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 cache dre

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

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

clear logging

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

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

clear users administrative

clear windows-domain-log

Syntax Description

cache	Clears cached objects.
dre	Clears the DRE cache.
cdp	Resets the Cisco Discovery Protocol (CDP) statistical data.
counters	Clears the CDP counters.
table	Clears the CDP tables.
ip access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
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).
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.
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.
inline	Clears the inline interception 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.
tfo	Clears the TCP flow optimization (TFO) statistics.
all	Clears all of the TFO statistics.
auto-discovery	Clears the TFO auto-discovery statistics.
blacklist	Clears the TFO blacklist statistics.
filtering	Clears the TFO filter table statistics.
peer	Clears the TFO peer statistics.
policy-engine	Clears the TFO application and pass-through statistics.
synq	Clears the TFO SynQ module statistics.
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

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

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

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

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

The **clear 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. To clear clock functions and calendar, use the **no** form of this command.

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

Syntax Description

read-calendar	Reads the calendar and updates the system clock.
set	Sets the time and date.
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

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

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy ftp

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

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

Syntax Description

ftp	Copies a file from an FTP server.
central	Copies a file to the software upgrade image repository.
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 Use the **copy ftp disk** EXEC command to copy a file from an FTP server to a SYSFS partition on the WAAS device.

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

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

Upgrading the BIOS

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

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

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

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

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

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

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

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

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

```
WAE# reload
```

The new BIOS takes effect after the system reboots.

Examples

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

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

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

```
WAE-7326# copy ftp install 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 files from an HTTP server to the WAAS device, use the **copy http** EXEC command.

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

Syntax Description

http	Copies the file from an HTTP server.
install	Copies the file from an HTTP server and installs the software release file to the local device.
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).
portnum	HTTP server port number (1–65535).
proxy	(Optional) Allows the request to be redirected to an HTTP proxy server.
proxy_portnum	HTTP proxy server port number (1–65535).
username	(Optional) 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 shows how to copy an image file from an HTTP server and install the file on the WAAS device:

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

The following example shows how to upgrade the BIOS. All output is written to a separate file (*/local1/.bios_upgrade.txt*) for traceability. The hardware 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

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

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy sysreport

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

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

Syntax Description

sysreport	Generates and saves a report containing WAAS system information in a file.
disk	Copies system information to a disk file.
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	(Optional) 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	(Optional) End date of information in the generated system report. If omitted, this date defaults to today's date. The report includes files through the end of this day.
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 shows how to copy system information to the file mysysinfo on the local WAAS device:

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

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

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

Related Commands

show running-config

show startup-config

wafs

copy system-status

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

copy system-status disk *filename*

Syntax Description

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

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

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy tech-support

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

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

Syntax Description

tech-support	Copies system information for technical support.
disk	Copies system information for technical support to disk file.
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

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

Related Commands

install

reload

show running-config

show startup-config

wafs

write

copy tftp

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

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

Syntax Description

tftp	Copies an image from a TFTP server.
disk	Copies an image from a TFTP server to a disk file.
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

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

Related Commands

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

cpfile

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

cpfile *oldfilename newfilename*

Syntax Description

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 central manager functions, use the **debug** EXEC command. To disable **debugging,** use the **no** form of the command. (See also the undebug command.)

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

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

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

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

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

debug cms

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

debug dhcp

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

debug epm

debug logging all

debug ntp

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

debug rbcp

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

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

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

debug translog export

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

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

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

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

debug aaa accounting

debug all

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

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

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

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

debug cms

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

debug dhcp

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

debug logging all

debug ntp

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

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

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

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

Syntax Description

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

packets	Enables packet-related CDP debugging.
cli	(Optional) Enables CLI debugging.
all	Enables all CLI debugging.
bin	Enables CLI command binary program debugging.
parser	Enables CLI command parser debugging.
cms	(Optional) Enables CMS debugging.
dataserver	(Optional) Enables data server debugging.
all	Enables all data server debugging.
clientlib	Enables data server client library module debugging.
server	Enables data server module debugging.
dhcp	(Optional) Enables DHCP debugging.
dre	(Optional) Enables DRE debugging.
aggregation	Enables DRE chunk-aggregation debugging.
all	Enables the debugging of all DRE commands.
cache	Enables DRE cache debugging.
connection	Enables DRE connection debugging.
aggregation [*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.
acl	ACL to limit connections traced.
core	Enables DRE core debugging.
message	Enables DRE message debugging.
misc	Enables DRE other debugging.
epm	(Optional) Enables the DCE-RPC EPM debugging.
logging	(Optional) Enables logging debugging.
all	Enables all logging debugging.
ntp	(Optional) Enables NTP debugging.
print-spooler	(Optional) Enables print spooler debugging.
all	Enables print spooler debugging using all debug features.
brief	Enables print spooler debugging using only brief debug messages.
errors	Enables print spooler debugging using only the error conditions.
warnings	Enables print spooler debugging using only the warning conditions.
rbcp	(Optional) Enables RBCP debugging.
snmp	(Optional) Enables SNMP debug commands.
all	Enables all SNMP debug commands.
cli	Enables SNMP CLI debugging.
main	Enables SNMP main debugging.
mib	Enables SNMP MIB debugging.

traps	Enables SNMP trap debugging.
stats	(Optional) Enables statistics debugging.
all	Enables all statistics debug commands.
collection	Enables collection statistics debugging.
computation	Enables computation statistics debugging.
history	Enables history statistics debugging.
tfo	(Optional) Enables TFO debugging.
buffer-mgr	Enables TFO buffer manager debugging.
connection	Enables TFO connection debugging.
auto-discovery [*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.
synq [*acl*]	Enables TFO connection debugging for the SynQ module.
acl	ACL to limit TFO connections.
stat-mgr	Enables TFO statistics manager debugging.
translog	Enables TFO transaction log debugging.
translog	(Optional) Enables transaction logging debug commands.
export	Enables transaction log FTP export debugging.
wafs	(Optional) Unsets the notification level (debug, info, warn, error) at which messages from the WAAS software component and utilities are logged.
all	Unsets the logging level for all software components and utilities at once.
core-fe	Unsets the logging level for WAEs s acting as a core File Engine.
edge-fe	Unsets the logging level for WAEs acting as an edge File Engine.
manager	Unsets the logging level for the Device Manager.
utilities	Unsets the logging level for WAAS utilities.
wccp	(Optional) Enables the WCCP information debugging.
all	Enables all WCCP debugging functions.
detail	Enables the WCCP detail debugging.
error	Enables the WCCP error debugging.
events	Enables the WCCP events debugging.
keepalive	Enables the debugging for WCCP keepalives that are sent to the applications.
packets	Enables the WCCP packet-related information debugging.
slowstart	Enables the WCCP slow-start debugging.

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

emdb	(Optional) Enables embedded database debugging.
level	(Optional) Enables the specified debug level for EMDB service.
levelnum	(Optional) Debug level to disable. (Level 0 disables debugging.)
rpc	(Optional) Enables the remote procedure calls (RPC) logs.
detail	Enables the RPC logs of priority "detail" level or higher.
trace	Enables the RPC logs of priority "trace" level or higher.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page xiv.

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

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

Examples

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

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

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

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

Related Commands

show debugging

undebug

delfile

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

delfile *filename*

Syntax Description

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 shows how to delete a temporary file from the */local1* directory using an absolute path.

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

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

deltree

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

deltree *directory*

Syntax Description

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

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

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

dir

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

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

lls

ls

disable

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

disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

```
WAE> enable
Password:
```

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

Examples

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

```
WAE# disable
WAE>
```

Related Commands

enable

disk

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

disk delete-partitions *diskname*

disk 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 to increase storage capacity or to increase 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

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

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

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

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

enable

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

enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

```
WAE> enable
Password:
```

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

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

Examples

The following example shows how to access privileged EXEC mode:

```
WAE> enable
WAE#
```

Related Commands

disable

exit

exit

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

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

All modes

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

```
WAE# exit
WAE>
```

find-pattern

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

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

Syntax Description

binary	Does not suppress the binary output.
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 shows how to search a file recursively for a case-sensitive pattern:

```
WAE# find-pattern case recursive admin removed_core
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw-------    1 admin    root     97054720 Jan 11 11:31 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14086
-rw-------    1 admin    root     96845824 Jan 11 11:32 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14823
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
-rw-------    1 admin    root     96759808 Jan 11 12:59 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.20016
-rw-------    1 admin    root     97124352 Jan 11 13:26 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.8095
```

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

```
WAE# find-pattern match 10 removed_core
Tue Oct 12 10:30:03 UTC 2004
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
```

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

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

Related Commands

cd

dir

lls

ls

help

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

help

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC and global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Two styles of help are provided:

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

Examples

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

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

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

install

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

install *imagefilename*

Syntax Description

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.

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

Examples

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

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

Related Commands

copy disk

reload

less

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

less *file_name*

Syntax Description

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 are as follows:

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

Examples

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

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

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

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

Examples

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

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

Related Commands

dir

lls

pwd

mkdir

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

mkdir *directory*

Syntax Description

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 shows how to create a new directory, *oldpaxfiles*:

```
WAE# mkdir /oldpaxfiles
```

Related Commands

cpfile

dir

lls

ls

pwd

rename

rmdir

mkfile

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

mkfile *filename*

Syntax Description		
	filename	Name of the file 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 shows how to create a new file, *traceinfo,* in the root directory:

```
WAE# mkfile traceinfo
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

ntpdate

To set the software clock (time and date) on a WAAS device using 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 shows how to set the software clock on the WAAS device using a NTP server:

```
WAE# ntpdate 10.11.23.40
```

Related Commands

clock

(config) clock

show clock

show ntp

ping

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

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

Syntax Description

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

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

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

pwd

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

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

```
WAE# pwd
/local1
```

Related Commands

cd

dir

lls

ls

reload

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

reload [**force**]

Syntax Description

force	(Optional) Forces a reboot without further prompting.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

```
WAE# reload force
```

Related Commands

write

rename

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

rename *oldfilename newfilename*

Syntax Description

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

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

Related Commands

cpfile

restore

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Backing up the Central Manager Database

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

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

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

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

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

Rolling Back the Configuration

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

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

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

Examples

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

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

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

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

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

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

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

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

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 shows how to delete the *oldfiles* directory from the *local1* directory:

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

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

scp

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

scp [**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 uses SSH for transferring data between hosts.

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

Related Commands

ssh

script

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Examples

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

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

setup

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

setup

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

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

Enter choice:

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

show aaa accounting

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

show aaa accounting

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Examples

Table 3-1 describes the fields shown in the **show aaa accounting** display.

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

Field	Description
Accounting Type	Displays the AAA accounting configuration for the following types of user accounts: Exec Command level 0 Command level 15 System
Record Event(s)	Displays the configuration of the AAA accounting notice that is sent to the accounting server.
stop-only	The WAAS device sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.
start-stop	The WAAS device sends a start record accounting notice at the beginning of an event and a stop record at the end of the event to the TACACS+ accounting server. The start accounting record is sent in the background. The requested user service begins regardless of whether or not the start accounting record was acknowledged by the TACACS+ accounting server.

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

Field	Description
wait-start	The WAAS device sends both a start and a stop accounting record to the TACACS+ accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.
disabled	Accounting is disabled for the specified event.
Protocol	Displays the accounting protocol that is configured.

