Eve: CLI_EVENT
```

```
      Delta Value Table:
   (5): 05 , Comment: esCifsOpenFiles, Sample: Abs, Freq: 60
         Test:  Boolean
         ObjectOwner: CLI, Object: CLI5
      Boolean Entry:
         Value: 4500, Cmp: 5, Start: 1
         ObjOwn: , Obj: , EveOwn: CLI, Eve: CLI_EVENT

      Delta Value Table:
   (6): 06 , Comment: esEvictedAge, Sample: Abs, Freq: 60
         Test:  Boolean
         ObjectOwner: CLI, Object: CLI6
      Boolean Entry:
         Value: 120960000, Cmp: 3, Start: 1
         ObjOwn: , Obj: , EveOwn: CLI, Eve: CLI_EVENT

      Delta Value Table:

Mgmt Events:
(1): Owner: CLI
  (1)Name: CLI_EVENT, Comment: , Action: Notify, Enabled: 1 Status: 1
      Notification Entry:
         ObjOwn: , Obj: , OID: 0.0

Object Table:Failures: Event = 0, Trigger = 0
```

Related Commands

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

snmp trigger

show ssh

To display the status and configuration information of the Secure Shell (SSH) service for a WAAS device, use the **show ssh** EXEC command.

show ssh

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the status and configuration of the SSH service:

```
WAE# show ssh
SSH server supports SSH2 protocol (SSH1 compatible).
Ssh service is not enabled.
Currently there are no active ssh sessions.
Number of successful SSH sessions since last reboot: 0
Number of failed SSH sessions since last reboot: 0
SSH key has not been generated or previous key has been removed.
SSH login grace time value is 300 seconds.
Allow 3 password guess(es).
```

Related Commands

(config) ssh-key-generate

(config) sshd

show standby

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

show standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

In the following sample command output, one standby group (Standby Group 1) is configured on this WAAS device. The command output also shows which member interface is the active interface. In this case, the active interface is the Gigabit Ethernet slot 1/port 0 interface.

```
WAE# show standby
Standby Group: 1
        Description: This a backup for Gigabit Ethernet 1/0.
        IP address: 192.168.10.10, netmask: 255.0.0.0
        Member interfaces:
                GigabitEthernet 2/0     priority: 100
        Active interface: GigabitEthernet 1/0
        Maximum errors allowed on the active interface: 500
```

Note To display information about a specific standby group configuration, enter the **show interface standby standby** *group_num* EXEC command.

Related Commands

show interface

show running-config

show startup-config

(config-if) standby

show startup-config

To display the startup configuration for a WAAS device, use the **show startup-config** EXEC command.

show startup-config

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this EXEC command to display the configuration used during an initial bootup, stored in NVRAM. Note the difference between the output of this command versus the **show running-config** command.

Examples

The following example displays the configuration saved for use on startup of the WAAS device:

```
WAE# show startup-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname Edge-WAE1
!
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 ip address 10.10.10.33 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
...
```

Related Commands

- configure
- copy running-config
- show running-config

show statistics authentication

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

show statistics authentication

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Authentication statistics display the number of access requests, denials, and allowances recorded. Use the **show statistics authentication** command to display the number of authentication accesses recorded.

Examples

The following example displays the statistics related to authentication on the WAAS device:

```
WAE# show statistics authentication
    Authentication  Statistics
    ---------------------------------------
    Number of access requests:        115
    Number of access deny responses:  12
    Number of access allow responses: 103
```

Related Commands

(config) authentication

clear

show authentication

show statistics content-distribution-network

To display the status of a WAE or device group that are registered with a WAAS Central Manager, use the **show statistics content-distribution-network** EXEC command. This command is available on only WAAS Central Managers.

show statistics content-distribution-network device status *device_id*

Syntax Description

device status	Displays the status of a WAE or device group that is registered with the WAAS Central Manager.
device_id	Name or ID of the device or device group.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

central-manager

Usage Guidelines

Use the **show statistics content-distribution-network** EXEC command to display the identification details about a WAE or WAEs in a device group, and verify if a WAE is online.

Examples

The following example displays the identification details of a WAE that that is registered with the WAAS Central Manager:

```
WAE# show statistics content-distribution-network device status edge-wae-11
Device id="CdmConfig_142" name="edge-wae-11" status="Online";
```

show statistics dre

To display Data Redundancy Elimination (DRE) general statistics for a WAE, use the **show statistics dre** EXEC command.

show statistics dre

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays DRE statistics:

```
WEA# show statistics dre
Cache:
   Total disk:  47622 MB, RAM size: 297 MB, Status: Usable
    Used disk:     28 MB, Oldest Data (age): 23 days 20 hours

Completed Connections: 2030
Encode:
  Overall: msg:       3620, in:   6181 KB, out:   5335 KB, ratio:  13.69%
      DRE: msg:       3620, in:   6181 KB, out:   6352 KB, ratio:   0.00%
       LZ: msg:       3619, in:   6321 KB, out:   5305 KB, ratio:  16.08%
   Bypass: msg:       3252, in:   4901 KB,
  Latency(Last 3 sec): max 3 ms, avg 0 ms
Decode:
  Overall: msg:       7162, in:   4969 KB, out:    209 MB, ratio:  97.69%
      DRE: msg:       7162, in:   5056 KB, out:    209 MB, ratio:  97.65%
       LZ: msg:        510, in:   1073 KB, out:   1160 KB, ratio:   7.46%
   Bypass: msg:         29, in:    289 KB
  Latency (Last 3 sec): max 1 ms, avg 0 ms
```

Related Commands

debug

show statistics dre connection

show statistics dre peer

show statistics dre connection

To display Data Redundancy Elimination (DRE) connection statistics for a WAE, use the **show statistics dre connection** EXEC command.

This command displays the statistics for individual TCP connections on which DRE compression is being applied. This information is updated in real time.

show statistics dre connection [**active** [**client-ip** {*ip_address* | *hostname*} | **client-port** *port* | **id** *connection_id* | **last** | **peer-no** *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*] | **client-ip** {*ip_address* | *hostname*} | **client-port** *port* | **id** *connection_id* | **last** | **peer-no** *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*]

Syntax Description

active	(Optional) Displays all active connection statistics.
client-ip	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
client-port	(Optional) Displays the connection statistics for the client with the specified port number.
id	(Optional) Displays the connection statistics for the connection with the specified identifier.
last	(Optional) Displays the last connection statistics.
peer-no	(Optional) Displays the connection statistics for the peer with the specified identifier.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port	(Optional) Displays the connection statistics for the server with the specified port number.
ip_address	The IP address of a client or server.
hostname	The hostname of a client or server.
port	The port number of a client or server (1–65535).
connection_id	A number from 0 to 4294967295 identifying a connection.
peer_id	A number from 0 to 4294967295 identifying a peer.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Using this command without any options displays a one-line summary of all the TCP connections on the WAE for which DRE is applied. To obtain detailed stastistics for a connection, use the command options to filter the connection.

Examples

The following example displays all active connection statistics:

```
WEA# show statistics dre connection
Conn-ID       Client-ip:port       Server-ip:port  Encode-in Decode-in PID Status
1151          10.10.10.10:2562     10.10.10.11:80        590  B       0  B   3 Closed-694s
1150          10.10.10.10:2561     10.10.10.11:80        590  B       0  B   3 Closed-694s
1149          10.10.10.10:2560     10.10.10.11:80       2440  B       0  B   3 Closed-694s
```

Related Commands

debug

show statistics dre connection

show statistics dre peer

To display Data Redundancy Elimination (DRE) peer statistics for a WAE, use the **show statistics dre peer** EXEC command.

show statistics dre peer {**context** *context-value* [**ip** *ip-address* | **peer-id** *peer-id* | **peer-no** *peer-no*] | **ip** *ip-address* [**context** *context-value* | **ip** *ip-address* | **peer-id** *peer-id* | **peer-no** *peer-no*] | **peer-id** *peer-id* [**context** *context-value* | **ip** *ip-address* | **peer-no** *peer-no*] | **peer-no** *peer-no* [**context** *context-value* | **ip** *ip-address* | **peer-id** *peer-id*]}

Syntax Description

context	Displays peer statistics for the specified context.
ip	(Optional) Specifies the IP address of the peer.
peer-id	(Optional) Specifies the MAC address of the peer.
peer-no	(Optional) Specifies the peer number.
context-value	The context (0–4294967295).
ip_address	The IP address of the peer.
peer-id	Peer ID (0–4294967295).
peer-no	Peer number.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays DRE peer statistics:

```
WAE# show statistics dre peer
peer-no: 0   Hostname: dc-425-jsmith
Peer-IP: 10.10.10.40   MAC-address: 00:0d:00:11:41:8e
------------------------------------------------------------------

