EXEC Mode Commands

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

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

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

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

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

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

```
WAE> enable
WAE#
```

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

```
WAE# exit
WAE>
```

cd

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

cd *directoryname*

Syntax Description		
	directoryname	Directory name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

deltree

dir

lls

ls

mkdir

pwd

clear arp-cache

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

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

Related Commands

license add

show interface

show license

show wccp

clear bmc

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

clear bmc [**event-log**]

Syntax Description		
	event-log	Clears BMC system events and logs.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

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

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

Related Commands

show bmc

clear cache

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

clear cache {**cifs** | **dre**}

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

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

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

Examples

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

```
WAE# clear cache cifs
```

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

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

Related Commands

license add

show cache http-metadatacache

show interface

show license

show wccp

clear cdp

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

```
WAE# clear cdp counters
```

Related Commands

license add

show interface

show license

show wccp

clear cifs msg-signing-servers

To clear the list of message signing servers, use the **clear cifs msg-signing-servers** EXEC command.

clear cifs msg-signing-servers {**all** | *list*}

Syntax Description

all	Clears the full list of message signing servers.
list	Clears only those servers specified in the colon separated list. Specify servers by IP address or fully qualified domain name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command operates only when the CIFS application accelerator is enabled.

Examples

The following example shows how to remove two message signing servers from the list:

```
WAE# clear cifs msg-signing-servers 10.11.12.13:10.11.20.34
```

Related Commands

show cifs

clear connection

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

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

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

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

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

Related Commands

show statistics connection

clear dre

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Examples

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

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

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

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

Related Commands

show dre

clear ip

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

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

Syntax Description

access-list	Clears the access list statistical information.
counters	Clears the IP access list counters.
acl-num	(Optional) Counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier of up to 30 characters, beginning with a letter.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

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

Related Commands

license add

show interface

show license

show wccp

clear license

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

clear license [*license-name*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

```
WAE# clear license
```

Related Commands

license add

show interface

show license

show wccp

clear logging

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

clear logging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Examples

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

```
WAE# clear logging

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

Related Commands

license add

show interface

show license

show wccp

clear service-policy

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

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

Examples

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

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

The following example shows how to clear only AppNav class map and policy map counters:

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

Related Commands

show class-map

show policy-map

show statistics class-map

show statistics policy-sub-class

clear statistics

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

clear statistics {**all** | **aoim** | **appnav-controller all** | **authentication** | **auto-discovery** {**all** | **blacklist**} | **class-map**{**appnav** | **waas**} | **datamover** | **directed-mode** | **dre** [**global**] | **exporter** | **filtering** | **flow monitor type performance-monitor tcpstat-v1** | **generic-gre** | **icmp** | **inline** | **ip** | **pass-through** | **peer dre** | **punt** | **radius** | **service-insertion** {**appnav-controller** *ip_address* | **appnav-controller-group** | **data-path** | **service-context** | **service-node** *ip_address* | **service-node-group** *name*} | **snmp** | **synq** | **tacacs** | **tcp** | **tfo** | **udp** | **wccp** | **windows-domain** | **windows-print**}

Syntax Description

all	Clears all statistics.
aoim	Clears all of the application accelerator information manager statistics.
appnav-controller all	Clears all of the AppNav Controller statistics.
authentication	Clears authentication statistics.
auto-discovery	Clears the auto-discovery statistics.
blacklist	Clears the auto-discovery statistics for the blacklist.
class-map	Clears all class map statistics.
appnav	Clears all statistics for AppNav class maps.
waas	Clears all statistics for WAAS class maps.
datamover	Clears all of the data mover statistics.
directed-mode	Clears the directed mode statistics.
dre	Clears the Data Redundancy Elimination (DRE) statistics.
exporter	Clears the exporter statistics.
global	(Optional Clears the global DRE statistics.
filtering	Clears the filter table statistics.
flow	Clears the network traffic flow statistics.
monitor	Clears the monitor flow performance statistics.
tcpstat-v1	Clears the tcpstat-v1 collector statistics.
generic-gre	Clears the generic GRE statistics.
icmp	Clears the ICMP statistics.
inline	Clears the inline interception statistics.
ip	Clears the IP statistics.
pass-through	Clears all of the pass-through statistics.
peer dre	Clears all peer DRE statistics.
punt	Clears all the punt statistics.
radius	Clears the RADIUS statistics.
service-insertion	Clears AppNav service-insertion statistics.
appnav-controller *ip_address*	Clears statistics for the AppNav Controller with the specified IP address.
appnav-controller-group	Clears statistics for the AppNav Controller group.
data-path	Clears statistics for the data path.

service-context	Clears statistics for the service context.
service-node *ip_address*	Clears statistics for the service node (WN) with the specified IP address.
service-node-group *name*	Clears statistics for the service node group (WNG) with the specified name.
snmp	Clears the SNMP statistics.
synq	Clears the SynQ module statistics.
tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
tfo	Clears the TCP flow optimization (TFO) statistics.
udp	Clears the UDP statistics.
wccp	Clears all of the WCCP statistics.
windows-domain	Clears the Windows domain statistics.
windows-print	Clears all of the Windows print statistics.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

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

Examples

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

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

Related Commands

clear statistics accelerator

clear statistics connection

clear statistics accelerator

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

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

Related Commands

clear statistics

clear statistics connection

clear statistics connection

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

clear statistics connection conn-id *connection_id*

clear statistics connection optimized [**client-ip** {*ip_address* | *hostname*} | **client-port** *port* | {**cifs** | **epm** | **http** | **ica** | **mapi** | **nfs** | **smb** | **ssl** | **tfo** | **video** | **wansecure**} **dre** | **peer-id** *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*]

Syntax Description

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

server-ip	(Optional) Clears the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Clears the connection statistics for the server with the specified port number. The port number is from 1 to 65535.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

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

Related Commands

clear statistics

clear statistics accelerator

clear statistics monitor appnav-controller traffic

To clear traffic monitoring statistics for an AppNav Controller Interface Module, use the **clear statistics monitor appnav-controller traffic** EXEC command.

clear statistics monitor appnav-controller traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Examples

The following example shows how to clear the traffic monitoring statistics:

```
ANC# clear statistics monitor appnav-controller traffic
```

Related Commands

monitor appnav-controller traffic

show statistics monitor appnav-controller traffic

clear statistics vn-service vpath

To clear VPATH statistics for your vWAAS device, use the **clear statistics vn-service vpath** EXEC command.

clear statistics vn-service vpath

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **clear statistics vn-service vpath** command removes all current entries from the *syslog.txt* file but does not make an archive of the file. It puts a "Syslog cleared" message in the *syslog.txt* file to indicate that the syslog has been cleared.

Examples

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

```
WAE# clear statistics vn-service vpath
```

Related Commands

show statistics vn-service vpath

(config) vn-service vpath

clear transaction-log

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

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

Related Commands

license add

show interface

show license

show wccp

clear users

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

clear arp-cache

(config) authentication strict-password-policy

clear windows-domain

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

show windows-domain

clear windows-domain-log

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

clear windows-domain-log

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to clear all entries in the Windows domain log file on the WAAS device:

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

Related Commands

license add

show interface

show license

show wccp

clock

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

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

Examples

The following example shows how to set the software clock on the WAAS device:

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

Related Commands

show clock

cms

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

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

cms database {**backup** {**config**}| **create** | **delete**

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

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

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

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

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

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

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

The naming convention for backup files includes the time stamp and the WAAS version number.

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to back up the cms database management tables on the WAAS Central Manager named waas-cm:

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

The following example shows how to validate the cms database management tables on the WAAS Central Manager named waas-cm:

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

Related Commands

(config) cms

show cms

cms secure-store

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

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

Syntax Description

init	Initializes secure store encryption on the WAE device and opens the secure store. This option is valid only on WAE devices.
open	Activates secure store encryption (the WAAS device encrypts the stored data using secure store encryption). On WAEs, secure store encryption must already be initialized using the **cms secure-store init** command. This option is valid on all types of devices. On the Central Manager, this command is valid only when in user-provided passphrase mode and it prompts you to enter the secure store encryption pass phrase.
change	Changes the secure store encryption pass phrase and encryption key. On the Central Manager, this command prompts you to enter the current pass phrase, new pass phrase, and confirm the new pass phrase. The WAAS device uses the pass phrase to generate the encryption key for secure disk encryption. After this option is used, the Central Manager is in user-provided passphrase mode. This option is valid only on the primary Central Manager and WAE devices.
clear	Disables secure store encryption. This option is valid only on WAE devices.
reset	Resets secure store to the uninitialized state. You must initialize but not open secure store encryption and you must be in user-provided passphrase mode, to use this option. This option is valid only on primary Central Manager devices.
mode	Sets the secure store mode of opening. This option is valid only on primary Central Manager devices.
user-passphrase	Sets secure store to require a user-provided pass phrase to open after a reboot.
auto-passphrase	Sets secure store to automatically open after a reboot by using a unique system-generated pass phrase.

Defaults

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

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

For secure store on the Central Manager, the data is encrypted using a key encryption key generated from the pass phrase with SHA-1 hashing and an AES 256-bit algorithm. When you enable secure store on a WAE device, the data is encrypted using a 256-bit key encryption key generated by SecureRandom, a cryptographically strong pseudorandom number. You can use your own password to enable secure store, but it is not necessary in auto-generated passphrase mode (the default), where the Central Manager generates a unique password automatically. A user-supplied password must conform to the following rules:

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

If you are using the user-provided passphrase mode, when you reboot the Central Manager, you must manually reopen secure store using the **cms secure-store open** command. Until you open the secure store, a critical alarm is displayed on the Central Manager and services that use encryption (such as the SSL application accelerator) are not available. If you are using the auto-generated passphrase mode (the default), the Central Manager automatically opens the secure store after a reboot by using its own generated pass phrase.

The secure store passphrase mode on the primary Central Manager is replicated to the standby Central Manager (within the standard replication time). If the primary Central Manager is switched to auto-generated passphrase mode, the standby Central Manager secure store changes to the open state. If the primary Central Manager is switched to user-provided passphrase mode or the passphrase is changed, the standby Central Manager secure store changes to the initialized but not open state and an alarm is raised. You must manually open the secure store on the standby Central Manager.

When you enable secure store on a WAE, the WAE initializes and retrieves a new encryption key from the Central Manager. The WAE uses this key to encrypt user passwords, CIFS preposition and dynamic share credentials, and CIFS password credentials stored on the WAE. When you reboot the WAE after enabling secure store, the WAE retrieves the key from the Central Manager automatically, allowing normal access to the data that is stored in the WAAS persistent storage. If key retrieval fails, an alarm is raised and secure store will be in the initialized but not open state. You must open secure store manually.

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

Use the **cms secure-store reset** command if you reload a Central Manager that is configured in user-provided passphrase mode and you forget the secure store password. This command deletes all encrypted data, certificate and key files, and key manager keys. The secure store is left in the open state using auto-generated passphrase mode. For the complete procedure for resetting the secure store, see the "Resetting Secure Store Encryption on a Central Manager" section on page 9-17 in the *Cisco Wide Area Application Services Configuration Guide*.

Examples

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

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


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

Enter new passphrase:
Confirm passphrase:

Starting cms.
```

Related Commands

show cms secure-store

configure

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

configure

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

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Examples

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

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

Related Commands

(config) end

(config) exit

show running-config

show startup-config

copy cdrom

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

copy cdrom install *filedir filename*

Syntax Description		
	install *filedir filename*	Installs the software release from the directory location and filename specified.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Examples

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

```
WAE# copy cdrom install
```

Related Commands

install

reload

show running-config

show startup-config

write

copy cdrom wow-recovery

To recover Windows on WAAS on a virtual blade from a CD, use the **copy cdrom wow-recovery** EXEC command.

copy cdrom wow-recovery *filedir filename*

Syntax Description

wow-recovery *filedir filename*	Recovers Windows on WAAS installation files on the virtual blade from the directory location and Windows filename.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

This command is available only on platforms that have a CD-ROM drive. For platforms without a CD-ROM drive, use the **copy usb wow-recovery** EXEC command.

Examples

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

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

Related Commands

copy ftp

copy cdrom

copy usb

virtual-blade

(config) virtual-blade

copy compactflash

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

copy compactflash install *filename*

Syntax Description		
	install *filename*	Installs a software release from an image filename.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Examples

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

```
WAE# copy compactflash install
```

Related Commands

install

reload

show running-config

show startup-config

write

copy disk

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

install

reload

show running-config

show startup-config

write

copy ftp

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

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

copy ftp install {*hostname* | *ip-address*} *remotefiledir remotefilename*

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Use the **copy ftp disk** EXEC command to copy a file from an FTP server to a SYSFS partition on the WAAS device. To show progress, this command prints a number sign (#) for each 1 MB of data that is copied.

Use the **copy ftp install** EXEC command to install an image file from an FTP server on a WAAS device. Part of the image goes to a disk and part goes to flash memory. This command can also be used to install a BIOS or other firmware update by specifying the appropriate update file.

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

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

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

Examples

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

```
WAE# copy ftp install 10.1.1.1 cisco/waas/4.1 WAAS-4.1.1-k9.bin
Enter username for remote ftp server:biff
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER biff
10.1.1.1 FTP server (Version) Mon Feb 28 10:30:36 EST
2000) ready.
Password required for biff.
Sending:PASS *****
User biff logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:CWD //ftp-sj.cisco.com/cisco/waas/4.0
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:RETR WAAS-4.1.1-k9.bin
Opening BINARY mode data connection for ruby.bin (87376881 bytes).
################################################################################
writing flash component:
.............................................................
The new software will run after you reload.
```

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

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

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

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

Related Commands

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

copy http

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

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

Syntax Description

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

Defaults

HTTP server port: 80

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

install

reload

show running-config

show startup-config

write

copy monitoring-log

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

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

Syntax Description

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

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

(config) stats-collector logging

copy running-config

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

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

Syntax Description

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

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

install

reload

show running-config

show startup-config

write

copy scp

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

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

Examples

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

```
WAE#copy scp install 2.43.65.21 /work/admin ruby.test.bin
Enter usename for remote scp server: admin

                                WARNING!!!
                        READ THIS BEFORE ATTEMPTING TO LOGON

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

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

admin@2.43.65.21's password:
ruby.test.bin        100% |*****************************|   432 MB    00:13
Backing up existing version WAAS 5.1.0-b67, built on 02:20:49 Nov 29 2012 by damaster
Converting Manifest files ...  Done
Rebuilding image based on current software ...  Done
Backing up flash configuration ...  Done
Reclaiming unused flash safe state sectors ...SSMGR RETURNING: 4 (Success)
Done.
Detected OE574
Installing phase3 bootloader...
Installing WAE 64-bit image.
buildsysimg: short write on /swstore/comp.basesystem: Inappropriate ioctl for device
/swstore/default_ruby_installer.sh: problem running buildsysimg
Remove /swstore/backup to free up space.
Installing system image to flash... The new software will run after you reload.
```

Related Commands

install

copy sysreport

copy tech-support

copy startup-config

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

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

Syntax Description

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

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

install

reload

show running-config

show startup-config

write

copy sysreport

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

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

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

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

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

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

Syntax Description

disk *filename*	Copies system information to a disk file. Specify the name of the file to be created on a disk. Note that .tar.gz is appended to the filename that you specify.
ftp	Copies system information to a FTP server.
hostname	Hostname of the server.
ip-address	IP address of the server.
remotedirectory	Remote directory where the system information file is to be created on the server.
remotefilename	Remote filename of the system information file to be created on the server.
scp	Copies system information to a SCP server.
hostname	Hostname of the server.
ip-address	IP address of the server.
remotedirectory	Remote directory where the system information file is to be created on the server.
remotefilename	Remote filename of the system information file to be created on the server.
start-date	(Optional) Specifies the start date of the information in the generated system report.
day month	Start date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.
year	Start date year (1993–2035).
end-date	(Optional) Specifies the end date of information in the generated system report. If omitted, this date defaults to today. The report includes files through the end of this day.
day month	End date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.

year	End date year (1993–2035).
tftp	Copies system information to a TFTP server.
start-date	(Optional) Specifies the start date of the information in the generated system report.
day month	Start date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.
year	Start date year (1993–2035).
end-date	(Optional) Specifies the end date of information in the generated system report. If omitted, this date defaults to today. The report includes files through the end of this day.
usb *filename*	Copies system information to a USB flash drive installed in a WAVE-294/594/694/7541/7571/8541 device. Specify the name of the file to be created on the USB flash drive. Note that .tar.gz is appended to the filename that you specify.

Defaults

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

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

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

copy system-status

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

copy system-status disk *filename*

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

install

reload

show running-config

show startup-config

write

copy tech-support

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

Examples

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

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

Related Commands

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

copy tftp

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

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

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Examples

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

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

Related Commands

install

reload

show running-config

show startup-config

write

copy usb

To copy files from an external USB drive, use the **copy usb** EXEC command.

copy usb { **install** | **wow-recovery** *filename*}

Syntax Description

usb	Copies the file from an external USB drive
install	Installs a software release from an image filename.
wow-recovery *filename*	Restores the Windows on WAAS recovery file on the virtual blade from the specified file on the USB drive. Not available on devices in appnav-controller mode.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

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

This command is available only on platforms without a CD-ROM drive. For platforms with a CD-ROM drive, use the **copy cdrom wow-recovery install** EXEC command.

Examples

The following example shows how to recover Windows on a virtual blade from an external USB:

```
WAE# copy usb wow-recovery WoW_RECOVERY
```

Related Commands

copy cdrom wow-recovery

copy ftp

install

reload

show running-config

show startup-config

write

copy virtual-blade

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

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

Syntax Description

vb_num	Virtual blade number of the virtual blade disk image to copy to.
disk *vb_disk*	Specifies the virtual blade disk number of the virtual blade disk image to copy to.
ftp	Writes to an FTP server.
hostname	Hostname of the specific server.
ip-address	IP address of the specific server.
remotefiledir	Directory where the image file to be copied is located.
remotefilename	Name of the file to be copied.

Defaults

No default behaviors or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

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

Related Commands

copy ftp

install

reload

show running-config

show startup-config

write

cpfile

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

cpfile *oldfilename newfilename*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Only SYSFS files can be copied.

Examples

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

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

Related Commands

deltree

dir

lls

ls

mkdir

pwd

rename

crypto delete

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

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

Examples

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

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

Related Commands

crypto export

crypto generate

crypto import

crypto export

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

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

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

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

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

Related Commands

crypto delete

crypto generate

crypto import

crypto generate

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

```
WAE# crypto generate self-signed-cert myfile.p12 exportable rsa modulus 512
Generating a 512 bit RSA private key
..........++++++++++++
...++++++++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

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

WAE#
```

Related Commands

crypto delete

crypto export

crypto import

crypto import

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

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

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

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

Syntax Description

ca-certificate *filename*	Imports a certificate authority certificate file. The name of the CA certificate file to be imported (PEM format) must have .ca extension.
pkcs12 *filename*	Specifies a certificate intended for the management or an accelerated service (PKCS12 format). A PKCS12 file contains both the private encryption key and the public key certificate. The name of the PKCS12 file to be imported must have a .p12 extension. DSA-encoded certificates are not supported and will not be imported.
admin	Specifies that the certificate and key are for the Central Manager admin service. This option can be used only on the Central Manager.
exportable	(Optional) Configures the imported certificate to be exportable.
ignore-cert-chain-order	(Optional) Allows to import a certificate chain that does not have a strict order.
pem-cert-key	Imports both the certificate and key in PEM format. When you use the **pem-cert-key** keyword, you must specify the *pathname* and *filename* or the *address* and *filename* for both the certificate file and the key file for **disk**, **ftp**, **sftp**, and **tftp**.
pkcs12	Imports both the certificate and key in PKCS12 format.
disk *pathname*	Imports from a disk. Type the disk filename including the full path.
ftp *address*	Imports from FTP. Type the FTP server's IP address or hostname.
sftp *address*	Imports from secure FTP. Type the secure FTP server's IP address or hostname.
scep *url*	Imports from a SCEP server. Type the SCEP server's IP address.
terminal	Imports from a terminal.
tftp *address*	Imports from TFTP. Type the TFTP server's IP address or hostname.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

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

Note DSA certificates and keys cannot be imported.

Examples

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

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

Related Commands

crypto delete

crypto export

crypto generate

crypto pki

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

crypto pki managed-store initialize

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

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

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

Related Commands

crypto export

crypto generate

crypto import

debug aaa accounting

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

debug aaa accounting

undebug aaa accounting

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug aaa accounting
```

Related Commands

show debugging

debug aaa authorization

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

debug aaa authorization

undebug aaa authorization

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug aaa authorization
```

Related Commands

show debugging

debug accelerator

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Syntax Description

generic	Enables generic accelerator debugging.
connection	Enables accelerator connection debugging.
misc	Enables generic accelerator miscellaneous debugging.
shell	Enables accelerator shell debugging.
stats	Enables generic accelerator statistics debugging.
all	Enables all accelerator debugging of a specified type.
http	Enables HTTP accelerator debugging.
bypass-list	Enables HTTP accelerator bypass list debugging.
cli	Enables configuration CLI debugging.
conditional-response	Enables HTTP accelerator metadata cache conditional response debugging.
dre-hints	Enables HTTP accelerator DRE hinting debugging.
metadatacache	Enables HTTP accelerator metadata cache debugging.
redirect-response	Enables HTTP accelerator metadata cache redirect response debugging.
subnet	Enables HTTP accelerator subnet configuration debugging.
supress-server-encoding	Enables HTTP accelerator supress-server-encoding debugging.
transaction	Enables HTTP accelerator transaction debugging.
unauthorized-response	Enables HTTP accelerator metadata cache unauthorized response debugging.
ica	Enables ICA accelerator debugging.
ao-connectionmgr	Enables ICA AO-ConnectionMgr debugging.
ao-parser	Enables ICA AO-Parser debugging.
cgp	Enables ICA CGP debugging.
connection	Enables ICA AO-Connection debugging.
crypto	Enables ICA CRYPTO debugging.
detectionparser	Enables ICA detectionparser debugging.
failure	Enables ICA allocation failure debugging.

hash	Enables ICA HASH debugging.
ica	Enables ICA parsing debugging.
initialization	Enables ICA initialization debugging.
io	Enables ICA IO debugging.
main	Enables ICA main debugging.
pipe	Enables ICA pipe debugging.
shell	Enables ICA shell debugging.
mapi	Enables MAPI accelerator debugging.
Common-flow	Enables MAPI common flow debugging.
DCERPC-layer	Enables MAPI DCERPC layer flow debugging.
EMSMDB-layer	Enables MAPI EMSMDB layer flow debugging.
IO	Enables MAPI IO flow debugging.
ROP-layer	Enables MAPI ROP layer flow debugging.
ROP-parser	Enables MAPI ROP parser flow debugging.
RCP-parser	Enables MAPI RCP parser flow debugging.
shell	Enables MAPI shell flow debugging.
Transport	Enables MAPI transport flow debugging.
Utilities	Enables MAPI utilities flow debugging.
nfs	Enables NFS accelerator debugging.
async-write	Enables NFS asynchronous write optimization debugging.
attributes-cache	Enables NFS attributes cache debugging.
nfs-v3	Enables NFS version 3 layer debugging.
read-ahead	Enables NFS read ahead optimization debugging.
rpc	Enables NFS RPC layer debugging.
shell	Enables NFS shell debugging.
utils	Enables NFS utilities debugging.
smb	Enables SMB accelerator debugging.
cmd-close	Enables SMB close commands debugging.
cmd-create	Enables SMB create commands debugging.
cmd-lock	Enables SMB lock commands debugging.
cmd-others	Enables SMB other commands debugging.
cmd-query-info	Enables SMB query-info commands debugging.
cmd-read	Enables SMB read commands debugging.
cmd-set-info	Enables SMB set-info commands debugging.
cmd-write	Enables SMB write commands debugging.
flow	Enables SMB flow debugging.
large-data-flush	Enables SMB large data flush debugging.
lock-manager	Enables SMB lock manager debugging.
meta-data	Enables SMB meta data debugging.
named-pipe	Enables SMB named pipe debugging.
not-found-cache	Enables SMB not-found metadata cache debugging.

packeter	Enables SMB packeter debugging.
parser	Enables SMB parser debugging.
read-ahead	Enables SMB read-ahead debugging.
shell	Enables SMB shell debugging.
vfn	Enables SMB VFN debugging.
ssl	Enables SSL accelerator debugging.
accelerated-svc	Enables accelerated service debugging.
alarm	Enables SSL AO alarm debugging.
am	Enables SSL auth manager debugging.
am-generic-svc	Enables SSL am generic service debugging.
bio	Enables SSL bio layer debugging.
ca	Enables SSL cert auth module debugging.
ca-pool	Enables SSL cert auth pool debugging.
cipherlist	Enables SSL cipher list debugging.
client-to-server	Enables SSL client-to-server datapath debugging.
dataserver	Enables SSL dataserver debugging.
flow-shutdown	Enables SSL flow shutdown debugging.
ocsp	Enables SSL ocsp debugging.
oom-manager	Enables SSL oom-manager debugging.
openssl-internal	Enables SSL openssl internal debugging.
parser	Enables SSL accelerator parser debugging.
peering-svc	Enables SSL peering service debugging.
session-cache	Enables SSL session cache debugging.
shell	Enables SSL shell debugging.
sm-alert	Enables SSL session manager alert debugging.
sm-generic	Enables SSL session manager generic debugging.
sm-io	Enables SSL session manager i/o debugging.
sm-pipethrough	Enables SSL session manager pipethrough debugging.
synchronization	Enables SSL synchronization debugging.
verify	Enables SSL certificate verification debugging.
waas-to-waas	Enables SSL waas-to-waas datapath debugging.
video	Enables video accelerator debugging.
gateway	Enables debugging of the media independent gateway module of the video accelerator.
windows-media	Enables debugging of the Windows Media module of the video accelerator.
client-ip *ip-addr*	Specifies the client IP address.
server-ip *ip-addr*	Specifies the server IP address.
wansecure	Enables WANSECURE debugging.
flow	Enables WANSECURE flow debugging.
mux	Enables WANSECURE mux debugging.
ocsp	Enables WANSECURE ocsp debugging.

shell	Enables WANSECURE shell debugging.
ssl	Enables WANSECURE ssl debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

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

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug accelerator all
```

Related Commands

show debugging

debug all

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

debug all

undebug all

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable all debug monitoring:

```
WAE# debug all
```

Related Commands

show debugging

debug appnav-controller connection

To enable connection-specific debugging on an AppNav Controller Interface Module, use the **debug appnav-controller connection** EXEC command. To disable debugging, use the **undebug** form of this command.

debug appnav-controller connection access-list *acl-name*

undebug appnav-controller connection

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The ACL specified in this command is shared by the **monitor appnav-controller traffic** and **packet-capture** commands.

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable connection-specific debug monitoring for an AppNav Controller Interface Module:

```
WAE# debug appnav-controller connection access-list myacl
```

Related Commands

show debugging

debug appnav-controller drop capture

To enable debugging on an AppNav Controller Interface Module to capture dropped packets, use the **debug appnav-controller drop capture** EXEC command. To disable debugging, use the **no** form of this command.

debug appnav-controller drop capture index *index* **limit** *limit*

no debug appnav-controller drop capture

Syntax Description

index *index*	The number of the index; the default index value is 255.
limit *limit*	The maximum size of the packet capture file. The default limit is 65535.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

To display the index, use the **show controllers np counters direct-access drop** command.

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

The output associated with the **debug** command is written to a new log file in PCAP format.

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

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

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

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

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

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

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

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

Examples

The following example shows how to show dropped packets for the AppNav Controller Interface Module using an index of 20 and a limit of 500:

```
WAE# debug appnav-controller drop capture index 20 limit 500
WAE# show debugging
Appnav Controller Drop Capture enabled
    Index = 20
    Limit = 500
```

Related Commands

show debugging

debug authentication

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug auto-discovery

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

debug auto-discoveryconnection

undebug auto-discovery connection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug buf

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug buff all
```

Related Commands

show debugging

debug cdp

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

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

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

Syntax Description

adjacency	Enables CDP neighbor information debugging.
events	Enables CDP events debugging.
ip	Enables CDP IP debugging.
packets	Enables packet-related CDP debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug cdp events
```

Related Commands

show debugging

debug cli

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug cli all
```

Related Commands

show debugging

debug cmm

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug cmm all
```

Related Commands

show debugging

debug cms

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

debug cms

undebug cms

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable CMS debug monitoring:

```
WAE# debug cms
```

Related Commands

show debugging

debug connection

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug connection all
```

Related Commands

show debugging

debug controllers

To monitor and record interface controller capture debugging, use the **debug controllers** EXEC command. To disable debugging, use the **undebug** form of this command.

debug controllers NP {**crash-dump** | **dump-cfg**}

undebug controllers NP {**crash-dump** | **dump-cfg**}

Syntax Description

crash-dump	Requests a crash dump that is saved to a file.
dump-cfg	Captures the NP configuration into NPSL format.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to request a crash dump:

```
WAE# debug controllers NP crash-dump
```

Related Commands

show debugging

debug dataserver

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug dataserver all
```

Related Commands

show debugging

debug dhcp

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

debug dhcp

undebug dhcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable DHCP debug monitoring:

```
WAE# debug dhcp
```

Related Commands

show debugging

debug directed-mode

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

debug directed-mode connection

undebug directed-mode connection

Syntax Description

connection	(Optional) Enables directed mode connection debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable directed mode connection debugging:

```
WAE# debug directed-mode connection
```

Related Commands

show debugging

debug dre

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug dre all
```

Related Commands

show debugging

debug egress-method

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

debug egress-method connection

undebug egress-method connection

Syntax Description

connection	(Optional) Enables egress method connection debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug encryption-service

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug fda

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug fda all
```

Related Commands

show debugging

debug fdm

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug fdm all
```

Related Commands

show debugging

debug filtering

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

debug filtering connection

undebug filtering connection

Syntax Description

connection	(Optional) Enables filtering module connection debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug filtering connection
```

Related Commands

show debugging

debug flow

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

debug flow monitor type performance-monitor tcpstat-v1

undebug flow monitor type performance-monitor tcpstat-v1

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug generic-gre

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

debug generic-gre

undebug generic-gre

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug hw-raid

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug imd

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug imd all
```

Related Commands

show debugging

debug inline

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug inline warn
```

Related Commands

show debugging

debug key-manager

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

debug key-manager

undebug key-manager

Syntax Description

key-manager	(Optional) Enables key manager debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

central-manager (primary only)

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

show debugging

debug logging

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

debug logging all

undebug logging all

Syntax Description

all	Enables all logging debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug logging all
```

Related Commands

show debugging

debug monapi

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

debug monapi

undebug monapi

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

central-manager (primary only)

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug monapi
```

Related Commands

show debugging

debug nplogd

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

debug nplogd all

undebug nplogd all

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

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

```
WAE# debug nplogd all
```

Related Commands

show debugging

debug ntp

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

debug ntp

undebug ntp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable NTP debug monitoring:

```
WAE# debug ntp
```

Related Commands

show debugging

debug punt

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

debug punt {**all** | **module** | **packets** | **socket**}

undebug punt {**all** | **module** | **packets** | **socket**}

Syntax Description

all	Enables all punt handler debugging.
module	Enables only punt handler module debugging.
packets	Enables only punt handler packet debugging.
socket	Enables only punt handler socket call debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable all punt handler debug monitoring:

```
WAE# debug punt all
```

Related Commands

show debugging

debug rbcp

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

debug rbcp

undebug rbcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

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

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

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

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

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

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

Examples

The following example shows how to enable RBCP debug monitoring:

```
WAE# debug rbcp
```

Related Commands

show debugging

debug rmd

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

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

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

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

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

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all route manager debug monitoring:

```
WAE# debug rmd all
```

Related Commands

show debugging

debug rpc

To monitor and record remote procedure calls (RPC) debugging, use the **debug rpc** EXEC command. To disable debugging, use the **undebug** form of this command.

debug rpc {**detail** | **trace**}

undebug rpc {**detail** | **trace**}

Syntax Description

detail	Displays RPC logs of priority detail or higher.
trace	Displays RPC logs of priority trace or higher.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable RPC detail debug monitoring:

```
WAE# debug rpd detail
```

Related Commands

show debugging

debug service-insertion

To trace connections in the service-insertion module, use the **debug service-insertion** EXEC command. To disable debugging, use the **undebug** form of this command.

debug service-insertion connection

undebug service-insertion connection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all service-insertion module debug monitoring:

```
WAE# debug service-insertion connection
```

Related Commands

show debugging

debug service-policy

To monitor and record service policy debugging, use the **debug service-policy** EXEC command. To disable debugging, use the **undebug** form of this command.

debug service-policy type {**appnav** | **waas**}

undebug service-policy type {**appnav** | **waas**}

Syntax Description

appnav	Enables AppNav service policy debugging.
waas	Enables WAAS service policy debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.*#*, where *#* is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable WAAS service policy debug monitoring:

```
WAE# debug service-policy waas
```

Related Commands

show debugging

debug snmp

To monitor and record SNMP debugging , use the **debug snmp** EXEC command. To disable debugging, use the **undebug** form of this command.

debug snmp {**all** | **cli** | **main** | **mib** | **traps**}

undebug snmp {**all** | **cli** | **main** | **mib** | **traps**}

Syntax Description

all	Enables all SNMP debug commands.
cli	Enables SNMP CLI debugging.
main	Enables SNMP main debugging.
mib	Enables SNMP MIB debugging.
traps	Enables SNMP trap debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all SNMP debug monitoring:

```
WAE# debug snmp all
```

Related Commands

show debugging

debug standby

To enable standby debugging, use the **debug standby** EXEC command. To disable debugging, use the **undebug** form of this command.

debug standby [all]

undebug standby [all]

Syntax Description

all	(Optional) Enables standby debugging using all debug features.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all standby debug monitoring:

```
WAE# debug standby all
```

Related Commands

show debugging

debug statistics

To monitor and record statistics debugging, use the **debug statistics** EXEC command. To disable debugging, use the **undebug** form of this command.

debug statistics {**all** | **ao** | **client** | **collector** | **ipc** | **messages** | **serializer** | **sqm**}

undebug statistics {**all** | **ao** | **client** | **collector** | **ipc** | **messages** | **serializer** | **sqm**}

Syntax Description

all	Enables all statistics debug commands.
ao	Enables statistics acceleration debugging.
client	Enables statistics client debugging.
collector	Enables statistics collector debugging.
ipc	Enables statistics IPC debugging.
messages	Enables statistics messages/buffers debugging.
serializer	Enables statistics serializer debugging.
sqm	Enables statistics computation debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

services-controller

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all statistics debug monitoring:

```
WAE# debug statistics all
```

Related Commands

show debugging

debug synq

To trace synq connections setup, use the **debug synq** EXEC command. To disable debugging**,** use the **undebug** form of this command.

debug synq connection

undebug synq connection

Syntax Description

connection	Enables synq module connection debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable synq module connection debugging:

```
WAE# debug synq connection
```

Related Commands

show debugging

debug tfo

To monitor and record TFO flow optimization debugging, use the **debug tfo** EXEC command. To disable debugging, use the **undebug** form of this command.

debug tfo {**all** | **buffer-mgr** | **dre-flow** | **netio** | **scheduler**}

undebug tfo {**all** | **buffer-mgr** | **dre-flow** | **netio** | **scheduler**}

Syntax Description

all	Enables all TFO debugging.
buffer-mgr	Enables TFO data-buffer from buffer manager debugging.
dre-flow	Enables TFO DRE flow debugging for all connections.
netio	Enables TFO connection debugging for the network input/output module.
scheduler	Enables TFO scheduler debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable all TFO flow optimization debug monitoring:

```
WAE# debug tfo all
```

Related Commands

show debugging

debug translog

To monitor and record transaction logging debugging, use the **debug translog** EXEC command. To disable debugging, use the **undebug** form of this command.

debug translog {**detail** | **export** | **info**}

undebug translog {**detail** | **export** | **info**}

Syntax Description

detail	Enables transaction log detailed debugging.
export	Enables transaction log FTP export debugging.
info	Enables transaction log high level debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable transaction logging detail debug monitoring:

```
WAE# debug translog detail
```

Related Commands

show debugging

debug wafs

To set the log level of the WAFS Device Manager component, use the **debug wafs** EXEC command. To disable debugging, use the **undebug** form of this command.

debug wafs manager {**debug** | **error** | **info** | **warn**}

undebug wafs manager {**debug** | **error** | **info** | **warn**}

Syntax Description

manager	Sets the logging level for the Device Manager.
debug	Specifies debug.
error	Specifies error.
info	Specifies info.
warn	Specifies warn.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to set the log level for all WAFS components to error level:

```
WAE# debug wafs manager error
```

Related Commands

show debugging

debug wccp

To monitor and record WCCP information debugging, use the **debug wccp** EXEC command. To disable debugging, use the **undebug** form of this command.

debug wccp {**all** | **detail** | **error** | **events** | **keepalive** | **packets**}

undebug wccp {**all** | **detail** | **error** | **events** | **keepalive** | **packets**}

Syntax Description

all	Enables all WCCP debugging functions.
detail	Enables the WCCP detail debugging.
error	Enables the WCCP error debugging.
events	Enables the WCCP events debugging.
keepalive	Enables the debugging for WCCP keepalives that are sent to the applications.
packets	Enables the WCCP packet-related information debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 24.

If the watchdog utility is not running, the message "WAAS is not running" appears.

Use the **show debugging** command to display enabled **debug** options.

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

Examples

The following example shows how to enable WCCP information debug monitoring:

```
WAE# debug wccp all
```

Related Commands

show debugging

delfile

To delete a file from the current directory, use the **delfile** EXEC command.

delfile *filename*

Syntax Description

filename	Name of the file to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **delfile** EXEC command to remove a file from a SYSFS partition on the disk drive of the WAAS device.

Examples

The following example shows how to delete a temporary file from the */local1* directory using an absolute path:

```
WAE# delfile /local1/tempfile
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

deltree

To remove a directory with all of its subdirectories and files, use the **deltree** EXEC command.

deltree *directory*

Syntax Description

directory	Name of the directory tree to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **deltree** EXEC command to remove a directory and all files within the directory from the WAAS SYSFS file system. No warning is given that you are removing the subdirectories and files.

Note Make sure that you do not remove files or directories required for the WAAS device to function properly.

Examples

The following example shows how to delete the *testdir* directory from the */local1* directory:

```
WAE# deltree /local1/testdir
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

dir

To view details of one file or all files in a directory, use the **dir** EXEC command.

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **dir** EXEC command to view a detailed list of files contained within the working directory, including information about the file name, size, and time created. The **lls** EXEC command produces the same output.

Examples

The following example shows how to create a detailed list of all the files for the current directory:

```
WAE# dir
size          time of last change             name
-------------  -------------------------          -----------
         4096  Fri Feb 24 14:40:00 2006  <DIR>    actona
         4096  Tue Mar 28 14:42:44 2006  <DIR>    core_dir
         4096  Wed Apr 12 20:23:10 2006  <DIR>    crash
         4506  Tue Apr 11 13:52:45 2006           dbupgrade.log
         4096  Tue Apr  4 22:50:11 2006  <DIR>    downgrade
         4096  Sun Apr 16 09:01:56 2006  <DIR>    errorlog
         4096  Wed Apr 12 20:23:41 2006  <DIR>    logs
        16384  Thu Feb 16 12:25:29 2006  <DIR>    lost+found
         4096  Wed Apr 12 03:26:02 2006  <DIR>    sa
        24576  Sun Apr 16 23:38:21 2006  <DIR>    service_logs
         4096  Thu Feb 16 12:26:09 2006  <DIR>    spool
      9945390  Sun Apr 16 23:38:20 2006           syslog.txt
     10026298  Thu Apr  6 12:25:00 2006           syslog.txt.1
     10013564  Thu Apr  6 12:25:00 2006           syslog.txt.2
     10055850  Thu Apr  6 12:25:00 2006           syslog.txt.3
     10049181  Thu Apr  6 12:25:00 2006           syslog.txt.4
         4096  Thu Feb 16 12:29:30 2006  <DIR>    var
          508  Sat Feb 25 13:18:35 2006           wdd.sh.signed
```

The following example shows how to display the detailed information for only the *logs* directory:

```
WAE# dir logs
size          time of last change             name
-------------  -------------------------          -----------
```

```
4096  Thu Apr  6 12:13:50 2006  <DIR>    actona
4096  Mon Mar  6 14:14:41 2006  <DIR>    apache
4096  Sun Apr 16 23:36:40 2006  <DIR>    emdb
4096  Thu Feb 16 11:51:51 2006  <DIR>    export
  92  Wed Apr 12 20:23:20 2006           ftp_export.status
4096  Wed Apr 12 20:23:43 2006  <DIR>    rpc_httpd
   0  Wed Apr 12 20:23:41 2006           snmpd.log
4096  Sun Mar 19 18:47:29 2006  <DIR>    tfo
```

Related Commands

lls

ls

disable

To turn off privileged EXEC commands, use the **disable** EXEC command.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the WAAS software CLI EXEC mode for setting, viewing, and testing system operations. This command mode is divided into two access levels, user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access level prompt and specify the admin password when prompted for a password.

```
WAE> enable
Password:
```

The **disable** command places you in the user-level EXEC shell (notice the prompt change).

Examples

The following example shows how to enter the user-level EXEC mode from the privileged EXEC mode:

```
WAE# disable
WAE>
```

Related Commands

enable

disk

To configure disks on a WAAS device, use the **disk** EXEC command.

disk delete-partitions *diskname*

disk delete-data-partitions

disk disk-name *diskxx* **enable force**

disk disk-name disk*xx* **replace**

disk insert *diskname*

disk recreate-raid

disk scan-errors *diskname*

Syntax Description

delete-partitions *diskname*	Deletes data on the specified logical disk drive. After using this command, the WAAS software treats the specified disk drive as blank. All previous data on the drive is inaccessible. Specify the name of the disk from which to delete partitions (disk00, disk01). For RAID-5 systems, this option is not available because only one logical drive is available.
delete-data-partitions	Deletes all data partitions on all logical drives. Data partitions include the CONTENT, PRINTSPOOL, and GUEST partitions. These partitions include all DRE and CIFS cache files, print spool files, and any virtual blade images.
disk-name *diskxx* **enable force**	Reenables a defunct drive (with or without removing it) that has been previously shut down. **Note** This option is available only on RAID-5 systems.
disk-name disk*xx* **replace**	Shuts down the physical disk with the name disk*xx* (disk00, disk01, etc.) so that it can be replaced in the RAID-5 array. **Note** This option is available only on RAID-5 systems.
insert *diskname*	Instructs the SCSI host to rescan the bus to detect and mount the newly inserted disk. Specify the name of the disk to be inserted (disk00, disk01). **Note** This option is available only on WAE-612 models.
recreate-raid	Recreates the RAID-5 array. **Note** This option is available only on RAID-5 systems.
scan-errors *diskname*	Scans SCSI or IDE disks for errors and remaps the bad sectors if they are unused. Specify the name of the disk to be scanned (disk00, disk01). For RAID-5 systems, this command scans the logical RAID device for errors. On these systems, there is no *diskname* option.

Defaults

No default behavior or values.

Command Modes EXEC

Device Modes application-accelerator

central-manager

Usage Guidelines The WAAS software supports hot-swap functionality for both failed disk replacement and scheduled disk maintenance. On the WAE-612, use the **disk disk-name** *diskxx* **shutdown** global configuration command to shut down a disk for scheduled disk maintenance. On the WAE-674, WAE-7341, and WAE-7371, if a disk is shut down using the **disk disk-name diskxx replace** EXEC command and the same disk is removed and reinserted, it can be reenabled using the EXEC command **disk disk-name diskxx enable force**. This command is applicable even if the disk is not removed and needs to be reenabled. This command is not applicable if a new disk is inserted. On the WAE-7341 and WAE-7371, use the **disk disk-name** *diskxx* **replace** EXEC command to shut down a disk. (For the scheduled disk maintenance procedure, see the chapter "Maintaining Your WAAS System" in the *Cisco Wide Area Application Services Configuration Guide*.)

The disk hot-swap functionality automatically disables a failed disk if the system detects one critical disk alarm. The software removes the failed disk automatically regardless of the setting for **disk error-handling**.

For WAE-7341 and WAE-7371 models, when you replace a failed disk that was automatically disabled by the software, the disk automatically returns to service. For WAE-612 models, when you replace a failed disk that was automatically disabled by the software, use the **disk insert** EXEC command to bring the disk back into service. For all other models, see the **(config) disk disk-name** command section.

To identify which disks have been identified as failed or bad, use the **show disks failed-disk-id** EXEC command. Do not reinsert any disk with a serial number shown in this list.

Note The **show disks failed-disk-id** command is not available on WAE-7341 and WAE-7371 models.

Use the **disk delete-partitions** EXEC command to remove all disk partitions on a single disk drive on a WAAS device or to remove the disk partition on the logical drive for RAID-5 systems.

Caution Be careful when using the **disk delete-partitions** EXEC command because the WAAS software treats the specified disk drive as blank. All previous data on the drive will become inaccessible.

Note When you use the **disk delete-partitions** EXEC command on the WAE-7341 or WAE-7371 models, the command deletes the entire logical volume. The individual disk name option is not available on these platforms.

The **disk delete-data-partitions** command deletes the DRE and CIFS caches and all installed virtual blade images. If you want to keep virtual blade images, back them up before using this command by using the **copy virtual-blade** EXEC command.

After using the **disk delete-data-partitions** command, you must reload the device and the data partitions are automatically recreated and the caches are initialized, which can take several minutes. DRE optimization is not done until the DRE cache has finished initializing. The **show statistics dre** EXEC command reports "TFO: Initializing disk cache" until then. It is best not to interrupt DRE cache

initialization by reloading the device again until after cache initialization has finished. However, if DRE cache initialization is interrupted, on the next reboot the disk is checked, which takes extra time, and DRE initialization is completed again.

Examples

The following example shows how to recreate the RAID-5 array:

```
WAE# disk recreate-raid
```

Related Commands

(config) disk disk-name

(config) disk error-handling

(config) disk logical shutdown

show disks

dnslookup

To resolve a host or domain name to an IP address, use the **dnslookup** EXEC command.

dnslookup {*hostname* | *domainname*}

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 example shows how the **dnslookup** command is used to resolve the hostname *myhost* to IP address 172.31.69.11:

```
WAE# dnslookup myhost
official hostname: myhost.abc.com
          address: 172.31.69.11
```

The following example shows how the **dnslookup** command is used to resolve the hostname *abd.com* to IP address 192.168.219.25:

```
WAE# dnslookup abc.com
official hostname: abc.com
         address: 192.168.219.25
```

The following example shows how the **dnslookup** command is used to resolve an IP address used as a hostname to 10.0.11.0:

```
WAE# dnslookup 10.0.11.0
official hostname: 10.0.11.0
          address: 10.0.11.0
```

enable

To access privileged EXEC commands, use the **enable** EXEC command.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the WAAS software CLI EXEC mode for setting, viewing, and testing system operations. This command mode is divided into two access levels: user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access level prompt and specify the admin password when prompted for a password.

If using TACACS+ authentication, there is an enable password feature in TACACS+ that allows an administrator to define a different enable password for each user. If a TACACS+ user enters the **enable** EXEC command to access privileged EXEC mode, that user must enter the admin password defined by the TACACS+ server.

The **disable** command takes you from privileged EXEC mode to user EXEC mode.

Examples

The following example shows how to access privileged EXEC mode:

```
WAE> enable
WAE#
```

Related Commands

disable

exit

exit

To terminate privileged-level EXEC mode and return to the user-level EXEC mode, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

All modes

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **exit** EXEC command is equivalent to pressing **Ctrl-Z** or entering the **end** command. Entering the **exit** command in the user level EXEC shell terminates the console or Telnet session.

Examples

The following example shows how to terminate privileged-level EXEC mode and return to the user-level EXEC mode:

```
WAE# exit
WAE>
```

Related Commands

(config) exit

find-pattern

To search for a particular pattern in a file, use the **find-pattern** command in EXEC mode.

find-pattern {**binary** *reg-express filename* | **count** *reg-express filename* | **lineno** *reg-express filename* | **match** *reg-express filename* | **nomatch** *reg-express filename* | **recursive** *reg-express filename*}

find-pattern case {**binary** *reg-express filename* | **count** *reg-express filename* | **lineno** *reg-express filename* | **match** *reg-express filename* | **nomatch** *reg-express filename* | **recursive** *reg-express filename*}

Syntax Description

binary *reg-express filename*	Does not suppress the binary output. Specifies the regular expression to be matched and the filename.
count *reg-express filename*	Prints the number of matching lines. Specifies the regular expression to be matched and the filename.
lineno *reg-express filename*	Prints the line number with output. Specifies the regular expression to be matched and the filename.
match *reg-express filename*	Prints the matching lines. Specifies the regular expression to be matched and the filename.
nomatch *reg-express filename*	Prints the nonmatching lines. Specifies the regular expression to be matched and the filename.
recursive *reg-express filename*	Searches a directory recursively. Specifies the regular expression to be matched and the filename.
case	Matches a case-sensitive pattern.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to search a file recursively for a case-sensitive pattern:

```
WAE# find-pattern case recursive admin removed_core
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw-------    1 admin    root     97054720 Jan 11 11:31 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14086
-rw-------    1 admin    root     96845824 Jan 11 11:32 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14823
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
-rw-------    1 admin    root     96759808 Jan 11 12:59 /local/local1/core_dir/
```

```
core.cache.3.0.0.b131.cnbuild.20016
-rw-------    1 admin    root     97124352 Jan 11 13:26 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.8095
```

The following example shows how to search a file for a pattern and print the matching lines:

```
WAE# find-pattern match 10 removed_core
Tue Oct 12 10:30:03 UTC 2004
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
```

The following example shows how to search a file for a pattern and print the number of matching lines:

```
WAE# find-pattern count 10 removed_core
3
```

Related Commands

cd

dir

lls

ls

help

To obtain online help for the command-line interface, use the **help** EXEC command.

help

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC and global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

You can obtain help at any point in a command by entering a question mark (**?**). If nothing matches, the help list will be empty, and you must back up until entering a **?** shows the available options.

Two styles of help are provided:

- Full help is available when you are ready to enter a command argument (for example, **show ?**) and describes each possible argument.
- Partial help is provided when you enter an abbreviated command and you want to know what arguments match the input (for example, **show stat?**).

Examples

The following example shows how to display the output of the **help** EXEC command:

```
WAE# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered.
```

Related Commands

(config) help

install

To install a new software image (such as the WAAS software) on the WAAS device, use the **install** EXEC command.

install *filename*

Syntax Description

filename	Specifies the name of the *.bin* file you want to install.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

The **install** command loads the system image into flash memory and copies the disk-based software component to the software file system (swfs) partition. This command can also be used to install a BIOS or other firmware update by specifying the appropriate update file.

Note If you are installing a system image that contains optional software, make sure that an SWFS partition is mounted.

To install a system image, copy the image file to the SYSFS directory *local1*. Before executing the **install** command, change the present working directory to the directory where the system image resides. When the **install** command is executed, the image file is expanded. The expanded files overwrite the existing files on the WAAS device. The newly installed version takes effect after the system image is reloaded.

Note The **install** command does not accept .pax files. Files should be of the type .bin (for example, *cache-sw.bin*). Also, if the release being installed does not require a new system image, then it may not be necessary to write to flash memory. If the newer version has changes that require a new system image to be installed, then the **install** command may result in a write to flash memory.

Close your browser and restart the browser session to the WAAS Central Manager, if you installed a new software image to the primary WAAS Central Manager.

Examples

The following example shows how to load the system image contained in the *wae512-cache-300.bin* file:

```
WAE# install wae512-cache-300.bin
```

Related Commands copy disk
reload

less

To display a file using the Less application, use the **less** EXEC command.

less *file_name*

Syntax Description

file_name	Name of the file to be displayed.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Less is a pager application that displays text files one page at a time. You can use Less to view the contents of a file, but not edit it. Less offers some additional features when compared to conventional text file viewer applications such as Type. These features include the following:

- Backward movement—Allows you to move backward in the displayed text. Use **k**, **Ctrl-k**, **y**, or **Ctrl-y** to move backward. See the summary of Less commands for more details; to view the summary, press **h** or **H** while displaying a file in Less.
- Searching and highlighting—Allows you to search for text in the file that you are viewing. You can search forward and backward. Less highlights the text that matches your search to make it easy to see where the match is.
- Multiple file support—Allows you to switch between different files, remembering your position in each file. You can also do a search that spans all the files you are working with.

Examples

The following example shows how to display the text of the *syslog.txt* file using the Less application:

```
WAE# less syslog.txt
```

Related Commands

type

license add

To add a software license to a device, use the **license add** EXEC command.

license add *license-name*

Syntax Description

license-name	Name of the software license to add. The following license names are supported: • Transport—Enables basic DRE, TFO, and LZ optimization. • Enterprise—Enables the EPM, HTTP, MAPI, NFS, SSL, CIFS, and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization. • Video—Enables the video application accelerator. Requires the Enterprise license to be configured first. • Virtual-Blade—Enables the virtualization feature. Requires the Enterprise license to be configured first.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to install the enterprise license:

```
WAE# license add Enterprise
```

Related Commands

clear arp-cache license

show license

lls

To view a long list of directory names, use the **lls** EXEC command.

lls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a long list of files.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **lls** command provides detailed information about files and subdirectories stored in the present working directory (including the size, date, time of creation, SYSFS name, and long name of the file). This information can also be viewed with the **dir** command.

Examples

The following example shows how to display a detailed list of the files in the current directory:

```
WAE# lls
size          time of last change             name
--------------  ------------------------          -----------
          4096  Fri Feb 24 14:40:00 2006  <DIR>    actona
          4096  Tue Mar 28 14:42:44 2006  <DIR>    core_dir
          4096  Wed Apr 12 20:23:10 2006  <DIR>    crash
          4506  Tue Apr 11 13:52:45 2006           dbupgrade.log
          4096  Tue Apr  4 22:50:11 2006  <DIR>    downgrade
          4096  Sun Apr 16 09:01:56 2006  <DIR>    errorlog
          4096  Wed Apr 12 20:23:41 2006  <DIR>    logs
         16384  Thu Feb 16 12:25:29 2006  <DIR>    lost+found
          4096  Wed Apr 12 03:26:02 2006  <DIR>    sa
         24576  Sun Apr 16 23:54:30 2006  <DIR>    service_logs
          4096  Thu Feb 16 12:26:09 2006  <DIR>    spool
       9951236  Sun Apr 16 23:54:20 2006           syslog.txt
      10026298  Thu Apr  6 12:25:00 2006           syslog.txt.1
          4096  Thu Feb 16 12:29:30 2006  <DIR>    var
           508  Sat Feb 25 13:18:35 2006           wdd.sh.signed
```

Related Commands

dir

lls

ls

ls

To view a list of files or subdirectory names within a directory on the device hard disk, use the **ls** EXEC command.

ls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a list of files.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **ls** *directory* command to list the filenames and subdirectories within a particular directory.

Use the **ls** command to list the filenames and subdirectories of the current working directory.

Use the **pwd** command to view the present working directory.

Examples

The following example shows how to display the files and subdirectories that are listed within the root directory:

```
WAE# ls
actona
core_dir
crash
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
var
wdd.sh.signed
```

Related Commands

dir

lls

pwd

lsusb

To view a list of files or subdirectory names within a directory on a USB storage device, use the **lsusb** EXEC command.

lsusb [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a list of files.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **lsusb** *directory* command to list the filenames and subdirectories within a particular directory on the USB device.

Use the **lsusb** command to list the filenames and subdirectories of the current working directory on the USB device.

This command is available only on WAAS devices that support external USB storage devices.

Examples

The following example shows how to display the files and subdirectories that are listed within the root directory of a USB device:

```
WAE# lsusb
directory1
afile.txt
bfile.txt
```

Related Commands

dir

lls

ls

pwd

mkdir

To create a directory, use the **mkdir** EXEC command.

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to create a new directory, *oldpaxfiles*:

```
WAE# mkdir /oldpaxfiles
```

Related Commands

cpfile

dir

lls

ls

pwd

rename

rmdir

mkfile

To create a new file, use the **mkfile** EXEC command.

mkfile *filename*

Syntax Description		
	filename	Name of the file that you want to create.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **mkfile** EXEC command to create a new file in any directory of the WAAS device.

Examples

The following example shows how to create a new file, *traceinfo,* in the root directory:

```
WAE# mkfile traceinfo
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

monitor appnav-controller traffic

To enable traffic monitoring on an AppNav Controller Interface Module, use the **monitor appnav-controller traffic** EXEC command.

monitor appnav-controller traffic {**access-list** *acl-name* | **disable**}

Syntax Description

access-list *acl-name*	Name of the access list that determines which flows are monitored.
disable	Disables flow monitoring.

Defaults

Monitoring is disabled.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

Use this command to enable the AppNav Controller Interface Module to supply monitoring statistics for traffic flows that match the specified ACL. The ACL must be defined by the **ip access-list** global configuration command.

The ACL specified in this command is shared by the **packet-capture** and **debug appnav-controller** commands.

Use the **show statistics monitor appnav-controller traffic** EXEC command to display the monitoring statistics.

Use the **show monitor** EXEC command to display the status of traffic monitoring.

Examples

The following example shows how to enable traffic monitoring with an ACL:

```
ANC# monitor appnav-controller traffic access-list myacl
```

Related Commands

clear statistics monitor appnav-controller traffic

show monitor

show statistics monitor appnav-controller traffic

ntpdate

To set the software clock (time and date) on a WAAS device using an NTP server, use the **ntpdate** EXEC command.

ntpdate {*hostname* | *ip-address*} [**key** {*authentication-key*}]

Syntax Description

hostname	NTP hostname.
ip-address	NTP server IP address.
key	(Optional) Specifies to use authentication with the NTP server.
authentication-key	Authentication key string to use with the NTP server authentication. This value must be between 0 and 4294967295.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **ntpdate** command to find the current time of day and set the current time on the WAAS device to match. You must save the time to the hardware clock using the **clock save** command if you want to restore the time after a reload.