Related Commands **(config) aaa accounting**

show adapter

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

show adapter epm

Syntax Description

epm	Specifies the Microsoft PortMapper adapter.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

Examples

Table 3-2 describes the fields shown in the **show adapter epm** display.

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

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

Related Commands

(config) adapter

show statistics epm

show alarms

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

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

Syntax Description

critical	(Optional) Displays critical alarm information.
detail	(Optional) Displays detailed information for each alarm.
support	(Optional) Displays additional information about each alarm.
history	(Optional) Displays information about the history of various alarms.
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, 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 as follows:

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

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

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

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

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

Examples

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

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

Field	Description
Op	Operation status of the alarm. Values are R–Raised or C–Cleared.
Sev	Severity of the alarm. Values are Cr–Critical, Ma–Major, or Mi–Minor.
Alarm ID	Type of event that caused the alarm. For example: wafs_edge_down, wafs_core_down.
Module/Submodule	Software module affected. For example: wafs
Instance	Object that this alarm event is associated with. For example, for an alarm event with the Alarm ID disk_failed, the instance would be the name of the disk that failed. The Instance field does not have pre-defined values and is application specific.

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

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

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

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

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

Related Commands

(config) alarm overload-detect

(config) snmp-server enable traps

show arp

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

show arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

Table 3-5 describes the fields shown in the **show arp** display.

Table 3-5 Field Descriptions for the show arp Command

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

Syntax Descriptions

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Examples

Table 3-6 describes the fields shown in the **show authentication user** display.

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

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

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

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

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

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

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

Related Commands

(config) authentication

clear

show statistics authentication

show auto-register

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

show auto-register

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-8 describes the output in the **show auto-register** display.

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

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

Related Commands

(config) auto-register

show banner

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

show banner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-9 describes the fields shown in the **show banner** display.

Table 3-9 Field Descriptions for the show banner Command

Field	Description
Banner is enabled.	Configuration status of the banner feature.
MOTD banner is: abc	(Message of the day) Displays the configured message of the day.
Login banner is: acb	Displays the configured login banner.
Exec banner is: abc	Displays the configured EXEC banner.

Related Commands

(config) auto-register

show bypass

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

show bypass list

Syntax Description

list	Displays the bypass list entries. Maximum of 50.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The maximum number of static bypass entries is 50.

Examples

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

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

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

Related Commands

(config) bypass

show cdp

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

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

Syntax Description

entry	(Optional) Displays information for a specific neighbor entry.
neighbor	Name of CDP neighbor entry.
protocol	(Optional) Displays the CDP protocol information.
version	(Optional) Displays the CDP version.
holdtime	(Optional) Displays length of time that CDP information is held by neighbors.
interface	(Optional) Displays interface status and configuration.
FastEthernet	(Optional) Displays Fast Ethernet configuration.
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	Displays 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) Displays detailed Gigabit Ethernet neighbor network information.
run	(Optional) Displays the CDP process status.
timer	(Optional) Displays the time when CDP information is resent to neighbors.
traffic	(Optional) Displays CDP statistical information.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

Table 3-11 Field Descriptions for the show cdp Command

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

(config) cdp

(config-if) cdp

clear

show 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. To display all first level time zone names organized into directories by region, use the **show clock standard-timezones region** EXEC command.

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

Examples

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

Table 3-22 Field Description for the show clock Command

Field	Description
Local time	Day of the week, month, date, time (hh:mm:ss), and year in local time relative to the UTC offset.

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

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

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

Related Commands

clock

(config) clock

show cms

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

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

Syntax Description

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

Table 3-24 describes the fields shown in the **show cms info** display for WAAS application engines.

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

cms

(config) cms

show debugging

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

show debugging

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

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

Examples

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

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

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

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

```
WAE# show device mode
```

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

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

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

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

Examples

Table 3-28 describes the field in the **show device-mode current** display.

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

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

Table 3-29 describes the field in the **show device-mode configured** display.

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

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

Related Commands

(config) device mode

show disks

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

show disks {**details** | **failed-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

Table 3-30 describes the fields shown in the **show disks details** display.

Table 3-30 Field Descriptions for the show disks details Command

Field	Description
Physical disk information	Lists the disks by number. WAE 7300 series appliances show information for 6 disk drives and WAE 500 and 600 series appliances show information for 2 disk drives.
disk00	Availability of the disk: Present, Not present or Not responding, or Not used (*). Disk identification number and type, for example: (h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB).
disk01	Same type of information is shown for each disk.
Mounted filesystems	Table containing the following column heads:
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.

Table 3-30 Field Descriptions for the show disks details Command (continued)

Field	Description
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name "md1" indicates that the partition is a raided partition and that the RAID type is RAID-1. (RAID-1 is the only RAID type supported in WAAS.)
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].

SMART support is vendor dependent; each disk vendor has a different set of supported SMART attributes. Table 3-31 describes some typical fields in the **show disks SMART-info** display.

Table 3-31 Field Descriptions for the show disks SMART-info Command

Field	Description
disk00—disk05	WAE 7300 series appliances show information for 6 disk drives, and WAE 500 and 600 series appliances show information for 2 disk drives.
Device	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time hh:mm:ss, year, clock standard. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.

Table 3-32 describes the fields in the **show disks SMART-info details** display. Details in this display depend on the drive manufacturer and vary between drives.

Table 3-32 Field Descriptions for the show disks SMART-info details Command

Field	Description
disk00—disk05	WAE 7300 series appliances show information for 6 disk drives and WAE 500 and 600 series appliances show information for 2 disk drives.
Device	Vendor number and version number of the disk.

Table 3-32 Field Descriptions for the show disks SMART-info details Command (continued)

Field	Description
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time hh:mm:ss, year, clock standard. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.
Current Drive Temperature	Temperature of the drive in degrees Celsius.
Manufactured in week XX of year	Manufacturing details.
Current start stop count	Number of times the device has stopped or started.
Recommended maximum start stop count	Maximum recommended count used to gauge the life expectancy of the disk.
Error counter log	Table displaying the error counter log. Counters for various types of disk errors.

Related Commands

disk

(config) disk

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

Table 3-33 describes the fields shown in the **show flash** display.

Table 3-33 Field Descriptions for the show flash Command

Field	Description
WAAS software version (disk-based code)	WAAS software version and build number that is running on the device.
System image on flash:	
Version	Version and build number of the software that is stored in flash memory.
System flash directory:	
System image	Number of sectors used by the system image.
Bootloader, rescue image, and other reserved areas	Number of sectors used by the bootloader, rescue image, and other reserved areas.
XX sectors total, XX sectors free	Total number of sectors. Number of free sectors.

show hardware

To display system hardware status for a WAAS device, use the **show hardware** EXEC command.

show hardware

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show hardware** command lists the system hardware status, including the version number, the startup date and time, the run time since startup, the microprocessor type and speed, the amount of physical memory available, and a list of disk drives.

Examples

Table 3-34 describes the fields shown in the **show hardware** display.

Table 3-34 Field Descriptions for the show hardware Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) year by Cisco Systems, Inc. Cisco Wide Area Application Services Software Release XXX (build bXXX month day year)	Software application, copyright, release, and build information.
Version	Version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Compile information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.
CPU 0 is	CPU manufacturer information.
Total X CPU	Number of CPUs on the device.

Table 3-34 Field Descriptions for the show hardware Command (continued)

Field	Description
XXXX Mbytes of Physical memory	Number of megabytes of physical memory on the device.
X CD ROM drive	Number of CD-ROM drives on the device.
X GigabitEthernet interfaces	Number of Gigabit Ethernet interfaces on the device.
X InlineGroup interfaces	Number of InlineGroup interfaces on the device.
X Console interface	Number of console interfaces on the device.
Manufactured As	Product identification information.
BIOS Information	Information about the BIOS.
Vendor	Name of the BIOS vendor.
Version	BIOS version number.
Rel. Date	(Release date) Date that the BIOS was released.
Cookie info	
SerialNumber	Serial number of the WAE.
SerialNumber (raw)	Serial number of the WAE as an ASCII value.
TestDate	Date that the WAE was tested.
ExtModel	Hardware model of the device, for example WAE612.
ModelNum (raw)	Internal model number (ASCII value) that corresponds to the ExtModel number.
HWVersion	Number of the current hardware version.
PartNumber	Not implemented.
BoardRevision	Number of revisions for the current system board.
ChipRev	Number of revisions for the current chipset.
VendID	Vendor ID of the cookie.
CookieVer	Version number of the cookie.
Chksum	Checksum of the cookie. showing whether the cookie is valid.
List of all disk drives	
Physical disk information	Disks listed by number. WAE 7300 series appliances show information for 6 disk drives and WAE 500 and 600 series appliances show information for 2 disk drives.
disk00	Availability of the disk: Present, Not present or not responding, or Not used (*). Disk identification number and type, for example:(h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB).
disk01	Same type of information is shown for each disk.
Mounted filesystems	Table containing the following column heads:
Mount point	Mount point for the file system. For example the mount point for SYSFS is /local/local1.

Table 3-34 Field Descriptions for the show hardware Command (continued)

Field	Description
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name “md1” indicates that the partition is a raided partition and that the RAID type is RAID-1. (RAID-1 is the only RAID type supported in WAAS.)
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].

Related Commands

show disks

show version

show hosts

To view the hosts on a WAAS device, use the **show hosts** EXEC command.

show hosts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

Table 3-35 describes the fields shown in the **show hosts** display.

Table 3-35 field Descriptions for the show hosts Command

Field	Description
Domain names	Domain names used by the WAE to resolve the IP address.
Name Server(s)	IP address of the DNS name server or servers.
Host Table	
hostname	FQDN (hostname and domain) of the current device.
inet address	IP address of the current host device.
aliases	Name configured for the current device based on the **host** global configuration command.

show inetd

To display the status of TCP/IP services on a WAAS device, use the **show inetd** EXEC command.

show inetd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show inetd** EXEC command displays the enabled or disabled status of TCP/IP services on the WAAS device. You can ignore the TFTP service status because TFTP is not supported on WAAS.

Examples

Table 3-36 describes the fields shown in the **show inetd** display.

Table 3-36 Field Descriptions for the show inetd Command

Field	Description
Inetd service configurations:	
ftp	Status of whether the FTP service is enabled or disabled.
rcp	Status of whether the RCP service is enabled or disabled.
tftp	Status of whether the TFTP service is enabled or disabled.

Related Commands

(config) inetd

show interface

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

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

Syntax Description

GigabitEthernet	Displays the Gigabit Ethernet interface device information (only on suitably equipped systems).
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).
InlineGroup	Displays the inline group information.
slot/grpnumber	Slot and inline group number for the selected interface.
InlinePort	Displays the inline port information.
slot/grpnumber/	Slot and inline group number for the selected interface.
lan	Displays the inline port information for the LAN port.
wan	Displays the inline port information for the WAN port.
PortChannel	Displays the port channel interface device information.
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

Table 3-37 describes the fields shown in the **show interface GigabitEthernet** display.

Table 3-37 Field Descriptions for the show interface GigabitEthernet Command

Field	Description
Description	Description of the device, as configured by using the **description** option of the **interface** global configuration command.
Type	Type of interface. Always Ethernet.
Ethernet address	Layer-2 MAC address.
Internet address	Internet IP address configured for this interface.
Broadcast address	Broadcast address configured for this interface.
Netmask	Netmask configured for this interface.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol to determine the most favorable route. Metrics are counted as additional hops to the destination network or host; the higher the metric value, the less favorable the route.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Interrupts	Number of packet interrupts at this interface.
Base address	Base address. hexidecimal value.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Speed setting, transmission mode, and transmission speed for this interface.