Cache:
  Used disk: 24 MB, Age: 23 days 21 hours

Connections:
  Total (cumulative)     : 67
  Concurrent (Last 2 min): max 23, avg 22
Encode:
  Overall: msg:        278, in:   1290 KB, out:   1254 KB, ratio:   2.82%
      DRE: msg:        278, in:   1290 KB, out:   1301 KB, ratio:   0.00%
       LZ: msg:        277, in:   1271 KB, out:   1224 KB, ratio:   3.71%
   Bypass: msg:         25, in:  12638  B,
  Latency(Last 3 sec): max 3 ms, avg 0 ms
Decode:
  Overall: msg:         42, in:  34694  B, out:    147 KB, ratio:  77.05%
      DRE: msg:         42, in:    121 KB, out:    147 KB, ratio:  17.62%
       LZ: msg:         42, in:  34694  B, out:    121 KB, ratio:  72.14%
   Bypass: msg:          0, in:      0  B
  Latency (Last 3 sec): max 1 ms, avg 0 ms
```

Related Commands

debug

show statistics dre connection

show statistics epm

To display EndPoint Mapper (EPM) statistics for a WAE, use the **show statistics epm** EXEC command. This command displays the number of total requests and responses recorded.

show statistics epm

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays EPM statistics for a WAE:

```
WAE# show statistics epm
EPM statistics
--------------
Total requests        = 1108
 success              = 781
 fault                = 0
Total responses       = 781
 success              = 0
 UUID not configured  = 695
 service unavailable  = 86
 fault                = 0
```

Related Commands

(config) policy-engine application map adaptor EPM

show statistics icmp

To display ICMP statistic 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

The following example displays the ICMP-related statistics on the WAAS device:

```
WAE# show statistics icmp
ICMP statistics
---------------
ICMP messages received           = 1351
ICMP messages receive failed     = 190
 Destination unreachable         = 431
 Timeout in transit              = 1
 Wrong parameters                = 0
 Source quenches                 = 0
 Redirects                       = 0
 Echo requests                   = 729
 Echo replies                    = 0
 Timestamp requests              = 0
 Timestamp replies               = 0
 Address mask requests           = 0
 Address mask replies            = 0
ICMP messages sent               = 2280
ICMP messages send failed        = 0
 Destination unreachable         = 1551
 Time exceeded                   = 0
 Wrong parameters                = 0
 Source quenches                 = 0
 Redirects                       = 0
 Echo requests                   = 0
 Echo replies                    = 729
 Timestamp requests              = 0
 Timestamp replies               = 0
 Address mask requests           = 0
 Address mask replies            = 0
```

Related Commands

clear

show statistics ip

To display IP statistics for a WAAS device, use the **show statistics ip** EXEC command.

show statistics ip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the IP-related statistics on the WAAS device:

```
WAE# show statistics ip
IP statistics
-------------
Total packets in                = 19959308
 with invalid header            = 0
 with invalid address           = 0
 forwarded                      = 0
 unknown protocol               = 0
 discarded                      = 0
 delivered                      = 10074121
Total packets out               = 44784
 dropped                        = 0
 dropped (no route)             = 0
Fragments dropped after timeout = 0
Reassemblies required           = 0
Packets reassembled             = 0
Packets reassemble failed       = 0
Fragments received              = 0
Fragments failed                = 0
Fragments created               = 0
```

Related Commands

clear

(config) ip

(config-if) ip

show ip routes

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

The following example displays the Internet socket connection statistics on the WAAS device:

```
WAE# show statistics netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      4 10.10.41.180:23         10.10.230.11:3105       ESTABLISHED
```

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

The following example displays the RADIUS-related statistics on the WAAS device:

```
WAE# show statistics radius
  RADIUS Statistics
  ----------------------------------------------
  Authentication:
    Number of access requests:                0
    Number of access deny responses:          0
    Number of access allow responses:         0

  Authorization:
    Number of authorization requests:         0
    Number of authorization failure responses: 0
    Number of authorization success responses: 0

  Accounting:
    Number of accounting requests:            0
    Number of accounting failure responses:   0
    Number of accounting success responses:   0
```

Related Commands

clear

(config) radius-server

show radius-server

show statistics services

To display services statistics for a WAAS device, use the **show statistics services** EXEC command.

show statistics services

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the service-related statistics for each port on the WAAS device:

```
WAE# show statistics services

                    Port Statistics
              Port          Total Connections
-------------------------------------------------------------
                20                    0
                21                    0
                22                    0
                23                    0
                42                    0
                49                    0
                53                    0
                69                    0
                80                    0
               123                    0
               137                    0
               138                    0
               139                    0
               161                    0
               443                    0
               514                    0
              2048                    0
              3130                    0
```

Related Commands

show services

show statistics snmp

To display SNMP statistics for a WAAS device, use the **show statistics snmp** EXEC command.

show statistics snmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the SNMP statistics:

```
WAE# show statistics snmp
Contact: Mary Brown, system admin, mbrown@acme.com 555-1111
Location: Building 2, Floor 1, LabA
146 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    120 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    120 Set-request PDUs
146 SNMP packets output
    0 Too big errors
    2048 Maximum packet size
    0 No such name errors
    0 Bad values errors
    0 General errors
    146 Response PDUs
    0 Trap PDUs
```

See the "show snmp" commands for a description of the fields shown in the **show snmp stats** display.

Related Commands

show snmp

(config) snmp-server user

(config) snmp-server view

show statistics tacacs

To display TACACS+ authentication and authorization statistics for a WAAS device, use the **show statistics tacacs** EXEC command.

show statistics tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the TACACS+-related statistics on the WAAS device:

```
WAE# show statistics tacacs
TACACS+ Statistics
-----------------------------------------------------------
Authentication:
  Number of access requests:                  3
  Number of access deny responses:            1
  Number of acess allow responses:              2

Authorization:
  Number of authorization requests:           1
  Number of authorization failure responses:  0
  Number of authorization success responses:  1
```

Related Commands

clear

(config) tacacs

show tacacs

show statistics tcp

To display TCP statistics for a WAAS device, use the **show statistics tcp** EXEC command.

show statistics tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the TCP-related statistics on the WAAS device:

```
WAE# show statistics tcp
TCP statistics
--------------
Server connection openings                  = 12
Client connection openings                  = 194
Failed connection attempts                  = 0
Connections established                     = 0
Connections resets received                 = 0
Connection resets sent                      = 7791
Segments received                           = 11368
Segments sent                               = 10895
Bad segments received                       = 0
Segments retransmitted                      = 28
Retransmit timer expirations                = 28
Server segments received                    = 135
Server segments sent                        = 143
Server segments retransmitted               = 0
Client segments received                    = 3438
Client segments sent                        = 10752
Client segments retransmitted               = 28

TCP extended statistics
-----------------------
Sync cookies sent                           = 0
Sync cookies received                       = 0
Sync cookies failed                         = 0
Embryonic connection resets                 = 0
Prune message called                        = 0
Packets pruned from receive queue           = 0
Out-of-order-queue pruned                   = 0
Out-of-window Icmp messages                 = 0
Lock dropped Icmp messages                  = 0
Arp filter                                  = 0
Time-wait sockets                           = 10
```

```
Time-wait sockets recycled                          = 0
Time-wait sockets killed                            = 0
PAWS passive                                        = 0
PAWS active                                         = 0
PAWS established                                    = 0
Delayed acks sent                                   = 82
Delayed acks blocked by socket lock                 = 0
Delayed acks lost                                   = 5
Listen queue overflows                              = 0
Connections dropped by listen queue                 = 0
TCP packets queued to prequeue                      = 0
TCP packets directly copied from backlog            = 0
TCP packets directly copied from prequeue           = 0
TCP prequeue dropped packets                        = 0
TCP header predicted packets                        = 324
Packets header predicted and queued to user         = 0
TCP pure ack packets                                = 1340
TCP header predicted acks                           = 106
TCP Reno failures                                   = 0
TCP SACK failures                                   = 1
TCP loss failures                                   = 0
TCP fast retransmissions                            = 0
TCP forward retransmissions                         = 0
TCP slowstart retransmissions                       = 0
TCP Timeouts                                        = 12
TCP Reno recovery fail                              = 0
TCP Sack recovery fail                              = 0
TCP scheduler failed                                = 0
TCP receiver collapsed                              = 0
TCP DSACK old packets sent                          = 12
TCP DSACK out-of-order packets sent                 = 0
TCP DSACK packets received                          = 0
TCP DSACK out-of-order packets received             = 0
TCP connections abort on sync                       = 0
TCP connections abort on data                       = 0
TCP connections abort on close                      = 0
TCP connections abort on memory                     = 0
TCP connections abort on timeout                    = 3
TCP connections abort on linger                     = 0
TCP connections abort failed                        = 0
TCP memory pressures                                = 0
```

Related Commands

clear

show tcp

(config) tcp

show statistics tfo

To display Traffic Flow Optimization (TFO) statistics for a WAE, use the **show statistics tfo** EXEC command.

show statistics tfo [**application** *app-name* | **pass-through** | **peer** | **saving** *app-name*]

Syntax Description

application	(Optional) Displays statistics per application.
app-name	The application name.
pass-through	(Optional) Displays the pass-through statistics.
peer	(Optional) Displays peer information.
saving	(Optional) Displays savings for all applications.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays TFO statistics for the application Other on a WAE:

```
WAE# show statistics tfo application Other
Application           In                    out
                      --------------------- ---------------------
Other
Optimized:
     Bytes                               0                     0
     Packets                             0                     0
Non Optimized:
     Bytes                           35448                 22664
     Packets                           554                   531
Internal Client:
     Bytes                               0                     0
     Packets                             0                     0
Internal Server:
     Bytes                          347701               1248795
     Packets                          4759                  4586
PT No Peer:
     Bytes                               0                     0
     Packets                             0                     0
PT Configured:
     Bytes                               0                     0
     Packets                             0                     0
PT Intermediate:
     Bytes                               0                     0
```

Related Commands

show tfo accelerators

show tfo bufpool

show tfo connection

show tfo status

show statistics udp

To display User Datagram Protocol (UDP) statistics for a WAAS device, use the **show statistics udp** EXEC command.

show statistics udp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the UDP-related statistics on the WAAS device:

```
WAE# show statistics udp
UDP statistics
--------------
Packets received                 = 222616
Packets to unknown port received = 904
Packet receive error             = 0
Packet sent                      = 25821
```

show statistics wccp

To display WCCP statistics for a WAE, use the **show statistics wccp** EXEC command.

show statistics wccp gre

Syntax Description		
	gre	Displays WCCP generic routing encapsulation packet-related statistics.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

GRE is a Layer 3 technique that allows datagrams to be encapsulated into IP packets at the WCCP-enabled router and then redirected to a WAE (the transparent proxy server). At this intermediate destination, the datagrams are decapsulated and then routed to an origin server to satisfy the request if a cache miss occurs. In doing so, the trip to the origin server appears to the inner datagrams as one hop. Usually, the redirected traffic using GRE is referred to as GRE tunnel traffic. With GRE, all redirection is handled by the router software.

With WCCP redirection, a Cisco router does not forward the TCP SYN packet to the destination because the router has WCCP enabled on the destination port of the connection. Instead, the WCCP-enabled router encapsulates the packet using GRE tunneling and sends it to the WAE that has been configured to accept redirected packets from this WCCP-enabled router.

After receiving the redirected packet, the WAE does the following:

1. Strips the GRE layer from the packet.
2. Decides whether it should accept this redirected packet and process the request for the content as follows:
   a. If the WAE accepts the request, it sends a TCP SYN ACK packet to the client. In this response packet, the WAE uses the IP address of the original destination (origin server) that was specified as the source address so that the WAE can be invisible (transparent) to the client; it acts as if it is the destination that the client's TCP SYN packet was trying to reach.
   b. If the WAE does not accept the request, it reencapsulates the TCP SYN packet in GRE and sends it back to the WCCP-enabled router. The router identifies that the WAE is not interested in this connection and forwards the packet to its original destination (the origin server).

For example, a WAE would not accept the request because it is configured to bypass requests that originate from a certain set of clients or that are destined to a particular set of servers.

Examples

The following example displays WCCP GRE statistics for the WAE:

```
WAE# show statistics wccp gre
Transparent GRE packets received:           3000622
Transparent non-GRE packets received:       0
Transparent non-GRE packets passed through: 0
Total packets accepted:                     245
Invalid packets received:                   0
Packets received with invalid service:      0
Packets received on a disabled service:     0
Packets received too small:                 0
Packets dropped due to zero TTL:            0
Packets dropped due to bad buckets:         0
Packets dropped due to no redirect address: 0
Packets dropped due to loopback redirect:   0
Connections bypassed due to load:           0
Packets sent back to router:                168
Packets sent to another WAE:                 0
GRE fragments redirected:                   0
Packets failed GRE encapsulation:           0
Packets dropped due to invalid fwd method:  0
Packets dropped due to insufficient memory: 0
Packets bypassed, no conn at all:           0
Packets bypassed, no pending connection:    168
Packets due to clean wccp shutdown:         0
Packets bypassed due to bypass-list lookup: 0
Packets received with client IP addresses:  0
Conditionally Accepted connections:         0
Conditionally Bypassed connections:         0
L2 Bypass packets destined for loopback:    0
Packets w/WCCP GRE received too small:      0
Packets dropped due to IP access-list deny: 3000209
Packets fragmented for bypass:              0
Packets dropped due to no route found       0
WAE#
```

The following table describes the fields shown in the **show statistics wccp gre** display.

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 Services Switch [CSS]) that redirects requests transparently to the WAE.
Transparent non-GRE packets passed through	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.

Field	Description
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the redirected packet's IP header has a zero TTL.
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
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.
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.

Field	Description
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no conn at all	Number of packets that failed to be associated with an existing flow because no TCP port was listening. WCCP can also handle asymmetric packet flows and always maintains a consistent mapping of web servers to caches regardless of the number of switches or routers used in a WCCP service group (up to 32 routers or switches communicating with up to 32 WAEs in a cluster).
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.
Packets due to clean wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Packets received with client IP addresses	Number of packets that are associated to a connection flow that is being spoofed. By spoofing a client's IP address, the WAE can receive packets with the client IP (which is different from the WAE's own IP address) and send the packet to the correct application that is waiting for the packet.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
L2 Bypass packets destined for loopback	Number of packets that are dropped by the WAE due to the destination IP address being the loopback address when the WCCP-enabled router or switch tries to perform Layer 2 redirection.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).

Field	Description
Packets fragmented for bypass	Number of GRE packets that do not contain enough data to hold an IP header.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.

Related Commands

(config) wccp access-list

(config) wccp cifs-cache

(config) wccp flow-redirect

(config) wccp router-list

(config) wccp shutdown

(config) wccp slow-start

(config) wccp tcp-promiscuous

(config) wccp tcp-promiscuous

show statistics windows-domain

To display Windows domain server information for a WAAS device, use the **show 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

After entering the s**how windows-domain** EXEC command to view the Windows domain server statistics, you can clear the counters for these statistics by entering the **clear statistics windows-domain** EXEC command.

Examples

The following example displays the Windows domain server statistics:

```
WAE# show statistics windows-domain
Windows Domain Statistics
  ------------------------------------------------
  Authentication:
    Number of access requests:                    9
    Number of access deny responses:              3
    Number of access allow responses:             6
  Authorization:
    Number of authorization requests:             9
    Number of authorization failure responses:    3
    Number of authorization success responses:    6
  Accounting:
    Number of accounting requests:                0
    Number of accounting failure responses:       0
    Number of accounting success responses:       0
```

Related Commands

windows-domain

(config) windows-domain

show sysfs

To display system file system (sysfs) information for a WAAS device, use the **show sysfs** EXEC command.

show sysfs volumes

Syntax Description

This command has no arguments or keywords.

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

The following example displays the disk volume number and its size:

```
WAE# show sysfs volumes
sysfs 00: /local/local1 17775600KB 96% free
sysfs 01: /local/local2 17782768KB 99% free
sysfs 02: /local/local3 17782768KB 99% free
sysfs 03: /local/local4 17782768KB 99% free
sysfs 04: /local/local5 15684592KB 99% free
```

Related Commands

disk

(config) disk

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

The following example displays the TACACS+ configuration on the WAAS device:

```
WAE# show tacacs
    Login Authentication for Console/Telnet Session: disabled
    Configuration Authentication for Console/Telnet Session: disabled

    TACACS+ Configuration:
    ----------------------
    TACACS+ Authentication is off
    Key        =
    Timeout    = 5
    Retransmit = 2
    Password type: pap

    Server                          Status
    ------------------------------  ------
    192.168.2.5                     primary
```

The following table describes the fields shown in the **show tacacs** display.

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.

Field	Description
Key	Secret key that the WAE uses to communicate with the TACACS+ server. The maximum number of characters in the TACACS+ key should not exceed 99 printable ASCII characters (except tabs).
Timeout	Number of seconds that the WAAS device waits for a response from the specified TACACS+ authentication server before declaring a timeout.
Retransmit	Number of times that the WAAS device is to retransmit its connection to the TACACS+ if the TACACS+ timeout interval is exceeded.
Password type	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.
Server	Hostname or IP address of the TACACS+ server.
Status	Indicates whether server is the primary or secondary host.

Related Commands

clear

show statistics tacacs

show tacacs

(config) tacacs

show tcp

To display TCP configuration information for a WAAS device, use the **show tcp** EXEC command.

show tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the TCP configuration on the WAAS device:

```
WAE# show tcp
==TCP Configuration==
TCP keepalive timeout 90 sec
TCP keepalive probe count 4
TCP keepalive probe interval 75 sec
TCP explicit congestion notification disabled
TCP cwnd base value 2
TCP initial slowstart threshold value 2
TCP increase(multiply) retransmit timer by 1
TCP memory_limit - Low water mark:  360 MB, High water mark (pressure): 380 MB,
High water mark (absolute): 400 MB
```

Related Commands

clear

show statistics tcp

(config) tcp

show tech-support

To view information necessary for Cisco's TAC to assist you, use the **show tech-support** EXEC command.

show tech-support [**page**]

Syntax Description

page	(Optional) Pages through output.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this command to view system information necessary for TAC to assist you with a WAAS device. We recommend that you log the output to a disk file. (See the "(config) logging" command.)

Examples

The following example displays technical support information:

Note Because the **show tech-support** command output can be long, excerpts are shown in the 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)
...
```

show telnet

To display Telnet services configuration for a WAAS device, use the **show telnet** EXEC command.