Examples

The following example shows how to set the software clock on the WAAS device using a NTP server:

```
WAE# ntpdate 10.11.23.40
```

Related Commands

clock

(config) clock

(config) ntp

show clock

show ntp

packet-capture

To capture packets on a device interface, use the **packet-capture** EXEC command.

packet-capture appnav-controller {**access-list** {*acl-name* | *acl-num*} | **interface** {**GigabitEthernet** *slot/port* | **TenGigabitEthernet** *slot/port* | **PortChannel** *index* | **standby** *grpnumber*} **access-list** {*acl-name* | *acl-num*}} [**file-size** *size* [**number-of-files** *num* | **stop-after-num-files** *num*]] [*capture-filename*]

packet-capture interface {**GigabitEthernet** *slot/port* | **TenGigabitEthernet** *slot/port* | **PortChannel** *index* | **standby** *grpnumber*} {**access-list** {*acl-name* | *acl-num*} | **destination-ip** {*hostname* | *ip-address*} | **destination-port** *port* | **source-ip** {*hostname* | *ip-address*} | **source-port** *port*} [**file-size** *size* [**number-of-files** *num* | **stop-after-num-files** *num*]] [*capture-filename*]

packet-capture decode [**destination-ip** {*hostname* | *ip-address*} | **destination-port** *port* | **source-ip** {*hostname* | *ip-address*} | **source-port** *port*] [**file-size** *size* [**number-of-files** *num* | **stop-after-num-files** *num*]] *capture-filename*

Syntax Description

appnav-controller	Capture packets on an AppNav Controller Interface Module interface.
access-list	Specifies an access list for which to capture packets across all AppNav Controller Interface Module interfaces. Applicable only if the **appnav-controller** keyword is specified.
acl-name	(Optional) Access list name.
acl-num	(Optional) Access list numeric identifier (0–99 for standard access lists and100–199 for extended access lists).
interface	Specifies the source interface from which to capture packets.
GigabitEthernet *slot/port*	Specifies a Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
TenGigabitEthernet *slot/port*	Specifies a 10-Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
PortChannel *index*	Specifies a port channel interface (1-4).
standby *grpnumber*	Specifies a standby group (1-2).
access-list	Specifies an access list for which to capture packets on the specified interface.
file-size *size*	(Optional) Specifies the maximum file size for captured output, from 1–100000 KB. After a file fills to capacity, another output file is created according to the following keywords.
number-of-files *num*	(Optional) Specifies the maximum number of output files to create (1–500), after which earlier files are overwritten as needed for more captured data.
stop-after-num-files *num*	(Optional) Specifies the maximum number of output files to create (1–500), after which packet capture is stopped.
capture-filename	(Optional) Specifies the name of a file to which output is saved. If no file is specified, output is sent to the console.
destination-ip	Captures packets matching the specified destination IP address.
hostname	Captures packets matching the specified destination or source hostname.
ip-address	Destination or source IP address.

destination-port *port*	Captures packets matching the specified destination port.
source-ip	Captures packets matching the specified source IP address.
source-port *port*	Captures packets matching the specified source port.
decode	Decodes captured packets.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Either packet capture or debug capture can be active, but not both simultaneously.

The **packet-capture** command is preferred over the deprecated commands **tcpdump** and **tethereal**, and is required to capture data plane traffic on an AppNav Controller Interface Module interface.

Examples

The following example shows how to capture packets on a normal interface:

```
WAE(config)# ip access-list extended 100 permit tcp any any range 23 35
WAE(config)# exit
WAE# packet-capture interface gig 0/1 access-list 100 mycapture
```

The following example shows how to capture packets on all interfaces on an AppNav Controller Interface Module:

```
WAE# packet-capture appnav-controller access-list 100 mycapture
```

Related Commands

tcpdump

tethereal

ping

To send echo packets for diagnosing basic network connectivity on networks, use the **ping** EXEC command.

ping [**management**] {*hostname* | *ip-address*}

Syntax Description

management	Uses the designated management interface for the ping.
hostname	Hostname of system to ping.
ip-address	IP address of system to ping.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

To use the **ping** command with the *hostname* argument, make sure that DNS functionality is configured on the WAAS device. To force the timeout of a nonresponsive host, or to eliminate a loop cycle, press **Ctrl-C**.

Examples

The following example shows how to send echo packets to a machine with address 172.19.131.189 to verify its availability on the network:

```
WAE# ping 172.19.131.189
PING 172.19.131.189 (172.19.131.189) from 10.1.1.21 : 56(84) bytes of
data.
64 bytes from 172.19.131.189: icmp_seq=0 ttl=249 time=613 usec
64 bytes from 172.19.131.189: icmp_seq=1 ttl=249 time=485 usec
64 bytes from 172.19.131.189: icmp_seq=2 ttl=249 time=494 usec
64 bytes from 172.19.131.189: icmp_seq=3 ttl=249 time=510 usec
64 bytes from 172.19.131.189: icmp_seq=4 ttl=249 time=493 usec

--- 172.19.131.189 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.485/0.519/0.613/0.047 ms
WAE#
```

Related Commands

traceroute

pwd

To view the present working directory on a WAAS device, use the **pwd** EXEC command.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to display the current working directory:

```
WAE# pwd
/local1
```

Related Commands

cd

dir

lls

ls

reload

To halt the operation and perform a cold restart on a WAAS device, use the **reload** EXEC command.

reload [**force** | **in** *m* | **cancel**]

Syntax Description

force	(Optional) Forces a reboot without further prompting.
in *m*	(Optional) Schedules a reboot after a specified interval (1-10080 minutes).
cancel	(Optional) Cancels a scheduled reboot.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

To reboot a WAAS device, use the **reload** command. If no configurations are saved to flash memory, you are prompted to enter configuration parameters upon a restart. Any open connections are dropped after you enter the **reload** command, and the file system is reformatted upon restart.

The **reload** command can include the option to schedule a reload of the software to take effect in a specified number of minutes. After entering this command, you are asked to confirm the reload by typing y and then confirm WCCP shutdown by typing y again (if WCCP is active).

You can use the **cancel** option to cancel a scheduled reload.

Examples

The following example shows how to halt the operation of the WAAS device and reboot with the configuration saved in flash memory. You are not prompted for confirmations during the process.

```
WAE# reload force
```

Related Commands

write

rename

To rename a file on a WAAS device, use the **rename** EXEC command.

rename *oldfilename newfilename*

Syntax Description

oldfilename	Original filename.
newfilename	New filename.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **rename** command to rename any SYSFS file without making a copy of the file.

Examples

The following example shows how to rename the *errlog.txt* file to *old_errlog.txt*:

```
WAE# rename errlog.txt old_errlog.txt
```

Related Commands

cpfile

restore

To restore the device to its manufactured default status by removing the user data from the disk and flash memory, use the **restore** EXEC command.

restore {**factory-default** [**preserve basic-config**] | **rollback**}

Syntax Description

factory-default	Resets the device configuration and data to their manufactured default status.
preserve	(Optional) Preserves certain configurations and data on the device.
basic-config	(Optional) Selects basic network configurations.
rollback	Rolls back the configuration to the last functional software and device configuration.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **restore** EXEC command to restore data on a disk and in flash memory to the factory default, while preserving particular time-stamp evaluation data, or to roll back the configuration to the last functional data and device configuration.

This command erases all existing content on the device; however, your network settings are preserved and the device is accessible through a Telnet and Secure Shell (SSH) session after it reboots.

Backing up the Central Manager Database

Before you use the **restore factory-default** command on your primary WAAS Central Manager or change over from the primary to a standby WAAS Central Manager, make sure that you back up the WAAS Central Manager database and copy the backup file to a safe location that is separate from the WAAS Central Manager. You must halt the operation of the WAAS Central Manager before you enter the **backup** and **restore** commands.

Caution The **restore** command erases user-specified configuration information stored in the flash image and removes data from a disk, user-defined disk partitions, and the entire Central Manager database. User-defined disk partitions that are removed include the SYSFS, WAAS, and PRINTSPOOLFS partitions. The configuration that is removed includes the starting configuration of the device.

By removing the WAAS Central Manager database, all configuration records for the entire WAAS network are deleted. If you do not have a valid backup file or a standby WAAS Central Manager, you must reregister every WAE with the WAAS Central Manager because all previously configured data is lost.

If you used your standby WAAS Central Manager to store the database while you reconfigured the primary, you can register the former primary as a new standby WAAS Central Manager.

If you created a backup file while you configured the primary WAAS Central Manager, you can copy the backup file to this newly reconfigured WAAS Central Manager.

Rolling Back the Configuration

You can roll back the software and configuration of a WAAS device to a previous version using the **restore rollback** command. You would roll back the software only in cases in which a newly installed version of the WAAS software is not functioning properly.

The **restore rollback** command installs the last saved WAAS.bin image on the system disk. A WAAS.bin image is created during software installation and stored on the system disk. If the WAAS device does not have a saved version, the software is not rolled back.

Note WAFS to WAAS migration is supported. Rollback from WAAS to WAFS is not supported.

Examples

The following examples show how to use the **restore factory-default** and **restore factory-default preserve basic-config** commands. Because configuration parameters and data are lost, prompts are given before initiating the restore operation to ensure that you want to proceed.

```
WAE# restore factory-default
This command will wipe out all of data on the disks
and wipe out WAAS CLI configurations you have ever made.
If the box is in evaluation period of certain product,
the evaluation process will not be affected though.

It is highly recommended that you stop all active services
before this command is run.

Are you sure you want to go ahead?[yes/no]

WAE# restore factory-default preserve basic-config
This command will wipe out all of data on the disks
and all of WAAS CLI configurations except basic network
configurations for keeping the device online.
The to-be-preserved configurations are network interfaces,
default gateway, domain name, name server and hostname.
If the box is in evaluation period of certain product,
the evaluation process will not be affected.

It is highly recommended that you stop all active services
before this command is run.

Are you sure you want to go ahead?[yes/no]
```

Note You can enter basic configuration parameters (such as the IP address, hostname, and name server) at this point, or you can enter these parameters later through entries in the command-line interface.

The following example shows how to verify that the **restore** command has removed data from the SYSFS, WAAS, and PRINTSPOOLFS partitioned file systems:

```
WAE# show disks details

Physical disk information:

  disk00: Normal                (h00 c00 i00 l00 - DAS)    140011MB(136.7GB)
  disk01: Normal                (h00 c00 i01 l00 - DAS)    140011MB(136.7GB)


Mounted filesystems:

  MOUNT POINT       TYPE       DEVICE           SIZE    INUSE     FREE USE%
  /                 root       /dev/root         35MB     30MB      5MB  85%
  /swstore          internal   /dev/md1         991MB    333MB    658MB  33%
  /state            internal   /dev/md2        3967MB     83MB   3884MB   2%
  /disk00-04        CONTENT    /dev/md4      122764MB     33MB 122731MB   0%
  /local/local1     SYSFS      /dev/md5        3967MB    271MB   3696MB   6%
  .../local1/spool  PRINTSPOOL /dev/md6         991MB     16MB    975MB   1%
  /sw               internal   /dev/md0         991MB    424MB    567MB  42%


Software RAID devices:

  DEVICE NAME  TYPE     STATUS                PHYSICAL DEVICES AND STATUS
  /dev/md0     RAID-1   NORMAL OPERATION      disk00/00[GOOD]  disk01/00[GOOD]
  /dev/md1     RAID-1   NORMAL OPERATION      disk00/01[GOOD]  disk01/01[GOOD]
  /dev/md2     RAID-1   NORMAL OPERATION      disk00/02[GOOD]  disk01/02[GOOD]
  /dev/md3     RAID-1   NORMAL OPERATION      disk00/03[GOOD]  disk01/03[GOOD]
  /dev/md4     RAID-1   NORMAL OPERATION      disk00/04[GOOD]  disk01/04[GOOD]
  /dev/md5     RAID-1   NORMAL OPERATION      disk00/05[GOOD]  disk01/05[GOOD]
  /dev/md6     RAID-1   NORMAL OPERATION      disk00/06[GOOD]  disk01/06[GOOD]
Currently content-filesystems RAID level is not configured to change.
```

The following example shows how to upgrade or restore an older version of the WAAS software. In the example, version Y of the software is installed (using the **copy** command), but the administrator has not switched over to it yet, so the current version is still version X. The system is then reloaded (using the **reload** command), and it verifies that version Y is the current version running.

The following example shows how to roll back the software to version X (using the **restore rollback** command), and reload the software:

```
WAE# copy ftp install server path waas.versionY.bin
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.0 (build b340 Mar 25 2
006)
Version: oe612-4.0.0.340

Compiled 17:26:17 Mar 25 2006 by cnbuild

System was restarted on Mon Mar 27 15:25:02 2006.
The system has been up for 3 days, 21 hours, 9 minutes, 17 seconds.

WAE# show version last
    Nothing is displayed.
WAE# show version pending
WAAS 4.0.1 Version Y
WAE# reload
...... reloading ......
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
...
WAE# restore rollback
```

```
WAE# reload
...... reloading ......
```

Because flash memory configurations were removed after the **restore** command was used, the **show startup-config** command does not return any flash memory data. The **show running-config** command returns the default running configurations.

Related Commands

reload

show disks

show running-config

show startup-config

show version

rmdir

To delete a directory on a WAAS device, use the **rmdir** EXEC command.

rmdir *directory*

Syntax Description

directory	Name of the directory that you want to delete.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **rmdir** EXEC command to remove any directory from the WAAS file system. The **rmdir** command only removes empty directories.

Examples

The following example shows how to delete the *oldfiles* directory from the *local1* directory:

```
WAE# rmdir /local1/oldfiles
```

Related Commands

cpfile

dir

lls

ls

mkdir

pwd

rename

scp

To copy files between network hosts, use the **scp** command.

scp [**4**][**6**][**B**][**C**][**p**][**q**][**r**][**v**] [**c** *cipher*] [**F** *config-file*] [**i** *id-file*] [**o** *ssh_option*] [**P** *port*] [**S** *program*] [[*user* @] *host* **:** *file*] [**...**] [[*user-n* @] *host-n* **:** *file-n*]

Syntax Description

4	(Optional) Forces this command to use only IPv4 addresses.
6	(Optional) Forces this command to use only IPv6 addresses.
B	(Optional) Specifies the batch mode. In this mode, the **scp** command does not ask for passwords or passphrases.
C	(Optional) Enables compression. The **scp** command passes this option to the **ssh** command to enable compression.
p	(Optional) Preserves the following information from the source file: modification times, access times, and modes.
q	(Optional) Disables the display of progress information.
r	(Optional) Recursively copies directories and their contents.
v	(Optional) Specifies the verbose mode. Causes the **scp** and **ssh** commands to print debugging messages about their progress. This option can be helpful when troubleshooting connection, authentication, and configuration problems.
c *cipher*	(Optional) Specifies the cipher to use for encrypting the data being copied. The **scp** command directly passes this option to the **ssh** command.
F *config-file*	(Optional) Specifies an alternative per-user configuration file for Secure Shell (SSH). The **scp** command directly passes this option to the **ssh** command.
i *id-file*	(Optional) Specifies the file containing the private key for RSA authentication. The **scp** command directly passes this information to the **ssh** command.
o *ssh_option*	(Optional) Passes options to the **ssh** command in the format used in ssh_config5. See the **ssh** command for more information about the possible options.
P *port*	(Optional) Specifies the port to connect to on the remote host.
S *program*	(Optional) Specifies the program to use for the encrypted connection.
user	(Optional) Username.
host	(Optional) Hostname.
file	(Optional) Name of the file to copy.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **scp** command uses SSH for transferring data between hosts.

This command prompts you for passwords or pass phrases when needed for authentication.

Related Commands

ssh

script

To execute a script provided by Cisco or check the script for errors, use the **script** EXEC command.

script {**check** | **execute**} *file_name*

Syntax Description

check	Checks the validity of the script.
execute	Executes the script. The script file must be a SYSFS file in the current directory.
file_name	Name of the script file.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **script** EXEC command opens the script utility, which allows you to execute Cisco-supplied scripts or check errors in those scripts. The script utility can read standard terminal input from the user if the script you run requires input from the user.

Note The script utility is designed to run only Cisco-supplied scripts. You cannot execute script files that lack Cisco signatures or that have been corrupted or modified.

Examples

The following example shows how to check for errors in the script file *test_script.pl*:

```
WAE# script check test_script.pl
```

setup

To configure basic configuration settings (general settings, device network settings, interception type, disk configuration, and licenses) on the WAAS device or to complete basic configuration after upgrading to the WAAS software, use the **setup** EXEC command.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

For instructions on using the **setup** command, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

For proper display of the **setup** command, leave the terminal length set to the default value of 24 lines.

show aaa accounting

To display the AAA accounting configuration information for a WAAS device, use the **show aaa accounting** EXEC command.

show aaa accounting

Syntax Description

This command has no arguments or keywords

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show aaa accounting** EXEC command to display configuration information for the following AAA accounting types:

- Exec shell
- Command (for normal users and superusers)
- System

Examples

Table 3-1 describes the fields shown in the **show aaa accounting** command display.

Table 3-1 Field Descriptions for the show aaa accounting Command

Field	Description
Accounting Type	AAA accounting configuration for the following types of user accounts: • Exec • Command level 0 • Command level 15 • System
Record Event(s)	Configuration of the AAA accounting notice that is sent to the accounting server.
stop-only	WAAS device that sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.

Table 3-1 Field Descriptions for the show aaa accounting Command (continued)

Field	Description
start-stop	WAAS device that sends a start record accounting notice at the beginning of an event and a stop record at the end of the event to the TACACS+ accounting server. The start accounting record is sent in the background. The requested user service begins regardless of whether the start accounting record was acknowledged by the TACACS+ accounting server.
wait-start	WAAS device that sends both a start and a stop accounting record to the TACACS+ accounting server. The requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.
disabled	Accounting that is disabled for the specified event.
Protocol	Accounting protocol that is configured.

Related Commands **(config) aaa accounting**

show aaa authorization

To display the AAA authorization configuration information for a WAAS device, use the **show aaa authorization** EXEC command.

show aaa authorization

Syntax Description

This command has no arguments or keywords

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show aaa authorizaiton** EXEC command to display configuration and state information related to AAA authorization.

Examples

Table 3-2 describes the fields shown in the **show aaa authorization** command display.

Table 3-2 Field Descriptions for the show aaa authorization Command

Field	Description
Authorization Type	AAA authorization configuration for the following types of user accounts: • Command level 0 • Command level 15
Protocol	Authorization protocol that is configured.

Related Commands

(config) aaa authorization commands

show accelerator

To display the status and configuration of the application accelerators, use the **show accelerator** EXEC command.

show accelerator [**cifs** | **detail** | **epm** | **http** [**debug**]| **ica** | **mapi** | **nfs** | **smb** | **ssl** | **video** | **wansecure**]

Syntax Description

cifs	(Optional) Displays the status for the CIFS application accelerator.
detail	(Optional) Displays the license information, configuration state, and operational state for all accelerators, and additional accelerator and policy engine configuration.
epm	(Optional) Displays the status for the EPM application accelerator.
http	(Optional) Displays the status for the HTTP application accelerator.
debug	(Optional) Displays more detailed status for the HTTP application accelerator.
ica	(Optional) Displays the status for the ICA application accelerator.
mapi	(Optional) Displays the status for the MAPI application accelerator.
nfs	(Optional) Displays the status for the NFS application accelerator.
smb	(Optional) Displays the status for the SMB application accelerator.
ssl	(Optional) Displays the status for the SSL application accelerator.
video	(Optional) Displays the status for the video application accelerator.
wansecure	(Optional) Displays the status for the WAN secure application accelerator.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

The following example displays the output for the **show accelerator http** command:

```
wae# show accelerator http
Accelerator     Licensed        Config State    Operational State
-----------     --------        ------------    -----------------
http            Yes             Enabled         Running

HTTP:
   Accelerator Config Item            Mode        Value
   -----------------------            ----        ------
   Suppress Server Encoding           Default     Disabled
                Access-List           Default     All
   DRE Hints                          User        Enabled
                Access-List           Default     All
   Metadatacache                      User        Enabled
                Access-List           Default     All
   HTTPS Metadatacache                User        Enabled
```

```
                  Access-List          Default     All
                  MaxAge               Default     86400
                  MinAge               Default     60
                  Filter-extension     Default     All
                  Redirect             Default     Enabled
                  Unauthorized           Default       Enabled
                  Conditional            Default       Enabled

   Policy Engine Config Item            Value
   -------------------------            -----
   State                                Registered
   Default Action                       Use Policy
   Connection Limit                     200
   Effective Limit                      200
   Keepalive timeout                    5.0 seconds
```

The following example displays the output for the **show accelerator smb** command:

```
wae# show accelerator smb

Accelerator     Licensed        Config State    Operational State
-----------     --------        ------------    -----------------
smb             Yes             Disabled        Shutdown

SMB:
   Accelerator Config Item              Mode          Value
   -----------------------              ----          ------
   Digital signing alarm                Default       Enabled
   Change Notification size             Default       10
   DRE hints                            Default       Enabled
   Highest dialect                      Default       smb2-1
       Exceed action                    Default       handoff
   Named pipe optimization              Default       Enabled
       Resp. cache lifetime (s)         Default       20
       Sess. cache lifetime (s)         Default       30
       NamedPipe-cache size (KB)        Default       160         (default: 160
 maximum: 480)
   NF metadata cache opt                Default       Enabled
       Max size (MB)                    Default       32
       Aging (s)                        Default       30
       Bypass patterns                  Default
   Microsoft Office optimization        Default       Enabled
   Optimization bypass pattern          User
   Read-ahead opt                       Default       Enabled
       Buffer size (MB)                 Default       50          (default: 50
maximum: 100)
   Directory listing opt                Default       Enabled
   Async-write opt                      Default       Enabled
       Quota threshold (MB)             Default       20
       Quota aging time (s)             Default       60
   Metadata-opt                         Default       Enabled
       Metadata-cache size (MB)         Default       50          (default: 50
maximum: 50)
   Batch-close-opt                      Default       Enabled
   Invalid-fid-opt                      Default       Enabled
   Iobuf size (MB)                      Default       50          (default: 50
maximum: 100)
       Max iobuf size for 1 pkt(KB)     Default       65
       Directory aging time             Default       30
   Dynamic share                        User          //1.1.1.1/test

   Policy Engine Config Item            Value
   -------------------------            -----
   State                                Registered
```

```
Default Action                          Use Policy
Connection Limit                        50
Effective Limit                         40
Keepalive timeout                       0.0 seconds
```

Table 3-3 describes the fields shown in the **show accelerator** command display for all application accelerators. Specific application accelerators display additional configuration status information.

Table 3-3 Field Description for the show accelerator Command

Field	Description
Accelerator	Name of the accelerator.
Licensed	Yes or No.
Config State	Accelerator is Enabled or Disabled.
Operational State	Shutdown, Initializing, Running, Cleaning Up, or Expired License.
Policy Engine Config Item: State	Registered (policy engine is communicating with the accelerator) or Not Registered (policy engine is not communicating with the accelerator; seen when the accelerator is disabled).
Policy Engine Config Item: Default Action	Drop or Use. Specifies the action to be taken if the accelerator refuses to handle the connection (because of overload or other reasons). Drop means the connection is dropped, and Use means the connection uses a reduced set of policy actions (such as TFO and DRE).
Policy Engine Config Item: Connection Limit	Connection limit. The limit configured by the accelerator which states how many connections may be handled before new connection requests are rejected.
Policy Engine Config Item: Effective Limit	Effective connection limit. The dynamic limit relating to how many connections may be handled before new connection requests are rejected. This limit is affected by resources that have been reserved, but not yet used.
Policy Engine Config Item: Keepalive timeout	Connection keepalive timeout in seconds. Keepalive messages are sent by each accelerator.

If you use the **show accelerator http** or the **show accelerator smb** command, the output contains an extra section called Accelerator Config Item, which appears before the Policy Engine Config Item section. In the Accelerator Config Item section, each item shows the status of an HTTP accelerator configuration item. The Mode column shows Default if the item is configured with the default setting or User if the item is configured with a different setting by the user. The Value column shows the current value of the item (Enabled, Disabled, or an alpha-numeric setting).

Related Commands

(config) accelerator cifs

(config) accelerator epm

(config) accelerator http

(config) accelerator ica

(config) accelerator mapi

(config) accelerator nfs

(config) accelerator smb

(config) accelerator ssl

(config) accelerator video

show statistics accelerator

show alarms

To display information about various types of alarms, their status, and history on a WAAS device, use the **show alarms** EXEC command.

show alarms critical [**detail** [**support**]]

show alarms detail [**support**]

show alarms history [*start_num* [*end_num* [**detail** [**support**]]]] | **critical** [*start_num* [*end_num* [**detail** [**support**]]]]

show alarms major [*start_num* [*end_num* [**detail** [**support**]]]]

show alarms minor [*start_num* [*end_num* [**detail** [**support**]]]]

show alarms status

Syntax Description

critical	Displays critical alarm information.
detail	(Optional) Displays detailed information for each alarm.
support	(Optional) Displays additional information about each alarm.
history	Displays information about the history of various alarms.
start_num	(Optional) Alarm number that appears first in the alarm history.
end_num	(Optional) Alarm number that appears last in the alarm history.
major	Displays information about major alarms.
minor	Displays information about minor alarms.
status	Displays the status of various alarms and alarm overload settings.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The Node Health Manager in the WAAS software enables WAAS applications to raise alarms to draw attention in error/significant conditions. The Node Health Manager, which is the data repository for such alarms, aggregates the health and alarm information for the applications, services, and resources (for example, disk drives) that are being monitored on the WAAS device. For example, this feature gives you a mechanism to determine if a WAE is receiving overwhelming number of alarms. These alarms are referred to as WAAS software alarms.

The WAAS software uses SNMP to report error conditions by generating SNMP traps. The following WAAS applications can generate a WAAS software alarm:

- Node Health Manager (alarm overload condition)
- System Monitor (sysmon) for disk failures

The three levels of alarms in the WAAS software are as follows:

- Critical—Alarms that affect the existing traffic through the WAE and are considered fatal (the WAE cannot recover and continue to process traffic).
- Major—Alarms that indicate a major service (for example, the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted.
- Minor—Alarms that indicate that a condition that will not affect a service has occurred, but that corrective action is required to prevent a serious fault from occurring.

You can configure alarms using the **snmp-server enable traps alarms** global configuration command.

Use the **show alarms critical** EXEC command to display the current critical alarms being generated by WAAS software applications. Use the **show alarms critical detail** EXEC command to display additional details for each of the critical alarms being generated. Use the **show alarms critical detail support** EXEC command to display an explanation about the condition that triggered the alarm and how you can find out the cause of the problem. Similarly, you can use the **show alarms major** and **show alarms minor** EXEC commands to display the details of major and minor alarms.

Use the **show alarms history** EXEC command to display a history of alarms that have been raised and cleared by the WAAS software on the WAAS device since the last software reload. The WAAS software retains the last 100 alarm raise and clear events only.

Use the **show alarms status** EXEC command to display the status of current alarms and the alarm overload status of the WAAS device and alarm overload configuration.

Examples

Table 3-4 describes the fields shown in the **show alarms history** command display.

Table 3-4 Field Descriptions for the show alarms history Command

Field	Description
Op	Operation status of the alarm. Values are R–Raised or C–Cleared.
Sev	Severity of the alarm. Values are Cr–Critical, Ma–Major, or Mi–Minor.
Alarm ID	Type of event that caused the alarm.
Module/Submodule	Software module affected.
Instance	Object that this alarm event is associated with. For example, for an alarm event with the Alarm ID disk_failed, the instance would be the name of the disk that failed. The Instance field does not have predefined values and is application specific.

Table 3-5 describes the fields shown in the **show alarms status** command display.

Table 3-5 Field Descriptions for the show alarms status Command

Field	Description
Critical Alarms	Number of critical alarms.
Major Alarms	Number of major alarms.

Table 3-5 Field Descriptions for the show alarms status Command (continued)

Field	Description
Minor Alarms	Number of minor alarms.
Overall Alarm Status	Aggregate status of alarms.
Device is NOT in alarm overload state.	Status of the device alarm overload state.
Device enters alarm overload state @ 999 alarms/sec.	Threshold number of alarms per second at which the device enters the alarm overload state.
Device exits alarm overload state @ 99 alarms/sec.	Threshold number of alarms per second at which the device exits the alarm overload state.
Overload detection is ENABLED.	Status of whether overload detection is enabled on the device.

Related Commands

(config) alarm overload-detect

(config) snmp-server enable traps

show appnav-controller flow-distribution

To display ANC flow distribution information, use the **show appnav-controller flow-distribution** EXEC command.

show appnav-controller flow-distribution [**client-ip** *ip_address* | **client-port** *port* | **peer-id** *peer_id* | **server-ip** *ip_address* | **server-port** *port*]

Syntax Description

client-ip *ip_address*	(Optional) Displays the flow information for the client with the specified IP address.
client-port *port*	(Optional) Displays the flow information for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the flow information for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip *ip_address*	(Optional) Displays the flow information for the server with the specified IP address.
server-port *port*	(Optional) Displays the flow information for the server with the specified port number (1–65535).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command can be used to determine how a flow would be classified and redirected.