The following example displays information for inlineGroup 0 in slot 1 configured on the WAE inline network adapter:

```
WAE612# show interface inlineGroup 1/0
Interface is in intercept operating mode.
Standard NIC mode is off.
Disable bypass mode is off.
Watchdog timer is enabled.
Timer frequency: 1600 ms.
Autoreset frequency 500 ms.
The watchdog timer will expire in 1221 ms.
```

Table 3-38 describes the fields shown in the **show interface InlinePort** display.

Table 3-38 Field Descriptions for the show interface InlinePort Command

Field	Description
Device name	Number identifier for this inlineport interface, such as eth0, eth1, and so forth.
Packets Received	Total number of packets received on this inlineport interface.
Packets Intercepted	Total number of packets intercepted. (Only TCP packets are intercepted.)
Packets Bridged	Number of packets that are bridged. Packets which are not intercepted are bridged.
Packets Forwarded	Number of packets sent from the inline interface.
Packets Dropped	Number of packets dropped.
Packets Received on native	Number of packets forwarded by the inline module that are received on the native (GigabitEthernet 1/0) interface.
n flows through this interface	Number of active TCP connections on this inlineport interface.
Ethernet Driver Status	
Type	Type of interface. Always Ethernet.
Ethernet address	Layer-2 MAC address.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol to determine the most favorable route. Metrics are counted as additional hops to the destination network or host; the higher the metric value, the less favorable the route.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.

Table 3-38 Field Descriptions for the show interface InlinePort Command (continued)

Field	Description
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Base address	Base address. hexidecimal value.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Speed setting, transmission mode, and transmission speed for this interface.

Table 3-39 describes the fields shown in the **show interface PortChannel** display.

Table 3-39 Field descriptions for the show interface PortChannel Command

Field	Description
Type	Type of interface. Always Ethernet.
Ethernet address	Layer-2 MAc address.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol. Higher metrics have the effect of making a route less favorable; metrics are counted as addition hops to the destination network or host.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.

Table 3-40 describes the field shown in the **show interface scsi** display.

Table 3-40 Field Description for the show interface scsi Command

Field	Description
SCSI interface X	Information for SCSI device number X. Shows the make, device ID number, model number, and type of SCSI device.

Table 3-41 describes the fields shown in the **show interface standby** display.

Table 3-41 Field Descriptions for the show interface standby Command

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the **description** option of the **interface** global configuration command.
IP address, netmask	IP address and netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigibitEthernet 1/0.
Active interface	Interfaces that are currently active in the standby group.

Related Commands

(config) interface

show running-config

show startup-config

show inventory

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

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show inventory** EXEC command allows you to view the UDI for a WAAS device. This identity information is stored in the WAAS device's nonvolatile memory.

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

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

Examples

Table 3-42 describes the fields shown in the **show inventory** display.

Table 3-42 Field Descriptions for the show inventory Command

Field	Description
PID	Product identification (ID) number of the device.
VID	Version ID number of the device. Displays as 0 if the version number is not available.
SN	Serial number of the device.

Related Commands

show tech-support

show ip access-list

To display the access lists that are defined and applied to specific interfaces or applications on a WAAS device, use the **show ip access-list** EXEC command.

show ip access-list [*acl-name* | *acl-num*]

Syntax Description

acl-name	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl-num	(Optional) Information for a specific access list, using a numeric identifier (0–99 for standard access lists and100–199 for extended access lists).

Defaults

Displays information about all defined access lists.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show ip access-list** EXEC command to display the access lists that have been defined on the WAAS device. Unless you identify a specific access list by name or number, the system displays information about all the defined access lists, including the following sections:

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

Examples

Table 3-43 describes the fields shown in the show **ip access-list** display.

Table 3-43 Field Descriptions for the show ip access-list Command

Field	Description
Space available:	
XX access lists	Number of access lists remaining out of 50 maximum lists allowed.
XXX access list conditions	Number of access list conditions remaining out of 500 maximum conditions allowed.
Standard IP access list	Name of a configured standard IP access list. Displays a list of the conditions configured for this list.

Table 3-43 Field Descriptions for the show ip access-list Command (continued)

Field	Description
Extended IP access list	Name of a configured extended IP access list. Displays a list of the conditions configured for this list.
Interface access list references	List of interfaces and the access lists with which they are associated, displayed in the following format: *interface slot/port* *interface direction* *access list number*
Application access list references	List of applications and the access lists with which they are associated, displayed in the following format: *application type* *access list type and number* *associated port*

Related Commands

clear

(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

Usage Guidelines

This command displays the IP route table, which lists all of the different routes that are configured on the WAE. The WAE uses this table to determine the next hop. This table includes routes from three sources: the WAE GigabitEthernet interfaces, any user-configured static routes, and the default gateway. The last line in this table shows the default route.

Examples

Table 3-44 describes the fields shown in the **show ip routes** display.

Table 3-44 Field Descriptions for the show ip routes Command

Field	Description
Destination	Destination IP addresses for each route.
Gateway	Gateway addresses for each route.
Netmask	Netmasks for each route.
Number of route cache entries	Number of entries in the route cache. The route cache is a separate entity and this field is not associated with the entries in the IP route table. The number of entries in the route cache can vary depending on the number of connections that are open.

Related Commands

(config) ip

(config-if) ip

show kerberos

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

show kerberos

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

Table 3-45 describes the fields shown in the **show kerberos** display.

Table 3-45 Field Descriptions for the show kerberos Command

Field	Description
Kerberos Configuration	
Local Realm	Local realm name.
DNS suffix	DNS suffix for the realm.
Realm for DNS suffix	DNS addresses of the computers that are part of this realm.
Name of host running KDC for realm	Name of the host running the Key Distribution Center for the realm.
Master KDC	Primary or main Key Distribution Center.
Port	Port that the Kerberos server is using for incoming requests from clients. The default is port 88.

Related Commands

clear

(config) logging

show logging

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

show logging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

The following 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

Table 3-46 describes the fields shown in the **show memory** display.

Table 3-46 Field Descriptions for the show memory Command

Field	Description
Total physical memory	Total amount of physical memory in kilobytes (KB).
Total free memory	Total available memory (in kilobytes).
Total buffer memory	Total amount of memory (in kilobytes) in the memory buffer.
Total cached memory	Total amount of memory (in kilobytes) in the memory cache.
Total swap	Total amount of memory (in kilobytes) for swap purposes.
Total free swap	Total available memory (in kilobytes) for swap purposes.

show ntp

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

show ntp status

Syntax Description

status	Displays NTP status.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-47 describes the fields shown in the **show ntp status** display.

Table 3-47 Field Descriptions for the show ntp status Command

Field	Description
NTP	Indicates whether NTP is enabled or disabled.
server list	NTP server IP and subnet addresses.
remote	Name (first 15 characters) of remote NTP server.
*	In the remote column, identifies the system peer to which the clock is synchronized.
+	In the remote column, identifies a valid or eligible peer for NTP synchronization.
space	In the remote column, indicates that the peer was rejected. (The peer could not be reached or excessive delay occurred in reaching the NTP server.)
x	In the remote column, indicates a false tick and is ignored by the NTP server.
-	In the remote column, indicates a reading outside the clock tolerance limits and is ignored by the NTP server.
refid	Clock reference ID to which the remote NTP server is synchronized.
st	Clock server stratum or layer. In this example, stratum 1 is the top layer.
t	Type of peer (**l**ocal, **u**nicast, **m**ulticast, or **b**roadcast).
when	Indicates when the last packet was received from the server in seconds.
poll	Time check or correlation polling interval in seconds.
reach	8-bit reachability register. If the server was reachable during the last polling interval, a 1 is recorded; otherwise, a 0 is recorded. Octal values 377 and above indicate that every polling attempt reached the server.
delay	Estimated delay (in milliseconds) between the requester and the server.

Table 3-47 Field Descriptions for the show ntp status Command (continued)

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

Related Commands

clock

(config) clock

(config) ntp

show policy-engine application

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) Name of an application classifier. The name should not exceed 30 characters.
dynamic	Shows the application dynamic match information.
name	Shows the application names list.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show policy-engine application dynamic** command to show auto-discovered CIFS file servers that are added to the list. The servers are visible in the dynamic listing for a limited time (3 minutes by default) after any activity stops, and then they are dropped from the dynamic list until another client request causes them to be auto-discovered again.

Examples

Table 3-48 describes the fields shown in the **show policy-engine application classifier** display.

Table 3-48 Field Descriptions for the show policy-engine application classifier Command

Field	Description
Number of Application Classifiers:	Number of application classifiers configured.

0 to *N*	Numbered list that includes the application name and the match statement that defines which traffic is interesting. For example:
	`0) AFS`
	`match dst port range 7000 7009`
	`1) Altiris-CarbonCopy`
	`match dst port eq 1680`

Table 3-49 describes the fields shown in the **show policy-engine application dynamic** display.

Table 3-49 Field Descriptions for the show policy-engine application dynamic Command

Field	Description
Dynamic Match Freelist Information	
Allocated	Total number dynamic policies that can be allocated.
In Use	Number of dynamic matches that are currently in use.
Max In Use	Maximum number of dynamic matches that have been used since the last reboot.
Allocations	Number times that the dynamic match entries have been added.
Individual Dynamic Match Information:	Displays the internally-configured match values for dynamic applications. Dynamic applications do not use statically assigned ports, but they negotiate for a port to handle that application traffic.
Number	Number of the match condition in the list.
Type	Type of traffic to match. For example, Any-->Local tests traffic from any source to the local WAE.
User Id	Name of the accelerator that inserted the entry.
Src	Value for the source match condition. Values can be ANY, LOCAL, an IP address, or a port to which the application applies.
Dst	Value for the destination match condition. Values can be ANY, LOCAL, an IP address, or a port to which the application applies.
Map Name	Policy engine application map that is invoked if the dynamic match entry matches a connection.
Flags	Operation flags specifying different connection handling options.
Seconds	Number of seconds specified as the time limit for the dynamic match entry to exist.
Remaining	Number of seconds remaining before the dynamic match entry expires and is deleted.
Hits	Number of connections that have matched.

Table 3-50 describes the fields shown in the **show policy-engine application name** display.

Table 3-50 Field Descriptions for the show policy-engine application name Command

Field	Description
Number of Applications: X	Number of applications defined on the WAE, including all of the default applications. WAAS includes over 150 default application policies. (For a list of default application policies, see the *Cisco Wide Area Application Services Configuration Guide*, Appendix A. The display next lists each application that is defined on the WAE by name:
1) Authentication (15)	Name of the application and its internal numerical identifier, which is used to manage the application name in the policy engine.
2) Backup (18)	
3) Call-Management (17)	
4) Conferencing (8)	
5) Console (4)	
6) Content-Management (21)	
7) Directory-Services (6)	
8) Email-and-Messaging (12)	
9) Enterprise-Applications (13)	
10) File-System (2)	
11) File-Transfer (16)	
12) Instant-Messaging (22)	
13) Name-Services (25)	
14) Network-Analysis (26)	
15) P2P (7)	
16) Printing (14)	
17) Remote-Desktop (5)	
18) Replication (20)	
19) SQL (1)	
20) SSH (24)	
21) Storage (27)	
22) Streaming (11)	
23) Systems-Management (3)	
24) VPN (23)	
25) Version-Management (9)	
26) WAFS (10)	
27) Web (19)	
28) Other (0)	

Related Commands

- (config) policy-engine application classifier
- (config) policy-engine application map adaptor EPM
- (config) policy-engine application map adaptor WAFS transport
- (config) policy-engine application map basic delete
- (config) policy-engine application map basic disable
- (config) policy-engine application map basic insert
- (config) policy-engine application map basic list
- (config) policy-engine application map basic move
- (config) policy-engine application map basic name
- (config) policy-engine application map other optimize DRE
- (config) policy-engine application map other optimize full
- (config) policy-engine application map other pass-through
- (config) policy-engine application name
- (config) policy-engine config

show policy-engine status

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

show policy-engine status

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-51 describes the fields shown in the **show policy-engine status** display.