show telnet

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays whether or not Telnet is enabled on the WAAS device:

```
WAE# show telnet
telnet service is enabled
```

Related Commands

telnet

(config) telnet enable

(config) exec-timeout

show tfo accelerators

To display Traffic Flow Optimization (TFO) accelerators information for a WAE, use the **show tfo accelerators** EXEC command.

show tfo accelerators

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays TFO accelerator information for the WAE:

```
WAE# show tfo accelerators
Name: TFO                    State: Registered,  Handling Level: 100%
  Keepalive timeout: 3.0 seconds,  Session timeouts: 0,  Total timeouts: 0
  Last keepalive received 00.5 Secs ago
  Last registration occurred 11:21:43:38.4 Days:Hours:Mins:Secs ago
Name: EPM                    State: Registered,  Handling Level: 100%
  Keepalive timeout: 5.0 seconds,  Session timeouts: 0,  Total timeouts: 0
  Last keepalive received 00.2 Secs ago
  Last registration occurred 11:21:43:36.7 Days:Hours:Mins:Secs ago
Name: CIFS                   State: Not Registered,  Handling Level: 0%
  Keepalive timeout: 0.0 seconds,  Session timeouts: 0,  Total timeouts: 0
  Last keepalive received -Never-
  Last Registration occurred -Never-
```

Related Commands

show tfo auto-discovery

show tfo bufpool

show tfo connection

show tfo filtering

show tfo status

show tfo auto-discovery

To display Traffic Flow Optimization (TFO) auto-discovery statistics for a WAE, use the **show tfo auto-discovery** EXEC command.

show tfo auto-discovery

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays TFO auto-discovery statistics for the WAE:

```
WAE# show tfo auto-discovery
Auto discovery structure allocations failure:         0
Auto discovery structure allocations success:         8207
Auto discovery structure deallocations:               8207
Auto discovery table bucket overflows:                0
Auto discovery table overflows:                       0
Auto discovery table entry adds:                      8207
Auto discovery table entry drops:                     8207
Auto discovery table lookups:                         8207
Auto discovery table entry count:                     0
Packets sent during auto discovery:                   8207
Packets received during auto discovery:               16414
Number of route lookup failures:                      0
Number of successful route lookups:                   0
Bind hash add failures:                               0
Accept socket pair allocation failures:               0
Sock allocation failures:                             0
Sock(u) allocation failures:                          0
Connect socket lookup failures:                       0
Auto discovery failures:                              8207
Number of resets received during auto discovery:      0
Packet memory allocation failures:                    0
Auto discovery failures due to insuff. option space:  0
Invalid connection state during auto discovery:       0
Auto discovery failures due to missing ack conf:      0
Successful auto discovery to internal server:         0
Successful auto discovery to external server:         0
Successful auto discovery for an internal client:     0
Successful auto discovery for an external client:     0
Intermediate device:                                  0
SYNs found with our device id:                        0
```

Related Commands

show statistics tfo
show tfo accelerators
show tfo bufpool
show tfo connection
show tfo filtering
show tfo status

show tfo bufpool

To display Traffic Flow Optimization (TFO) buffer pool information for a WAE, use the **show tfo bufpool** EXEC command.

show tfo bufpool {**accounting** | **from-index** *index* | **owner-connection** *conn-id* | **owner-module** {**RElib** | **tcpproxy**} [**from-index** *index* | **owner-connection***conn-id* | **state** {**free** | **in-use**} [**from-index** *index* | **owner-connection** *conn-id* | **to-index** *index*] | **to-index** *index*] | **state** {**free** | **in-use**} [**from-index** *index* | **owner-connection***conn-id* | **to-index** *index*] | **to-index** *index*}

Syntax Description

accounting	Displays the buffer pool overall usage.
from-index	The starting index of the buffer units to be displayed.
owner-connection	The owner connection of the buffer units.
owner-module	The owner module of the buffer units.
state	The state (free or used) of the buffer units.
to-index	The ending index of the buffer units to be displayed.
RElib	Shows the buffer units owned by the RE-library.
tcpproxy	Shows the buffer units owned by the TCP proxy.
index	Index of a buffer unit (0–4294967295).
conn-id	The connection ID (0–4294967295).

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays TFO buffer pool information for the WAE:

```
WAE# show tfo bufpool accounting
Total buffer pool size: 80740352 bytes
Free buffer: 80740352 bytes, in 78848 units (unit size: 1024 bytes)
Used buffer: 0 bytes, in 0 units
      Buffer usage by module:
          Tcpproxy: using 0 bytes, in 0 units
          RElib: using 0 bytes, in 0 units
          LZlib: using 0 bytes, in 0 units
      Buffer usage by connection:
```

Related Commands

show tfo accelerators
show tfo auto-discovery
show tfo connection
show tfo filtering
show tfo status
show statistics tfo

show tfo connection

To display Traffic Flow Optimization (TFO) connection information for a WAE, use the **show tfo connection** EXEC command.

show tfo connection [[summary] | [client-ip *host-address* **| client-port** *port* **| peer-id** *mac* **| server-ip** *host-address* **| server-port** *port*]]

Syntax Description

summary	(Optional) Displays a summary list of connections.
client-ip	(Optional) Source IP address.
client-port	(Optional) IP address of the source client.
peer-id	(Optional) Displays the connection statistics for a specific peer.
server-ip	(Optional) IP address of the destination server.
server-port	(Optional) Destination port number.
host-address	Hostname or IP address.
mac	The MAC address of a peer host.
port	The port number on the client or server.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Using this command without options displays detailed information about each of the TFO connections for a WAE. To display a summary list of the connections, use the **summary** option.

For the listed connections that have the F, D or L optimization policy, you can find additional information on DRE statistics by using the **show statistics dre connection** command with the **id** option to identify a specific connection id.

Examples

The following example displays a summary of TFO optimized connections for the WAE:

```
WAE# show tfo connection summary

Optimized Connection List
Policy summary order: Our's, Peer's, Negotiated, Applied
F: Full optimization, D: DRE only, L: LZ Compression, T: TCP Optimization

Local-IP:Port         Remote-IP:Port        ConId   PeerId            Policy
10.77.156.99:59950    10.77.156.106:10005   21      00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59951    10.77.156.106:10007   22      00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59952    10.77.156.106:10008   23      00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59953    10.77.156.106:10009   24      00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59954    10.77.156.106:10010   25      00:11:25:ac:3e:04 F,F,F,F
```

Related Commands

- show statistics dre connection
- show statistics tfo
- show tfo accelerators
- show tfo auto-discovery
- show tfo bufpool
- show tfo filtering
- show tfo status

show tfo filtering

To display information about the incoming and outgoing TFO flows that the WAE currently has, use the **show tfo filtering** EXEC command.

show tfo filtering [**list**]

Syntax Description

list	(Optional) Lists TCP flows that the WAE is currently optimizing or passing through.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

This command lists TCP flows that the WAE is currently optimizing. It also includes TCP flows that are not being optimized but that are being passed through by the WAE. A "P" in the State column indicates a passed through flow.

Examples

The following examples display TFO connection information for the WAE:

```
WAE# show tfo filtering
Number of filtering tuples:                          2
Packets dropped due to ttl expiry:                   0
Packets dropped due to bad route:                    0
Syn packets dropped with our own id in the options:  0
Syn packets received and dropped on estab. conn:     0
Syn-Ack packets received and dropped on estab. conn: 0
Packets recvd on in progress conn. and not handled:  0
Packets dropped due to peer connection alive:        0
Packets dropped due to invalid TCP flags:            0


WAE# show tfo filtering list
E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough
B: Bypass, T: Timedout, C: Closed

    Local-IP:Port        Remote-IP:Port          Tuple(Mate)       State
   10.99.11.200:1398    10.99.22.200:80    0xcba709c0(0xcba70a00)   E
   10.99.11.200:1425    10.99.22.200:80    0xcba70780(0xcba707c0)   E
   10.99.11.200:1439    10.99.22.200:5222  0xcba703c0(0xcba70b40)   Sr
   10.99.11.200:1440    10.99.22.200:5222  0xcba70400(0xcba70440)   Sr
   10.99.22.200:1984    10.99.11.200:80    0xcba70600(0xcba70640)   E
   10.99.22.200:1800    10.99.11.200:23    0xcba70480(0x0       )   PE
   10.99.11.200:1392    10.99.22.200:80    0xcba70f80(0x0       )   E
   10.99.22.200:20      10.99.11.200:1417  0xcba701c0(0xcba70180)   E
   10.99.11.200:1417    10.99.22.200:20    0xcba70180(0x0       )   E
   10.99.22.200:1987    10.99.11.200:80    0xcba70240(0xcba70200)   E
   10.99.11.200:1438    10.99.22.200:5222  0xcba70900(0xcba70580)   Sr
   10.99.22.200:1990    10.99.11.200:80    0xcba70100(0xcba70140)   E
   10.99.22.200:80      10.99.11.200:1426  0xcba70740(0xcba70700)   E
```

```
10.99.22.200:80       10.99.11.200:1425  0xcba707c0(0xcba70780)   E
10.99.22.200:1985     10.99.11.200:80    0xcba70a40(0xcba70a80)   E
10.99.22.200:80       10.99.11.200:1410  0xcba70500(0xcba70540)   E
10.99.22.200:80       10.99.11.200:1398  0xcba70a00(0xcba709c0)   E
10.99.22.200:80       10.99.11.200:1392  0xcba70f40(0xcba70f80)   E
```