Examples

The following is sample output from the **show appnav-controller flow-distribution** command that shows how a flow would be redirected:

```
ANC# show appnav-controller flow-distribution peer-id 58:8d:01:02:04:3a client-ip
192.168.1.2 server-ip 192.168.5.2 server-port 443
WARNING: One or more inputs are wildcards. The flow distribution lookup may not
be accurate
Did not find existing application, session or connection

Policy lookup results
---------------------

Connection will be redirected
Matched class: class-default:HTTPS
Monitored Accl: SSL
Configured redirect SNG: WNG-Default
Selected SNG: WNG-Default
```

```
Bucket #: 4
Selected SN: 2.76.243.11
```

Related Commands

(config) service-insertion

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.

On an ISR-WAAS device, no ARP entries are present for IP addresses on the same subnet as the ISR-WAAS device; there is an entry only for the defined gateway.

Examples

Table 3-6 describes the fields shown in the **show arp** command display.

Table 3-6 Field Descriptions for the show arp Command

Field	Description
Protocol	Type of protocol.
State	Cache entry state.
Address	IP address of the hostname.
Flags	Current ARP flag status.
Hardware Addr	Hardware IP address given as six hexadecimal bytes separated by colons.
Type	Type of wide-area network.
Interface	Name and slot/port information for the interface.

show authentication

To display the authentication configuration for a WAAS device, use the **show authentication** EXEC command.

show authentication {**user** | **strict-password-policy**}

Syntax Descriptions

user	Displays authentication configuration for user login to the system.
strict-password-policy	Displays strict password policy configuration information.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

When the WAAS device authenticates a user through an NTLM, LDAP, TACACS+, RADIUS, or Windows domain server, a record of the authentication is stored locally. As long as the entry is stored, subsequent attempts to access restricted Internet content by the same user do not require additional server lookups. To display the local and remote authentication configuration for user login, use the **show authentication user** EXEC command.

To display the strict password policy configuration information , use the **show authentication strict-password-policy** EXEC command.

Examples

Table 3-7 describes the fields shown in the **show authentication user** command display.

Table 3-7 Field Descriptions for the show authentication user Command

Field	Description
Login Authentication: Console/Telnet/Ftp/SSH Session	Authentication service that is enabled for login authentication and the configured status of the service.
Windows domain RADIUS TACACS+ Local	Operation status of the authentication service. Values are enabled or disabled. Priority status of each authentication service. Values are primary, secondary, or tertiary.
Configuration Authentication: Console/Telnet/Ftp/SSH Session	Authentication service that is enabled for configuration authentication and the configured status of the service.

Table 3-7 Field Descriptions for the show authentication user Command (continued)

Field	Description
Windows domain RADIUS TACACS+ Local	Operation status of the authentication service. Values are enabled or disabled. Priority status of each authentication service. Values are primary, secondary, or tertiary.

Table 3-8 describes the fields in the **show authentication strict-password-policy** command display. If the strict password policy is not enabled, the command displays, "Strict password policy is disabled."

Table 3-8 Field Description for the show authentication strict-password-policy Command

Field	Description
Password validity	Number of days for which strict passwords are valid.
Password expiry warning	Number of days in advance that users are warned before strict passwords expire.
Maximum login retry attempts	Number of login retry attempts allowed before the user is locked out.

Related Commands

(config) authentication configuration

(config) authentication strict-password-policy

clear arp-cache

show statistics authentication

show auto-discovery

To display Traffic Flow Optimization (TFO) auto-discovery information for a WAE, use the **show auto-discovery** EXEC command.

show auto-discovery {**blacklist** [**netmask** *netmask*] | **list** [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}] | **asymmetric-connections**}

Syntax Description

blacklist	Displays the entries in the blacklist server table.
netmask *netmask*	(Optional) Displays the network mask to filter the table output (A.B.C.D/).
list	Lists TCP flows that the WAE is currently optimizing or passing through.
|	(Optional) Specifies the output modifier.
begin *regex*	Begins with the line that matches the regular expression. You can enter multiple expressions.
exclude *regex*	Excludes lines that match the regular expression. You can enter multiple expressions.
include *regex*	Includes lines that match the regular expression. You can enter multiple expressions.
asymmetric-connections	Displays asymmetric connections.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The **asymmetric-connections** option displays the last 1000 asymmetric connections seen on the device.

Examples

The following is sample output from the **show auto-discovery list** command:

```
WAE# show auto-discovery list

E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough

      Src-IP:Port           Dst-IP:Port     Orig-St  Term-St
```

Related Commands

show statistics auto-discovery

show statistics filtering

show statistics tfo

show statistics connection closed

show auto-register

To display the status of the automatic registration feature on a WAE, use the **show auto-register** EXEC command.

show auto-register

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-9 describes the output in the **show auto-register** command display.

Table 3-9 Field Description for the show auto-register Command

Field	Description
Auto registration is enabled.	Configuration status of the autoregistration feature.
Auto registration is disabled.	Configuration status of the autoregistration feature.

Related Commands

(config) auto-register

show banner

To display the message of the day (MOTD), login, and EXEC banner settings, use the **show banner** EXEC command.

show banner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-10 describes the fields shown in the **show banner** command display.

Table 3-10 Field Descriptions for the show banner Command

Field	Description
Banner is enabled	Configuration status of the banner feature.
MOTD banner is: abc	Configured message of the day.
Login banner is: acb	Configured login banner.
Exec banner is: abc	Configured EXEC banner.

Related Commands

(config) auto-register

show bmc

To display the Baseboard Management Controller (BMC) system event log, use the **show bmc** EXEC command.

show bmc {**info** | **fru** | **event-log [all** | **event** | **range** | **|] | management** |}

Syntax Description

info	Displays the BMC information.
fru	Displays the BMC Field Replaceable Unit.
event-log	Displays the BMC system event log (by default, the last 10 events).
all	Displays all events from the BMC system event log.
event	Displays a single event number from the BMC system event log.
range	Displays the range of events from the BMC system event log.
management	Displays the BMC management related information.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following is a sample output from the **show bmc** command:

```
WAE#show bmc ?
event-log   Display BMC System Event Log (default is the last 10 events)
fru         Display BMC Field Replaceable Unit
info        Display BMC information
management  Display BMC management information

WAVE-694-K9#sh bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.44
IPMI Version              : 2.0
Manufacturer ID           : 5771
Manufacturer Name         : Unknown (0x168B)
Product ID                : 161 (0x00a1)
Product Name              : Unknown (0xA1)
Device Available          : yes
Provides Device SDRs      : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info     :
    0x0b
```

```
    0x04
    0x1b
    0x01
SEL Information
Version          : 1.5 (v1.5, v2 compliant)
Entries          : 4
Free Space       : 9136 bytes
Percent Used     : 0%
Last Add Time    : 05/20/2011 05:26:56
Last Del Time    : 05/20/2011 05:26:55
Overflow         : false
Supported Cmds   : 'Delete' 'Reserve'
Self Test Results    : passed
System Power         : on
Power Overload       : false
Power Interlock      : inactive
Main Power Fault     : false
Power Control Fault  : false
Power Restore Policy : always-off
Last Power Event     :
Chassis Intrusion    : inactive
Front-Panel Lockout  : inactive
Drive Fault          : false
Cooling/Fan Fault    : false
Current Time     : 05/24/2011 06:45:29


WAVE-694-K9#sh bmc fru
FRU Device Description : Builtin FRU Device (ID 0)
 Chassis Type          : Rack Mount Chassis
 Chassis Part Number   : 800-34889-01
 Chassis Serial        : FCH1445V03Y
 Board Mfg Date        : Mon May  2 22:00:00 2011
 Board Mfg             : CISCO
 Board Serial          : FCH1448709T
 Board Part Number     : 74-7814-01
 Product Manufacturer  : CISCO
 Product Name          : WAVE-694-K9
 Product Version       : V01
 Product Extra         : Wide Area Virtualization Engine
 Product Extra         : Small fan: FAN-WAVE-40MM=
 Product Extra         : Big fan: FAN-WAVE-60MM=

WAE#show bmc event-log
all    Display all events from BMC System Event Log
event  Display a single event number from BMC System Event Log
range  Display the range of events from BMC System Event Log
|      Output Modifiers

WAE#show bmc manangement
Watchdog Timer Use:     SMS/OS (0x44)
Watchdog Timer Is:      Started/Running
Watchdog Timer Actions: Power Cycle (0x03)
Pre-timeout interval:   0 seconds
Timer Expiration Flags: 0x00
Initial Countdown:      900 sec
Present Countdown:      740 sec
```

Related Commands

clear bmc

show bridge

To display bridge interface information for an AppNav Controller using inline interception, use the **show bridge** EXEC command.

show bridge *index*

Syntax Description

index	Bridge group index from 1–5.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Examples

Table 3-11 describes the fields shown in the **show bridge** command display.

Table 3-11 Field Descriptions for the show bridge Command

Field	Description
lsp	Displayed only if interface is configured with link state propagation.
flow sync	Flow synchronization status.
Member Interfaces	Lists the member interfaces in the bridge group.
Link state propagation	Status of link state propagation setting (enabled or disabled).
VLAN interception	Lists the VLANs intercepted by this bridge group.
Interception Statistics (for each member interface)	
Operation State	Operational state of the interface.
Input Packets Forwarded/Bridged	Number of incoming packets bridged.
Input Packets Redirected	Number of incoming packets redirected.
Input Packets Punted	Number of incoming packets punted.
Input Packets Dropped	Number of incoming packets dropped.
Output Packets Forwarded/Bridged	Number of outgoing packets bridged.
Output Packets Injected	Number of outgoing packets injected.
Output Packets Dropped	Number of outgoing packets dropped.

Related Commands (config) bridge

show cache http-metadatacache

To display HTTP metadata cache information for a WAE, use the **show cache http-metadatacache** EXEC command.

show cache http-metadatacache https {**conditional-response** | **redirect-response** | **sharepoint-prefetch** | **unauthorized-response**}

show cache http-metadatacache {**all** | **conditional-response** | **redirect-response** | **sharepoint-prefetch** | **unauthorized-response**} [*url*]

Syntax Description

https	Displays cache entries for HTTPS metadata cache response types, which includes the active entries only, not the URLs.
conditional-response	Displays cache entries for conditional responses (304).
redirect-response	Displays cache entries for redirect responses (301).
sharepoint-prefetch	Displays cache entries of the prefetched data.
unauthorized-response	Displays cache entries for authorization required responses (401).
all	Displays cache entries for all HTTP metadata cache response types.
url	(Optional) Displays cache entries that match only the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-12 describes the fields shown in the **show cache http-metadatacache all** command display.

Table 3-12 Field Descriptions for the show cache http-metadatacache all Command

Field	Description
Redirect Cache	
Active HTTP entries	Number of current HTTP redirect cache entries.
Active HTTPS entries	Number of current HTTPS redirect cache entries.
Max Entries	Maximum number of redirect cache entries allowed.
URL	URL and expiration time (in seconds) for each redirect cache entry.
Conditional Cache	
Active HTTP entries	Number of current HTTP conditional cache entries.

Table 3-12 Field Descriptions for the show cache http-metadatacache all Command (continued)

Field	Description
Active HTTPS entries	Number of current HTTPS conditional cache entries.
Max Entries	Maximum number of conditional cache entries allowed.
URL	URL and expiration time (in seconds) for each conditional cache entry.
Unauthorized Cache	
Active HTTP entries	Number of current HTTP unauthorized cache entries.
Active HTTPS entries	Number of current HTTPS unauthorized cache entries.
Max Entries	Maximum number of unauthorized cache entries allowed.
URL	URL and expiration time (in seconds) for each unauthorized cache entry.

Related Commands

(config) accelerator http

clear cache

show cdp

To display CDP configuration information, use the **show cdp** EXEC command.

show cdp entry {***** | *neighbor*} [**protocol** | **version**]

show cdp interface
[**GigabitEthernet** *slot/port* | **TenGigabitEthernet** *slot/port* | **InlinePort** *slot/port* {**lan** | **wan**}]

show cdp neighbors
[**detail** | **GigabitEthernet** *slot/port* [**detail**] | **TenGigabitEthernet** *slot/port* [**detail**] | **InlinePort** *slot/port*/{**lan/wan**}[**detail**]]

show cdp {**holdtime** | **run** | **timer** | **traffic**}

Syntax Description

entry	(Optional) Displays information for a specific CDP neighbor entry.
*****	Specifies all neighbors.
neighbor	CDP neighbor entry to display.
protocol	(Optional) Displays the CDP protocol information.
version	(Optional) Displays the CDP version.
interface	Displays the interface status and configuration.
GigabitEthernet *slot/port*	(Optional) Displays the Gigabit Ethernet configuration for the designated interface.
TenGigabitEthernet *slot/port*	(Optional) Displays the 10-Gigabit Ethernet configuration for the designated interface.
InlinePort *slot/port* {**lan** | **wan**}	(Optional) Displays Inline Port configuration for the designated interface.
neighbors	Displays CDP neighbor entries.
detail	(Optional) Displays detailed information.
holdtime	Displays the length of time that CDP information is held by neighbors.
run	Displays the CDP process status.
timer	Displays the time when CDP information is resent to neighbors.
traffic	Displays CDP statistical information.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show cdp** command displays information about how frequently CDP packets are resent to neighbors, the length of time that CDP packets are held by neighbors, the disabled status of CDP Version 2 multicast advertisements, CDP Ethernet interface ports, and general CDP traffic information. This command supports VLAN (802.1Q) tagged packets

Examples

Table 3-13 describes the fields shown in the **show cdp** command display.

Table 3-13 Field Descriptions for the show cdp Command

Field	Description
Sending CDP packets every XX seconds	Interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.
Sending a holdtime value of XX seconds	Time (in seconds) that the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.
Sending CDPv2 advertisements is XX	Transmission status for sending CDP Version-2 type advertisements. Possible values are enabled or not enabled.

Table 3-14 describes the fields shown in the **show cdp entry** *neighbor* command display.

Table 3-14 Field Descriptions for the show cdp entry Command

Field	Description
Device ID	Name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	
IP address	IP address of the neighbor device.
CLNS address	Non-IP network address. The field depends on the type of neighbor.
DECnet address	Non-IP network address. The field depends on the type of neighbor.
Platform	Product name and number of the neighbor device.
Interface	Protocol being used by the connectivity media.
Port ID (outgoing port)	Port number of the port on the neighbor device.
Capabilities	Capability code discovered on the neighbor device. This is the type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater

Table 3-14 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 3-15 describes the fields shown in the **show cdp entry** *neighbor* **protocol** command display.

Table 3-15 Field Descriptions for the show cdp entry protocol Command

Field	Description
Protocol information for XX	Name or identifier of the neighbor device.
IP address	IP address of the neighbor device.
CLNS address	Non-IP network address. The field depends on the type of neighbor.
DECnet address	Non-IP network address. The field depends on the type of neighbor.

Table 3-16 describes the fields shown in the **show cdp entry** *neighbor* **version** command display.

Table 3-16 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 3-17 describes the field in the **show cdp holdtime** command display.

Table 3-17 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 3-18 describes the fields shown in the **show cdp interface** command display.

Table 3-18 Field Descriptions for the show cdp interface Command

Field	Description
Interface_slot/port is XX	Operation status of the CDP interface. Values are up or down.
Encapsulation	Encapsulation.
Sending CDP packets every XX seconds	Time interval at which CDP packets are sent.

Table 3-18 Field Descriptions for the show cdp interface Command (continued)

Field	Description
Holdtime	Time, in seconds, that the current device will hold the CDP advertisement from a transmitting router before discarding it.
CDP protocol is XX	Protocol being used by the connectivity media.

Table 3-19 describes the fields shown in the **show cdp neighbors** command display.

Table 3-19 Field Descriptions for the show cdp neighbors Command

Field	Description
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Local Intrfce	Local interface where the device is connected. Gig refers to a Gigabit Ethernet interface, Ten refers to a 10 Gigabit Ethernet interface, and Inline refers to an inline interface.
Holdtime	Time, in seconds, that the current device will hold the CDP advertisement from a transmitting router before discarding it.
Capability	Capability code discovered on the device. This is the type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router 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 3-20 describes the fields shown in the **show cdp neighbors detail** command display.

Table 3-20 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.

Table 3-20 Field Descriptions for the show cdp neighbors detail Command (continued)

Field	Description
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.
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 3-21 describes the field in the **show cdp run** command display.

Table 3-21 Field Description for the show cdp run Command

Field	Description
CDP is XX.	Whether CDP is enabled or disabled.

Table 3-22 describes the field in the **show cdp timer** command display.

Table 3-22 Field Description for the show cdp timer Command

Field	Description
cdp timer XX	Time when CDP information is resent to neighbors.

Table 3-23 describes the fields shown in the **show cdp traffic** command display.

Table 3-23 Field Descriptions for the show cdp traffic Command

Field	Description
Total packets Output	(Total number of packets sent) Number of CDP advertisements sent by the local device. This value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
Input	(Total number of packets received) Number of CDP advertisements received by the local device. This value is the sum of the CDP Version-1 advertisements input and CDP Version 2 advertisements input fields.
Hdr syntax	(Header Syntax) Number of CDP advertisements with bad headers received by the local device.
Chksum error	(CheckSum Error) Number of times that the checksum (verifying) operation failed on incoming CDP advertisements.
Encaps failed	(Encapsulations Failed) Number of times that CDP failed to transmit advertisements on an interface because of a failure caused by the bridge port of the local device.

Table 3-23 Field Descriptions for the show cdp traffic Command (continued)

Field	Description
No memory	Number of times that the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid packet	Number of invalid CDP advertisements received and sent by the local device.
Fragmented	Number of times fragments or portions of a single CDP advertisement were received by the local device instead of the complete advertisement.
CDP version 1 advertisements Output	Number of CDP Version 1 advertisements sent by the local device.
Input	Number of CDP Version 1 advertisements received by the local device.
CDP version 2 advertisements Output	Number of CDP Version 2 advertisements sent by the local device.
Input	Number of CDP Version 2 advertisements received by the local device.

Related Commands

(config) cdp

(config-if) cdp

clear arp-cache

debug cdp

show cifs

To display CIFS application accelerator information, use the **show cifs** EXEC command.

show cifs cache {**disk-use** | **entry-count**}

show cifs msg-signing-servers

show cifs open-files {**count** | **max-count**}

show cifs requests {**count** | **waiting**}

show cifs sessions {**count** | **list**}

Syntax Description

cache	Displays CIFS cache information.
disk-use	Displays the total disk usage for CIFS cache.
entry-count	Displays the count of internal cache resources used for cached files.
msg-signing-servers	Displays a list of the IP addresses of servers requiring message signing.
open-files	Displays CIFS open files information.
count	Displays the current number of open files on a WAE.
max-count	Displays the maximum number of CIFS files that can be opened on a WAE.
requests	Displays run-time information on active CIFS requests.
count	Displays the number of pending CIFS requests.
waiting	Displays the number of waiting CIFS requests.
sessions	Displays run-time information on active CIFS sessions.
count	Displays the connected session count.
list	Displays the list of connected CIFS sessions.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command displays information about the CIFS application accelerator and operates only when it is enabled. For additional information on the CIFS application accelerator, use the **show accelerator** or **show statistics accelerator** commands.

Use the **show cifs cache** command to view information about caching efficiency. You might use this command to determine if the cache contains sufficient space or if more space is needed. If you have a performance issue, you might use this command to see whether or not the cache is full.

Use the **show cifs msg-signing-servers** command to view a list of servers that require message signing.

Use the **show cifs open-files** command to view the maximum value that can be configured on the WAE for the open file count and what is being currently used. The maximum value of the open-files count is platform dependent. For WAE 294, the maximum number of open files can be preconfigured to 500, for WAE 574, the maximum number is 1500, for WAE 674, the maximum number is 12000, and for WAE 7571, the maximum number of open files is 64000.

Use the **show cifs requests count** or **show cifs requests waiting** command to monitor the load for CIFS traffic. You might also use this command for debugging purposes to isolate requests that are not processing.

Use the **show cifs sessions** count or **show cifs sessions list** command to view session information. You might use this command to monitor connected users during peak and off-peak hours.

Related Commands

clear cifs msg-signing-servers

show accelerator

show statistics accelerator

show class-map

To display the matching criteria configured for an AppNav or optimization class map, use the **show class-map** EXEC command.

show class-map type {**appnav** | **waas**} [*classmap-name*]

Syntax Description

appnav	Displays the specified AppNav class map, or all class maps if no class map is specified.
waas	Displays the specified WAAS optimization class map, or all class maps if no class map is specified.
classmap-name	Class map name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command displays the matching criteria for all class maps or a specified class map in the active policy. It also displays the number of flows that have matched each condition, in all uses of the class map, including in nested policy maps.

Examples

The following is sample output from the **show class-map type appnav** command.

```
WAE# show policy-map type appnav
Class-map type appnav match-any epmap
 Match tcp destination port 135 (56 flow-matches)
Class-map type appnav match-any NFS
 Match tcp destination port 2049 (0 flow-matches)
Class-map type appnav match-any Citrix-ICA
 Match tcp destination port 1494 (0 flow-matches)
Class-map type appnav match-any Citrix-CGP
 Match tcp destination port 2598 (0 flow-matches)
Class-map type appnav match-any HTTP
 Match tcp destination port 80 (1234 flow-matches)
 Match tcp destination port 3128 (0 flow-matches)
 Match tcp destination port 8000 (0 flow-matches)
 Match tcp destination port 8080 (246 flow-matches)
 Match tcp destination port 8088 (0 flow-matches)
Class-map type appnav match-any CIFS
 Match tcp destination port 139 (0 flow-matches)
 Match tcp destination port 445 (0 flow-matches)
Class-map type appnav match-any MAPI
 Match tcp destination epm mapi (0 flow-matches)
```

```
Class-map type appnav match-any HTTPS
 Match tcp destination port 443 (0 flow-matches)
Class-map type appnav match-any RTSP
 Match tcp destination port 554 (0 flow-matches)
 Match tcp destination port 8554 (0 flow-matches)
Class-map type appnav match-any class-default
 Match tcp (2468 flow-matches)
```

Related Commands

(config) class-map

show policy-map

show policy-sub-class

show statistics class-default

show statistics class-map

show clock

To display information about the system clock on a WAAS device, use the **show clock** EXEC command.

show clock [**detail** | **standard-timezones** {**all** | **details** *timezone* | **regions** | **zones** *region-name*}]

Syntax Description

detail	(Optional) Displays detailed information; indicates the clock source (NTP) and the current summer time setting (if any).
standard-timezones	(Optional) Displays information about the standard time zones.
all	Displays all of the standard time zones (approximately 1500 time zones). Each time zone is listed on a separate line.
details *timezone*	Displays detailed information for the specified time zone.
regions	Displays the region name of all the standard time zones. All 1500 time zones are organized into directories by region.
zones *region-name*	Displays the name of every time zone that is within the specified region.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The WAAS device has several predefined standard time zones. Some of these time zones have built-in summer time information while others do not. For example, if you are in an eastern region of the United States (US), you must use the US/Eastern time zone that includes summer time information for the system clock to adjust automatically every April and October. There are about 1500 standard time zone names.

Strict checking disables the **clock summertime** command when you configure a standard time zone is configured. You can configure summer time only if the time zone is not a standard time zone (that is, if the time zone is a customized zone).

The **show clock standard-timezones all** EXEC command enables you to browse through all standard timezones and choose from these predefined time zones so that you can choose a customized name that does not conflict with the predefined names of the standard time zones. Most predefined names of the standard time zones have two components, a region name and a zone name. You can list time zones by several criteria, such as regions and zones. To display all first level time zone names organized into directories by region, use the **show clock standard-timezones region** EXEC command.

The **show clock** command displays the local date and time information and the **show clock detail** command shows optional detailed date and time information.

Examples

Table 3-24 describes the field in the **show clock** command display.

Table 3-24 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 3-25 describes the fields shown in the **show clock detail** command display.

Table 3-25 Field Descriptions for the show clock detail Command

Field	Description
Local time	Local time relative to UTC.
UTC time	Universal time clock date and time.
Epoch	Number of seconds since Jan. 1, 1970.
UTC offset	UTC offset in seconds, hours, and minutes.

Related Commands

clock

(config) clock

show cms

To display Centralized Management System (CMS) embedded database content and maintenance status and other information for a WAAS device, use the **show cms** EXEC command.

show cms {**database content** {**dump** *filename* | **text** | **xml**} | **info** | **secure-store** | **device status** *name*}

Syntax Description

database	Displays embedded database maintenance information.
content	Writes the database content to a file.
dump *filename*	Dumps all database content to a text file. Specifies the name of the file to be saved under local1 directory.
text	Writes the database content to a file in text format.
xml	Writes the database content to a file in XML format.
info	Displays CMS application information.
secure-store	Displays the status of the CMS secure store.
device status *name*	Displays status for the device or device group indicated by *name*, the name of the device or device group.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show cms device status** command is not available on a standby Central Manager.

Examples

Table 3-26 describes the fields shown in the **show cms info** command display for WAAS application engines.

Table 3-26 Field Descriptions for the show cms info Command for WAAS Application Engines

Field	Description
Device registration information	
Device Id	Unique identifier given to the device by the Central Manager at registration, which is used to manage the device.
Device registered as	Type of device used during registration: WAAS Application Engine or WAAS Central Manager.

Table 3-26 Field Descriptions for the show cms info Command for WAAS Application Engines

Field	Description
Current WAAS Central Manager	Address of the Central Manager as currently configured in the **central-manager address** global configuration command. This address may differ from the registered address if a standby Central Manager is managing the device instead of the primary Central Manager with which the device is registered.
Registered with WAAS Central Manager	Address of the Central Manager with which the device is registered.
Status	Connection status of the device to the Central Manager. This field may contain one of three values: online, offline, or pending.
Time of last config-sync	Time when the device management service last contacted the Central Manager for updates.
CMS services information	
Service cms_ce is running	Status of the WAE device management service (running or not running). This field is specific to the WAE only.

Table 3-27 describes the fields shown in the **show cms info** command display for WAAS Central Managers.

Table 3-27 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 3-28 describes the field in the **show cms database content text** command display.

Table 3-28 Field Description for the show cms database content text Command

Field	Description
Database content can be found in /local1/cms-db-12-12-2002-17:06:08:070.txt.	Name and location of the database content text file. The **show cms database content text** command requests the management service to write its current configuration to an automatically generated file in text format.

Table 3-29 describes the field in the **show cms database content xml** command display.

Table 3-29 Field Description for the show cms database content xml Command

Field	Description
Database content can be found in /local1/cms-db-12-12-2002-17:07:11:629.xml.	Name and location of the database content XML file. The **show cms database content xml** command requests the management service to write its current configuration to an automatically generated file in XML format.

Related Commands

cms

(config) cms

show cms secure-store

To display secure store status, use the **show cms secure-store** EXEC command.

show cms secure-store

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show cms secure-store** command will display one of the following status messages (Table 3-30):

Table 3-30 Status Messges for the show cms secure-store Command

Message	Description
WAE Messages	
secure-store not initialized	Secure store is not initialized.
secure-store is initialized, enter pass-phrase to open store	Secure store is initialized and not open.
secure-store initialized and open	Secure store is initialized and open.
Central Manager Messages	
Secure store is in CM 'auto-generated passphrase' mode in 'Open' state.	Secure store is initialized and open and in the auto-passphrase mode.
Secure store is in 'User-provided passphrase' mode in 'Not Open' state. Use the command 'cms secure-store open' to open the secure store.	Secure store is initialized but not open because it is in the user-passphrase mode and the passphrase has not been entered.
Secure store is in 'User-provided passphrase' mode in 'Open' state.	Secure store is initialized and open and the user-passphrase has been entered.

Examples

The following is sample output from the **show cms secure-store** command:

```
WAE# show cms secure-store
Secure store is in 'User-provided passphrase' mode in 'Open' state.


***** WARNING : If Central Manager device is reloaded, you must reopen Secure St
ore with the correct passphrase. Otherwise disk encryption and the CIFS preposit
```

```
ion features will not operate on WAE (s).*****
```

Related Commands

cms secure-store

show crypto

To display crypto layer information, use the **show crypto** EXEC command.

show crypto {**certificate-detail** {**factory-self-signed** | **management** | **admin** | *filename*} | **certificates** | **ssl services** {**accelerated-service** *service* | **host-service peering**}}

Syntax Description

certificate-detail	Displays a certificate in detail.
factory-self-signed	Displays WAAS self-signed certificates in detail.
management	Displays WAAS management certificates in detail.
admin	Displays the certificate details for the Central Manager admin service certificate. This option can be used only on the Central Manager.
filename	Filename of the certificate to display.
certificates	Displays a summary of all PKI certificates. This option can be used only on the WAE.
ssl services	Displays status of SSL services. This option can be used only on the WAE.
accelerated-service *service*	Displays status of SSL accelerated service with the specified service name.
host-service peering	Displays status of the SSL host peering service.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-31 describes the fields in the **show crypto certificate-detail** command display.