Table 3-51 Field Descriptions for the show policy-engine status Command

Field	Description
Policy-engine resources usage:	Table columns are Total, Used, and Available.
Application names	Total number of application names. Number of application names being used. Number of application names available.
Classifiers	Total number of classifiers configured. Number of classifiers being used. Number of classifiers available. The maximum number of classifiers allowed is 512.
Conditions	Total number of conditions configured. Number of conditions being used. Number of conditions available. The maximum number of match conditions allowed is 1024.
Policies	Total number of policies configured. Number of policies being used. Number of policies available. The maximum number of policies allowed is 512.

Related Commands

(config) policy-engine application classifier

(config) policy-engine application map adaptor EPM

(config) policy-engine application map adaptor WAFS transport

(config) policy-engine application map basic delete

(config) policy-engine application map basic disable

(config) policy-engine application map basic insert

(config) policy-engine application map basic list

(config) policy-engine application map basic move

(config) policy-engine application map basic name

(config) policy-engine application map other optimize DRE

(config) policy-engine application map other optimize full

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

(config) policy-engine application name

(config) policy-engine config

show print-services

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

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

Syntax Description

process	Displays information about the print server and print spooler.
drivers	Displays printer drivers on this print server.
user *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

Table 3-52 describes the fields shown in the **show print-services process** display.

Table 3-52 Field Descriptions for the show print-services process Command

Field	Description
Print server is running.	Operation status of the print server.
Print spooler is running.	Operation status of the print spooler.
Print Server Status	
Samba version 3.0.20	Samba version being used.
PID	Process ID. Process identification number of the Samba process on the WAE Linux appliance.
Username	UNIX user that has started the Samba process.
Group	UNIX group to which the user belongs.
Machine	Machine name and IP address. The machine name is the same as the NetBIOS name.
Service	Remote procedure call (RPC) port that is used by clients to connect to the print server. Value is always IPC$.
pid	Process ID. Process identification number of the Samba process on the WAE Linux appliance.
machine	Machine name.
Connected at	Date and time of connection to the print server.

Table 3-52 Field Descriptions for the show print-services process Command (continued)

Field	Description
No locked files	Comment line.
Print Spooler Status	
scheduler is running	Operation status of the print spooler scheduler.
system default destination	Default print destination for WAAS (VistaPrinterOnWAAS).
device for (VistaPrinterOnWAAS)	Socket address for the system default print destination.
(VistaPrinterOnWAAS) accepting requests	Availability status of the system default print destination.
printer (VistaPrinterOnWAAS) is idle. enabled	Operation status of the system default printer.

Related Commands

(config) authentication

(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

Table 3-53 describes the fields shown in the **show processes** display.

Table 3-53 Field Descriptions for the show processes Command

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

show radius-server

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

show radius-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-54 describes the fields shown in the **show radius-server** display.

Table 3-54 Field Descriptions for the show radius-server Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether a RADIUS server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether a RADIUS server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Indicates whether the WAAS devices fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method.
RADIUS Configuration	RADIUS authentication settings.
Key	Key used to encrypt and authenticate all communication between the RADIUS client (the WAAS device) and the RADIUS server.
Timeout	Number of seconds that the WAAS device waits for a response from the specified RADIUS authentication server before declaring a timeout.
Servers	RADIUS servers that the WAAS device is to use for RADIUS authentication.
IP	Hostname or IP address of the RADIUS server.
Port	Port number on which the RADIUS server is listening.

Related Commands (config) radius-server

show running-config

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

show running-config

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

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

Table 3-55 describes the fields shown in the **show snmp alarm-history** display.

Table 3-55 Field Descriptions for the show snmp alarm-history Command

Field	Description
Index	Displays serial number of the listed alarms.
Type	Indicates whether the alarm has been Raised (R) or Cleared (C).
Sev	Levels of alarm severity: Critical (Cr), Major (Ma), or Minor (Mi)
Alarm ID	Traps sent by a WAE contain numeric alarm IDs.
ModuleID	Traps sent by a WAE contain numeric module IDs. (See the table below to map module names to module IDs.)
Category	Traps sent by a WAE contain numeric category IDs. (See the table below to map category names to category IDs.)
Descr	Provides description of the WAAS software alarm and the application that generated the alarm.

Table 3-56 summarizes the mapping of module names to module IDs.

Table 3-56 Summary of Module Names to ID Numbers

Module Name	Module ID
AD_DATABASE	8000
NHM	1
NHM/NHM	2500
nodemgr	2000
standby	4000
sysmon	1000
UNICAST_DATA_RECEIVER	5000
UNICAST_DATA_SENDER	6000

Table 3-57 summarizes the mapping of category names to category IDs.

Table 3-57 Summary of Category Names to ID Numbers

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

Table 3-58 describes the fields shown in the **show snmp engineID** display.

Table 3-58 Field Descriptions for the show snmp engineID

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

Table 3-59 describes the fields shown in the **show snmp event** display. The **show snmp event** command displays information about the SNMP events that were set using the "snmp trigger" command:

Table 3-59 Field Descriptions for the show snmp event Command

Field	Description
Mgmt Triggers	Output for management triggers, which are numbered 1, 2, 3, and so on in the output.
(1): Owner:	Name of the person who configured the trigger. "CLI" is the default owner; the system has a default trigger configured.

Table 3-59 Field Descriptions for the show snmp event Command (continued)

Field	Description
(1):	Name for the trigger. This name is locally-unique and administratively assigned. For example, this field might contain the "isValid" trigger name. Numbering indicates that this is the first management trigger listed in the **show** output.
Comment:	Description of the trigger's function and use. For example: WAFS license file is not valid.
Sample:	Basis on which the test sample is being evaluated. For example: Abs (Absolute) or Delta.
Freq:	Frequency. Number of seconds to wait between trigger samplings. To encourage consistency in sampling, the interval is measured from the beginning of one check to the beginning of the next and the timer is restarted immediately when it expires, not when the check completes.
Test:	Type of trigger test to perform based on the SNMP trigger configured. The Test field may contain the following types of tests: Absent—Absent existence of a test Boolean—Boolean value test Equal—Equality threshold test Falling—Falling threshold test Greater-than—Greater-than threshold test Less-than—Less-than threshold test On-change—Changed existence test Present—Present present test Rising—Rising threshold test
ObjectOwner:	Name of the object owner who created the trigger using the **snmp trigger create** global configuration command or by using an SNMP interface. "CLI" is the default owner.
Object:	String identifying the object.
Boolean Entry:	
Value:	Object identifier of the MIB object to sample to see whether the trigger should fire.
Cmp:	Comparison. Type of boolean comparison to perform. The numbers 1–6 correspond to these Boolean comparisons: unequal (1) equal (2) less (3) lessOrEqual (4) greater (5) greaterOrEqual (6)

Table 3-59 Field Descriptions for the show snmp event Command (continued)

Field	Description
Start:	Starting value for which this instance will be triggered.
ObjOwn:	Object owner.
Obj:	Object.
EveOwn:	Event owner.
Eve:	Event. Type of SNMP event. For example: CLI_EVENT.
Delta Value Table:	Table containing trigger information for delta sampling.
(0):	
Thresh:	Threshold value to check against if the trigger type is threshold.
Exis:	Type of existence test to perform. Values are 1 or 0.
Read:	Indicates whether the MIB instance has been queried or not.
OID:	Object ID (Same as MIB instance).
val:	Value ID.
(2):	MIB instance on which the trigger is configured. This is the second management trigger listed in the **show** output. The fields are repeated for each instance listed in this **show** command.

Table 3-60 describes the fields shown in the **show snmp group** display.

Table 3-60 Field Descriptions for the show snmp group Command

Field	Description
groupname	Name of the SNMP group, or collection of users who have a common access policy.
security_model	Security model used by the group (either v1, v2c, or v3).
readview	String identifying the read view of the group.
writeview	String identifying the write view of the group.
notifyview	string identifying the notify view of the group.

Table 3-61 describes the fields shown in the **show snmp stats** display.

Table 3-61 Field Descriptions for the show snmp stats Command

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.

Table 3-61 Field Descriptions for the show snmp stats Command (continued)

Field	Description
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Table 3-62 describes the fields shown in the **show snmp user** display.

Table 3-62 Field Descriptions for the show snmp user Command

Field	Description
User name	String identifying the name of the SNMP user.
Engine ID	String identifying the name of the copy of SNMP on the device.
Group Name	Name of the SNMP group, or collection of users who have a common access policy.

Related Commands

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

snmp trigger

show ssh

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

show ssh

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-63 describes the fields shown in the **show ssh** display.

Table 3-63 Field Descriptions for the show ssh Command

Field	Description
SSH server supports SSH2 protocol (SSH1 compatible).	Protocol support statement.
SSH service is not enabled.	Status of whether the SSH service is enabled or not enabled.
Currently there are no active SSH sessions.	Number of active SSH sessions.
Number of successful SSH sessions since last reboot:	Number of successful SSH sessions since last reboot.
Number of failed SSH sessions since last reboot:	Number of failed SSH sessions since last reboot.
SSH key has not been generated or previous key has been removed.	Status of the SSH key.
SSH login grace time value is 300 seconds.	Time allowed for login.
Allow 3 password guess(es).	Number of password guesses allowed.

Related Commands

(config) ssh-key-generate

(config) sshd

show standby

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

show standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

Table 3-64 describes the fields shown in the **show standby** display.

Table 3-64 Field Descriptions for the show standby Command

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the **description** option of the **interface** global configuration command.
IP address	IP address of the standby group.
netmask	Netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
priority	Priority status of each interface.
Active interface	Interfaces that are currently active in the standby group.
Maximum errors allowed on the active interface	Maximum number of errors allowed on the active interface.

Related Commands

show interface

show running-config

show startup-config

(config-if) standby

show startup-config

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

show startup-config

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

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

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

Examples

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

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

Related Commands

(config) authentication

clear

show authentication

show statistics 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 is registered with the WAAS Central Manager:

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

show statistics dre

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

show statistics dre

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-65 describes the fields shown in the **show statistics dre** display. This command shows the aggregated statistics for all connections.