Related Commands

show tfo accelerators

show tfo auto-discovery

show tfo bufpool

show tfo connection

show tfo status

show tfo status

To display global Traffic Flow Optimization (TFO) status information for a WAE, use the **show tfo status** EXEC command.

show tfo status

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example displays global TFO status information for the WAE:

```
WEA# show tfo status
Optimization Status:
     Configured: optimize full
     Current: optimize full
  TFO is up since Sat Feb 25 13:18:51 2006
  TFO is functioning normally.
  Total number of optimized connections since start:       0
  Number of active connections:                            0
  Total number of peers:                                   0
```

Related Commands

show statistics tfo

show tfo accelerators

show tfo auto-discovery

show tfo bufpool

show tfo connection

show tfo filtering

show 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

To display information about the current configuration of transaction logging on a WAE, use the **show transaction-log** or **show transaction-logging** EXEC commands. Both of these EXEC commands display the same output. Transaction log file information is displayed for HTTP and WMT MMS caching proxy transactions and TFTP and ICAP transactions.

Note For security reasons, passwords are never displayed in the output of the **show transaction-log** EXEC command.

Examples

The following example displays information about the current configuration of transaction logging on a WAE:

```
WAAE# show transaction-logging
Transaction log configuration:
--------------------------------------
TFO Logging is disabled.
TFO Archive interval: every-day every 1 hour
TFO Maximum size of archive file: 2000000 KB

TFO logging to remote syslog host is disabled.
TFO remote syslog host is not configured.
TFO facility is the default "*" which is "user".

Exporting files to ftp servers is disabled.
```

Related Commands

clear

transaction-log

(config) transaction-logs

show user

To display user identification number and username information for a particular user of a WAAS device, use the **show user** EXEC command.

show user {**uid** *number* | **username** *name*}

Syntax Description

uid	Displays user information based on the identification number of the user.
number	Identification number (0–65535).
username	Displays user information based on the name of the user.
name	Name of user.

Command Default

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following examples display user-specific configuration information based on username and user identification, respectively:

```
WAE# show user username jdoe
Uid                 : 1426
Username            : jdoe
Password            : *****
Privilege           : super user
Configured in       : Local database

WAE# show user uid 1426
Uid                 : 1426
Username            : jdoe
Password            : *****
Privilege           : super user
Configured in       : Local database
```

Related Commands

clear

show users administrative

(config) username

show users administrative

To display users with administrative privileges to the WAAS device, use the **show users** EXEC command.

show users administrative

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 displays user who have administrative privileges:

```
WAE# show users administrative
       UID USERNAME
         0 admin
```

Related Commands

clear

(config) username

show version

To display version information about the WAAS software that is running on the WAAS device, use the **show version** EXEC command.

show version [last | pending]

Syntax Description

last	Displays the version information for the last saved image.
pending	Displays the version information for the pending upgraded image.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays the version information for the last saved image:

```
WAE# show version last
Saved version is WAAS 4.0.0-b330, built on 18:28:11 Mar 23 2006 by cnbuild
It can be restored by running restore rollback command
```

The following example displays the version information for the pending upgraded image:

```
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.0 (build b340 Mar 25 2
006)
Version: fe611-4.0.0.340

Compiled 17:26:17 Mar 25 2006 by cnbuild

System was restarted on Mon Mar 27 15:25:01 2006.
The system has been up for 3 days, 21 hours, 26 minutes, 15 seconds.
```

show wccp

To display Web Cache Connection Protocol (WCCP) information for a WAE, use the **show wccp** EXEC command.

show wccp file-engines

show wccp flows {**cifs-cache** | **tcp-promiscuous**} [**summary**]

show wccp gre

show wccp masks {**cifs-cache** | **tcp-promiscuous**} [**summary**]

show wccp modules

show wccp routers

show wccp services [**detail**]

show wccp slowstart {**cifs-cache** | **tcp-promiscuous**} [**summary**]

show wccp status

Syntax Description

file-engines	Displays which WAEs are seen by which routers.
flows	Displays WCCP packet flows.
cifs-cache	Displays CIFS caching service packet flows.
tcp-promiscuous	Displays TCP-PROMISCUOUS caching service packet flows.
summary	(Optional) Displays summarized information about CIFS caching service packet flows or TCP-PROMISCUOUS caching service packet flows.
gre	Displays WCCP generic routing encapsulation packet-related information.
masks	Displays WCCP mask assignments for a given service.
modules	Displays running status of WCCP registered modules.
routers	Displays routers seen and not seen by this WAE.
services	Displays WCCP services configured.
detail	(Optional) Displays detail of services.
slowstart	Displays WCCP slow start state for the selected service.
status	Displays version of WCCP that is enabled and running.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows the output of the **show wccp gre** command:

```
WAE# show wccp gre
Transparent GRE packets received:           0
Transparent non-GRE packets received:       0
Transparent non-GRE packets passed through: 0
Total packets accepted:                     0
Invalid packets received:                   0
Packets received with invalid service:      0
Packets received on a disabled service:     0
Packets received too small:                 0
Packets dropped due to zero TTL:            0
Packets dropped due to bad buckets:         0
Packets dropped due to no redirect address: 0
Packets dropped due to loopback redirect:   0
Connections bypassed due to load:           0
Packets sent back to router:                0
Packets sent to another CE:                 0
GRE fragments redirected:                   0
Packets failed GRE encapsulation:           0
Packets dropped due to invalid fwd method:  0
Packets dropped due to insufficient memory: 0
Packets bypassed, no conn at all:           0
Packets bypassed, no pending connection:    0
Packets due to clean wccp shutdown:         0
Packets bypassed due to bypass-list lookup: 0
```

For a description of the fields in the output of the **show wccp gre** command, see the **show statistics wccp** command.

The following example shows the output of the **show wccp modules** command:

```
WAE# show wccp modules

Modules registered with WCCP on this WAE

Module  Socket  Expire(sec)  Name            Supported Services
------  ------  -----------  --------------- ------------------
0       18      3            ?            CIFS Cache
```

The following example shows the output of the **show wccp services** command:

```
WAE# show wccp services
Services configured on this File Engine
        TCP Promiscuous 61
        TCP Promiscuous 62
```

The following example is partial output from the **show wccp services detail** command:

```
WAE# show wccp services detail
Service Details for TCP Promiscuous 61 Service
       Service Enabled                   : Yes
       Service Priority                  : 34
       Service Protocol                  : 6
       Application                       : Unknown
       Service Flags (in Hex)            : 501
       Service Ports                     :      0     0     0     0
                                         :      0     0     0     0
       Security Enabled for Service      : No
       Multicast Enabled for Service     : No
       Weight for this Web-CE            : 0
       Negotiated forwarding method      : GRE
       Negotiated assignment method      : HASH
       Negotiated return method          : GRE
       Received Values:
```

```
        Source IP mask (in Hex)             : 0
        Destination IP mask (in Hex)        : 0
        Source Port mask (in Hex)           : 0
        Destination Port mask (in Hex)      : 0
        Calculated Values:
        Source IP mask (in Hex)             : 0
        Destination IP mask (in Hex)        : 1741
        Source Port mask (in Hex)           : 0
        Destination Port mask (in Hex)      : 0

Service Details for TCP Promiscuous 62 Service
        Service Enabled                     : Yes
        Service Priority                    : 34
        Service Protocol                    : 6
        Application                         : Unknown
        Service Flags (in Hex)              : 502
        Service Ports                       :      0     0     0     0
                                            :      0     0     0     0
        Security Enabled for Service        : No
        Multicast Enabled for Service       : No
        Weight for this Web-CE              : 0
        Negotiated forwarding method        : GRE
        Negotiated assignment method        : HASH
        Negotiated return method            : GRE
        Received Values:
        Source IP mask (in Hex)             : 0
        Destination IP mask (in Hex)        : 0
        Source Port mask (in Hex)           : 0
        Destination Port mask (in Hex)      : 0
        Calculated Values:
        Source IP mask (in Hex)             : 0
        Destination IP mask (in Hex)        : 1741
        Source Port mask (in Hex)           : 0
        Destination Port mask (in Hex)      : 0
```

The following example is the output from the **show wccp routers** command:

```
WAE# show wccp routers
Router Information for Service: TCP Promiscuous 61
       Routers Configured and Seeing this File Engine(1)
               Router Id        Sent To        Recv ID
               0.0.0.0          10.10.20.1     00000000
       Routers not Seeing this File Engine
               10.10.20.1
       Routers Notified of but not Configured
               -NONE-
       Multicast Addresses Configured
               -NONE-
Router Information for Service: TCP Promiscuous 62
       Routers Configured and Seeing this File Engine(1)
               Router Id        Sent To        Recv ID
               0.0.0.0          10.10.20.1     00000000
       Routers not Seeing this File Engine
              10.10.20.1
       Routers Notified of but not Configured
               -NONE-
       Multicast Addresses Configured
               -NONE-
```

The following example is the output from the **show wccp status** command:

```
WAE# show wccp status
WCCP version 2 is enabled and currently active
```

Related Commands

(config) wccp access-list

(config) wccp cifs-cache

(config) wccp flow-redirect

(config) wccp router-list

(config) wccp shutdown

(config) wccp slow-start

(config) wccp tcp-promiscuous

(config) wccp version

show windows-domain

To display Windows domain configuration information for a WAAS device, use the **show windows-domain** EXEC command.

show windows-domain

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example displays Windows domain configuration information:

```
WAE# show windows-domain
Login Authentication for Console/Telnet Session: disabled
  Configuration Authentication for Console/Telnet Session: disabled

  Windows domain Configuration:
  -----------------------------
    Workgroup:
    Comment:
    Net BIOS:
    Realm:
    WINS Server: 0.0.0.0
    Password Server: 0.0.0.0
    Security: domain
    Administrative groups:
      Super user group:
      Normal user group:
```

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.