Table 3-31 Field Descriptions for the show crypto certificate-detail Command

Field	Description
Version	Certificate version.
Serial Number	Certificate serial number.
Signature Algorithm	Certificate signature algorithm.
Issuer	Information on the signer of the certificate.
Validity	
Not Before	The date and time before which the certificate is not valid.
Not After	The date and time after which the certificate is not valid.

Table 3-31 Field Descriptions for the show crypto certificate-detail Command

Field	Description
Subject	Information on the holder of the certificate.
Subject Public Key Info	
Public Key Algorithm	Fields display X.509 certificate information as defined in RFC 5280.
RSA Public Key	
Modulus	
Exponent	
X509v3 extensions	
X509v3 Subject Key Identifier	Fields display X.509 certificate information as defined in RFC 5280.
X509v3 Authority Key Identifier	
X509v3 Basic Constraints	
Signature Algorithm	
BEGIN CERTIFICATE	Actual certificate follows until the End Certificate line.
END CERTIFICATE	Line that signifies the end of the certificate.

Table 3-32 describes the fields in the **show crypto certificates** command display.

Table 3-32 Field Descriptions for the show crypto certificates Command

Field	Description
Certificate Only Store	Certificate Authority (CA) certificates.
Managed Store	User-defined certificates. Used under the server-cert-key section of SSL accelerated services. This certificate is used as a server certificate for client-to-WAE connections.
Local Store	Certificates that are configured on the WAE by default.
Machine Self signed Certificate	Certificate from the WAE to the server when client authentication is requested by the server.
Format	Format of the certificate (PEM or PKCS12).
Subject	The name of the holder of the certificate.
Issuer	Who signed the certificate.
Management Service Certificate	Certificate used to identify the WAE with the Central Manager.
Format	Format of the certificate (PEM or PKCS12).
EEC: Subject	Name of the holder of the certificate.
Issuer	Who signed the certificate.

Related Commands **show statistics crypto ssl ciphers**

show debugging

To display the state of each debugging option that was previously enabled on a WAAS device, use the **show debugging** EXEC command.

show debugging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show debugging** command shows which debug options have been enabled or disabled. If there are no debug options configured, the **show debugging** command shows no output.

The **dre**, **epm**, **flow**, **print-spooler**, **rbcp**, **tfo**, **translog**, and **wccp** command options are supported in the application-accelerator device mode only. The **emdb** and **rpc** command options are supported in the central manager device mode only.

The **show debugging** command displays only the type of debugging enabled, not the specific subset of the command.

Examples

The following is sample output from the **show debugging** command:

```
WAE# debug tfo buffer-mgr
WAE# debug tfo connection
WAE# show debugging
tfo bufmgr debugging is on
tfo compmgr debugging is on
tfo connmgr debugging is on
tfo netio debugging is on
tfo statmgr debugging is on
tfo translog debugging is on
```

In this example, the **debug tfo buffer-mgr** and the **debug tfo connection** commands coupled with the **show debugging** command display the states of **tfo buffer-mgr** and **tfo connection** debugging options.

Related Commands

debug all

show device-id

To display the device ID of a WAAS device, use the **show device-id** EXEC command.

show device-id

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

This command displays the device ID, as follows:

```
WAE# show device-id
System Device ID is: 00:1a:64:f2:22:37
```

Related Commands

(config) peer

show device-mode

To display the configured or current device mode of a WAAS device, use the **show device-mode** EXEC command.

show device-mode {**configured** | **current**}

Syntax Description

configured	Displays the configured device mode, which has not taken effect yet.
current	Displays the current device mode.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

To display the configured device mode that has not yet taken effect, enter the **show device-mode configured** EXEC command. For example, if you had entered the **device mode central-manager** global configuration command on a WAAS device to change its device mode to central manager but have not yet entered the **copy run start EXEC** command to save the running configuration on the device, then if you were to enter the **show device-mode configured** command on the WAAS device, the command output would indicate that the configured device mode is central-manager.

Examples

The following is sample output from the **show device mode** command. It displays the current mode in which the WAAS device is operating.

```
WAE# show device-mode current

Current device mode: application-accelerator
```

Table 3-33 describes the field in the **show device-mode current** command display.

Table 3-33 Field Description for the show device-mode current Command

Field	Description
Current device mode	Current mode in which the WAAS device is operating.

The following is sample output from the **show device configured** command. It displays the configured device mode that has not yet taken effect.

```
WAE# show device-mode configured

Configured device mode: central-manager
```

Table 3-34 describes the field in the **show device-mode configured** command display.

Table 3-34 Field Description for the show device-mode configured Command

Field	Description
Configured device mode	Device mode that has been configured, but has not yet taken effect.

Related Commands **(config) device mode**

show directed-mode

To view the status and port assigned to directed mode on a device, use the **show directed-mode** EXEC command.

show directed-mode

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following is sample output from the **show directed-mode** EXEC command:

```
WAE# show directed-mode

Configuration Status:  Disabled
Config Item                          Mode          Value
-----------                          ----          ------
UDP port                             Default       4050
```

This example shows that directed mode is enabled and it is using UDP port 4050.

Related Commands

show statistics directed-mode

show statistics connection closed

(config) directed-mode

show disks

To view information about the WAAS device disks, use the **show disks** EXEC command.

show disks {**details** | **failed-disk-id** | **failed-sectors** [*disk_name*] | **tech-support** [**details** | **fwlogs**]}

Syntax Description

details	Displays currently effective configurations with more details.
failed-disk-id	Displays a list of disk serial numbers that have been identified as failed. **Note** This option is not available on WAE-7341 and WAE-7371 models.
failed-sectors	Displays a list of failed sectors on all the disks.
disk_name	(Optional) Name of the disk for which failed sectors are displayed (disk00 or disk01).
tech-support	Displays SSD/HDD attributes for SSD/HDD devices. Displays hard drive diagnostic information and information about impending disk failures. Displays all available information from the RAID controller, including disk status (logical and physical), disk vendor ID, and serial numbers. This command replaces the **show disk smart-info** EXEC command.
details	(Optional) Displays more detailed SMART disk monitoring information.
fwlogs	(Optional) Displays disk controller firmware logs (available only on WAVE-75xx/85xx devices).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show disks details** EXEC command displays the percentage or amount of disk space allocated to each file system, and the operational status of the disk drives, after reboot.

The WAAS software supports filtering of multiple syslog messages for a single, failed section on IDE, SCSI, and SATA disks.

Note When the system software recovery procedure is used and the system reboots and begins optimizing traffic, the show **disks details command** may show that the /dre1 partition is 98% or more used, due to the preallocation of DRE cache space. Use the **show statistics dre** command to display the actual DRE cache usage.

Proactively Monitoring Disk Health with SMART

The ability to proactively monitor the health of disks is available using SMART. SMART provides you with hard drive diagnostic information and information about impending disk failures.

SMART is supported by most disk vendors and is a standard method used to determine how healthy a disk is. SMART attributes include several read-only attributes (for example, the power on hours attribute, the load and unload count attribute) that provide the WAAS software with information regarding the operating and environmental conditions that may indicate an impending disk failure.

SMART support is vendor and drive technology (IDE, SCSI, and Serial Advanced Technology Attachment [SATA] disk drive) dependent. Each disk vendor has a different set of supported SMART attributes.

Even though SMART attributes are vendor dependent there is a common way of interpreting most SMART attributes. Each SMART attribute has a normalized current value and a threshold value. When the current value exceeds the threshold value, the disk is considered to have "failed." The WAAS software monitors the SMART attributes and reports any impending failure through syslog messages, SNMP traps, and alarms.

To display SMART information, use the **show disks tech-support** EXEC command. To display more detailed SMART information, enter the **show disks tech-support details** EXEC command. The output from the **show tech-support** EXEC command also includes SMART information.

Examples

The following is sample output from the **show disks failed-sectors** command. It displays a list of failed sectors on all disk drives.

```
WAE# show disks failed-sectors
disk00
=========
89923
9232112

disk01
=========
(None)
```

The following is sample output from the **show disks failed-sectors** command when you specify a disk drive. It displays a list of failed sectors for disk01.

```
WAE# show disks failed-sectors disk01
disk01
=========
(None)
```

If there are disk failures, a message is displayed, notifying you about this situation when you log in.

Table 3-35 describes the fields shown in the **show disks failed-disk-id** command display.

Table 3-35 Field Description for the show disks failed-disk-id Command

Field	Description
Diskxx	Number and location of the physical disk.
Alpha-numeric string	Serial number of the disk.

Table 3-36 describes the fields shown in the **show disks details** command display.

Table 3-36 Field Descriptions for the show disks details Command

Field	Description
Physical disk information or RAID Physical disk information	Lists the disks by number. On RAID-5 systems, this field is called RAID Physical disk information.
disk00	Availability of the disk: Present, Not present or Not responding, Not used (*), or Online (for RAID-5 disks). Disk identification number and type, for example: (h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB). Lists attributes such as serial number, the technology family(SATA/SAS) and the capacity of the SSD or HDD.
disk01	Same type of information is shown for each disk.
RAID Logical drive information	RAID-5 logical drive status and error conditions and total size. (Only shown for RAID-5 systems.)
Mounted filesystems	Table containing the following column heads:
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name “md1” indicates that the partition is a raided partition and that the RAID type is RAID-1.
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].
Disk encryption feature	Indicates whether the disk encryption feature is enabled or disabled.
Disk object cache extend status	Indicates whether the extended object cache feature is enabled or disabled.

The following is sample output from the **show disks tech-support** command. The output shows that partition 04 and partition 05 on disks disk00 and disk01 are GOOD, and the RAIDed partitions /dev/md4 & /dev/md5 are in NORMAL OPERATION. However, the RAIDed partition /dev/md8 has an issue with one of the drives. Disk04 with partition 00 is GOOD, but the status shows ONE OR MORE DRIVES ABNORMAL because there is no pair on this partition.

```
WAE# show disks tech-support

/dev/md4      RAID-1    NORMAL OPERATION       disk00/04[GOOD]
disk01/04[GOOD]
/dev/md5      RAID-1    NORMAL OPERATION       disk00/05[GOOD]
disk01/05[GOOD]
...
/dev/md8      RAID-1    ONE OR MORE DRIVES ABNORMAL  disk04/00[GOOD]
```

Table 3-37 describes some typical fields in the **show disks tech-support** command display for a RAID-1 appliance that supports SMART. SMART attributes are vendor dependent; each disk vendor has a different set of supported SMART attributes.

Table 3-37 Field Descriptions for the show disks tech-support Command (RAID-1)

Field	Description
disk00—disk05	Number of drives shown depends on the hardware platform.
SSD Statistics	
Lifetime remaining	Displays the percentage remaining lifetime of the SSD disk.
Total bytes written	Displays total bytes written to the SSD disk.
Write Amplification Factor	Displays the quotient of data written to physical NAND internally by the SSD itself divided by data transferred to the SSD from the host.
Device	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time hh:mm:ss, year, clock standard. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.

Table 3-38 describes the fields shown in the **show disks tech-support** command display for a RAID-5 appliance.

Table 3-38 Field Descriptions for the show disks tech-support Command (RAID-5)

Field	Description
Controllers found	Number of RAID controllers found.
Controller information	

Table 3-38 Field Descriptions for the show disks tech-support Command (RAID-5) (continued)

Field	Description
Controller Status	Functional status of the controller.
Channel description	Description of the channel transport protocols.
Controller Model	Make and model of the controller.
Controller Serial Number	Serial number of the ServeRAID controller.
Physical Slot	Slot number.
Installed memory	Amount of memory for the disk.
Copyback	Status of whether copyback is enabled or disabled.
Data scrubbing	Status of whether data scrubbing is enabled or disabled.
Defunct disk drive count	Number of defunct disk drives.
Logical drives/Offline/Critical	Number of logical drives, number of drives that are offline, and number of critical alarms.
Controller Version Information	
BIOS	Version number of the BIOS.
Firmware	Version number of the Firmware.
Driver	Version number of the Driver.
Boot Flash	Version number of the Boot Flash.
Controller Battery Information	
Status	Functional status of the controller battery.
Over temperature	Over temperature condition of the battery.
Capacity remaining	Percent of remaining battery capacity.
Time remaining (at current draw)	Number of days, hours, and minutes of battery life remaining based on the current draw.
Controller Vital Product Data	
VPD Assigned#	Number assigned to the controller vital product data (VPD).
EC Version#	Version number.
Controller FRU#	Number assigned to the controller field-replaceable part.
Battery FRU#	Number assigned to the battery field-replaceable part.
Logical drive information	
Logical drive number	Number identifying the logical drive to which the information applies.
Logical drive name	Name of the logical drive.
RAID level	RAID level of the logical drive.
Status of logical drive	Functional status of the logical drive.
Size	Size (in megabytes) of the logical drive.
Read-cache mode	Configuration status of read-cache mode: Enabled or Disabled.
Write-cache mode	Configuration status of write-cache mode for write-back: Enabled or Disabled.

Table 3-38 Field Descriptions for the show disks tech-support Command (RAID-5) (continued)

Field	Description
Write-cache setting	Configuration status of the write-cache setting for write-back: Enabled or Disabled.
Partitioned	Partition state. Values are Yes or No.
Number of chunks	Number of disks participating in the RAID-5 array.
Stripe-unit size	Amount of data storage per stripe unit. The default is 256 KB per disk in the logical array. This parameter is not configurable.
Stripe order (Channel,Device)	Order in which data is striped across a group of physical drives that are grouped in a RAID array.
Bad stripes	Flag for bad stripes. Flag values are Yes or No.
Physical drive information	
Device #	Device number for which the information applies.
Device is a xxxx	Type of device.
State	State of the device: Online or Offline.
Supported	Status showing if the device is supported.
Transfer Speed	Device transfer speed.
Reported Channel,Device	Provides channel information for all the disks participating in the RAID-5 array.
Reported Enclosure,Slot	Device number and slot number.
Vendor	Vendor identification number.
Model	Model number.
Firmware	Firmware number.
Serial number	Serial number.
Size	Size (in megabytes) of the physical drive.
Write Cache	Status of whether the write cache is enabled.
FRU	Field Replaceable Unit number. A RAID defunct drive FRU event occurs when a specified hard disk drive with the provided FRU number fails in a RAID configuration. The default value for this field is NONE.
PFA	Predictive Failure Analysis flag. The flag default value is No. If the RAID predicts a drive failure, this field is set to Yes and a critical alarm is raised on the WAE.

Table 3-39 describes the fields in the **show disks tech-support details** command display for a RAID-1 appliance that supports SMART. Details in this display depend on the drive manufacturer and vary between drives.

Table 3-39 Field Descriptions for the show disks tech-support details Command

Field	Description
disk00—disk05	Number of drives shown depends on the hardware platform.
Device	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time hh:mm:ss, year, clock standard. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.
Current Drive Temperature	Temperature of the drive in degrees Celsius.
Manufactured in week XX of year	Manufacturing details.
Current start stop count	Number of times the device has stopped or started.
Recommended maximum start stop count	Maximum recommended count used to gauge the life expectancy of the disk.
Error counter log	Table displaying the error counter log. Counters for various types of disk errors.

Related Commands

disk

(config) disk error-handling

show tech-support

show dre

To view DRE configuration information, use the **show dre** EXEC command.

show dre [**auto-bypass**]

Syntax Description

auto-bypass	Displays the auto bypass table entries.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

The following is sample output from the **show dre** EXEC command:

```
WAE# show dre

DRE configuration:
  Mac-id: 50:3d:e5:9c:8f:a5
  DRE-peer-id: 50:3d:e5:9c:8f:a5-01319249ed67-92f8dea8
  Max concurrent connections: 200, max fan-out: 700
  DRE auto bypass threshold 7074 MB
```

Related Commands

clear dre

(config) dre

show filtering list

To display information about the incoming and outgoing TFO flows that the WAE currently has, use the **show filtering list** EXEC command.

show filtering list [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*] }] [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}]

Syntax Description

|	(Optional) Output modifier.
begin *regex*	Begins with the line that matches the regular expression. You can enter multiple expressions.
exclude *regex*	Excludes lines that match the regular expression. You can enter multiple expressions.
include *regex*	Includes lines that match the regular expression. You can enter multiple expressions.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **show filtering list** command lists TCP flows that the WAE is currently optimizing. It also includes TCP flows that are not being optimized but that are being passed through by the WAE. A “P” in the State column indicates a passed through flow.

Examples

The following is sample output from the **show filtering list** command. It displays TFO connection information for the WAE.

```
WAE# show filtering list
E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough
B: Bypass, L: Last Ack, W: Time Wait, D: Done
T: Timedout, C: Closed

    Local-IP:Port        Remote-IP:Port          Tuple(Mate)       State
   10.99.11.200:1398     10.99.22.200:80    0xcba709c0(0xcba70a00)   E
   10.99.11.200:1425     10.99.22.200:80    0xcba70780(0xcba707c0)   E
   10.99.11.200:1439     10.99.22.200:5222  0xcba703c0(0xcba70b40)   Sr
   10.99.11.200:1440     10.99.22.200:5222  0xcba70400(0xcba70440)   Sr
   10.99.22.200:1984     10.99.11.200:80    0xcba70600(0xcba70640)   E
   10.99.22.200:1800     10.99.11.200:23    0xcba70480(0x0       )   PE
   10.99.11.200:1392     10.99.22.200:80    0xcba70f80(0x0       )   E
   10.99.22.200:20       10.99.11.200:1417  0xcba701c0(0xcba70180)   E
   10.99.11.200:1417     10.99.22.200:20    0xcba70180(0x0       )   E
   10.99.22.200:1987     10.99.11.200:80    0xcba70240(0xcba70200)   E
```

```
10.99.11.200:1438     10.99.22.200:5222  0xcba70900(0xcba70580)   Sr
10.99.22.200:1990     10.99.11.200:80    0xcba70100(0xcba70140)   E
10.99.22.200:80       10.99.11.200:1426  0xcba70740(0xcba70700)   E
10.99.22.200:80       10.99.11.200:1425  0xcba707c0(0xcba70780)   E
10.99.22.200:1985     10.99.11.200:80    0xcba70a40(0xcba70a80)   E
10.99.22.200:80       10.99.11.200:1410  0xcba70500(0xcba70540)   E
10.99.22.200:80       10.99.11.200:1398  0xcba70a00(0xcba709c0)   E
10.99.22.200:80       10.99.11.200:1392  0xcba70f40(0xcba70f80)   E
10.0.19.5:54247       10.1.242.5:80      0xc9e5b400(0xc9e5b100)   ED
```

Note The "ED" state occurs when one socket in the pair is closed (D), but the mate is still established (E).

Related Commands

show accelerator

show statistics filtering

show statistics auto-discovery

show statistics connection closed

show flash

To display the flash memory version and usage information for a WAAS device, use the **show flash** EXEC command.

show flash

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-40 describes the fields shown in the **show flash** command display.

Table 3-40 Field Descriptions for the show flash Command

Field	Description
WAAS software version (disk-based code)	WAAS software version and build number that is running on the device.
System image on flash:	
Version	Version and build number of the software that is stored in flash memory.
System flash directory:	
System image	Number of sectors or bytes used by the system image.
Bootloader, rescue image, and other reserved areas, or Rescue image Bootloader & others	Number of sectors used by the bootloader, rescue image, and other reserved areas. On some devices, the number of bytes used by the rescue image is shown separately from the number of bytes used by the bootloader and other areas.
XX sectors total, XX sectors free, or Total Used Total Free	Total number of sectors in the flash memory and the number of free sectors available. Some devices show the total number of bytes used and the total free bytes available.

show flow record

To display collection information for a WAAS device, use the **show flow record** EXEC command. Collection information includes source and destination address, source and destination port, class name, number of optimized and unoptimized packets, input/output information for DRE and LZ compression, and average latency encode/decode information for DRE and LZ compression.

show flow record {*RecordName* **[template] | waas-all }**

Syntax Description

RecordName	The name of the flow record
template	The identity of the template associated with this flow record.
waas-all	Collects all WAAS statistics.

Defaults

No default behavior or values.

Device Modes

application-accelerator

central-manager

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

show hardware

To display system hardware status for a WAAS device, use the **show hardware** EXEC command.

show hardware

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show hardware** command lists the system hardware status, including the version number, the startup date and time, the run time since startup, the microprocessor type and speed, the amount of physical memory available, and a list of disk drives.

Examples

Table 3-41 describes the fields shown in the **show hardware** command display. The display may vary depending on the hardware platform.

Table 3-41 Field Descriptions for the show hardware Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) *year* by Cisco Systems, Inc. Cisco Wide Area Application Services (universal-k9) Software Release *X.X.X* (build b*nnn month day year*)	Software application, copyright, release, and build information. Displays universal-k9 for the full software image, accelerator-k9 for the accelerator only software image, and universal-npe-k9 or accelerator-npe-k9 for the NPE versions of those images. The NPE image versions have the disk encryption feature disabled for use in countries where disk encryption is not permitted.
Version	Device model identifier and version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Compile information for the software build.
Device Id	The device ID.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.

Table 3-41 Field Descriptions for the show hardware Command (continued)

Field	Description
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.
CPU 0 is	CPU manufacturer information (appears once for each CPU core).
Total X CPU	Number of CPUs on the device. Also reports number of cores and threads available on multi-core devices.
XXXX Mbytes of Physical memory	Number of megabytes of physical memory on the device.
XXXX Mbytes of flash memory	Number of megabytes of flash memory on the device.
X CD ROM drive	Number of CD-ROM drives on the device (if applicable).
X GigabitEthernet interfaces X TenGigabitEthernet interfaces	Number of Gigabit Ethernet and 10-Gigabit Ethernet interfaces on the device.
X InlineGroup interfaces	Number of InlineGroup interfaces on the device (if applicable).
X Console interface	Number of console interfaces on the device.
X external USB interface	Number of USB interfaces on the device.
Device Model Number	Product model identification information.
BIOS Information	Information about the BIOS.
Vendor	Name of the BIOS vendor.
Version	BIOS version number.
Rel. Date	(Release date) Date that the BIOS was released.
Mainboard info	
Model	Hardware model identifier of the device.
Serial Number	Serial number of the WAE.
Detailed Memory Device (DIMM) configuration	Size and location of the installed memory.
List of all disk drives	
Physical disk information or RAID Physical disk information	Disks listed by number.
disk00, and so on	Availability of the disk: Present, Not present or not responding, or Not used (*). For RAID disks: ONLINE or OFFLINE. For each disk, shows the size and disk identification number.
RAID Logical drive information	Size and other information about the RAID logical drive (appears only if the device contains a logical RAID drive).
Mounted filesystems	Table containing the following column heads:
Mount point	Mount point for the file system. For example the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.

Table 3-41 Field Descriptions for the show hardware Command (continued)

Field	Description
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name "md1" indicates that the partition is a raided partition and that the RAID type is RAID-1.
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].
Disk encryption feature	Whether the disk encryption feature is enabled or disabled.
Primary Power Supply Unit	Whether the primary power supply is installed and powered. (Shown for devices that support reporting power supply information.)
Redundant Power Supply Unit	Whether the redundant power supply is installed and powered. (Shown for devices that support reporting redundant power supply information.)
Total number of system fans is	Number of fans installed in the device. (Shown for devices that support reporting fan information.)
Disk object cache extend	Whether the extended disk object cache is enabled or disabled. (Shown for devices that support the extended disk object cache.)

Related Commands

show disks

show version

show hosts

To view the hosts on a WAAS device, use the **show hosts** EXEC command.

show hosts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show hosts** command lists the name servers and their corresponding IP addresses. It also lists the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary.

Examples

Table 3-42 describes the fields shown in the **show hosts** command display.

Table 3-42 field Descriptions for the show hosts Command

Field	Description
Domain names	Domain names used by the WAE to resolve the IP address.
Name Server(s)	IP address of the DNS name server or servers.
Host Table	
hostname	FQDN (hostname and domain) of the current device.
inet address	IP address of the current host device.
aliases	Name configured for the current device based on the **host** global configuration command.

Related Commands

(config) ip hosts

show inetd

To display the status of TCP/IP services on a WAAS device, use the **show inetd** EXEC command.

show inetd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show inetd** EXEC command displays the enabled or disabled status of TCP/IP services on the WAAS device. You can ignore the TFTP service status because TFTP is not supported on WAAS.

Examples

Table 3-43 describes the fields shown in the **show inetd** command display.

Table 3-43 Field Descriptions for the show inetd Command

Field	Description
Inetd service configurations:	
ftp	Status of whether the FTP service is enabled or disabled.
rcp	Status of whether the RCP service is enabled or disabled.

Related Commands

(config) inetd

show interception-method

To display the configured interception method, use the **show interception-method** EXEC command.

show interception-method

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

The following is sample output from the **show interception-method** command:

```
WAE# show interception-method
Interception-method: wccp
WCCP Interception :
Configured State :  Enabled
Operational State : Enabled

Services Enabled on this WAE:
        TCP Promiscuous 61
```

Related Commands

(config) interception-method

show interface

To display the hardware interface information for a WAAS device, use the **show interface** EXEC command.

show interface {**GigabitEthernet** *slot/port* | **InlineGroup** *slot*/*grpnumber* | **InlinePort** *slot*/*grpnumber* {**lan** | **wan**} | **PortChannel** *index* | **standby** *grpnumber* | **virtual** *slot/port* | **TenGigabitEthernet** *slot/port* | **bvi** *bridge-id*} [**detail**]

Syntax Description

GigabitEthernet *slot/port*	Displays Gigabit Ethernet interface device information. Slot and port number for the Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
InlineGroup *slot*/*grpnumber*	Displays the inline group information and the slot and inline group number for the selected interface.
InlinePort	Displays the inline port information and the slot and inline group number for the selected interface.
lan	Displays the inline port information for the LAN port.
wan	Displays the inline port information for the WAN port.
PortChannel *index*	Displays the port channel interface (1-4) device information.
standby *grpnumber*	Displays the standby group (1-2) information.
virtual *slot/port*	Displays the virtual interface device information. Slot and port number for the virtual interface. The slot range is 1–2; the port range is 0.
TenGigabitEthernet *slot/port*	Displays 10-Gigabit Ethernet interface device information. Slot and port number for the Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
bvi *bridge-id*	Displays the bridge virtual interface (1-4) information.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

On an AppNav Controller device with a port-channel interface configured, interception statistics are collected only for the port-channel interface, not for the individual member interfaces.

Examples

The following is sample output from the **show interface** command. It displays information for GigabitEthernet interface 0 in slot 0:

```
WAE-231-03# show interface gigabitethernet 0/0
```

```
Ethernet Address                    : 50:3d:e5:9c:8f:a5
Internet Address                    : 2.43.65.52
Netmask                             : 255.255.255.0
Admin State                         : Up
Operation State                     : Running
Maximum Transfer Unit Size          : 1500
Input Errors                        : 0
Input Packets Dropped               : 0
Packets Received                    : 4074292
Output Errors                       : 0
Output Packets Dropped              : 0
Load Interval                       : 30
Input Throughput                    : 12538 bits/sec, 13 packets/sec
Output Throughput                   : 23235 bits/sec, 11 packets/sec
Packets Sent                        : 3334662
Auto-negotiation                    : On
Full Duplex                         : Yes
Speed                               : 1000 Mbps
```

Table 3-44 describes the fields shown in the **show interface GigabitEthernet** command. Most of the other **show interface** command options display similar output.

Table 3-44 Field Descriptions for the show interface GigabitEthernet command

Field	Description
Description	Description of the interface, including member interfaces. Displayed only for logical interfaces.
lsp	Displayed only if interface is configured with link state propagation.
flow sync	Flow synchronization status. Displayed only if interface is on an AppNav Controller Interface Module.
Ethernet address	Layer-2 MAC address.
Internet address	Internet IP address configured for this interface.
Netmask	Netmask configured for this interface.
Admin State	Administrative state.
Operational State	Administrative state.
Maximum Transfer Unit Size	Current configured MTU value.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Packets Received	Total number of packets received by this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Load Interval	Interval at which the interface is polled for statistics and to calculate throughput.
Input Throughput	Input throughput in bits per second and packets per second.
Output Throughput	Output throughput in bits per second and packets per second.
Packets Sent	Total number of packets sent from this interface.

Table 3-44 Field Descriptions for the show interface GigabitEthernet command (continued)

Field	Description
Auto-negotiation	State of auto-negotiation for transmission speed and mode. Shown only for physical interfaces.
Full Duplex	State of full duplex transmission mode. Shown only for physical interfaces.
Speed	Configured speed. Shown only for physical interfaces.
Interception Statistics (appears only for AppNav Controller Interface Module interfaces)	
Input Packets Forwarded/Bridged	Number of input packets forwarded or bridged.
Input Packets Redirected	Number of input packets redirected.
Input Packets Punted	Number of input packets punted.
Input Packets Dropped	Number of input packets dropped.
Output Packets Forwarded/Bridged	Number of output packets forwarded or bridged.
Output Packets Injected	Number of output packets injected.
Output Packets Dropped	Number of output packets dropped.

Table 3-44 describes the fields shown in the **show interface InlineGroup** command.