Table 3-65 Field Descriptions for the show statistics dre Command

Field	Description
Cache	Aggregated DRE cache data statistics.
Status	Current DRE status. Status values include: Initializing, Usable, Temporarily Fail, and Fail.
Oldest Data (age)	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s). For example, "1d1h" means 1 day, 1 hour.
Total usable disk size	Total disk space allocated to the DRE cache.
Used (%)	Percentage of the total DRE cache disk space being used.
Hash table RAM size	Amount of memory allocated for the DRE hash table.
Used (%)	Percentage of allocated memory being used for the DRE hash table.
Completed Connections	
Total (cumulative):	Number of cumulative connections that have been processed.
Active:	Number of connections that are still open.
Encode	Statistics for compressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for compressed messages. msg = Total number of messages. in = Number of bytes before compression. out = Number of bytes after compression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE bypass	Number of DRE messages that were bypassed for compression.

Table 3-65 Field Descriptions for the show statistics dre Command (continued)

Field	Description
LZ: [msg | in | out | ratio]	Number of LZ messages. **Note** LZ compression is applied after DRE compression is applied. (DRE compression is always applied first.)
LZ Bypass: [msg | in | out | ratio]	Number of LZ messages that were bypassed for compression.
Average Latency	Average time to compress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Decode	Statistics for decompressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for decompressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were decompressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass [msg | in]	Number of DRE messages that were bypassed for decompression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for decompression.
Latency (Last 3 sec): [max | avg]	Maximum time to decompress one message for both DRE and LZ in milliseconds (ms). Average time to decompress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)

Related Commands

debug

show statistics dre connection

show statistics dre peer

show statistics dre connection

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

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

Syntax Description

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

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

Using this command without any options displays a one-line summary of all the TCP connections on the WAE for which DRE is applied. To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as, peer no.) show summary information and not details.

Examples

Table 3-66 describes the fields shown in the **show statistics dre connection** display.

Table 3-66 Field Descriptions for the show statistics dre connection Command

Field	Description
Conn-ID	Connection ID assigned by the device for each connection.
Peer No.	Number assigned to the peer compression device.
Client-ip:port	IP address and port of the client device that initialized the TCP connection, such as the user's PC or laptop.
Server-ip:port	IP address and port of the server.
Encode-in	Number of bytes in for compression.
Decode-in	Number of bytes in for decompression.
PID	Peer ID. MAC address of the peer device.
Status	State of the connection and the duration of that state. Possible values are Active or Closed. A = active C = closed For example, C(22h) shows that the connection has been closed for 22 hours.

Related Commands

debug

show statistics dre connection

show statistics dre peer

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

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

Syntax Description

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

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-67 describes the fields shown in the **show statistics dre peer** display. This command shows the DRE peer device connection information.

Table 3-67 Field Descriptions for the show statistics dre peer Command

Field	Description
Peer-No	Number assigned to the peer compression device.
Context	Context ID for the DRE debugging trace.
Peer-ID	MAC address of the peer device.
Hostname	Hostname of the peer device.
Cache	DRE cache data statistics as shown by the peer.
Used disk:	Number of megabytes (MB) used on the disk for the DRE cache.
Age:	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s).
Connections:	
Total (cumulative):	Number of cumulative connections that have been processed.
Active:	Number of connections that are still open.

Table 3-67 Field Descriptions for the show statistics dre peer Command (continued)

Field	Description
Concurrent connections (Last 2 min):	
max	Maximum number of concurrent connections in the last two minutes.
avg	Average number of concurrent connections in the last two minutes.
Encode	Statistics for compressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for compressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for compression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for compression.
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Decode	Statistics for decompressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for decompressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were decompressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for decompression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for decompression.
Latency (Last 3 sec): [max | avg]	Maximum time to decompress one message for both DRE and LZ in milliseconds (ms). Average time to decompress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)

Related Commands

debug

show statistics dre connection

show statistics epm

To display EndPoint Mapper (EPM) statistics for a WAE, use the **show statistics epm** EXEC command.

show statistics epm

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

This command displays the number of total requests and responses recorded.

Examples

Table 3-68 describes the fields shown in the **show statistics epm** display.

Table 3-68 Field Descriptions for the show statistics epm Command

Field	Description
Total requests	Number of requests processed by the EPM adaptor (incremented once for each connection).
success	Number of EPM requests which were successfully parsed by the EPM adaptor.
fault	Number of connections which were not successfully handled because of a bad client request (or a valid request that does not require processing by the EPM adaptor).
Total responses	Number of responses processed by the EPM adaptor (incremented once for each connection).
policy match	Number of connections which were successfully handled by the EPM adaptor, such as “dynamic match created,” for example.
UUID not configured	Number of times that a client requested a service that is not configured in the policy engine.
service unavailable	Number of times that a client requested a service, which the server reported to be unavailable.
fault	Number of connections which were not successfully handled because of a bad client response or because of an internal error which occurred while processing the client response.

Related Commands

(config) policy-engine application map adaptor EPM

show statistics 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

Table 3-69 describes the fields shown in the **show statistics icmp** display.

Table 3-69 Field Descriptions for the show statistics icmp Command

Field	Description
ICMP messages received	Total number of Internet Control Message Protocol (ICMP) messages which the entity received, including all those counted as ICMP input errors.
ICMP messages receive failed	Number of ICMP messages which the entity received but determined as having ICMP-specific errors, such as bad ICMP checksums, bad length, and so forth.
Destination unreachable	Number of ICMP messages of this type received.
Timeout in transit	Number of ICMP messages of this type received.
Wrong parameters	Number of ICMP messages of this type received.
Source quenches	Number of ICMP messages of this type received.
Redirects	Number of ICMP messages of this type received.
Echo requests	Number of ICMP messages of this type received.
Echo replies	Number of ICMP messages of this type received.
Timestamp requests	Number of ICMP messages of this type received.
Timestamp replies	Number of ICMP messages of this type received.
Address mask requests	Number of ICMP messages of this type received.
Address mask replies	Number of ICMP messages of this type received.

Table 3-69 Field Descriptions for the show statistics icmp Command (continued)

Field	Description
ICMP messages sent	Total total number of ICMP messages which this entity attempted to send. This counter includes all those counted as ICMP output errors.
ICMP messages send failed	Number of number of ICMP messages which this entity did not send because of problems discovered within ICMP, such as a lack of buffers.
Destination unreachable	Number of ICMP messages of this type sent out.
Time exceeded	Number of ICMP messages of this type sent out.
Wrong parameters	Number of ICMP messages of this type sent out.
Source quenches	Number of ICMP messages of this type sent out.
Redirects	Number of ICMP messages of this type sent out.
Echo requests	Number of ICMP messages of this type sent out.
Echo replies	Number of ICMP messages of this type sent out.
Timestamp requests	Number of ICMP messages of this type sent out.
Timestamp replies	Number of ICMP messages of this type sent out.
Address mask requests	Number of ICMP messages of this type sent out.
Address mask replies	Number of ICMP messages of this type sent out.

Related Commands clear

show statistics ip

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

show statistics ip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-70 describes the fields shown in the **show statistics ip** display.

Table 3-70 Field Descriptions for the show statistics ip Command

Field	Description
IP statistics	
Total packets in	Total number of input datagrams received from interfaces, including all those counted as input errors.
with invalid address	Number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as, 0.0.0.0) and addresses of unsupported Classes (such as, Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
with invalid header	Number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatches other format errors, time-to-live exceeded errors, and errors discovered in processing their IP options.
forwarded	Number of input datagrams for which this entity was not their final IP destination, and as a result, an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were source-routed by way of this entity, and the source-route option processing was successful.

Table 3-70 Field Descriptions for the show statistics ip Command (continued)

Field	Description
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).
Total packets out	Total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
dropped	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (such as, for lack of buffer space). This counter includes datagrams counted in the forwarded field if any such packets meet this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in the forwarded field which meet this no-route criterion, including any datagrams that a host cannot route because all of its default gateways are down.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Total number of IP datagrams that have been successfully fragmented at this entity.
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented because their Don’t Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Related Commands

clear

(config) ip

(config-if) ip

show ip routes

show statistics netstat

To display Internet socket connection statistics for a WAAS device, use the **show statistics netstat** EXEC command.

show statistics netstat

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-71 describes the fields shown in the **show statistics netstat** display.

Table 3-71 Field Descriptions for the show statistics netstat Command

Field	Description
Active Internet connections (w/o servers)	The following output prints the list of all open Internet connections to and from this WAE.
Proto	Layer 4 protocol used on the Internet connection, such as, TCP, UDP, and so forth.
Recv-Q	Amount of data buffered by the Layer 4 protocol stack in the receive direction on a connection.
Send-Q	Amount of data buffered by the Layer 4 precool stack in the send direction on a connection.
Local Address	IP address and Layer 4 port used at the WAE end point of a connection.
Foreign Address	IP address and Layer 4 port used at the remote end point of a connection.
State	Layer 4 state of a connection. TCP states include the following: ESTABLISHED, TIME-WAIT, LAST-ACK, CLOSED, CLOSED-WAIT, SYN-SENT, SYN-RCVD, SYN-SENT, SYN-ACK-SENT, and LISTEN.

show statistics radius

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

show statistics radius

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-72 describes the fields shown in the **show statistics radius** display.

Table 3-72 Field Descriptions for the show statistics radius Command

Field	Description
RADIUS Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.
Number of authorization success responses	Number of authorization success responses.
Accounting	
Number of accounting requests	Number of accounting requests.

Table 3-72 Field Descriptions for the show statistics radius Command (continued)

Field	Description
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands

clear

(config) radius-server

show radius-server

show statistics services

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

show statistics services

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-73 describes the fields shown in the **show statistics services** display.

Table 3-73 Field Descriptions for the show statistics services Command

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

Related Commands

show services

show statistics snmp

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

show statistics snmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-74 describes the fields shown in the **show statistics snmp** display.

Table 3-74 Field Descriptions for the show statistics snmp Command

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.

Table 3-74 Field Descriptions for the show statistics snmp Command (continued)

Field	Description
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Related Commands

show snmp

(config) snmp-server user

(config) snmp-server view

show statistics tacacs

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

show statistics tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-75 describes the fields shown in the **show statistics tacacs** display.

Table 3-75 Field Descriptions for the show statistics tacacs Command

Field	Description
TACACS+ Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.
Number of authorization success responses	Number of authorization success responses.
Accounting	
Number of accounting requests	Number of accounting requests.

Table 3-75 Field Descriptions for the show statistics tacacs Command (continued)

Field	Description
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands

clear

(config) tacacs

show tacacs

show statistics tcp

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

show statistics tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-76 describes the fields shown in the **show statistics tcp** display.

Table 3-76 Field Descriptions for the show statistics tcp Command

Field	Description
TCP statistics	
Server connection openings	Number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Client connection openings	Number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Failed connection attempts	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Connections established	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Connections resets received	Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Connection resets sent	Number of TCP segments sent containing the RST flag.
Segments received	Total number of segments received, including those received in error. This count includes segments received on currently established connections.