The following table describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

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 1 or SSH version 2) to perform shutdown on a WAAS device.

To perform a shutdown on a WAAS device, enter the **shutdown** EXEC command as follows:

```
WAE# shutdown
```

When you are asked if you want to save the system configuration, enter **yes**.

```
System configuration has been modified. Save?[yes]:yes
```

When you are asked if you want to proceed with the shutdown, press **Enter** to proceed with the shutdown operation.

```
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
```

A message appears, reporting that all services are being shut down on this WAE.

```
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

After the system is shut down (the system has halted), a WAAS software shutdown shell displays the current state of the system (for example, "System has been shut down") on the console. You are asked whether you want to perform a software power off (the **Power down system by software** option), or if you want to reload the system through the software.

```
================= SHUTDOWN SHELL =================
System has been shut down.
You can either
   Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

To power down the WAAS device, press and hold the power button on the WAAS device, or use one of the following methods to perform a shutdown poweroff:

- From the console command line, enter **2** when prompted, as follows:

```
================= SHUTDOWN SHELL =================
System has been shut down.
You can either
   Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

- From the WAAS CLI, enter the **shutdown poweroff** EXEC command as follows:

```
WAE# shutdown poweroff
```

When you are asked if you want to save the system configuration, enter **yes**.

```
System configuration has been modified. Save?[yes]:yes
```

When you are asked to confirm your decision, press **Enter**.

```
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

Examples

In the following example, the **shutdown** command is used to close all applications and stop all system activities.

```
WAE1# shutdown
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

In the following example, the **shutdown poweroff** command is used to close all applications, stop all system activities, and then turn off power to the WAAS device.

```
WAE2# shutdown poweroff
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

snmp trigger

To configure thresholds for a user-selected MIB object for monitoring purposes on a WAAS device, use the **snmp trigger** EXEC command. Use the **no** form of this command to return the setting to the default value.

snmp trigger {**create** *mibvar* [**wildcard**] [*wait-time* [**absent** [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **equal** [**absolute** *value* [[*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] | **falling** [**absolute** *value* [*LINE* | **mibvar1** *mibvar*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] | **greater-than** [**absolute** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] | **less-than** [**absolute** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] | **on-change** [[*LINE* | **mibvar1** *mibvar1*][*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] | **present** [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **rising** [**absolute** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]]] | **delete** *mibvar*}

Syntax Description

create	Configure a threshold for a MIB object.
mibvar	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) Treat the specified MIB variable name as having a wildcard.
wait-time	Number of seconds, 60-600, to wait between trigger samples.
absent	(Optional) Apply the absent existence test.
LINE	Description of the threshold being created.
mibvar1, mibvar2, mibvar3	(Optional) Add a MIB object to the notification.
mibvar1, mibvar2, mibvar3	Name of the MIB object to add to the notification.
equal	Apply the equality threshold test.
absolute	(Optional) Use an absolute sample type.
value	(Optional) Absolute or delta value for sample.
delta	Use a delta sample type.
falling	Apply the falling threshold test.
greater-than	Apply the greater-than threshold test.
less-than	Apply the less-than threshold test.
on-change	Apply the changed existence test.
present	Apply the present test.
rising	Apply the rising threshold test.
delete	Remove a threshold for a MIB object.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Using the **snmp trigger** global configuration command, you can define additional SNMP traps for other MIB objects of interest to your particular configuration. You can select any MIB object from any of the support MIBs for your trap. The trap can be triggered based on a variety of tests:

- absent—A specified MIB object that was present at the last sampling is no longer present as of the current sampling.
- equal—The value of the specified MIB object is equal to the specified threshold.
- falling—The value of the specified MIB object has fallen below the specified threshold value. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value rises above the threshold value and then falls below the falling threshold value again.
- greater-than—The value of the specified MIB object is greater than the specified threshold value.
- less-than—The value of the specified MIB object is less than the specified threshold value.
- on-change—The value of the specified MIB object has changed since the last sampling.
- present—A specified MIB object is present as of the current sampling that was not present at the previous sampling.
- rising—The value of the specified MIB object has risen above the specified threshold. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value falls below the threshold value and then rises above the rising threshold value again.

The threshold value can be based on an *absolute* sample type or on a *delta* sample type. An absolute sample type is one in which the test is evaluated against a fixed integer value between zero and 4294967295. A delta sample type is one in which the test is evaluated against the change in the MIB object value between the current sampling and the previous sampling.

After you configure SNMP traps, you must use the **snmp-server enable traps event** global configuration command for the event traps you just created to be generated. Also, to preserve SNMP trap configuration across a system reboot, you must configure event persistence using the **snmp mib persist event** global configuration command, and save the MIB data using the **write mib-data** EXEC command.

Examples

The following example shows how to create a threshold for the MIB object *esConTabIsConnected* so that a trap is sent when the connection from the Edge WAE to the Core WAE is lost:

```
WAE# snmp trigger create esConTabIsConnected ?
  <60-600>  The number of seconds to wait between trigger sample
  wildcard  Option to treat the MIB variable as wildcarded
WAE# snmp trigger create esConTabIsConnected wildcard 600 ?
  absent        Absent existence test
  equal         Equality threshold test
  falling       Falling threshold test
  greater-than  Greater-than threshold test
  less-than     Less-than threshold test
  on-change     Changed existence test
  present       Present present test
  rising        Rising threshold test
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling ?
  absolute Absolute sample type
  delta   Delta sample type
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute ?
  <0-4294967295>  Falling threshold value
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 ?
  LINE     Trigger-comment
  mibvar1  Optional mib object to add to the notification
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 "Lost the
connection with the core server."
WAE# configure
WAE(config)# snmp-server enable traps event
```

Once you have configured the WAE to send SNMP traps, you can view the results of these newly created traps using the **show snmp events** EXEC command.

You can also delete user-created SNMP traps. The following example shows how to delete the trap set for *esConTabIsConnected* that we created in the previous example.

```
WAE# snmp trigger delete esConTabIsConnected
```

Related Commands

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

ssh

To allow secure encrypted communications between an untrusted client machine and a WAAS device over an insecure network, use the **ssh** EXEC command.

ssh *options*

Syntax Description

options	The options to use with the **ssh** EXEC command. For more information about the possible options, see Request for Comments (RFC 4254) at http://www.rfc-archive.org/getrfc.php?rfc=4254.

Defaults

By default, the Secure Shell (SSH) feature is disabled on a WAAS device.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

Note The Telnet daemon can still be used with the WAAS device. SSH does not replace Telnet.

Related Commands

(config) sshd

(config) ssh-key-generate

tcpdump

To dump network traffic, use the **tcpdump** EXEC command.

tcpdump [*LINE*]

Syntax Description

LINE	(Optional) Specifies dump options.

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.