Table 3-45 Field Descriptions for the show interface InlineGroup command

Field	Description
General Statistics Of The Group	
Internet address	Internet IP address configured for this interface.
Netmask	Netmask configured for this interface.
Interface Operating Mode	Operating mode of interface: • Intercept—Intercepting traffic • Bypass—Bypassing traffic.
Standard NIC Mode	Standard NIC mode. Off when in inline mode.
Disable Bypass Mode	Unused.
Watchdog Timer	Watchdog timer status.
Timer frequency(in ms)	Timer frequency in ms. If the timer is not reset before this interval, the interface switches into bypass mode.
Autoreset Frequency(in ms)	WAAS resets the watchdog timer at this interval.
The watchdog timer expiry(in ms)	Watchdog timer expiration in ms.
VLAN IDs configured for interception	List of VLAN IDs configured for interception. All means all VLANS are configured for interception.
Inline Port Statistics Of The Group (WAN port and LAN port shown in separate columns)	
Packets Received Inline	Number of packets received by this interface.
Packets Bridged	Number of non-TCP packets or other packets that the device does not want to intercept.

Table 3-45 Field Descriptions for the show interface InlineGroup command (continued)

Field	Description
Packets Forwarded	Number of packets considered for optimization or pass-through, including host-generated packets.
Packets Received on native	Number of packets received on a built-in interface (not on the interface module) that were previously seen on the bridge interface. This implies a routing loop in the network.
Active flows on the interface	Number of active flows on the interface.

Related Commands

(config) interface GigabitEthernet

(config) interface InlineGroup

show running-config

show startup-config

show inventory

To display the system inventory information for a WAAS device, use the **show inventory** EXEC command.

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show inventory** EXEC command allows you to view the UDI for a WAAS device. This identity information is stored in the nonvolatile memory of the WAAS device.

The UDI is electronically accessed by the product operating system or network management application to enable identification of unique hardware devices. The data integrity of the UDI is vital to customers. The UDI that is programmed into the nonvolatile memory of the WAAS device is equivalent to the UDI that is printed on the product label and on the carton label. This UDI is also equivalent to the UDI that can be viewed through any electronic means and in all customer-facing systems and tools. Currently, there is only CLI access to the UDI; there is no SNMP access to the UDI information.

You can also use the **show tech-support** EXEC command to display the WAAS device UDI.

Examples

Table 3-46 describes the fields shown in the **show inventory** command display.

Table 3-46 Field Descriptions for the show inventory Command

Field	Description
Name	Chassis for an appliance or slot number for an installed interface card.
DESCR	Description of the device.
PID	Product identification (ID) number of the device.
VID	Version ID number of the device. Displays as 0 if the version number is not available.
SN	Serial number of the device.

Related Commands

show tech-support

show ip access-list

To display the access lists that are defined and applied to specific interfaces or applications on a WAAS device, use the **show ip access-list** EXEC command.

show ip access-list [*acl-name* | *acl-num*]

Syntax Description

acl-name	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl-num	(Optional) Information for a specific access list, using a numeric identifier (0–99 for standard access lists and100–199 for extended access lists).

Defaults

Displays information about all defined access lists.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Use the **show ip access-list** EXEC command to display the access lists that have been defined on the WAAS device and what rules are being hit. Unless you identify a specific access list by name or number, the system displays information about all the defined access lists, including the following sections:

- Available space for new lists and conditions
- Defined access lists
- References by interface and application

Interception access lists are shown under the Application access list references section.

Examples

Table 3-47 describes the fields shown in the **show ip access-list** command display.

Table 3-47 Field Descriptions for the show ip access-list Command

Field	Description
Space available:	
XX access lists	Number of access lists remaining out of 50 maximum lists allowed.
XXX access list conditions	Number of access list conditions remaining out of 500 maximum conditions allowed.
XXX TCAM Entries	Number of remaining TCAM entries on an ANC.

Table 3-47 Field Descriptions for the show ip access-list Command (continued)

Field	Description
Standard IP access list	Name of a configured standard IP access list. Displays a list of the conditions configured for this list.
Extended IP access list	Name of a configured extended IP access list. Displays a list of the conditions configured for this list.
Interface access list references	List of interfaces and the access lists with which they are associated, displayed in the following format: *interface slot/port* *interface direction* *access list number*
Application access list references	List of applications and the access lists with which they are associated, displayed in the following format: *application type* *access list type and number* *associated port*

Related Commands

clear arp-cache

(config) interception

(config) ip access-list

show ip routes

To display the IP routing table for a WAAS device, use the **show ip routes** EXEC command.

show ip routes [**data** | **management**]

Syntax Description

data	Displays the routing table for data traffic.
management	Displays the routing table for management traffic.

Defaults

Displays the routing table for both data and management traffic.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

The **show ip routes** command displays the IP route table, which lists all of the different routes that are configured on the WAE. The WAE uses this table to determine the next hop. This table includes routes from three sources: the WAE interfaces, any user-configured static routes, and the default gateway. The last line in the Data Routes table shows the default route.

Examples

Table 3-48 describes the fields shown in the **show ip routes** command display.

Table 3-48 Field Descriptions for the show ip routes Command

Field	Description
Destination	Destination IP addresses for each route.
Netmask	Netmask for each route.
Gateway	Gateway address for each route.
Interface	Interface on which each route is configured.

Related Commands

(config) ip

(config-if) ip

show kdump

To display the kernel crash dump information for a WAAS device, use the **show kdump** EXEC command.

show kdump

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-49 describes the fields shown in the **show kdump** command display.

Table 3-49 Field Descriptions for the show kdump Command

Field	Description
Kdump state	Enabled or not enabled.
Kdump operation	Operational or not operational.
Kdump installed	If the kdump package is not installed, this line alerts you.
Kdump crashkernel	Crash kernel information (Memory @ Base Address).

Related Commands

(config) kernel kdump enable

(config) logging console

show kerberos

To display the Kerberos authentication configuration for a WAAS device, use the **show kerberos** EXEC command.

show kerberos

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-50 describes the fields shown in the **show kerberos** command display.

Table 3-50 Field Descriptions for the show kerberos Command

Field	Description
Kerberos Configuration	
Local Realm	Local realm name.
DNS suffix	DNS suffix for the realm.
Realm for DNS suffix	DNS addresses of the computers that are part of this realm.
Name of host running KDC for realm	Name of the host running the Key Distribution Center for the realm.
Master KDC	Primary or main Key Distribution Center.
Port	Port that the Kerberos server is using for incoming requests from clients. The default is port 88.

Related Commands

clear arp-cache

(config) logging console

show key-manager

To display the key manager information for a WAAS Central Manager, use the **show key-manager** EXEC command.

show key-manager {**key-token** | **status**}

Syntax Description

key-token	Displays the encryption key token for each registered WAE device.
status	Displays the encryption status for each registered WAE device.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

central-manager

Usage Guidelines

This command is not available on a standby Central Manager.

Examples

Table 3-51 describes the fields shown in the **show key-manager key-token** command display. The set of fields is displayed for each key used on each WAE registered to the Central Manager.

Table 3-51 Field Descriptions for the show key-manager key-token Command

Field	Description
WAE Device	WAE device name.
Key Token	The encryption token.
Creation Time	Time the encryption key was created.
Encryption Algorithm	Type of encryption algorithm used.
Type	Type of key.

Related Commands

(config) disk encrypt

cms secure-store

show license

To display license information for a WAAS device, use the **show license** EXEC command.

show license

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following is sample output from the **show license** command. It lists the WAAS licenses, giving the name, status, date applied, and the name of the user that applied the license for each active license.

```
WAE# show license
License Name       Status       Activation Date       Activated by
-------------------------------------------------------------------------
Transport          not active
Enterprise         active       11/12/2008            admin
Video              not active
Virtual-Blade      not active
```

Related Commands

clear arp-cache

license add

show logging

To display the system message log configuration for a WAAS device, use the **show logging** EXEC command.

show logging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the system message log to view information about events that have occurred on a WAAS device. The *syslog.txt* file is contained in the */local1* directory.

Examples

The following is sample output from the **show logging** command. It displays the syslog host configuration on a WAAS device.

```
WAE# show logging
Syslog to host is disabled
Priority for host logging is set to:  warning

Syslog to console is disabled
Priority for console logging is set to:  warning

Syslog to disk is enabled
Priority for disk logging is set to:  notice
Filename for disk logging is set to:  /local1/syslog.txt

Syslog facility is set to *

Syslog disk file recycle size is set to 1000000
```

Related Commands

clear arp-cache

(config) logging console

show sysfs volumes

show memory

To display memory blocks and statistics for a WAAS device, use the **show memory** EXEC command.

show memory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-52 describes the fields shown in the **show memory** command display.

Table 3-52 Field Descriptions for the show memory Command

Field	Description
Total memory	Total amount of system memory in kilobytes (KB), not including the amount reserved for the rescue kernel.
Total free memory	Total available memory (in kilobytes).
Total buffer memory	Total amount of memory (in kilobytes) in the memory buffer.
Total cached memory	Total amount of memory (in kilobytes) in the memory cache.
Total swap	Total amount of memory (in kilobytes) for swap purposes.
Total free swap	Total available memory (in kilobytes) for swap purposes.

show monitor

To show the status of traffic monitoring on an AppNav Controller Interface Module, use the **show monitor** EXEC command.

show monitor

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Examples

The following example shows how to display traffic monitoring status:

```
ANC# show monitor
AppNav Controller connection monitoring
enabled for specified ACL: myacl.
```

Related Commands

clear statistics monitor appnav-controller traffic

monitor appnav-controller traffic

show statistics monitor appnav-controller traffic

show ntp

To display the NTP parameters for a WAAS device, use the **show ntp** EXEC command.

show ntp status

Syntax Description

status	Displays the NTP status.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-53 describes the fields shown in the **show ntp status** command display.

Table 3-53 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 3-53 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 peer optimization

To display the configured serial peers for a WAAS device, use the **show peer optimization** EXEC command.

show peer optimization

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows how to display the device IDs of the configured nonoptimizing peer devices:

```
WAE# show peer optimization
Configured Non-optimizing Peers:
        Peer Device Id: 00:21:5e:28:87:54
```

Related Commands

show device-id

(config) peer

show policy-map

To display the policy map rules configured for an AppNav or optimization class map, use the **show policy-map** EXEC command.

show policy-map type {**appnav** | **waas**} [*policymap-name*]

Syntax Description

appnav	Displays the specified AppNav policy map, or all policy maps if no policy map is specified.
waas	Displays the specified WAAS optimization policy map, or all policy maps if no policy map is specified.
classmap-name	Policy map name.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command displays the policy rules for all policy maps or a specified policy map. It also displays the number of flows that have matched each class map and the total number of flows that have matched the policy. For nested policy maps, a match is counted for each policy map involved in the classification of a connection.

Examples

The following is sample output from the **show policy-map type appnav** command.

```
WAE# show policy-map type appnav
Policy-map type appnav appnav_default (245 total)
Class MAPI (25 flow-matches)
  distribute service-node-group mapi-group
Class HTTP (100 flow-matches)
  distribute service-node-group http-group
Class class-default (120 flow-matches)
  distribute service-node-group WNG-Default
  service-policy waas_app_default
```

Related Commands

(config) policy-map

show class-map

show policy-sub-class

show policy-sub-class

To display the matching criteria and flows for an AppNav class map, use the **show policy-sub-class** EXEC command.

show policy-sub-class type appnav [**all** | **level1-class** *classmap-name* [**level2-class** *classmap-name*]]

Syntax Description

appnav	Displays a summary of the class maps in the active AppNav policy map and any nested policy maps.
all	Displays detailed information for the class maps in the active AppNav policy map and any nested policy maps.
level1-class *classmap-name*	Displays detailed information for the specified class map in the top-level policy map.
level2-class *classmap-name*	Displays detailed information for the specified class map in a nested policy map.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

The **show policy-sub-class type appnav** command displays a list of all the class maps in the active AppNav policy map and any nested policy maps. It also displays the number of flows that have matched each class map, in all uses of the class map, including in all nested policy maps.

The **show policy-sub-class type appnav all** command displays a list of class maps and their matching criteria for all class maps in the active AppNav policy map and any nested policy maps. It also displays the number of flows that have matched each class map and condition, in all uses of the class map, including in all nested policy maps.

The **show policy-sub-class type appnav level1-class** *classmap-name* command displays the matching criteria for the specified class map in the top-level AppNav policy map, including matching criteria for all class maps in any nested policies. It also displays the number of flows that have matched each class map and condition, in all uses of the class map within the specified top-level class map.

The **show policy-sub-class type appnav level1-class** *classmap-name* **level2-class** *classmap-name* command displays the matching criteria for the specified class map in a nested AppNav policy map. It also displays the number of flows that have matched the class map and each condition, only within the nested policy map level for the specified top-level class map.

Examples

The following is sample output from the **show policy-sub-class type appnav all** command.

```
ANC# show policy-sub-class type appnav all
```

```
Service-insertion service-policy: appnav_default
   Class-map type appnav match-any class-default (8428593 flow-matches)
      Match tcp any (8428593 flow-matches)
   Service-policy : waas_app_default
   Class-map type appnav match-any MAPI (0 flow-matches)
      Match tcp destination epm mapi (0 flow-matches)
   Class-map type appnav match-any HTTPS (11898 flow-matches)
      Match tcp destination port 443 (11898 flow-matches)
   Class-map type appnav match-any HTTP (344769 flow-matches)
      Match tcp destination port 80 (344520 flow-matches)
      Match tcp destination port 3128 (58 flow-matches)
      Match tcp destination port 8000 (68 flow-matches)
      Match tcp destination port 8080 (68 flow-matches)
      Match tcp destination port 8088 (55 flow-matches)
   Class-map type appnav match-any CIFS (0 flow-matches)
      Match tcp destination port 139 (0 flow-matches)
      Match tcp destination port 445 (0 flow-matches)
   Class-map type appnav match-any Citrix-ICA (53 flow-matches)
      Match tcp destination port 1494 (53 flow-matches)
   Class-map type appnav match-any Citrix-CGP (57 flow-matches)
      Match tcp destination port 2598 (57 flow-matches)
   Class-map type appnav match-any epmap (0 flow-matches)
      Match tcp destination port 135 (0 flow-matches)
   Class-map type appnav match-any NFS (59 flow-matches)
      Match tcp destination port 2049 (59 flow-matches)
   Class-map type appnav match-any class-default (8071757 flow-matches)
      Match tcp (8071757 flow-matches)
```

The following sample output show statistics from a nested class map.

```
ANC# show policy-sub-class type appnav level1-class class-default level2-class NFS
Service-insertion service-policy: appnav_default
   Class-map type appnav match-any class-default
   Service-policy : waas_app_default
   Class-map type appnav match-any NFS (59 flow-matches)
      Match tcp destination port 2049 (59 flow-matches)
```

Related Commands

(config) policy-map

show class-map

show policy-map

show statistics policy-sub-class

show processes

To display CPU or memory processes for a WAAS device, use the **show processes** EXEC command.

show processes [**cpu** | **debug** *pid* | **memory** | **system** [**delay** *secs* | **count** *num*]]

Syntax Description

cpu	(Optional) Displays CPU utilization.
debug *pid*	(Optional) Prints the system call and signal traces for a specified process identifier to display system progress.
memory	(Optional) Displays memory allocation processes.
system	(Optional) Displays system load information in terms of updates.
delay *secs*	(Optional) Specifies the delay between updates, in seconds (1–60).
count *num*	(Optional) Specifies the number of updates that are displayed (1–100).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the EXEC commands shown in this section to track and analyze system CPU utilization. For real time CPU utilization information, use the top EXEC command.

The **show processes debug** command displays extensive internal system call information and a detailed account of each system call (along with arguments) made by each process and the signals it has received.

Use the **show processes system** command to display system load information in terms of updates. The **delay** option specifies the delay between updates, in seconds. The **count** option specifies the number of updates that are displayed. The **show processes debug** command displays these items:

- A list of all processes in wide format.
- Two tables listing the processes that utilize CPU resources. The first table displays the list of processes in descending order of utilization of CPU resources based on a snapshot taken after the processes system (ps) output is displayed. The second table displays the same processes based on a snapshot taken 5 seconds after the first snapshot.
- Virtual memory used by the corresponding processes in a series of five snapshots, each separated by 1 second.

Note CPU utilization and system performance are severely affected when you use these commands. We therefore recommend that you avoid using these commands, especially the **show processes debug** command, unless it is absolutely necessary.

Examples

Table 3-54 describes the fields shown in the **show processes** command display.

Table 3-54 Field Descriptions for the show processes Command

Field	Description
CPU utilization	CPU utilization since the last reload as a percentage for user, system overhead, and idle. Includes average usage (calculated every 10 minutes).
Overall current CPU utilization	Current CPU utilization over all CPUs in the system.
PID	Process identifier.
STATE	Current state of corresponding processes. R = running S = sleeping in an interruptible wait D = sleeping in an uninterruptible wait or swapping Z = zombie T = traced or stopped on a signal
PRI	Priority of processes.
User T	User time utilization in seconds.
Sys T	System time utilization in seconds.
COMMAND	Process command.
Total	Total available memory in bytes.
Used	Memory currently used in bytes.
Free	Free memory available in bytes.
Shared	Shared memory currently used in bytes.
Buffers	Buffer memory currently used in bytes.
Cached	Cache memory currently used in bytes.
SwapTotal	Total available memory in bytes for swap purposes.

Related Commands

top

show radius-server

To display RADIUS configuration information for a WAAS device, use the **show radius-server** EXEC command.

show radius-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-55 describes the fields shown in the **show radius-server** command display.

Table 3-55 Field Descriptions for the show radius-server Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether a RADIUS server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether a RADIUS server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Indicates whether the WAAS devices fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method.
RADIUS Configuration	RADIUS authentication settings.
Key	Key used to encrypt and authenticate all communication between the RADIUS client (the WAAS device) and the RADIUS server.
Timeout	Number of seconds that the WAAS device waits for a response from the specified RADIUS authentication server before declaring a timeout.
Servers	RADIUS servers that the WAAS device is to use for RADIUS authentication.
IP	Hostname or IP address of the RADIUS server.
Port	Port number on which the RADIUS server is listening.

Related Commands (config) radius-server

show reload

To display scheduled reload information, use the **show reload** EXEC command.

show reload

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Related Commands

reload

show running-config

To display a WAAS device current running configuration on the terminal, use the **show running-config** EXEC command. The **show running-config** command replaces the **write terminal** command.

show running-config [interface | no-policy | policy | snmp | virtual-blade | wccp]

Syntax Description

no-policy	(Optional) Does not display the policy engine configuration.
interface	(Optional) Displays interface configuration.
policy	(Optional) Displays policy engine configuration.
snmp	(Optional) Displays SNMP configuration.
virtual-blade	(Optional) Displays virtual-blade configuration on a WAAS device supporting a virtual-blade.
wccp	(Optional) Displays WCCP configuration.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Use this EXEC command in conjunction with the **show startup-config** command to compare the information in running memory to the startup configuration used during bootup.

Examples

The following is sample output from the **show running-config** command. It displays the currently running configuration of a WAAS device.

```
WAE# show running-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname waas-cm
!
!
!
!
!
exec-timeout 60
!
!
```

```
primary-interface GigabitEthernet 1/0
!
!
...
s
```

Related Commands

configure

copy running-config

copy startup-config

show service-insertion

To display information about the entities (WNs, WNGs, ANCs, ANCG, and a service context) defined in an AppNav Cluster configuration and the cluster status, use the **show service-insertion** EXEC command.

show service-insertion {**data-path mtu** | **pass-through offload** | **service-context** [**detail**] | **appnav-controller** *ip-address* | **appnav-controller-group** | **service-node** [*ip-address*] | **service-node-group** [*sngroupname*]}

Syntax Description

data-path mtu	Displays the MTU of the data path from this device to each of the other ANCs in the cluster.
pass-through offload	Displays the pass-through offload configuration.
service-context	Displays service context information. Available only on ANCs.
detail	Displays service context information and includes details about the ANCG, ANCs, and WNGs that are part of the service context.
appnav-controller *ip-address*	Displays information about the specified ANC. Available only on ANCs.
appnav-controller-group	Displays information about the ANCG. Available only on ANCs.
service-node [*ip-address*]	Displays information about the WN on this device or the specified device. If an IP address is specified, the information is the local device's view of the specified device.
service-node-group *sngroupname*	Displays information about the specified WNG. If the group name is not specified, it shows information about all WNGs. Available only on ANCs.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command returns minimal information if the entity or service context is disabled, or if the entity is not attached to the service context.

Examples

Table 3-56 describes the fields shown in the **show service-insertion service-context** command display.

Table 3-56 Field Descriptions for the show service-insertion service-context Command

Field	Description
Service Context	Service context name.
Service Policy	Name of the AppNav policy map that is attached to the service context.
Cluster protocol ICIMP version	Cluster ICIMP protocol version.
Cluster protocol DMP version	Cluster DMP protocol version.
Time service context was enabled	Time the service context was enabled.
Current FSM state	Current cluster finite state machine state: • Operational—Stable and operational. All ANCs in the cluster have converged on a stable view of the devices in the cluster. • Degraded—Partially stable state and operational. All ANCs cannot converge on a stable view of devices in the cluster but cluster can operate in pass-through mode. • Converging—Performing the convergence process due to a device change. Devices are exchanging information about each device's view of the cluster. • Admin Disabled—Configured but not enabled. • Initializing—Cluster is initializing. • Internal Error—Internal error condition due to convergence failing after 5 minutes.
Time FSM entered current state	Time the cluster finite state machine entered the current state.
Last FSM state	Last cluster finite state machine state. See the Current FSM State field for details.
Time FSM entered last state	Time the cluster finite state machine entered the last state.
Joining state	Current joining state: • Started—Device has started to join the cluster gracefully. • Completed—The graceful join operation completed successfully. • Aborted—Graceful join was started and then disabled before completing. • Not Configured—Device did not join the cluster gracefully. • Unknown—State is unknown (default).
Time joining state entered	Time the device entered the joining state.

Table 3-56 Field Descriptions for the show service-insertion service-context Command

Field	Description
Cluster operational state	Cluster operational state: • Operational—All ANCs are redirecting new flows to WNs. This is the overall cluster state if all ANCs have a FSM state of Operational or a cluster was Operational and a device is added. (This makes the FSM state go to Converging, but the operational state stays as Operational because the existing devices are handling new flows.) • Degraded—ANCs are not redirecting new flows to WNs but existing flows may be redirected to WNs. New flows are passed through. This is the overall cluster state if any ANCs have a FSM state other than Operational.
Interception Readiness State	Interception readiness state of this device: • Ready—Ready to intercept traffic. This state occurs two minutes after the cluster has reached stable convergence. (This state can exist even with a degraded cluster operational state because traffic is passed through in these cases.) • Not Ready—Not ready to intercept traffic (could be due to cluster convergence)
Device Interception State	Interception state of this device: • Shutdown—Device is not intercepting traffic. • Not Shutdown—Device is intercepting traffic. • Unknown—State is unknown (default).
Stable AC View	IP addresses of the ANCs in the stable view of this device. The stable view is the view of the devices after the convergence period in which all ANCs in the cluster have implicitly agreed on the view of all devices in the cluster.
Stable SN View	IP addresses of the WNs in the stable view of this device.
Current AC View	IP addresses of the ANCs in the current view of this device. The current view is the immediate view of the devices in the cluster. This could differ from the stable view if a device was newly added.
Current SN View	IP addresses of the WNs in the current view of this device.

Table 3-57 describes the additional fields shown in the **show service-insertion service-context detail** command display. The AppNav Controller Group and AppNav Controller sections of this table also describe the fields shown in the **show service-insertion appnav-controller-group** command display. The AppNav Controller section of this table also describes the fields shown in the **show service-insertion appnav-controller** command display.

The Service Node Group and Service Node sections of this table also describe the fields shown in the **show service-insertion service-node-group** command display. The Service Node section of this table also describes the fields shown in the **show service-insertion service-node** command display.

Table 3-57 Field Descriptions for the show service-insertion service-context detail Command

Field	Description
Service Context	Service context name.
Service Context configured state	State of service context (enabled or disabled). If disabled, some output fields are not shown.
AppNav Controller Group	ANCG name.
Member AppNav Controller count	Number of ANCs in the ANCG.
Members	IP addresses of the member ANCs in the ANCG.
Member (removed from config) AppNav Controller count	Number of ANCs that have been recently removed from the ANCG. These appear until the cluster converges on agreement that these are removed.
Members (removed from config)	IP addresses of the member ANCs recently removed from the ANCG.
An AppNav Controller section appears for each ANC in the cluster.	
AppNav Controller	IP address of the ANC. A (local) indication means that this is the device on which you are running this command.
AppNav Controller ID	Identifier for the ANC.
Current status of AppNav Controller	Current status of communication to this ANC: • Alive—This device can communicate with the ANC. • Alive (Removed from config)—This device was recently removed from the configuration but can still communicate with the ANC. • Dead—This device cannot communicate with the ANC. • Inactive—This device was added to a full cluster that had recently removed an ANC. Until the removal process completes or the removed ANC stops responding, this device cannot join the cluster and remains in Inactive state.
Time current status was reached	Time current status was reached.
Joining status of AppNav Controller	Current joining status of the ANC: • Joining—The ANC is in the process of joining the cluster defined on the local ANC. • Joined—The ANC has successfully joined the cluster defined on the local ANC.
Secondary IP address	IP address that the ANC is using as its source address when communicating with this ANC.
Cluster protocol ICIMP version	Cluster ICIMP protocol version running on this ANC.
Cluster protocol incarnation number	Internal information.

Table 3-57 Field Descriptions for the show service-insertion service-context detail Command

Field	Description
Cluster protocol last sent sequence number	Internal information.
Cluster protocol last received sequence number	Internal information.
Current AC View of AppNav Controller	IP addresses of the member ANCs in the ANCG, as viewed by this ANC.
Current SN View of AppNav Controller	IP addresses of the member WNs in the ANCG, as viewed by this ANC.
A Service Node Group section appears for each WNG in the cluster.	
Service Context	Service context name.
Service Context configured state	State of service context (enabled or disabled). If disabled, some output fields are not shown.
Service Node Group name	WNG name.
Service Node Group ID	Identifier for the WNG.
Member Service Node count	Number of WNs in the WNG.
Members	IP addresses of the member WNs in the WNG.
A Service Node section appears for each WN in the WNG.	
Service Node	IP address of the WN.
Service Node ID	Identifier for the WN.
Current status of Service Node	Current status of communication to this WN: • Alive—This device can communicate with the WN. • Dead—This device cannot communicate with the WN due to connectivity or not configured. • Excluded—This device can communicate with the WN, but another ANC cannot communicate with the WN. New flows are not redirected to this WN by any ANC, but existing flows could still be redirected if the device had previously been Alive and receiving flows.
Time current status was reached	Time current status was reached.
Secondary IP address	IP address that the WN is using as its source address when communicating with this ANC.
Cluster protocol DMP version	Cluster ICIMP protocol version running on this WN.
Cluster protocol incarnation number	Internal information.
Cluster protocol last sent sequence number	Internal information.

Table 3-57 Field Descriptions for the show service-insertion service-context detail Command

Field	Description
Cluster protocol last received sequence number	Internal information.
Accelerator State (appears for each WN in the WNG)	
Accl	Application accelerator name.
State	Application accelerator state: • GREEN—Operating normally and accepting new flows. • YELLOW—Servicing existing flows but not accepting new flows due to overload, license removed, or policy engine timeout. • RED—Not running due to not configured, not licensed, or unresponsive.
For	Amount of time the application accelerator has been in this state.
SNG Availability per Accelerator (for the whole WNG)	
Accl	Application accelerator name.
Available	Availability status: • Yes—In GREEN state on at least one WN in the WNG. • No—In YELLOW or RED state on all WNs in the WNG.
Since	Amount of time the application accelerator has been available.

Related Commands

(config) service-insertion

show statistics service-insertion

show service-policy

To display information about the optimization or AppNav policies, use the **show service-policy** EXEC command.

show service-policy type {**appnav** {**dynamic** [**detail** | **server-ip** *ip_address* | **server-port** *port*]| **epm** | **status**} |
waas {**application-name** | **dynamic** [**app-id** {*app-id* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**}| **detail** | **dm-index** *index* | **server-ip** *ip_address* | **server-port** *port*]| **epm** | **status**}}

Syntax Description

appnav	Displays AppNav policy information.
dynamic	Displays policy information for dynamic matched flows.
detail	(Optional) Displays detailed policy information for dynamic matched flows.
server-ip *ip_address*	(Optional) Displays the policy information for dynamic matched flows for the server with the specified IP address.
server-port *port*	(Optional) Displays the policy information for dynamic matched flows for the server with the specified port number (1–65535).
epm	Displays policy information for EPM flows
status	Displays how many policy resources are in use and available.
waas	Displays WAAS optimization policy information.
application-name	Displays the configured application names on the device.
app-id *app-id*	Displays the policy information for dynamic matched flows for the application with the specified application number (0-1023) or the specified traffic type.
mapi	Microsoft Exchange MAPI aka Exchange Server Store EMSMDB,
ms-ad-rep	Microsoft Active Directory Replication (drsuapi),
ms-exch-nspi	Microsoft Active Directory Name Service Provider (NSP),
ms-frs	Microsoft File Replication Services (FRS),
ms-frs-api	Microsoft File Replication API,
ms-rfr	Microsoft Exchange Directory RFR Interface,
ms-sql	Microsoft SQL,
msn-messenger	Microsoft Messenger Service,
netlogon	Netlogon RPC
dm-index *index*	Displays the policy information for dynamic matched flows for the application with the specified DM index.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

Table 3-58 describes the fields shown in the **show service-policy type appnav status** command display.