Table 3-76 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
Segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Bad segments received	Number of bad segments received.
Segments retransmitted	Total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Retransmit timer expirations	Number of TCP packets retransmitted due to retransmit timer expiry.
Server segments received	Number of TCP packets received from the server.
Server segments sent	Number of TCP packets sent to the server.
Server segments retransmitted	Number of TCP packets retransmitted to the server.
Client segments received	Number of TCP packets received from the client.
Client segments sent	Number of TCP packets sent to the client.
Client segments retransmitted	Number of TCP packets retransmitted to the client.
TCP extended statistics	
Sync cookies sent	Number of SYN-ACK packets sent with SYN cookies in response to SYN packets.
Sync cookies received	Number of ACK packets received with the correct SYN cookie that was sent in the SYN-ACK packet by the device.
Sync cookies failed	Number of ACK packets received with the incorrect SYN cookie that was sent in the SYN-ACK packet by the device.
Embryonic connection resets	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state, the SYN-SENT state, or the SYN-ACK-SENT state.
Prune message called	Number of times that the device exceeded the memory pool allocated for the connection.
Packets pruned from receive queue	Number of packets dropped from the receive queue of the connection because of a memory overrun.
Out-of-order-queue pruned	Number of times that the out-of-order queue was pruned because of a memory overrun.
Out-of-window Icmp messages	Number of ICMP packets received on a TCP connection that were out of the received window.
Lock dropped Icmp messages	Number of ICMP packets dropped because the socket is busy.
Arp filter	Number of ICMP responses dropped because of the ARP filter.
Time-wait sockets	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets recycled	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets killed	Number of times that the TCP connection made a transition to the CLOSED state from TIME-WAIT state.

Table 3-76 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
PAWS passive	Number of incoming SYN packets dropped because of a PAWS check failure.
PAWS active	Number of incoming SYN-ACK packets dropped because of a PAWS check failure.
PAWS established	Number of packets dropped in ESTABLISHED state because of a PAWS check failure.
Delayed acks sent	Number of delayed ACKs sent.
Delayed acks blocked by socket lock	Number of delayed ACKs postponed because the socket is busy.
Delayed acks lost	Number of delayed ACKs lost.
Listen queue overflows	Number of incoming TCP connections dropped because of a listening server queue overflow.
Connections dropped by listen queue	Number of incoming TCP connections dropped because of an internal error.
TCP packets queued to prequeue	Number of incoming TCP packets prequeued to a process.
TCP packets directly copied from backlog	Number of incoming TCP packets copied from the backlog queue directly to a process.
TCP packets directly copied from prequeue	Number of incoming TCP packets copied from the prequeue directly to a process.
TCP prequeue dropped packets	Number of packets removed from the TCP prequeue.
TCP header predicted packets	Number of TCP header-predicted packets.
Packets header predicted and queued to user	Number of TCP packets header-predicted and queued to the user.
TCP pure ack packets	Number of ACK packets received with no data.
TCP header predicted acks	Number of header-predicted TCP ACK packets.
TCP Reno recoveries	Number of TCP Reno recoveries.
TCP SACK recoveries	Number of TCP SACK recoveries.
TCP SACK reneging	Number of TCP SACK reneging.
TCP FACK reorders	Number of TCP FACK reorders.
TCP SACK reorders	Number of TCP SACK reorders.
TCP Reno reorders	Number of TCP Reno reorders.
TCP TimeStamp reorders	Number of TCP TimeStamp reorders.
TCP full undos	Number of TCP full undos.
TCP partial undos	Number of TCP partial undos.
TCP DSACK undos	Number of TCP DSACK undos.
TCP loss undos	Number of TCP loss undos.
TCP losses	Number of TCP losses.
TCP lost retransmit	Number of TCP lost retransmit.
TCP Reno failures	Number of TCP Reno failures.

Table 3-76 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
TCP SACK failures	Number of TCP SACK failures.
TCP loss failures	Number of TCP loss failures.
TCP fast retransmissions	Number of TCP fast retransmissions.
TCP forward retransmissions	Number of TCP forward retransmissions.
TCP slowstart retransmissions	Number of TCP slow start retransmissions.
TCP Timeouts	Number of TCP timeouts.
TCP Reno recovery fail	Number of TCP Reno recovery fail.
TCP Sack recovery fail	Number of TCP Sack recovery failures.
TCP scheduler failed	Number of TCP scheduler failures.
TCP receiver collapsed	Number of TCP receiver collapsed failures.
TCP DSACK old packets sent	Number of TCP DSACK old packets sent.
TCP DSACK out-of-order packets sent	Number of TCP DSACK out-of-order packets sent.
TCP DSACK packets received	Number of TCP DSACK packets received.
TCP DSACK out-of-order packets received	Number of TCP DSACK out-of-order packets received.
TCP connections abort on sync	Number of TCP connections aborted on sync.
TCP connections abort on data	Number of TCP connections aborted on data.
TCP connections abort on close	Number of TCP connections aborted on close.
TCP connections abort on memory	Number of TCP connections aborted on memory.
TCP connections abort on timeout	Number of TCP connections aborted on timeout.
TCP connections abort on linger	Number of TCP connections aborted on linger.
TCP connections abort failed	Number of TCP connections abort failed.
TCP memory pressures	Number of times the device approaches the allocated memory pool for the TCP stack.

Related Commands

clear

show tcp

(config) tcp

show statistics tfo

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

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

Syntax Description

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

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-77 describes the fields shown in the **show statistics tfo** command.

Table 3-77 Field Descriptions for the show statistics tfo Command

Field	Description
Total number of optimized connections	Total number of TCP connections that were optimized since the last TFO statistics reset.
No. of active connections	Total number of TCP optimized connections.
No. of pending (to be accepted) connections	Number of TCP connections that will be optimized but are currently in the setup stage.
No. of connections closed normally	Number of optimized connections closed without any issues using TCP FIN.
No. of connections closed with error	Number of optimized connection closed with some issues or using TCP RST.
Total number of peers	Number of active peer WAEs. (Every connection is optimized between two WAEs: this one and a peer WAE.)
No. of entries into overload mode	Number of times the WAE entered into an overload state. (In the overload state, new connections are set to pass-through. This state occurs for various reasons, such as reaching the maximum number of concurrent connections.
No. of connections reset due to	Details for number of connections closed with error.
Socket write failure	Failed to write on a socket (either on the LAN or WAN side).
Socket read failure	Failed to read from a socket (either LAN or WAN side).

Table 3-77 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
Opt socket close while waiting to write	The socket between two WAEs (WAN socket) closed before completing writing into it.
Unopt socket close while waiting to write	The socket between the WAE and the client/server (LAN socket) closed before completing writing into it.
Opt socket error close while waiting to read	The socket between two WAEs (WAN socket) closed before completing reading from it.
Unopt socket error close while waiting to read	The socket between the WAE and the client/server (LAN socket) closed before completing reading from it.
DRE decode failure	DRE internal error while decoding data. (Should not happen.)
DRE encode failure	DRE internal error while encoding data. (Should not happen.)
Connection init failure	Failed to setup the connection although auto-discovery finished successfully.
Opt socket unexpected close while waiting to read	The socket between two WAEs (WAN socket) closed before completing reading from it.
Exceeded maximum number of supported connections	Connection closed ungracefully because the WAE reached its scalability limit.
Buffer allocation or manipulation failed	Internal memory allocation failure. (Should not happen.)
Peer received reset from end host	TCP RST sent by the server or client. (Can be normal behavior and does not necessarily indicate a problem.)
DRE connection state out of sync	DRE internal error. (Should not happen.)
Memory allocation failed for buffer heads	Internal memory allocation failure. (Should not happen.)

Related Commands

show tfo accelerators

show tfo bufpool

show tfo connection

show tfo status

show statistics udp

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

show statistics udp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-78 describes the fields shown in the **show statistics udp** display.

Table 3-78 Field Descriptions for the show statistics udp Command

Field	Description
UDP statistics	
Packets received	Total number of UDP datagrams delivered to UDP users.
Packets to unknown port received	Total number of received UDP datagrams for which there was no application at the destination port.
Packet receive error	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Packet sent	Total number of UDP datagrams sent from this entity.

show statistics wccp

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

show statistics wccp gre

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

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

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

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

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

Examples

Table 3-79 describes the fields shown in the **show statistics wccp gre** display.

Table 3-79 Field Descriptions for the show statistics wccp gre Command

Field	Description
Transparent GRE packets received	Total number of GRE packets received by the WAE, regardless of whether or not they have been intercepted by WCCP. GRE is a Layer 3 technique that allows packets to reach the WAE, even if there are any number of routers in the path to the WAE.
Transparent non-GRE packets received	Number of non-GRE packets received by the WAE, either using the traffic interception and redirection functions of WCCP in the router hardware at Layer 2 or Layer 4 switching (a Content Switching Module [CSM]) that redirects requests transparently to the WAE.
Transparent non-GRE packets passed through	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the redirected packet's IP header has a zero TTL.
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.

Table 3-79 Field Descriptions for the show statistics wccp gre Command (continued)

Field	Description
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.
Packets failed encapsulated reassembly	Number of reassembled GRE encapsulated packets that were dropped because they failed the reassembly sanity check. Reassembled GRE encapsulated packets are composed of two or more GRE encapsulated fragments. This field is related to the previous statistic.
Packets failed GRE encapsulation	Number of GRE packets that are dropped by the WAE because they could not be redirected due to problems while encapsulating the packet with a GRE header.
Packets dropped due to invalid fwd method	Number of GRE packets that are dropped by the WAE because it was redirected using GRE but the WCCP service was configured for Layer 2 redirection.
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no conn at all	Number of packets that failed to be associated with an existing flow because no TCP port was listening. WCCP can also handle asymmetric packet flows and always maintains a consistent mapping of web servers to caches regardless of the number of switches or routers used in a WCCP service group (up to 32 routers or switches communicating with up to 32 WAEs in a cluster).
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.

Table 3-79 Field Descriptions for the show statistics wccp gre Command (continued)

Field	Description
Packets due to clean wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Packets received with client IP addresses	Number of packets that are associated to a connection flow that is being spoofed. By spoofing a client's IP address, the WAE can receive packets with the client IP (which is different from the WAE's own IP address) and send the packet to the correct application that is waiting for the packet.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
Packets dropped due to received on loopback	Number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined to a local address of the device. There is no valid or usable route for the packet.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).
Packets fragmented for bypass	Number of GRE packets that do not contain enough data to hold an IP header.
Packet pullups needed	Number of times a packet had to be consolidated as part of its processing. Consolidation is required when a packet is received as fragments and the first fragment does not contain all the information needed to process it.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.

Related Commands

(config) wccp access-list

(config) wccp flow-redirect

(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

Use the **show windows-domain** EXEC command to view the Windows domain server statistics, then clear the counters for these statistics by entering the **clear statistics windows-domain** EXEC command.

Examples

Table 3-80 describes the fields shown in the **show statistics windows-domain** display.

Table 3-80 Field Descriptions for the show statistics windows-domain Command

Field	Description
Windows Domain Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.
Number of authorization success responses	Number of authorization success responses.
Accounting	

Table 3-80 Field Descriptions for the show statistics windows-domain Command (continued)

Field	Description
Number of accounting requests	Number of accounting requests.
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands

windows-domain

(config) windows-domain

show sysfs

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

Table 3-81 describes the fields shown in the **show sysfs volumes** display.

Table 3-81 Field Descriptions for the show sysfs volumes Command

Field	Description
sysfs 00–04	System file system and disk number.
/local/local1–5	Mount point of the volume.
nnnnnnKB	Size of the volume in kilobytes.
nn% free	Percentage of free space in the SYSFS partition.

Related Commands

disk

(config) disk

show tacacs

To display TACACS+ authentication protocol configuration information for a WAAS device, use the **show tacacs** EXEC command.

show tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-82 describes the fields shown in the **show tacacs** display.