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 this 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 ]
```

Examples

The following example starts a network traffic dump to a file named *tcpdump.txt*:

```
WAE# tcpdump -F tcpdump.txt
```

Related Commands

less

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*]

Syntax Description

hostname	Hostname of the network device.
ip-address	IP address of the network device.
portnum	(Optional) Port number (1–65535). Default port number is 23.

Defaults

The default port number is 23.

Command Modes

EXEC

Device Modes

application-accelerator

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 examples show several ways you can log in to a WAAS device using the Telnet client:

```
WAE# telnet cisco-wae
WAE# telnet 10.168.155.224
WAE# telnet cisco-wae 2048
WAE# telnet 10.168.155.224 2048
```

Related Commands

(config) telnet enable

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal** EXEC command.

terminal {**length** *length* | **monitor** [**disable**]}

Syntax Description

length	Sets the length of the display on the terminal.
length	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.

Examples

The following example sets the number of lines to display to 20:

```
WAE# terminal length 20
```

The following example configures the terminal for no pausing:

```
WAE# terminal length 0
```

Related Commands

All **show** commands

tethereal

To analyze network traffic from the command line, use the **tethereal** EXEC command.

tethereal [*LINE*]

Syntax Description		
	LINE	(Optional) Specifies options.

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.

The following example shows the options available with the WAAS **tethereal** command:

```
WAE# tethereal -h
This is GNU tethereal 0.10.6
 (C) 1998-2004 Gerald Combs <gerald@ethereal.com>
Compiled with GLib 1.2.9, with libpcap 0.6, with libz 1.1.3, without libpcre,
without UCD-SNMP or Net-SNMP, without ADNS.
NOTE: this build does not support the "matches" operator for Ethereal filter
syntax.
Running with libpcap (version unknown) on Linux 2.4.16.

tethereal [ -vh ] [ -DlLnpqSVx ] [ -a <capture autostop condition> ] ...
        [ -b <number of ring buffer files>[:<duration>] ] [ -c <count> ]
        [ -d <layer_type>==<selector>,<decode_as_protocol> ] ...
        [ -f <capture filter> ] [ -F <output file type> ] [ -i <interface> ]
        [ -N <resolving> ] [ -o <preference setting> ] ... [ -r <infile> ]
        [ -R <read filter> ] [ -s <snaplen> ] [ -t <time stamp format> ]
        [ -T pdml|ps|psml|text ] [ -w <savefile> ] [ -y <link type> ]
        [ -z <statistics string> ]
Valid file type arguments to the "-F" flag:
        libpcap - libpcap (tcpdump, Ethereal, etc.)
        rh6_1libpcap - RedHat Linux 6.1 libpcap (tcpdump)
        suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdump)
        modlibpcap - modified libpcap (tcpdump)
        nokialibpcap - Nokia libpcap (tcpdump)
        lanalyzer - Novell LANalyzer
        ngsniffer - Network Associates Sniffer (DOS-based)
        snoop - Sun snoop
        netmon1 - Microsoft Network Monitor 1.x
        netmon2 - Microsoft Network Monitor 2.x
        ngwsniffer_1_1 - Network Associates Sniffer (Windows-based) 1.1
        ngwsniffer_2_0 - Network Associates Sniffer (Windows-based) 2.00x
```

```
visual - Visual Networks traffic capture
5views - Accellent 5Views capture
niobserverv9 - Network Instruments Observer version 9
default is libpcap
```

Related Commands tcpdump

traceroute

To trace the route between a WAAS device to a remote host, use the **traceroute** EXEC command.

traceroute {*hostname* | *ip-address*}

Syntax Description

hostname	Name of remote host.
ip-address	IP address of remote host.

Defaults

No default behavior values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Traceroute is a widely available utility on most operating systems. Much like ping, it is a valuable tool for determining connectivity in a network. Ping allows the user to find out if there is a connection between two end systems. Traceroute does this as well, but also lists the intermediate routers between the two systems. Users can therefore see the possible routes packets can take from one system to another. Use **traceroute** to find the route to a remote host, when either the hostname or the IP address is known.

Examples

The following example traces the route between the WAAS device and a device with an IP address of 10.0.0.0:

```
WAE# traceroute 10.0.0.0
traceroute to 10.0.0.0 (10.0.0.0), 30 hops max, 38 byte packets
 1  sblab2-rtr.abc.com (192.168.10.1)  0.959 ms  0.678 ms  0.531 ms
 2  192.168.1.1 (192.168.1.1)  0.665 ms  0.576 ms  0.492 ms
 3  172.24.115.66 (172.24.115.66)  0.757 ms  0.734 ms  0.833 ms
 4  sjc20-sbb5-gw2.abc.com (192.168.180.93)  0.683 ms  0.644 ms  0.544 ms
 5  sjc20-rbb-gw5.abc.com (192.168.180.9)  0.588 ms  0.611 ms  0.569 ms
 6  sjce-rbb-gw1.abc.com (172.16.7.249)  0.746 ms  0.743 ms  0.737 ms
 7  sj-wall-2.abc.com (172.16.7.178)  1.505 ms  1.101 ms  0.802 ms
 8  * * *
 9  * * *
 .
 .
 .
29  * * *
30  * * *
```

Related Commands

ping

transaction-log

To force the exporting or the archiving of the transaction log, use the **transaction-log** EXEC command.

transaction-log {**export** | **tfo force archive**}

Syntax Description

export	Forces the archiving of a WAE's transaction file.
tfo force archive	Forces the archiving of the Traffic Flow Optimization (TFO) transaction log file.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example forces the archiving of the transaction file on the WAE:

```
WAE# transaction-log export
```

The following example forces the archiving of a WAE's TFO transaction log file:

```
WAE# transaction-log tfo force archive
```

Related Commands

(config) transaction-logs

show transaction-logging

type

To display a file, use the **type** EXEC command.

type *filename*

Syntax Description

filename	Name of file.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this EXEC command to display the contents of a file within any file directory on a WAAS device. This command may be used to monitor features such as transaction logging or system logging (syslog).

Examples

The following example shows how to display the contents of the *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** command in EXEC mode.

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	Identifies the line at which to begin file display.
LINE	Regular expression to match in the file where you want to begin display, or that is to be included or excluded from display.
exclude	Indicates lines that are to be excluded from the file display.
include	Indicates lines that are to be included in the file display.

Defaults

Last ten lines are shown.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

This EXEC command allows you to monitor a log file by letting you view the end of the file. You can specify the number of lines at the end of the file that you want to view, or you can follow the last line of the file as it continues to log new information. To stop the last line from continuously scrolling as with the **follow** option, use the key sequence **Ctrl-C**.

You can further indicate the type of information to display using the output modifiers. These allow you to include or exclude specific lines or to indicate where to begin displaying the file.

Examples

The following example looks for a list of log files in the */local1* directory and then displays the last ten lines of the *syslog.txt* file. In this example, the number of lines to display is not specified, so the default of ten lines is used:

```
WAE# ls /local1
actona
core_dir
crash
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed

WAE# type-tail /local1/syslog.txt
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get https
equest throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/ftp connection 5
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/ftp' from dataserver
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get ftp-ov
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 follows the *syslog.txt* file as it grows:

```
WAE# type-tail /local1/syslog.txt follow
```

undebug

To disable debugging functions, use the **undebug** EXEC command. Also see the **debug** EXEC command. See the "debug" command for more information about debug functions.

undebug [**aaa accounting** | **all** | **authentication** [**print-services** | **user**] | **buf** [**all** | **dmbuf** | **dmsg**] | **cdp** [**adjacency** | **events** | **ip** | **packets**] | **cli** [**all** | **bin** | **parser**] | **dataserver** [**all** | **clientlib** | **server**] | **dhcp** | **logging** [**all**] | **ntp** | **print-spooler** [**all** | **brief** | **errors** | **warnings**] | **snmp** [**all** | **cli** | **main** | **mib** | **traps**] | **wccp** [**all** | **detail** | **error** | **events** | **keepalive** | **packets** | **slowstart**]]

Note The following **undebug** command options are supported in the application-accelerator device mode only: **dre**, **epm**, **print-spooler**, **tfo**, **wafs**, and **wccp**.

Syntax Description

Valid values for the *option* argument are as follows:

aaa accounting	Disables AAA accounting actions.
all	Disables all debugging options.
authentication	Disables authentication debugging.
print-services	Disables Print services authentication debugging.
user	Disables debugging of the user login against the system authentication.
buf	Disables buffer manager debugging.
all	Disables all buffer manager debugging.
dmbuf	Disables only dmbuf debugging.
dmsg	Disables only dmsg debugging.
cdp	Disables CDP debugging.
adjacency	Disables CDP neighbor information debugging.
events	Disables CDP events debugging.
ip	Disables CDP IP debugging.
packets	Disables packet-related CDP debugging.
cli	Disables CLI debugging.
all	Disables all CLI debugging.
bin	Disables CLI command binary program debugging.
parser	Disables CLI command parser debugging.
cms	Disables CMS debugging.
dataserver	Disables data server debugging.
all	Disables all data server debugging.
clientlib	Disables data server client library module debugging.
server	Disables data server module debugging.
dhcp	Disables DHCP debugging.

dre	Disables DRE debugging.
aggregation	Disables DRE chunk-aggregation debugging.
all	Disables the debugging of all DRE commands.
cache	Disables DRE cache debugging.
connection	Disables DRE connection debugging.
aggregation *acl*	Disables DRE chunk-aggregation debugging for a specified connection.
cache *acl*	Disables DRE cache debugging for a specified connection.
core *acl*	Disables DRE core debugging for a specified connection.
message *acl*	Disables DRE message debugging for a specified connection.
misc *acl*	Disables DRE other debugging for a specified connection.
core	Disables DRE core debugging.
message	Disables DRE message debugging.
misc	Disables DRE other debugging.
emdb	Disables embedded database debugging.
logging	Disables logging debugging.
all	Disables all logging debugging.
ntp	Disables NTP debugging.
print-spooler	Disables print spooler debugging.
all	(Optional) Debug the print spooler using all debug features.
brief	(Optional) Debug the print spooler using only brief debug messages.
errors	(Optional) Debug the print spooler using only the error conditions.
warnings	(Optional) Debug the print spooler using only the warning conditions.
rpc	Displays the remote procedure calls (RPC) logs.
detail	Displays the RPC logs of priority "detail" level or higher.
trace	Displays the RPC logs of priority "trace" level or higher.
stats	Debugs the statistics.
all	Debugs all statistics functions.
collection	Debugs the statistics collection.
computation	Debugs the statistics computation.
history	Debugs the statistics history.