Table 3-58 Field Descriptions for the show service-policy type appnav status Command

Field	Description
Policy Maps	Number of total allowed, used, and available AppNav policy maps.
Class Maps	Number of total allowed, used, and available AppNav class maps.
Matches	Number of total allowed, used, and available AppNav match conditions.
TCAM Entries in use	Number of TCAM entries in use.
TCAM Entries available	Number of TCAM entries available.

Table 3-59 describes the fields shown in the **show service-policy type waas status** command display.

Table 3-59 Field Descriptions for the show service-policy type waas status Command

Field	Description
Application names	Number of total allowed, used, and available WAAS application names.
Class Maps	Number of total allowed, used, and available WAAS class maps.
Matches	Number of total allowed, used, and available WAAS match conditions.
Optimization policy map	Name of optimization policy map in use.

Table 3-60 describes the fields shown in the **show service-policy type appnav epm** command display.

Table 3-60 Field Descriptions for the show service-policy type appnav epm Command

Field	Description
Keyword	An EPM-related application name.
App-Id	Application ID.
Ref Count	Number of times this application is referenced in the policy map.
Hits	Number of hits on this application since the device started up.

The following is sample output from the **show service-policy type appnav epm** command:

```
ANC# show service-policy type appnav epm
        Keyword          App-Id      Ref Count           Hits
---------------   ------------   ------------   ------------
           mapi              78              1              0
```

Table 3-61 describes the fields shown in the **show service-policy type waas application-name** command display.

Table 3-61 Field Descriptions for the show service-policy type waas application-name Command

Field	Description
Number of application names	Number of defined WAAS application names.
#	Number of a defined application.
Application Name	Name of a defined application.
Occurrences	Number of occurrences of the application in the policy map.

Table 3-62 describes the fields shown in the **show service-policy type waas epm** command display.

Table 3-62 Field Descriptions for the show service-policy type waas epm Command

Field	Description
Keyword	An EPM-related application name.
App-Id	Application ID.
UUID	UUID associated with this traffic type.
Ref Count	Number of times this application is referenced in the policy map.
Hits	Number of hits on this application since the device started up.
SC Add Count	Number of ???.

The following is sample output from the **show service-policy type waas epm** command:

```
ANC# show service-policy type waas epm
Keyword             App-Id    UUID
----------------    --------  ----------------------------------------
mapi                78        a4f1db00ca471067b31f00dd010662da
     Ref Count:           1  Hits:           0  SC Add Count =           0

ms-ad-rep           1252      e35142354b0611d1ab0400c04fc2dcd2
     Ref Count:           1  Hits:           0  SC Add Count =           0

ms-exch-nspi        1249      f5cc5a184264101a8c5908002b2f8426
     Ref Count:           1  Hits:           0  SC Add Count =           0

ms-rfr              1253      1544f5e0613c11d193df00c04fd7bd09
     Ref Count:           1  Hits:           0  SC Add Count =           0

ms-frs              1250      f5cc59b44264101a8c5908002b2f8426
     Ref Count:           1  Hits:           0  SC Add Count =           0

ms-sql              4098      3f99b9004d87101b99b7aa0004007f07
     Ref Count:           1  Hits:           0  SC Add Count =           0
```

Related Commands **(config) service-insertion**

show services

To display services-related information for a WAAS device, use the **show services** EXEC command.

show services {**ports** [*port-num*] | **summary**}

Syntax Description

ports	Displays services by port number.
port-num	(Optional) Up to 8 port numbers (1–65535).
summary	Displays the services summary.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following is sample output from the **show services** command. It displays a summary of the services.

```
WAE# show services summary

Service        Ports
-----------------------------------------------------
                CMS          1100  5256
                NLM          4045
               WAFS          1099
               emdb          5432
              MOUNT          3058
         MgmtAgent           5252
       WAFS_tunnel           4050
     CMS_db_vacuum           5257
```

show smb-conf

To view the current values of the Samba configuration file, *smb.conf*, on a WAAS device, use the **show smb-conf** EXEC command.

show smb-conf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show smb-conf** command displays the global, print$, and printers parameters values of the *smb.conf* file for troubleshooting purposes. For a description of these parameters and their values, see the **(config) smb-conf** command.

Examples

The following is sample output from the **show smb-conf** command. It displays all of the parameter values for the current configuration.

```
WAE# show smb-conf

Current smb-conf configurations -->

smb-conf section "global" name "ldap ssl" value "start_tls"
smb-conf section "printers" name "printer admin" value "root"

Output of current smb.conf file on disk -->


================================================

# File automatically generated


[global]
idmap uid = 70000-200000
idmap gid = 70000-200000
winbind enum users = no
winbind enum groups = no
winbind cache time = 10
winbind use default domain = yes
printcap name = cups
load printers = yes
printing = cups
```

```
cups options = "raw"
force printername = yes
lpq cache time = 0
log file = /local/local1/errorlog/samba.log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
smb ports = 50139
local master = no
domain master = no
preferred master = no
dns proxy = no
template homedir = /local/local1/
template shell = /admin-shell
ldap ssl = start_tls
comment = Comment:
netbios name = MYFILEENGINE
realm = ABC
wins server = 10.10.10.1
password server = 10.10.10.10
security = domain

[print$]
path = /state/samba/printers
guest ok = yes
browseable = yes
read only = yes
write list = root


[printers]
path = /local/local1/spool/samba
browseable = no
guest ok = yes
writable = no
printable = yes
printer admin = root

===============================================
```

Related Commands

(config) smb-conf

windows-domain

(config) windows-domain

show snmp

To check the status of SNMP communications for a WAAS device, use the **show snmp** EXEC command.

show snmp {**alarm-history** | **engineID** | **event** | **group** | **stats** | **user**}

Syntax Description

alarm-history	Displays SNMP alarm history information.
engineID	Displays local SNMP engine identifier.
event	Displays events configured through the Event MIB. This keyword applies only to application-accelerator device mode.
group	Displays SNMP groups.
stats	Displays SNMP statistics.
user	Displays SNMP users.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show snmp alarm-history** command provides information on various SNMP variables and statistics on SNMP operations.

Examples

Table 3-63 describes the fields shown in the **show snmp alarm-history** command display.

Table 3-63 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 3-64 summarizes the mapping of module names to module IDs.

Table 3-64 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 3-65 summarizes the mapping of category names to category IDs.

Table 3-65 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 3-66 describes the fields shown in the **show snmp engineID** command display.

Table 3-66 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 3-67 describes the fields shown in the **show snmp event** command display. The **show snmp event** command displays information about the SNMP events that were set using the **snmp trigger** command:

Table 3-67 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 3-67 Field Descriptions for the show snmp event Command (continued)

Field	Description
(1):	Name for the trigger. This name is locally-unique and administratively assigned. For example, this field might contain the "isValid" trigger name. Numbering indicates that this is the first management trigger listed in the **show** output.
Comment:	Description of the trigger function and use. For example: License is not valid.
Sample:	Basis on which the test sample is being evaluated. For example: Abs (Absolute) or Delta.
Freq:	Frequency. Number of seconds to wait between trigger samplings. To encourage consistency in sampling, the interval is measured from the beginning of one check to the beginning of the next and the timer is restarted immediately when it expires, not when the check completes.
Test:	Type of trigger test to perform based on the SNMP trigger configured. The Test field may contain the following types of tests: Absent—Absent existence of a test Boolean—Boolean value test Equal—Equality threshold test Falling—Falling threshold test Greater-than—Greater-than threshold test Less-than—Less-than threshold test On-change—Changed existence test Present—Present present test Rising—Rising threshold test
Wildcard	True or False.
ObjectOwner:	Name of the object owner who created the trigger using the **snmp trigger create** global configuration command or by using an SNMP interface. "CLI" is the default owner.
Object:	String identifying the object.
Boolean Entry:	
Value:	Object identifier of the MIB object to sample to see whether the trigger should fire.

Table 3-67 Field Descriptions for the show snmp event Command (continued)

Field	Description
Cmp:	Comparison. Type of boolean comparison to perform. The numbers 1–6 correspond to these Boolean comparisons: unequal (1) equal (2) less (3) lessOrEqual (4) greater (5) greaterOrEqual (6)
Start:	Starting value for which this instance will be triggered.
ObjOwn:	Object owner.
Obj:	Object.
EveOwn:	Event owner.
Eve:	Event. Type of SNMP event. For example: CLI_EVENT.
Delta Value Table:	Table containing trigger information for delta sampling.
(0):	
Thresh:	Threshold value to check against if the trigger type is threshold.
Exis:	Type of existence test to perform. Values are 1 or 0.
Read:	Indicates whether the MIB instance has been queried or not.
OID:	Object ID (Same as MIB instance).
val:	Value ID.
(2):	MIB instance on which the trigger is configured. This is the second management trigger listed in the **show** output. The fields are repeated for each instance listed in this **show** command.

Table 3-68 describes the fields shown in the **show snmp group** command display.

Table 3-68 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 3-69 describes the fields shown in the **show snmp stats** command display.

Table 3-69 Field Descriptions for the show snmp stats Command

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Table 3-70 describes the fields shown in the **show snmp user** command display.

Table 3-70 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 3-71 describes the fields shown in the **show ssh** command display.

Table 3-71 Field Descriptions for the show ssh Command

Field	Description
SSH server supports the SSH version 2 protocol only.	Protocol support statement.
SSH service is not enabled.	Status of whether the SSH service is enabled or not enabled.
Currently there are no active SSH sessions.	Number of active SSH sessions.
Number of successful SSH sessions since last reboot:	Number of successful SSH sessions since last reboot.
Number of failed SSH sessions since last reboot:	Number of failed SSH sessions since last reboot.
SSH key has not been generated or previous key has been removed.	Status of the SSH key.
SSH login grace time value is 300 seconds.	Time allowed for login.
Allow 3 password guess(es).	Number of password guesses allowed.

Related Commands

(config) ssh-key-generate

(config) sshd

show startup-config

To display the startup configuration for a WAAS device, use the **show startup-config** EXEC command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use this EXEC command to display the configuration used during an initial bootup, stored in NVRAM. Note the difference between the output of this command versus the **show running-config** command.

Examples

The following is sample output from the **show startup-config** command. It displays the configuration saved for use on startup of the WAAS device.

```
WAE# show startup-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname Edge-WAE1
!
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 ip address 10.10.10.33 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
...
```

Related Commands

configure

copy running-config

show running-config

show statistics accelerator

To display application accelerator general statistics for a WAAS device, use the **show statistics accelerator** EXEC command.

show statistics accelerator cifs [**detail** | **expert** *mbean attrib*]

show statistics accelerator detail

show statistics accelerator epm [**detail**]

show statistics accelerator generic {**connections** {**cifs** | **epm** | **http** | **ica** | **mapi** | **nfs** | **smb** | **ssl** | **video**}| **detail**}

show statistics accelerator http [**debug** | **detail** | **https**]

show statistics accelerator ica [**detail**]

show statistics accelerator mapi [**detail**]

show statistics accelerator nfs [**detail**]

show statistics accelerator smb [**debug** | **detail** | **inc Print** | **request**]

show statistics accelerator ssl [**detail** | **payload** {**http** | **other**}]

show statistics accelerator video [**detail**]

show statistics accelerator wansecure [**detail**]

Syntax Description

cifs	Displays statistics for the CIFS application accelerator.
detail	(Optional) Displays detailed statistics.
expert *mbean attrib*	(Optional) Displays CIFS accelerator expert mode attributes. Mbean name and Mbean attribute name.
epm	Displays statistics for the EPM application accelerator.
generic	Displays statistics for the generic application accelerator.
connections	Displays generic connection statistics.
http	Displays statistics for the HTTP application accelerator.
ica	Displays statistics for the ICA application accelerator.
mapi	Displays statistics for the MAPI application accelerator.
nfs	Displays statistics for the NFS application accelerator.
smb	Displays statistics for the SMB application accelerator.
request	Displays SMB application accelerator statistics on requests.
ssl	Displays statistics for the SSL application accelerator.
video	Displays statistics for the video application accelerator.
wansecure	Displays statistics for the WAN secure application accelerator.
debug	(Optional) Displays debug statistics.
https	Displays statistics for the HTTPS application accelerator.

payload	(Optional) Displays the SSL payload type.
other	Displays the unidentified protocol flows within SSL.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Using the **show statistics accelerator** command with no options displays a summary of the statistical information for all application accelerators. To obtain detailed statistics for an application accelerator, use the command options to filter the results.

Examples

Table 3-72 describes the fields shown in the **show statistics accelerator cifs** command display.

Table 3-72 Field Descriptions for the show statistics accelerator cifs detail Command

Field	Description
Time Accelerator was started	Time that the accelerator was started.
Time Statistics were Last Reset/Cleared	Time that the statistics were last reset or cleared.
Total Handled Connections	Connections handled since the accelerator was started or its statistics last reset.
Total Optimized Connections	Connections previously and currently optimized by the accelerator.
Total Pushed Down Connections	Connections initially accepted by accelerator, but later handed off to generic optimization with no acceleration. Occurs if the CIFS server requires a digital signature.
Total Dropped Connections	Connections dropped for reasons other than client/server socket errors or close.
Current Active Connections	Current active connections.
Current Pending Connections	Current connections pending to be accepted.
Maximum Active Connections	Maximum active connections handled simultaneously.
Local response number	Number of local CIFS command responses sent to the client without waiting for a response from the peer WAE.
Average local response time	Average time used for local responses, in microseconds.
Remote response number	Number of CIFS commands forwarded to the CIFS server for a response.

Table 3-72 Field Descriptions for the show statistics accelerator cifs detail Command (continued)

Field	Description
Average remote response time	Average time used for remote responses, in microseconds.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during auto-discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing auto-discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.

Table 3-72 Field Descriptions for the show statistics accelerator cifs detail Command (continued)

Field	Description
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to the accelerator not being present, or a queue overflow.
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include the accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Table 3-73 describes the fields shown in the **show statistics accelerator epm detail** command display.

Table 3-73 Field Descriptions for the show statistics accelerator epm Command

Field	Description
Global TCP AO connection statistics	
Time Accelerator was started	Time that the accelerator was started.

Table 3-73 Field Descriptions for the show statistics accelerator epm Command (continued)

Field	Description
Time Statistics were Last Reset/Cleared	Time that the statistics were last reset or cleared.
Total Handled Connections	Total connections handled.
Total Optimized Connections	Total optimized connections.
Total Pushed Down Connections	Total pushed down connections.
Total Dropped Connections	Total dropped connections.
Current Active Connections	Current active connections.
Current Pending Connections	Current pending connections.
Maximum Active Connections	Maximum active connections.
Total Requests	Total requests.
Total Requests Successfully Parsed	Total requests successfully parsed.
Total Request Errors	Total request errors.
Total Responses	Total responses.
Total Responses Successfully Parsed	Total responses successfully parsed.
Total Service-unavailable Responses	Total service-unavailable responses.
Total Requests for UUID not in Policy Engine Map	Total requests for UUID not in policy engine map.
Total Response Errors	Total response errors.

Table 3-74 describes the fields shown in the **show statistics accelerator generic connections detail** command display. This command shows the aggregated statistics for all connections.

Table 3-74 Field Descriptions for the show statistics accelerator generic Command

Field	Description
Time elapsed since "clear statistics"	Time that has elapsed since the statistics were last reset.
Time Accelerator was started	Local time accelerator was started or restarted.
Time Statistics were Last Reset/Cleared	Local time accelerator was last started or restarted, or the **clear statistics** command was executed since accelerator was last started or restarted.
Total Handled Connections	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented. This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.

Table 3-74 Field Descriptions for the show statistics accelerator generic Command (continued)

Field	Description
Total Optimized Connections	Connections previously and currently optimized by the accelerator. This includes: Current Active Connections + Total Fast Connections + Fast connections initiated by peer.
Total Connections Handed-off with Compression Policies Unchanged	Connections initially accepted by accelerator, but later handed off to generic optimization without policy changes so the current negotiated policies for compression (DRE/LZ) will be used.
Total Dropped Connections	Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources).
Current Active Connections	Number of WAN side connections currently established and either in use or free for fast connection use. WAN side connections currently established and in use can be calculated as follows: Current Active Connections - Total Active Connections Free For Fast Connection Use Not cleared using **clear statistics accelerator** command.
Current Pending Connections	Number of SYN requests queued waiting for the accelerator to accept.
Maximum Active Connections	Highest number of active connections since accelerator was last started/restarted. Not cleared using the **clear statistics accelerator** command.
Global Generic AO Connection Statistics	
Total number of connections handled	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented. This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total number of active connections	Total number of hits that represent either active connections using the accelerator application.
Total number of bytes transferred from client	Total number of bytes transferred from the client side.
Total number of bytes transferred from server	Total number of bytes transferred from the server side.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.

Table 3-74 Field Descriptions for the show statistics accelerator generic Command (continued)

Field	Description
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.

Table 3-74 Field Descriptions for the show statistics accelerator generic Command (continued)

Field	Description
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched

Table 3-75 describes the fields shown in the **show statistics accelerator http detail** command display.

Table 3-75 Field Descriptions—show statistics accelerator http detail Command

Field	Description
Time Accelerator was started	Local time accelerator was started or restarted.
Time Statistics were Last Reset/Cleared	Local time accelerator was last started or restarted, or the **clear statistics accelerator [http | all]** command was executed since accelerator was last started or restarted.

Table 3-75 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total Handled Connections	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented. This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total Optimized Connections	Connections previously and currently optimized by the HTTP Accelerator. This includes: Current Active Connections + Total Fast Connections + Fast connections initiated by peer.
Total Connections Handed-off with Compression Policies Unchanged	Connections initially accepted by accelerator, but later handed off to generic optimization without policy changes so the current negotiated policies for compression (DRE/LZ) will be used.
Total Dropped Connections	Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources).
Current Active Connections.	Number of WAN side connections currently established and either in use or free for fast connection use. WAN side connections currently established and in use can be calculated as follows: Current Active Connections - Total Active Connections Free For Fast Connection Use Not cleared using **clear statistics accelerator [http | all]** command.
Current Pending Connections	Number of SYN requests queued waiting for for accelerator to accept.
Maximum Active Connections	Highest number of active connections since accelerator was last started/restarted. Not cleared using the **clear statistics accelerator [http | all]** command.
Total Time Saved (ms)	Total time saved in milliseconds. Incremented on client side WAE by 1 RTT whenever an idle fast connection is reused instead of establishing a new WAN connection.
Current Active Connections Free for Fast Connection Use	Number of Current Active Connections that are idle and available for reuse as a fast connection. Incremented when an in-use active connection becomes idle and is available for reuse as a fast connection. Decremented when an available idle active connection is reused or its idle timeout (5 secs) is reached. Not cleared using the **clear statistics accelerator [http | all]** command.

Table 3-75 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total Connections Handed-off	Total Pushed Down Connections + Total Connections Handed-off with Compression Policies Disabled.
Total Connections Handed-off with Compression Policies Disabled	Total number of connections handed off to generic optimization with compression policies disabled. This statistic includes handoffs for SSL CONNECT requests received by the HTTP Accelerator.
Total Connections Handed-off to SSL	Total number of connections handed off to the SSL accelerator as a result of SSL CONNECT requests received by the HTTP Accelerator.
Total Connection Hand-off Failures	Total number of connections that were attempted to be handed off but the hand off failed.
Total Fast Connection Successes	Total number of times a client side idle active WAN connection was able to be reused instead of establishing a new WAN connection.
Total Fast Connection Failures	Total number of times a client side idle active WAN connection was attempted to be reused, but the reuse failed.
Maximum Fast Connections on a Single Connection	Maximum number of times a single connection was reused. This is the “best case” of number of reuses on a single connection. Limited to be less than maximum session reuse count (currently defined as 100 - an arbitrary max).
Total CONNECT Requests with Incomplete Message	Total number of SSL CONNECT requests with an incomplete message.
Percentage of connection time saved	(Total Time Saved / (Total Time Saved + Total Round Trip Time For All Connections)) * 100.
Total Round Trip Time for All Connections (ms)	Total RTT for all WAN connections that have been established.
Total Fast Connections Initiated by Peer	Total number of times the server side WAN connection was a fast connection initiated by the client side peer. This statistic should match the Total Fast Connections on the peer WAE.
Total SYN Timeouts	Total number of SYN timeouts because the HTTP accelerator was temporarily busy.
Total Time for Metadata Cache Miss (ms)	Total time for metadata cache misses, in milleseconds.
RTT saved by Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving redirect (301) responses, in milliseconds.
RTT saved by Authorization Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving authentication required (401) responses, in milliseconds.
RTT saved by Content Refresh Check Metadata Cache (ms)	Round trip time saved by caching and locally serving conditional (304) responses, in milliseconds.
Total Time Saved by Fast Connection Use (ms)	Total time saved by fast connection reuse, in milliseconds.

Table 3-75 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total Locally Served Redirect Responses	Number of locally served redirect (301) responses.
Total Locally Served Unauthorized Responses	Number of locally served authentication required (401) responses.
Total Locally Served Conditional Responses	Number of locally served conditional (304) responses.
Total Remotely Served Redirect Responses	Number of remotely served redirect (301) responses (cache misses).
Total Remotely Served Unauthorized Responses	Number of remotely served authentication required (401) responses (cache misses).
Total Remotely Served Conditional Responses	Number of remotely served conditional (304) responses (cache misses).
Total Requests with URL Longer than 255 Characters	Number of requests not cached because the URL is longer than 255 characters.
Total Requests with HTTP Pipelining	Number of requests not cached due to HTTP pipelining.
Total Transactions Handled	Number of HTTP transactions handled.
Total Server Compression Suppression	Number of times server compression was suppressed.
Total Requests Requiring Server Content-Revalidation	Number of requests that required content to be revalidated with the origin server, as specified by a Cache-Control header.
Total Responses not to be Cached	Number of 200, 301, 304, and 401 responses not to be cached, as specified by a Cache-Control header.
Total Connections Expecting Authentication	Number of connections expecting authentication.
Total Connections with Unsupported HTTP Requests	Number of connections with unsupported HTTP requests.
Total Connections with Unsupported HTTP Responses	Number of connections with unsupported HTTP responses.
Total Hints Sent to DRE Layer to Flush Data	Number of DRE hints to flush data.
Total Hints Sent to DRE Layer to Skip LZ	Number of DRE hints to skip LZ compression.
Total Hints Sent to DRE Layer to Skip Header Information	Number of DRE hints to skip header information.
Total ACL Lookups for Subnet feature	Total number of system calls made for ACL lookup.
Total Sessions using Global enable/disable settings	Total number of sessions using global configuration for all four HTTP AO optimization features.
Total Sessions using ACL-selected settings	Total number of sessions using subnet configuration for at least one HTTP AO optimization feature.
Total sessions using SharePoint optimization	Number of sessions using SharePoint optimization feature to access objects from SharePoint server.
Total sessions using SharePoint pre-fetch optimization	Number of sessions where pre-fetch optimization for SharePoint objects ((MS Office applications) is enabled.

Table 3-75 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total SharePoint objects prefetched	Number of SharePoint objects that have been prefetched due to client requests.
Total locally served SharePoint prefetch objects	Number of SharePoint objects that have been prefetched and have been displayed on the client.
Total RTT saved by SharePoint optimization (ms)	Total response time (in milliseconds) saved in accessing SharePoint objects by enabling SharePoint optimization.
Total RTT saved by SharePoint prefetch cache hit (ms)	Total response time (in milliseconds) saved in accessing SharePoint data that has already been prefetched and stored in the cache.
Total remotely served SharePoint prefetch objects	Number of SharePoint objects that have been prefetched and displayed remotely.
Total time for SharePoint cache miss (ms)	Total time (in milliseconds) lost in accessing SharePoint data that is not already stored in the cache.
Total time for SharePoint prefetch cache miss (ms)	Total time (in milliseconds) lost in finding prefetched data that was not stored in cache.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.

Table 3-75 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Table 3-76 describes the fields shown in the **show statistics accelerator http debug** command display.

Table 3-76 Field Descriptions—show statistics accelerator http debug Command

Field	Description
Total HTTP Parser Errors	Number of times that various HTTP parser errors occurred.
Total HTTP Transactions	HTTP transaction statistics.
Total Memory Allocation Errors	Number of times that various memory allocation errors occurred.
Total HTTP Requests	Number of various HTTP requests received.
Total HTTP Responses	Number of various HTTP responses.
Total HTTP Requests Processing Errors	Number of various HTTP request processing errors.
Total HTTP Responses Processing Errors	Number of various HTTP response processing errors.
Total HTTP 1-0 Requests	Total HTTP 1.0 requests.
Total HTTP 1-1 Requests	Total HTTP 1.1 requests.
Total HTTP 1-0 Responses	Total HTTP 1.0 responses.
Total HTTP 1-1 Responses	Total HTTP 1.1 responses.
Total 301 Cached Responses	Total 301 cached responses.
Total 301 Non-Cached due to Long HTTP Header	Number of 301 responses not cached due to a long HTTP header.
Total 301 Non-Cached due to Unsupported HTTP Header	Number of 301 responses not cached due to an unsupported HTTP header.
Total 301 Non-Cached due to Cache Control Directives	Number of 301 responses not cached due to cache control directives.
Total 301 Non-Cached due to Authentication Flag Being Set	Number of 301 responses not cached due to the authentication flag being set.
Total 301 Non-Cached due to Metadata Cache Thrashing Limit	Number of 301 responses not cached due to metadata cache thrashing limit.
Total 301 Non-Cached due to a long URL	Number of 301 responses not cached due to a long URL. The URL length includes the length of the destination IP address.
Total 301 Non-Cached due to a Webdav Method	Number of 301 responses not cached due to a webdav method.
Total 401 Cached Responses	Total 401 cached responses.
Total 401 Non-Cached due to Long HTTP Header	Number of 401 responses not cached due to a long HTTP header.
Total 401 Non-Cached due to Unsupported HTTP Header	Number of 401 responses not cached due to an unsupported HTTP header.
Total 401 Non-Cached due to Cache Control Directives	Number of 401 responses not cached due to cache control directives.
Total 401 with Unsupported Authentication Mechanism	Number of 401 responses with unsupported authentication mechanisms.

Table 3-76 Field Descriptions—show statistics accelerator http debug Command (continued)

Field	Description
Total 401 Non-Cached due to Metadata Cache Thrashing Limit	Number of 401 responses not cached due to metadata cache thrashing limit.
Total Type-2 401 responses	Number of 401 responses that use type 2 NTLM authentication.
Total 401 Non-Cached due to a long URL	Number of 401 responses not cached due to a long URL.
Total 401 Non-Cached due to a Webdav Method	Number of 401 responses not cached due to a webdav method.
Total HTTP Requests With Cache Control Checks	Total HTTP requests with cache control checks.
Total HTTP Responses With Cache Control Checks	Total HTTP responses with cache control checks.
Total Conditional Requests with max-age header	Total conditional requests with max-age header.
Total Conditional Requests with 'If-Range' Header	Total conditional requests with If-Range header.
Total Conditional Requests with If-None-Match header	Total conditional requests with If-None-Match header.
Total Conditional Requests With If-None-Match value >63 chars	Total conditional requests with If-None-Match value longer than 63 characters.
Total Conditional Requests with If-Modified-Since header	Total conditional requests with If-Modified-Since header.
Total Conditional Requests with invalid If-Modified-Since header	Total conditional requests with invalid If-Modified-Since header.
Total Conditional Requests with Connection: Keep-alive header	Total conditional requests with Connection: Keep-alive header.
Total Conditional Requests with Connection: Close header	Total conditional requests with Connection: Close header.
Total Conditional Requests with an HTTP Parser Error	Total conditional requests with an HTTP parser error.
Total Conditional Requests Cache Lookup Failure	Total conditional requests with a cache lookup failure.
Total Conditional Requests not Matching Etag/LM values in cache	Total conditional requests with nonmatching Etag or Last Modified values in the cache (such requests are not served from the cache).
Total Memory Allocation Errors in Conditional Request Process	Total memory allocation errors in conditional request processing.
Total Cache Pointer Errors in Conditional Request Process	Total cache pointer errors in conditional request processing.
Total 200/304 Cached Responses	Total 200/304 cached responses.
Total 200/304 Non-Cached due to Metadata Cache Thrashing Limit	Total 200/304 noncached responses due to metadata cache thrashing limit.