Table 3-82 Field Descriptions for the show tacacs Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for authorization or configuration authentication.
TACACS+ Configuration	TACACS+ server parameters.
TACACS+ Authentication	Indicates whether TACACS+ authentication is enabled on the the WAAS device.
Key	Secret key that the WAE uses to communicate with the TACACS+ server. The maximum number of characters in the TACACS+ key should not exceed 99 printable ASCII characters (except tabs).
Timeout	Number of seconds that the WAAS device waits for a response from the specified TACACS+ authentication server before declaring a timeout.
Retransmit	Number of times that the WAAS device is to retransmit its connection to the TACACS+ if the TACACS+ timeout interval is exceeded.
Password type	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.

Table 3-82 Field Descriptions for the show tacacs Command (continued)

Field	Description
Server	Hostname or IP address of the TACACS+ server.
Status	Indicates whether server is the primary or secondary host.

Related Commands

clear

show statistics tacacs

show tacacs

(config) tacacs

show tcp

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

show tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-83 describes the fields shown in the **show tcp** display. This command displays the settings configured with the **tcp** global configuration command.

Table 3-83 Field Descriptions for the show tcp Command

Field	Description
TCP Configuration	
TCP keepalive timeout XX sec	Length of time that the WAAS device is set to keep a connection open before disconnecting.
TCP keepalive probe count X	Number of times the WAAS device will retry a connection before the connection is considered unsuccessful.
TCP keepalive probe interval XX sec	Length of time (in seconds) that the WAAS device is set to keep an idle connection open.
TCP explicit congestion notification disabled	Configuration status of the TCP explicit congestion notification feature. Values are enabled or disabled.
TCP cwnd base value X	Value (in segments) of the send congestion window.
TCP initial slowstart threshold value X	Threshold (in segments) for slow start.
TCP increase (multiply) retransmit timer by X	Number of times set to increase the length of the retransmit timer base value.
TCP memory_limit	
Low water mark	Lower limit (in MB) of memory pressure mode, below which TCP enters into normal memory allocation mode.
High water mark (pressure)	Upper limit (in MB) of normal memory allocation mode, beyond which TCP enters into memory pressure mode.
High water mark (absolute)	Absolute limit (in MB) on TCP memory usage.

Related Commands

clear

show statistics tcp

(config) tcp

show tech-support

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

show tech-support [**page**]

Syntax Description

page	(Optional) Displays output page by page.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

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)
...
```

Related Commands

show version

show hardware

show disks details

show running-config

show processes

show processes memory
show memory
show interface
show cdp entry
show cdp neighbors
show statistics wccp
show alarms all
show statistics tfo
show statistics tfo application
show statistics tfo saving
show statistics tfo pass-through
show statistics tfo peer
show tfo auto-discovery
show tfo status
show tfo accelerators
show tfo bufpool accounting
show policy-engine status
show policy-engine application
show statistics dre
show statistics dre peer
show statistics tcp
show statistics ip
show statistics icmp
show standby
show statistics netstat
show disks SMART-info
show disks SMART-info details
show disks failed-sectors

show telnet

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

show telnet

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

EXEC

Device Modes

application-accelerator

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 [**blacklist** {**entries** [**netmask** *netmask*] [|] | **statistics** [|]}] [**list**] [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}]

Syntax Description

blacklist	(Optional) Displays the blacklist servers table.
entries	Displays all of the entries in the auto-discovery blacklist server table.
netmask	Displays the network mask to filter the table output.
netmask	Network mask (A.B.C.D/) for which you want to show the matching addresses.
statistics	Displays the auto-discovery blacklist server table management statistics.
list	(Optional) Lists TCP flows that the WAE is currently optimizing or passing through.
|	(Optional) Output modifier.
begin	Begins with the line that matches the regular expression.
regex	Regular expression to match. You can enter multiple expressions.
exclude	Excludes lines that match the regular expression.
include	Includes lines that match the regular expression.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

```
WAE# show tfo auto-discovery
Auto discovery structure:
       Allocation Failure:                          0
       Allocation Success:                          6615
       Deallocations:                               6615
       Timed Out:                                   0
Auto discovery table:
       Bucket Overflows:                            0
       Table Overflows:                             0
       Entry Adds:                                  6615
       Entry Drops:                                 6615
       Entry Count:                                 0
       Lookups:                                     6624
Bind hash add failures:                             0
Route Lookup:
       Failures:                                    0
       Success:                                     0
Socket:
       Allocation failures:                         0
       Accept pair allocation failures:             0
```

```
        Unix allocation failures:                    0
        Connect lookup failures:                     0
Packets:
        Memory allocation failures:                  0
        Total Sent:                                  6624
        Total Received:                              13228
        Incorrect length or checksum received:       0
        Invalid filtering tuple received:            0
        Received for dead connection:                0
        Ack dropped in synack received state:        0
        Non Syn dropped in nostate state:            0
Auto discovery failure:
        No peer or asymmetric route:                 6604
        Insufficient option space:                   0
        Invalid connection state:                    0
        Missing Ack conf:                            0
Auto discovery success TO:
        Internal server:                             0
        External server:                             0
Auto discovery success FOR:
        Internal client:                             0
        External client:                             0
Auto discovery success SYN retransmission:
        Zero retransmit:                             0
        One retransmit:                              0
        Two+ retransmit:                             0
Auto discovery Miscellaneous:
        Intermediate device:                         0
        RST received:                                0
        SYNs found with our device id:               0
        SYN retransmit count resets:                 0
ce105-16-docs-ce1#
```

Related Commands

show statistics tfo

show tfo accelerators

show tfo bufpool

show tfo connection

show tfo filtering

show tfo status

show tfo bufpool

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

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

Syntax Description

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

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

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

Related Commands

show tfo accelerators

show tfo auto-discovery

show tfo connection

show tfo filtering

show tfo status

show statistics tfo

show tfo connection

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

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

Syntax Description

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

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

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

Examples

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

```
WAE# show tfo connection summary

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

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

Related Commands

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

show tfo 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** [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*] }]] [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}]

Syntax Description

list	(Optional) Lists TCP flows that the WAE is currently optimizing or passing through.
|	(Optional) Output modifier.
begin	Begins with the line that matches the regular expression.
regex	Regular expression to match. You can enter multiple expressions.
exclude	Excludes lines that match the regular expression.
include	Includes lines that match the regular expression.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

Examples

The following examples display TFO connection information for the WAE:

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

```
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:

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

Related Commands

show statistics tfo

show tfo accelerators

show tfo auto-discovery

show tfo bufpool

show tfo connection

show tfo filtering

show tfo synq

To display the cumulative statistics for the SynQ module, use the **show tfo synq** EXEC command.

show tfo synq [**list** [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}]] [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}]

Syntax Description

list	(Optional) Lists the connections tracked in the SynQ module.
|	(Optional) Output modifier.
begin	Begins with the line that matches the regular expression.
regex	Regular expression to match. You can enter multiple expressions.
exclude	Excludes lines that match the regular expression.
include	Includes lines that match the regular expression.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show tfo synq list** command to list connections that are currently being tracked in the SynQ module.

Examples

The following example displays the output for the **show tfo synq** command:

```
WWAE# show tfo synq
Synq structures allocations success:                  0
Synq structures allocations failure:                  0
Synq structures deallocations:                        0
Synq table entry adds:                                0
Synq table entry drops:                               0
Synq table entry lookups:                             0
Synq table overflows:                                 0
Synq table entry count:                               0
Packets received by synq:                             0
Packets received with invalid filtering tuple:        0
Non-syn packets received:                             0
Locally originated/terminating syn packets received:  0
Retransmitted syn packets received while in Synq:     0
Synq user structure allocations success:              0
Synq user structure allocations failure:              0
Synq user structure deallocations:                    0
```

show transaction-logging

To display the transaction log configuration settings and a list of archived transaction log files for a WAE, use the **show transaction-logging** EXEC command.

show transaction-logging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

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

Examples

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

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

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

Exporting files to ftp servers is disabled.
```

Related Commands

clear

transaction-log

(config) transaction-logs

show user

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

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

Syntax Description

uid	Displays user information based on the identification number of the user.
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

Table 3-84 describes the fields shown in the **show user** display.

Table 3-84 Field Descriptions for the show user Command

Field	Description
Uid	User ID number.
Username	Username.
Password	Login password. This field does not display the actual password.
Privilege	Privilege level of the user.
Configured in	Database in which the login authentication is configured.

Related Commands

clear

show users administrative

(config) username

show users administrative

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

Table 3-85 describes the fields shown in the **show users administrative history** display.

Table 3-85 Field Descriptions for the show users administrative history Command

Field	Description
Username	Users that have logged in to this appliance CLI during the historical period.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that logged in to this appliance.
Loggin details	Day of the week, month, date, time, and whether or not the user is still logged in.

Table 3-86 describes the fields shown in the **show users administrative logged-in** display.

Table 3-86 Field Descriptions for the show users administrative logged-in Command

Field	Description
Username	Users currently logged in to the appliance CLI.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that is logged in to this appliance.
Loggin details	Day of week, month, date, and time that each user logged in.

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

Table 3-87 describes the fields shown in the **show version** display.

Table 3-87 Field Descriptions for the show version Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) year by Cisco Systems, Inc. Cisco Wide Area Application Services Software Release XXX (build bXXX month day year)	Software application, copyright, release, and build information.
Version	Version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Comple information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.

show 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 {**tcp-promiscuous**} [**summary**]

show wccp gre

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

show wccp modules

show wccp routers

show wccp services [**detail**]

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

show wccp status

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-88 describes the fields shown in the **show wccp gre** display.

Table 3-88 Field Descriptions for the show wccp gre Command

Field	Description
Transparent GRE packets received	Total number of GRE packets received by the WAE, regardless of whether or not they have been intercepted by WCCP. GRE is a Layer 3 technique that allows packets to reach the WAE, even if there are any number of routers in the path to the WAE.
Transparent non-GRE packets received	Number of non-GRE packets received by the WAE, either using the traffic interception and redirection functions of WCCP in the router hardware at Layer 2 or Layer 4 switching (a Content Switching Module [CSM]) that redirects requests transparently to the WAE.
Transparent non-GRE packets passed through	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the redirected packet's IP header has a zero TTL.
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.

Table 3-88 Field Descriptions for the show wccp gre Command (continued)

Field	Description
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.
Packets failed encapsulated reassembly	Number of reassembled GRE encapsulated packets that were dropped because they failed the reassembly sanity check. Reassembled GRE encapsulated packets are composed of two or more GRE encapsulated fragments. This field is related to the previous statistic.
Packets failed GRE encapsulation	Number of GRE packets that are dropped by the WAE because they could not be redirected due to problems while encapsulating the packet with a GRE header.
Packets dropped due to invalid fwd method	Number of GRE packets that are dropped by the WAE because it was redirected using GRE but the WCCP service was configured for Layer 2 redirection.
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no conn at all	Number of packets that failed to be associated with an existing flow because no TCP port was listening. WCCP can also handle asymmetric packet flows and always maintains a consistent mapping of web servers to caches regardless of the number of switches or routers used in a WCCP service group (up to 32 routers or switches communicating with up to 32 WAEs in a cluster).
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.

Table 3-88 Field Descriptions for the show wccp gre Command (continued)

Field	Description
Packets due to clean wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Packets received with client IP addresses	Number of packets that are associated to a connection flow that is being spoofed. By spoofing a client's IP address, the WAE can receive packets with the client IP (which is different from the WAE's own IP address) and send the packet to the correct application that is waiting for the packet.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
Packets dropped due to received on loopback	Number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined to a local address of the device. There is no valid or usable route for the packet.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).
Packets fragmented for bypass	Number of GRE packets that do not contain enough data to hold an IP header.
Packet pullups needed	Number of times a packet had to be consolidated as part of its processing. Consolidation is required when a packet is received as fragments and the first fragment does not contain all the information needed to process it.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.