tfo	Enables TFO debugging.
buffer-mgr	Enables TFO buffer manager debugging.
connection	Enables TFO connection debugging.
auto-discovery *acl*	Enables TFO connection debugging for the auto-discovery module.
comp-mgr *acl*	Enables TFO connection debugging for the compression module.
conn-mgr *acl*	Enables TFO connection debugging for the connection manager.
filtering *acl*	Enables TFO connection debugging for filtering module.
netio-engine *acl*	Enables TFO connection debugging for network input/output module.
policy-engine *acl*	Enables TFO connection debugging of application policies.
stat-mgr	Enables TFO statistics manager debugging.
translog	Enables TFO transaction log debugging.
wafs	Sets the notification level (debug, info, warn, error) at which messages from the WAAS software component and utilities are logged.
all	Sets the logging level for all software components and utilities at once.
core-fe	Sets the logging level for WAEs s acting as a core file engine.
edge-fe	Sets the logging level for WAEs acting as an edge file engine.
manager	Sets the logging level for the Device Manager.
utilities	Sets the logging level for WAAS utilities.
wccp	Debugs the WCCP information.
all	Debugs all WCCP functions.
detail	Debugs the WCCP details.
error	Debugs the WCCP errors.
events	Debugs the WCCP events.
keepalive	Debugs the WCCP keepalives that are sent to the applications.
packets	Debugs the WCCP packet-related information.
slowstart	Debugs the WCCP slow start.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Related Commands

debug

show debugging

wafs

To backup, restore, or create a system report about the Wide Area File Services (WAFS)-related network configuration, plus the configurations of file servers, printers, users, and so forth, on a WAE, use the **wafs** EXEC command.

wafs {**backup-config** *filename* | **restore-config** *filename* |
sysreport [*filename* | **date-range** *from_date end_date filename*]}

Note Executing the **wafs sysreport** command can temporarily impact the performance of your WAE.

Syntax Description

backup-config	Copies current WAFS-related configuration information to a file.
filename	Name of the file, in *xxxx.tar.gz* format, where you want to save the WAFS configuration. This file is saved to the */local/local1* directory.
restore-config	Loads saved WAFS-related configuration information from a file.
filename	(Optional) Name of the file, in *xxxx.tar.gz* format, where the desired WAFS configuration information has been stored. This file should be in the */local/local1* directory.
sysreport	Deprecated; use **copy sysreport**.
date-range	(Optional) Range of time that the system report is to cover.
from_date	Start date of information in the generated system report.
to_date	End date of information in the generated system report.
filename	Name of the file, in *xxxx.tar.gz* format, in which the system information is to be stored.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **wafs backup-config** EXEC command is used when back up of basic network configuration is not sufficient (performed using the **copy running-config** command), for example, when you want to back up system configurations before making any changes using the WAAS CLI global configuration mode and you want to protect the current configuration from loss of data by erroneous operations.

The **wafs restore-config** automatically performs a reload function. We strongly recommend that you re-register your WAE on completion of this command.

This **wafs** command is also useful when backup and system restoration, or generation of a system report, are not available from the WAAS Central Manager GUI.

Examples

The following example creates a backup file of the WAFS configuration information:

```
WAE# wafs ?
  backup-config   backup system configurations to a file.
  restore-config  restore system configurations from a file. WARNING: After
                  restoring configuration, the system needs to be restarted and
                  re-registered.
  sysreport       system report to a file

WAE# wafs backup-config backup.tar.gz
  system configuration is stored in file /local/local1/backup.tar.gz
```

The following example restores a system with previously saved WAAS configuration information:

```
WAE# wafs restore-config backup.tar.gz
Restoring configurations ...
After upload is completed the File Engine will be reloaded. We strongly recommend you
re-register after the engine is reloaded.
```

Related Commands

copy running-config

whoami

To display the username of the current user, use the **whoami** EXEC command.

whoami

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this EXEC command to display the username of the current user.

Examples

The following example displays your username:

```
WAE# whoami
admin
```

Related Commands

pwd

windows-domain

To access the Windows domain utilities on a WAAS device, use the **windows-domain** EXEC command.

windows-domain diagnostics {**findsmb** | **getent** | **net** | **nmblookup** | **smbclient** | **smbstatus** | **smbtree** | **tdbbackup** | **tdbdump** | **testparm** | **wbinfo**}

Syntax Description

diagnostics	Enables selection of Windows domain diagnostic utilities.
findsmb	Utility for troubleshooting NetBIOS name resolution and browsing.
getent	Utility to get unified list of both local and PDC users and groups.
net	Utility for administration of remote CIFS servers.
nmblookup	Utility for troubleshooting NetBIOS name resolution and browsing.
smbclient	Utility for troubleshooting the Windows environment and integration.
smbstatus	Utility for inspecting the Samba server status, connected clients, etc.
smbtree	Utility for inspecting the Windows network neighborhood structure and content.
tdbbackup	Utility for backing up, verifying and restoring Samba database files.
tdbdump	Utility for inspecting the Samba database files.
testparm	Utility to validate *smb.conf* file correctness.
wbinfo	Utility for Winbind and domain integration troubleshooting.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this command to activate the selected Windows domain diagnostic utility.

The following example shows the options available for the Get Entity utility:

```
WAE# windows-domain diagnostics getent --help
Usage: getent [OPTION...] database [key ...]
getent - get entries from administrative database.

  -s, --service=CONFIG       Service configuration to be used
  -?, --help                 Give this help list
      --usage                Give a short usage message
  -V, --version              Print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.
```

```
Supported databases:
aliases ethers group hosts netgroup networks passwd protocols rpc
services shadow
```

The following example shows the options available for the NMB Lookup Utility for troubleshooting NetBIOS name resolution and browsing:

```
WAE# windows-domain diagnostics nmblookup -h
Usage: [-?TV] [--usage] [-B BROADCAST-ADDRESS] [-f VAL] [-U STRING] [-M VAL]
        [-R VAL] [-S VAL] [-r VAL] [-A VAL] [-d DEBUGLEVEL] [-s CONFIGFILE]
        [-l LOGFILEBASE] [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP]
        [-i SCOPE] <NODE> ...
```

The following example shows the options available for the Samba Client Utility for troubleshooting the Windows environment and integration:

```
WAE# windows-domain diagnostics smbclient -h
Usage: [-?EgVNkP] [--usage] [-R NAME-RESOLVE-ORDER] [-M HOST] [-I IP] [-L HOST]
        [-t CODE] [-m LEVEL] [-T <c|x>IXFqgbNan] [-D DIR] [-c STRING] [-b BYTES]
        [-p PORT] [-d DEBUGLEVEL] [-s CONFIGFILE] [-l LOGFILEBASE]
        [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP] [-i SCOPE]
        [-U USERNAME] [-A FILE] [-S on|off|required] service <password>
```

The following example shows the options available for the TDB Backup Utility:

```
WAE# windows-domain diagnostics tdbbackup -h
Usage: tdbbackup [options] <fname...>

   -h            this help message
   -s suffix     set the backup suffix
   -v            verify mode (restore if corrupt)
```

The following example shows the use of the -u option of the WinBind Utility to view the information about a user registered in a Windows domain:

```
WAE# windows-domain diagnostics wbinfo -u
administrator
guest
user98
tuser1

WAE# show user username user98
Uid             : 70012
Username        : user98
Password        : *****
Privilege       : super user
Configured in   : Windows Domain database

WAE# show user uid 70012
Uid             : 70012
Username        : user98
Password        : *****
Privilege       : super user
Configured in   : Windows Domain database
```

The following example shows how to register a Windows domain:

```
WAE# windows-domain diagnostics
        net join -S<domain server> -U<domain admin username>%<domain admin password>
```

Related Commands

(config) windows-domain

write

To save startup configurations on a WAAS device, use the **write** EXEC command.

write [**erase** | **memory** | **mib-data** | **terminal**]

Syntax Description

erase	(Optional) Erases startup configuration from NVRAM.
memory	(Optional) Writes the configuration to NVRAM. This is the default location for saving startup information.
mib-data	(Optional) Saves MIB persistent configuration data to disk.
terminal	(Optional) Writes the configuration to a terminal session.

Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this command to either save running configurations to NVRAM or to erase memory configurations. Following a **write erase** command, no configuration is held in memory, and a prompt for configuration specifics occurs after you reboot the WAAS device.

Use the **write terminal** command to display the current running configuration in the terminal session window. The equivalent command is **show running-config**.

Examples

The following example saves the current startup configuration to memory:

```
WAE# write memory
```

Related Commands

copy running-config

copy startup-config

show running-config

show startup-config