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 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

Table 3-89 describes the fields shown in the **show windows-domain** display.

Table 3-89 Field Descriptions for the show windows-domain Command

Field	Description
Login Authentication for Console/Telnet Session:	Status of the primary login authentication method for the session: enabled or disabled.
Configuration Authentication for Console/Telnet Session: enabled (secondary)	Status of the secondary login authentication method for the session:enabled or disabled.
Windows domain Configuration:	Shows the Windows domain configuration settings.
Workgroup	Workgroup identification string.
Comment	Comment line.
Net BIOS	Windows NetBIOS name for the WAE.
Realm	Kerberos Realm (similar to the Windows domain name, except for Kerberos)
WINS Server	IP address of the WINS server.
Password Server	Kerberos server DNS name.
Security	Type of authentication configured, either “Domain” for NTLM or “ADS” for Kerberos.
Administrative groups	
Super user group	Active Directory(AD) group name. Users in this group have administrative rights.
Normal user group	AD group name. Users in this group have the normal/default privilege level in the WAE.

Related Commands windows-domain
(config) windows-domain

shutdown

To shut down the WAAS device use the **shutdown** EXEC command.

shutdown [**poweroff**]

Syntax Description		
	poweroff	(Optional) Turns off the power after closing all applications and operating system.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

A controlled shutdown refers to the process of properly shutting down a WAAS device without turning off the power on the device. With a controlled shutdown, all of the application activities and the operating system are properly stopped on a WAE, but the power remains on. Controlled shutdowns of a WAAS device can help you minimize the downtime when the WAAS device is being serviced.

Caution If a controlled shutdown is not performed, the WAAS file system can be corrupted. Rebooting the WAAS device takes longer if it was not properly shut down.

Note A WAAS device cannot be powered on again through the WAAS software after a software poweroff. You must press the power button once on a WAAS device to bring it back online.

The **shutdown** EXEC command facilitates a proper shutdown for WAAS device, and is supported on all WAE hardware models. The **shutdown poweroff** command is also supported by all of the WAE hardware models as they support the ACPI.

The **shutdown** command closes all applications and stops all system activities, but keeps the power on. The fans continue to run and the power LED is on, indicating that the device is still powered on. The device console displays the following menu after the shutdown process is completed:

```
================= SHUTDOWN SHELL =================
System has been shut down.


You can
0. Power down system by pressing and holding power button
1. Reload system by software
2. Power down system by software
[1-2]?
```

The **shutdown poweroff** command closes all applications and the operating system, stops all system activities, and turn off the power. The fans stop running and the power LED starts flashing, indicating that the device has been powered off.

Note If you use the **shutdown** or **shutdown poweroff** commands, the device does not perform a file system check when you power on and boot the device the next time.

Table 3-90 describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

Table 3-90 Description of the shutdown Command Operations

Activity	Process
User performs a shutdown operation on the WAE	Shutdown poweroff `WAE# shutdown poweroff`
User intervention to bring WAE back online	After a shutdown poweroff, you must press the power button once to bring the WAAS device back online.
File system check	Is *not* performed after you turn the power on again and reboot the WAAS device.

You can enter the **shutdown** EXEC command from a console session or from a remote session (Telnet or SSH version 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	Configures 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) Treats the specified MIB variable name as having a wildcard.
wait-time	(Optional) Number of seconds, 60–600, to wait between trigger samples.
absent	(Optional) Applies the absent existence test.
LINE	(Optional) Description of the threshold being created.
mibvar1, mibvar2, mibvar3	(Optional) Adds a MIB object to the notification.
mibvar1, mibvar2, mibvar3	Name of the MIB object to add to the notification.
equal	Applies the equality threshold test.
absolute	(Optional) Uses an absolute sample type.
value	(Optional) Absolute or delta value for sample.
delta	Uses a delta sample type.
falling	Applies the falling threshold test.
greater-than	Applies the greater-than threshold test.
less-than	Applies the less-than threshold test.
on-change	Applies the changed existence test.
present	Applies the present test.
rising	Applies the rising threshold test.
delete	Removes a threshold for a MIB object.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

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	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) 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 -w 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) 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. (See also the **no** form of the **debug** EXEC command.)

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

undebug aaa accounting

undebug all

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

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

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

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

undebug cms

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

undebug dhcp

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

undebug epm

undebug logging all]

undebug ntp

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

undebug rbcp

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

undebug tfo {**buffer-mgr** | **connection** [**auto-discovery** [*acl*] | **comp-mgr** [*acl*] | **conn-mgr** [*acl*] | **filtering** [*acl*] | **netio-engine** [*acl*] | **policy-engine** [*acl*] | **synq** [*acl*] | *acl*] | **stat-mgr** | **translog**}

undebug translog export

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

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

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

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

undebug aaa accounting

undebug all

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

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

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

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

undebug cms

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

undebug dhcp

undebug emdb [**level** [*levelnum*]]

undebug logging all

undebug ntp

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

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

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

Syntax Description

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

cli	(Optional) Disables CLI debugging.
all	Disables all CLI debugging.
bin	Disables CLI command binary program debugging.
parser	Disables CLI command parser debugging.
cms	(Optional) Disables CMS debugging.
dataserver	(Optional) Disables data server debugging.
all	Disables all data server debugging.
clientlib	Disables data server client library module debugging.
server	Disables data server module debugging.
dhcp	(Optional) Disables DHCP debugging.
dre	(Optional) Disables DRE debugging.
aggregation	Disables DRE chunk-aggregation debugging.
all	Disables the debugging of all DRE commands.
cache	Disables DRE cache debugging.
connection	Disables DRE connection debugging.
aggregation [*acl*]	Disables DRE chunk-aggregation debugging for a specified connection.
cache [*acl*]	Disables DRE cache debugging for a specified connection.
core [*acl*]	Disables DRE core debugging for a specified connection.
message [*acl*]	Disables DRE message debugging for a specified connection.
misc [*acl*]	Disables DRE other debugging for a specified connection.
acl	ACL to limit connections traced.
core	Disables DRE core debugging.
message	Disables DRE message debugging.
misc	Disables DRE other debugging.
epm	(Optional) Disables the DCE-RPC EPM debugging.
logging	(Optional) Disables logging debugging.
all	Disables all logging debugging.
ntp	(Optional) Disables NTP debugging.
print-spooler	(Optional) Disables print spooler debugging.
all	Disables print spooler debugging using all debug features.
brief	Disables print spooler debugging using only brief debug messages.
errors	Disables print spooler debugging using only the error conditions.
warnings	Disables print spooler debugging using only the warning conditions.
rbcp	(Optional) Disables RBCP debugging.
snmp	(Optional) Disables SNMP debug commands.
all	Disables all SNMP debug commands.
cli	Disables SNMP CLI debugging.
main	Disables SNMP main debugging.
mib	Disables SNMP MIB debugging.

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

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

emdb	(Optional) Disables embedded database debugging.
level	(Optional) Disables the specified debug level for EMDB service.
levelnum	(Optional) Debug level to disable. (Level 0 disables debugging.)
rpc	(Optional) Disables the remote procedure calls (RPC) logs.
detail	Disables the RPC logs of priority “detail” level or higher.
trace	Disables the RPC logs of priority “trace” level or higher.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

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) Displays the 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	Displays the utility for troubleshooting NetBIOS name resolution and browsing.
getent	Displays the utility to get unified list of both local and PDC users and groups.
net	Displays the utility for administration of remote CIFS servers.
nmblookup	Displays the utility for troubleshooting NetBIOS name resolution and browsing.
smbclient	Displays the utility for troubleshooting the Windows environment and integration.
smbstatus	Displays the utility for inspecting the Samba server status, connected clients, etc.
smbtree	Displays the utility for inspecting the Windows network neighborhood structure and content.
tdbbackup	Displays the utility for backing up, verifying and restoring Samba database files.
tdbdump	Displays the utility for inspecting the Samba database files.
testparm	Displays the utility to validate *smb.conf* file correctness.
wbinfo	Displays the utility for Winbind and domain integration troubleshooting.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this command to activate the selected Windows domain diagnostic utility.

Examples

The following example shows the options available for the Get Entity utility:

```
WAE# windows-domain diagnostics getent --help
Usage: getent [OPTION...] database [key ...]
getent - get entries from administrative database.

  -s, --service=CONFIG       Service configuration to be used
  -?, --help                 Give this help list
      --usage                Give a short usage message
  -V, --version              Print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

Supported databases:
aliases ethers group hosts netgroup networks passwd protocols rpc
services shadow
```

The following example shows the options available for the NMB Lookup Utility for troubleshooting NetBIOS name resolution and browsing:

```
WAE# windows-domain diagnostics nmblookup -h
Usage: [-?TV] [--usage] [-B BROADCAST-ADDRESS] [-f VAL] [-U STRING] [-M VAL]
        [-R VAL] [-S VAL] [-r VAL] [-A VAL] [-d DEBUGLEVEL] [-s CONFIGFILE]
        [-l LOGFILEBASE] [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP]
        [-i SCOPE] <NODE> ...
```

The following example shows the options available for the Samba Client Utility for troubleshooting the Windows environment and integration:

```
WAE# windows-domain diagnostics smbclient -h
Usage: [-?EgVNkP] [--usage] [-R NAME-RESOLVE-ORDER] [-M HOST] [-I IP] [-L HOST]
        [-t CODE] [-m LEVEL] [-T <c|x>IXFqgbNan] [-D DIR] [-c STRING] [-b BYTES]
        [-p PORT] [-d DEBUGLEVEL] [-s CONFIGFILE] [-l LOGFILEBASE]
        [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP] [-i SCOPE]
        [-U USERNAME] [-A FILE] [-S on|off|required] service <password>
```

The following example shows the options available for the TDB Backup Utility:

```
WAE# windows-domain diagnostics tdbbackup -h
Usage: tdbbackup [options] <fname...>

   -h            this help message
   -s suffix     set the backup suffix
   -v            verify mode (restore if corrupt)
```

The following example shows the use of the -u option of the WinBind Utility to view the information about a user registered in a Windows domain:

```
WAE# windows-domain diagnostics wbinfo -u
administrator
guest
user98
tuser1

WAE# show user username user98
Uid             : 70012
Username        : user98
Password        : *****
Privilege       : super user
Configured in   : Windows Domain database

WAE# show user uid 70012
Uid             : 70012
```

```
Username        : user98
Password        : *****
Privilege       : super user
Configured in   : Windows Domain database
```

The following example shows how to register a Windows domain:

```
WAE# windows-domain diagnostics
        net join -S<domain server> -U<domain admin username>%<domain admin password>
```

Related Commands

(config) windows-domain

write

To save startup configurations on a WAAS device, use the **write** EXEC command.

write [**erase** | **memory** | **mib-data** | **terminal**]

Syntax Description

erase	(Optional) Erases startup configuration from NVRAM.
memory	(Optional) Writes the configuration to NVRAM. This is the default location for saving startup information.
mib-data	(Optional) Saves MIB persistent configuration data to disk.
terminal	(Optional) Writes the configuration to a terminal session.

Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC

Device Modes

application-accelerator

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