Table 3-76 Field Descriptions—show statistics accelerator http debug Command (continued)

Field	Description
Total 200/304 Non-Cached due to Vary Header	Total 200/304 noncached responses due to having a Vary header.
Total 200 Responses with no Etag/LM	Total 200 responses with no Etag or Last Modified header (such responses are not cached).
Total 200/304 Responses with max-age header	Total 200/304 responses with max-age header.
Total 200/304 Responses with s-maxage header	Total 200/304 responses with s-maxage header.
Total 200/304 Responses with Expires header	Total 200/304 responses with Expires header.
Total 200/304 Responses with Invalid Expires header	Total 200/304 responses with invalid Expires header.
Total 200/304 Responses with Etag header	Total 200/304 responses with Etag header.
Total 200/304 Responses with Too Long Etag value (> 64 chars)	Total 200/304 responses with Etag value that is longer than 64 characters.
Total 200/304 Responses with Last-Modified header	Total 200/304 responses with Last-Modified header.
Total 200/304 Responses with invalid Last-Modified header	Total 200/304 responses with invalid Last-Modified header.
Total 200/304 Responses with Content-Type header	Total 200/304 responses with Content-Type header.
Total 200/304 Responses with Server Header	Total 200/304 responses with Server header.
Total 200/304 Responses too long Server Header (>99 chars)	Total 200/304 responses with Server header that is longer than 99 characters.
Total 200/304 Responses with Content-Location Header	Total 200/304 responses with Content-Location header.
Total 200/304 Responses too long Content-Location (>99 chars)	Total 200/304 responses with Content-Location header that is longer than 99 characters.
Total 304 Response Not Cached Because of Filter-Extension	Total 304 responses not cached because of Filter-Extension.
Total 304 Responses with an HTTP Parser Error	Total 304 responses with an HTTP parser error.
Total 304 Memory Allocation Errors in 304 Response Process	Total 304 memory allocation errors in 304 response processing.
Total 304 Cache Pointer Errors in 304 Response Process	Total 304 cache pointer errors in 304 response processing.
Total 200 OK with object size less than 1 KB	Total 200 OK responses with object size less than 1 KB.
Total 200 OK with object size less than 5 KB	Total 200 OK responses with object size less than 5 KB.

Table 3-76 Field Descriptions—show statistics accelerator http debug Command (continued)

Field	Description
Total 200 OK with object size less than 8 KB	Total 200 OK responses with object size less than 8 KB.
Total 200 OK with object size more than 8 KB	Total 200 OK responses with object size more than 8 KB.
Total Connections Bypassed due to URL Based Bypass List	Total connections bypassed due to URL-based bypass list.
Total Connections Bypassed due to IP Based Bypass List	Total connections bypassed due to IP-based bypass list.
Total Connections Not Been Reused due to Unread WAN Data	Total connections not reused due to unread WAN data.
Total Connections with first message initiated from server	Total connections with first message initiated from server.

Table 3-77 describes the fields shown in the **show statistics accelerator http https** command display.

Table 3-77 Field Descriptions—show statistics accelerator http https Command

Field	Description
Total Optimized HTTPS Connections	HTTPS connections previously and currently optimized by the HTTP Accelerator.
Total Handled HTTPS Connections	HTTPS connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted. Never decremented. This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator. Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total Active HTTPS Connections	Number of HTTPS connections currently being handled and optimized by both SSL and HTTP optimization.
Total Proxy-Connect HTTPS Connections	Total number of HTTPS connection started as HTTP and upgraded to HTTPS. For such connections both SSL and HTTP optimizations are applied.
Total Proxy-Connect HTTPS Insert Failures	Number of HTTPS connections started as HTTP for which the SSL optimization upgrade failed.
RTT saved by HTTPS Content Refresh Check Metadata Cache (ms)	Round trip time saved by caching and locally serving conditional (304) responses, in milliseconds.
RTT saved by HTTPS Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving redirect (301) responses, in milliseconds.

Table 3-77 Field Descriptions—show statistics accelerator http https Command (continued)

Field	Description
RTT saved by HTTPS Authorization Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving authentication required (401) responses, in milliseconds.
Total Locally Served HTTPS Conditional Responses	Number of locally served conditional (304) responses.
Total Locally Served HTTPS Redirect Responses	Number of locally served redirect (301) responses.
Total Locally Served HTTPS Unauthorized Responses	Number of locally served authentication required (401) responses.
Total Remotely Served HTTPS Conditional Responses	Number of remotely served conditional (304) responses (cache misses).
Total Remotely Served HTTPS Redirect Responses	Number of remotely served redirect (301) responses (cache misses).
Total Remotely Served HTTPS Unauthorized Responses	Number of remotely served authentication required (401) responses (cache misses).
Total Hints Sent to DRE Layer to Skip Header Information - HTTPS	Number of DRE hints to skip header information.
Total Hints Sent to DRE Layer to Flush Data - HTTPS	Number of DRE hints to flush data.
Total Hints Sent to DRE Layer to Skip LZ - HTTPS	Number of DRE hints to skip LZ compression.
Total Server Compression Suppression - HTTPS	Number of times server compression was suppressed.
Total Time Saved from all HTTPS metadata cache hits	Total round-trip time saved by the three metadata caches (conditional response, redirect response, and unauthorized response) in milliseconds.
Total Time HTTPS Cache Miss (ms)	Total time for HTTPS metadata cache misses, in milleseconds.
Total HTTPS Requests Requiring Server Content-Revalidation	Number of requests that required content to be revalidated with the origin server, as specified by a Cache-Control header.
Total HTTPS Responses not to be Cached	Number of 200, 301, 304, and 401 responses not to be cached, as specified by a Cache-Control header.
Total HTTPS Connections Bypassed due to URL Based Bypass List	Number of connection flows that are bypassed due to a URL based bypass list.
Total HTTPS Connections Bypassed due to IP Based Bypass List	Number of connection flows that are bypassed due to a bypass list entry.
Total HTTPS sessions using SharePoint optimization	Number of HTTPS sessions using the SharePoint optimization feature to access objects from the SharePoint server.
Total HTTPS sessions using SharePoint prefetch optimization	Number of HTTPS sessions where the prefetch optimization for SharePoint objects (MS Office applications) is enabled.

Table 3-77 Field Descriptions—show statistics accelerator http https Command (continued)

Field	Description
Total HTTPS SharePoint objects prefetched	Number of SharePoint objects that have been prefetched due to client requests using HTTPS sessions.
Total HTTPS locally served SharePoint prefetch objects	Number of SharePoint objects that have been prefetched and have been displayed on the client using HTTPS sessions.
Total HTTPS RTT saved by SharePoint optimization (ms)	For HTTPS sessions, the total response time (in milliseconds) saved in accessing SharePoint objects by enabling the SharePoint optimization.
Total HTTPS RTT saved by SharePoint prefetch cache hit (ms)	For HTTPS sessions, the total response time (in milliseconds) saved in accessing SharePoint data that has already been prefetched and stored in the cache.
Total HTTPS remotely served SharePoint prefetch objects	For HTTPS sessions, the number of SharePoint objects that have been prefetched and displayed remotely.
Total HTTPS time for SharePoint cache miss (ms)	For HTTPS sessions, the total time (in milliseconds) lost in accessing SharePoint data that is not already stored in the cache.
Total HTTPS time for SharePoint prefetch cache miss (ms)	For HTTPS sessions, the total time (in milliseconds) lost in finding prefetched data that was not stored in the cache.

Table 3-78 describes the fields shown in the **show statistics accelerator mapi detail** command display.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command

Field	Description
Global Statistics	
Time Accelerator was started	Time that the accelerator was started.
Time statistics were Last Reset/Cleared	Time that the statistics were last reset.
Total Handled Connections	Number of connections handled since the accelerator was started.
Total Optimized Connections	Number of connections handled since the accelerator was started, from start to finish.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections received by the accelerator but to which only generic optimizations were done (no acceleration).
Total Dropped Connections	Number of connections dropped for reasons other than client/server socket errors or close.
Current Active Connections	Number of connections currently being handled by the accelerator.
Current Pending Connections	Number of connections pending to be accepted.
Maximum Active Connections	Maximum number of simultaneous connections handled by the accelerator.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Total Secured Connections	Number of connections to Outlook clients that use encryption. Such connections are not accelerated by the MAPI accelerator but are passed through.
Number of Synch Get Buffer Requests	Number of MAPI SyncGetBuffer calls made. Each call downloads a chunk of data from a cached folder.
Minimum Synch Get Buffer Size (bytes)	Minimum chunk size downloaded by the MAPI SyncGetBuffer call.
Maximum Synch Get Buffer Size (bytes)	Maximum chunk size downloaded by the MAPI SyncGetBuffer call.
Average Synch Get Buffer Size (bytes)	Average chunk size downloaded by the MAPI SyncGetBuffer call.
Number of Read Stream Requests	Number of MAPI ReadStream calls made. Each call downloads a chunk of data from a noncached folder.
Minimum Read Stream Buffer Size (bytes)	Minimum chunk size downloaded by the MAPI ReadStream call.
Maximum Read Stream Buffer Size (bytes)	Maximum chunk size downloaded by the MAPI ReadStream call.
Average Read Stream Buffer Size (bytes)	Average chunk size downloaded by the MAPI ReadStream call.
Minimum Accumulated Read Ahead Data Size (bytes)	Minimum data size for MAPI read ahead.
Maximum Accumulated Read Ahead Data Size (bytes)	Maximum data size for MAPI read ahead.
Average Accumulated Read Ahead Data Size (bytes)	Average data size for MAPI read ahead.
Local Response Count	Number of local MAPI command responses sent to the client without waiting for a response from the peer WAE.
Average Local Response Time (usec)	Average time used for local responses, in microseconds.
Remote Response Count	Number of MAPI commands forwarded to the Exchange server for a response.
Average Remote Response Time (usec)	Average time used for remote responses, in microseconds.
Number of Write Stream Requests	Number of write stream requests.
Minimum Async Write Stream Buffer Size (bytes)	Minimum size of the asynchronous request stub sent on the WAN, calculated from the minimum stub size across all sessions.
Maximum Async Write Stream Buffer Size (bytes)	Maximum size of the asynchronous request stub sent on the WAN, calculated from the maximum stub size across all sessions.
Average Async Write Stream Buffer Size (bytes)	Average size of the asynchronous request stub sent on the WAN, calculated by taking the average of the stub size across all sessions.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Current 2000 Accelerated Sessions	Number of accelerated sessions to Outlook 2000 clients. Sessions (users), not TCP connections.
Current 2003 Accelerated Sessions	Number of accelerated sessions to Outlook 2003 clients. Sessions (users), not TCP connections.
Current 2007 Accelerated Sessions	Number of accelerated sessions to Outlook 2007 clients. Sessions (users), not TCP connections.
Current 2010 Accelerated Sessions	Number of accelerated sessions to Outlook 2010 clients. Sessions (users), not TCP connections.
Lower than 2000 Sessions	Number of sessions to clients using a version of Outlook lower than Outlook 2000. Such connections are not accelerated by the MAPI accelerator but are passed through.
Unsupported Higher Client Version Sessions	Number of sessions to clients using a version of Outlook higher than that supported. Such connections are not accelerated by the MAPI accelerator but are passed through.
Async Write Optimization Statistics	
Current Number Of Async Write Stubs On WAN	Current number of asynchronous requests on the WAN.
Current Number Of Requests Queued Due To Flow Control	Current number of client session flows that were blocked due to threshold limit.
Current Number Of Requests Queued Due To RopBackOff	Current number of client session flows that were blocked due to ropbackoff response.
Total Number Of RopBackOff Response Received	Total number of ropbackoff responses received across all connections.
Total RopBackOff Duration (msec)	Cumulative time of ropbackoff durations across all connections, in milliseconds.
Total Wait Time Of Requests Queued Due To FlowControl (msec)	Cumulative wait time of requests queued due to flow control across all connections, in milliseconds.
Total Wait Time Of Requests Queued Due To RopBackOff (msec)	Cumulative wait time of requests queued due to ropbackoff across all connections, in milliseconds.
Connection Hand-Off Reasons	Number of connections handed off from the MAPI accelerator to the generic accelerator for various reasons.
Association Group (AG) Statistics	
Average Active AGs In The Last Hour	Average number of active AGs in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average Active Connections Used By AGs In The Last Hour	Average number of active connections used by AGs in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average Active AGs In The Last 5min	Average number of active AGs in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Average Active Connections Used By AGs In The Last 5min	Average number of active connections used by AGs in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Current Active AGs	Number of current active AGs.
Current Active Connections Used By AGs	Number of current active connections used by AGs.
Max Active AGs Since Last Reset/Cleared	Number of max active AGs since last reset/cleared.
Active Connections When Max Active AGs Since Last Reset/Cleared	Number of active connections when max active AGs since last reset/cleared.
Max Active Connections Within an AG Since Last Reset/Cleared	Number of max active connections within an AG since last reset/cleared.
Max Total Active Connections Since Last Reset/Cleared	Number of max total active connections since last reset/cleared.
AGs When Max Total Active Connections Since Last Reset/Cleared	Number of AGs when max total active connections since last reset/cleared.
Total AGs	Number of total AGs.
Total Handed Off AGs due to Reservation Failure	Number of total handed off AGs due to reservation failure.
Total Handed Off AGs Tracked by MAPI AO	Number of total handed off AGs tracked by MAPI AO.
Current Handed Off AGs Tracked by MAPI AO	Number of current handed off AGs tracked by MAPI AO.
Reserved Connections Pool Statistics	
Current In-Use Connections	Number of current in-use connections.
Current Reserved (Unused) Connections	Number of current reserved but still not used connections.
Average In-Use Connections in Last One Hour	Average number of average in-use connections in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average Reserved (Unused) Connections in Last One Hour	Average number of average reserved but unused connections in the last hour. This number is zero if statistics were reset/cleared within one hour.
Average In-Use Connections in Last 5min	Average number of average in-use connections in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Average Reserved (Unused) Connections in Last 5min	Average number of reserved (unused) connections in the last five minutes. This number is zero if statistics were reset/cleared within five minutes.
Configured Maximum Reserved (Unused) Connections	Maximum reserved connections configured but not used.
ReadAhead (RAH) Optimization Statistics	Several statistics for read ahead optimization, including the number of active read aheads and bytes read by the read ahead optimizer.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Exchange Server Error Statistics	Number of errors of various types that were returned by the Exchange server.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Rejected Connections Of Interest Due To Unavailable Resources	Number of connections rejected due to unavailable resources. Incremented when a new MAPI connection arrives that matches an existing MAPI specific dynamic policy but there are no resources available in the reserved pool to accept it; the connection is passed through.
Rejected Connections Of Interest Due To Unavailable Peer	Number of connections rejected due to unavailable peer. Incremented when a new MAPI connection arrives that matches an existing MAPI specific dynamic policy but there is no remote MAPI peer or the remote peer is unable to accept it; the connection is passed through.
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.

Table 3-78 Field Descriptions—show statistics accelerator mapi detail Command (continued)

Field	Description
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Table 3-79 describes the fields shown in the **show statistics accelerator nfs detail** command display.

Table 3-79 Field Descriptions for the show statistics accelerator nfs detail Command

Field	Description
Time Accelerator was started	Time that the accelerator was started.
Time Statistics were Last Reset/Cleared	Time that the statistics were last reset.
Total Handled Connections	Number of connections handled since the accelerator was started.
Total Optimized Connections	Number of connections optimized by the accelerator.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections received by the accelerator but to which only generic optimizations were done (no acceleration).
Total Dropped Connections	Number of connections dropped for reasons other than client/server socket errors or close.
Current Active Connections	Number of connections currently being handled by the accelerator.
Current Pending Connections	Number of connections currently pending for the accelerator.
Maximum Active Connections	Maximum number of simultaneous connections handled by the accelerator.
Total RPC Calls per Authentication Flavor	Array of the number of RPC calls for each NFS authentication type.
Total RPC Calls with Unknown Authentication Flavor	Number of RPC calls with an unknown authentication type.
Total RPC Calls per NFS version	Array of the number of RPC calls for each NFS version.
Total RPC Calls with Unknown NFS Version	Number of RPC calls with an unknown NFS version.
Total Requests	Total number of NFS requests received.
Total Local Replies	Number of requests that resulted in WAAS generating a local reply.
Percentage of Requests Served Locally	Percentage of requests served locally by the WAAS device.

Table 3-79 Field Descriptions for the show statistics accelerator nfs detail Command (continued)

Field	Description
Percentage of Requests Served Remotely	Percentage of requests served remotely by the NFS server.
Average Time to Generate Local READ Reply (ms)	Average time to generate a local read reply, in milliseconds.
Average Time to Generate Local WRITE Reply (ms)	Average time to generate a local write reply, in milliseconds.
Average Time to Generate Local GETATTR Reply (ms)	Average time to generate a local GETATTR reply, in milliseconds.
Average Time to Generate Local Reply (ms)	Average time to generate a local reply, in milliseconds.
Average Time to Receive Remote Reply (ms)	Average time to receive a remote reply from the NFS server, in milliseconds.
Meta-Data Cache Access Count	Number of times the meta data cache as accessed.
Meta-Data Cache Hit Count	Number of meta data cache hits.
Remaining number Of Entries in Meta-Data Cache	Number of available entries in the meta data cache.
Meta-Data Cache Hit Ratio	Percentage of meta data accesses served from the meta data cache.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.

Table 3-79 Field Descriptions for the show statistics accelerator nfs detail Command (continued)

Field	Description
Completed Connections	Number of hits that have made use of the accelerator application and have completed.
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.

Table 3-79 Field Descriptions for the show statistics accelerator nfs detail Command (continued)

Field	Description
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Table 3-80 describes the fields shown in the **show statistics accelerator smb detail** command display.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total Handled Connections	Number of connections handled since the accelerator was started or its statistics last reset.
Total Optimized Connections	Number of connections previously and currently optimized by the accelerator.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections initially accepted by the SMB accelerator, but later handed off to generic optimization without poliby changes so the current negotiated policies for compression (DRE/LZ) will be used.
Total Dropped Connections	Number of connections dropped.
Total Active Connections	Number of connections currently being optimized by the SMB accelerator.
Current Pending Connections	Number of connections that have been determined to be accelerated by the SMB accelerator, and have been queued to be picked up by the accelerator.
Maximum Active Connections	Maximum value reached by the Current Active Connections counter. This counter will be reset if the accelerator is restarted or statistics are cleared.
Total Number of SMB1 Sessions Optimized	Total number of SMB1 sessions optimized by the accelerator.
Total Number of SMB1 Signed Sessions (L4 Opt)	Total number of SMB1 signed sessions (Layer 4 optimization).
Total Number of SMB1 Sessions Not Optimized	Total number of SMB1 sessions not optimized by the accelerator.
Total Number of SMB2 Sessions Not Optimized (handoff on request)	Total number of SMB2 sessions not optimized by the accelerator.
Total Number of SMB2 Sessions (L4 optimization, handoff on request)	Total number of SMB2 sessions optimized (Layer 4 optimization)

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total Number of SMB2_0 Sessions Optimized	Total number of SMB2 sessions optimized.
Total Number of SMB2 _0 Signed Sessions (L4 Opt)	Number of SMB2_0 signed sessions (Layer 4 optimization)
Total Number of SMB2_0 Sessions Not Optimized	Number of SMB2_1 session optimized.
Total Number of SMB2_1 Sessions Optimized	Number of SMB2_1 sessions optimized.
Total Number of SMB2_1 Signed Sessions (L4 Opt)	Number of SMB2_1 signed sessions (Layer 4 optimization)
Total Number of SMB2_1 Sessions Not Optimized	Number of SMB2_1 sessions not optimized.
Total Number of SMB3_0 Sessions Optimized (L4 Opt)	Number of SMB3_0 sessions (Layer 4 optimization).
Total Number of Requests Processed	Number of requests processed (including successful and unsuccessful responses).
Total Number of Requests Served Locally	Number of requests served locally by the WAAS device.
Total Number of Requests Sent to File Servers	Number of requests sent to file servers.
Total Number of SMB1 Requests Processed	Number of SMB1 requests processed (including successful and unsuccessful responses).
Total Number of SMB2 Requests Processed	Number of SMB2 requests processed (including successful and unsuccessful responses).
Total Number of VFN Requests Processed	Number of VFN requests processed (including successful and unsuccessful responses).
Total Number of Active Requests	Number of active SMB requests.
Total Number of Open Files	Number of open files on the WAE. The SMB accelerator performs below the optimum level if there are too many open files. The maximum value of the open-file count is platform-dependent. Use **(config) threshold-monitor** to configure monitoring thresholds.
Total Number of Bytes Read from Cache	Number of bytes read from cache.
Total Number of Bytes Written to Cache	Number of bytes written to the cache.
Total Number of Bytes Written to LAN (Original)	Number of unoptimized bytes written to the LAN.
Total Number of Bytes Read from LAN (Original)	Number of unoptimized bytes read from the LAN.
Total Number of Bytes Read from WAN (Optimized)	Number of optimized bytes read from the WAN.
Total Number of Bytes Written to WAN (Optimized)	Number of optimized bytes written to the WAN.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total Number of Signed SMB Bytes Read from LAN (Original)	Number of unoptimized signed SMB bytes read from the LAN.
Total Number of Signed SMB Bytes Written to LAN (Original)	Number of unoptimized signed SMB bytes writte to the LAN.
Total Number of Signed SMB Bytes Read from WAN (L4 Optimized)	Number of Layer 4 optimized signed SMB bytes read from the WAN.
Total Number of Signed SMB Bytes Written to WAN (L4 Optimized)	Number of Layer 4 optimized signed SMB bytes written to the WAN.
Average Response Time (ms) for Requests Served Locally	Average response time for requests served locally, in milliseconds.
Average Response Time (ms) for Requests Sent to File Servers	Average response time for requests sent to file servers, in milliseconds.
Total Round Trip Time (ms) for All Requests	Total round trip time for all requests, in milliseconds.
Total Amount of Time Saved (ms) Due to Optimization	Total time saved due to optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Read-ahead	Total time saved due to read-ahead, in milliseconds.
Total Amount of Time Saved (ms) Due to Metadata Optimization	Total time saved due to metadata optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Microsoft Optimization	Total time saved due to Microsoft optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Not-found-metadata Cache	Total time saved due to not-found metadata cache, in milliseconds.
Total Amount of Time Saved (ms) Due to Async Request Handling	Total time saved due to asynchronous request handling, in milliseconds.
Total Amount of Time Saved (ms) Due to DCE-RPC Optimization	Total time saved due to DCE-RPC optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Print Optimization	Total time saved due to print optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Other Optimization	Total time saved due to other, non-print optimization, in milliseconds.
Current Allocated Memory Usage of Not-found Metadata Cache	Currentallocated memory usage of not-found metadata cache.
Number of Entries in Not-found Metadata Cache	Number of entries in not-found metadata cache.
Not-found Metadata Cache Hit Count	Number of not-found metadata cache hits.
Not-found Metadata Cache Access Attempts Count	Number of not-found metadata cache access attempts.
Not-found Metadata Cache Allowed Access Count	Number of not-found metadata cache allowed accesses.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Not-found Metadata Cache Update Attempts Count	Number of not-found metadata cache update attempts.
Not-found Metadata Cache Allowed Updates Count	Number of not-found metadata cache allowed updates.
Not-found Metadata Cache Hash Bucket Count	Number of not-found metadata cache hash buckets. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster.
Read-ahead Buffer Hit Rate (%)	The hit rate of the read-buffer, as a percent.
Read-ahead Buffer Hit Count	Number of read-ahead buffer hits.
Read-ahead Buffer Hit Bytes	Number of read-ahead buffer hits, in bytes.
Read-ahead Buffer Miss Bytes	Number of read-ahead buffer misses, in bytes.
Read-ahead Buffer Total Bytes Read from Files Servers	Number of read-ahead buffer bytes read from file servers.
Read-ahead Buffer Pass-through Bytes	Number of read-ahead buffer pass-through bytes.
Read-ahead Buffer Wait Blocks	Number of read-ahead buffer wait blocks.
Read-ahead Buffer Active IO Blocks	Number of read-ahead buffer active IO blocks.
Read-ahead Buffer Block Size in Bytes	The read-ahead buffer block size, in bytes.
Read-ahead Buffer Usage (in Blocks)	The read-ahead buffer usage, in blocks.
Read-ahead Buffer Total Size (in Blocks)	Total size of the read-ahead buffer, in blocks.
Read-ahead Buffer Blocks Evicted	Number of read-ahead buffer blocks evicted.
Read-ahead Buffer Blocks Evicted Before Use	Number of read-ahead buffer blocks evicted before use.
Read-ahead Buffer Blocks Invalidated	Number of read-ahead buffer blocks invalidated.
Total Number of Files in Read-ahead Buffer	Number of files in the read-ahead buffer.
Read-ahead Buffer Last Evicted Item Age (Seconds)	The age of the last evicted item in the read-ahead buffer, in seconds.
Read-ahead Buffer Min Eviction Age (Seconds)	The minimum amount of time, in seconds, before an item is evicted from the read-ahead buffer.
Metadata Cache Total Size (Bytes)	The size of the metadata cache, in bytes.
Metadata Cache Hit Rate (%)	The hit rate of the metdata cache, as a percent.
Metadata Cache Hit Count	Number of metadata cache hits.
Total Number of File Oplocks Acquired on Behalf of the Client	Number of opportunistic locks acquired on behalf of the client.
Total Number of Write-opt Requests Served Locally	Number of write-optimization requests served locallyu.
Total Number of Other Requests Served Locally	Number of other requests served locally.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total Number of Metadata Cached Resources	Number of metadata cached references.
Total SMB1 Named Pipe Open Requests Processed	Number of SMB1 NT_Create_AndX requests for non \spoolss pipe seen by the edge WAE.
Total SMB1 Named Pipe Open Requests Served Locally	Number of SMB1 NT_Create_AndX requests for non \spoolss pipe served locally by the edge WAE, due to cached-open and delayed-close optimization.
Total SMB1 Named Pipe Open Requests Forward to Server	Number of SMB1NT_Create_AndX requests for non \spoolss pipe that were forwarded to the server by the edge WAE (requests that could not be served locally).
Total SMB1 Named Pipe Close requests processed	Number of SMB1 Close requests for non \spoolss pipe see by the edge WAE.
Total SMB1 Named Pipe Close requests served locally	Number of SMB1 Close requests for non \spoolss pipe served locally by the edge WAE as part of delayed-close optimization.
Total SMB1 Named Pipe Close requests forwarded to server	Number of SMB1 Close requests for non \spoolss pipe that were forwarded to the server by the dge WAE (requests that could not be served locally). This total includes only the Close requests that are sent synchronously to the server (when the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests that are first served locally and then sent to the server at a later point in time).
Named Pipe Cache Access Attempts Count	Number of named pipe cache access attempts.
Named Pipe Cache Hit Count	Number of named pipe cache hits.
Named Pipe Entry Count	Number of named pipe entries.
Named Pipe Cache Size	The size of the named pipe cache.
Total Amount of Time Saved (ms) Due to Print Optimization	Total time saved (since the last counters were cleared) due to all print optimizations being performed, in milliseconds.
Total SMB1 Print Open requests	Number of SMB1 NT_Create_AndX requests for \spoolss pipe seen by the edge WAE.
Total SMB1 Print Open requests served locally	Number of SMB1 NT_Create_AndX requests for \spoolss pipe served locally by the edge WAE due to cached open and delayed close optimization.
Total SMB1 Print Open requests forwarded to server	Number of SMB1 NT_Create_AndX requests for \spoolss pipe forwarded to the server by the edge WAE (could not be served locally).
Total SMB1 Print Close requests processed	Number of SMB1 Close requests for \spoolss pipe seen by the edge WAE.
Total SMB1 Print Close requests served locally	Number of SMB1 Close requests served locally by the edge WAE as part of delayed close optimization.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total SMB1 Print Close requests forwarded to the server	Number of SMB1 Close requests forwarded to the server by the edge WAE (could not be served locally). This total includes only the Close requests that are sent *synchronously* to the server (the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests first served locally and then sent to the server at a later point in time).
Print SMB1 Documents Spooled count	Number of SMB1 Transact EndDocPrinter messages (DCE-RPC opnum 23) for the \spoolss pipe seen by the edge WAE.
Print SMB1 Pages Spooled count	Number of SMB1 Transact EndDocPrinter messages (DCE-RPC opnum 20) for the \spoolss pipe seen by the edge WAE. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async Write count	Number of SMB1 Write_AndXmessages for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization.
Print SMB1 Async StartPagePrinter count	Number of SMB1 Transact StartPagePrinter messages (DCE-RPC opnum 18) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async EndPagePrinter count	Number of SMB1 Transact EndPagePrinter messages (DCE-RPC opnum 20) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async WritePrinter count	Number of SMB1 Transact WritePagePrinter messages (DCE-RPC opnum 19) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Remote Command Count	The number of SMB1 Transact commands for the \spoolss pipe seen by the edge WAE that are not parsed and are sent to the core.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total Number of Read Requests with Office Optimization	Number of read requests with Microsoft Office optimization.
Total Number of Write Requests with Office Optmization	Number of write requests with Microsoft Office Optimization.
Total SMB1_Create_AndX requests processed	Number of SMB1 Create_AndX requests processed.
Total SMB1_Write_AndX requests processed	Number of SMB1 Write_AndX requests processed.
Total SMB1_Write_AndX requests served locally	Number of SMB1 Write_AndX requests served locally.
Total SMB1_Write_AndX requests forwarded to file server	Number of SMB1 Write_AndX requests forwarded to the file server.
Total SMB1_Read_AndX requests processed	Number of SMB1 Read_AndX requests processed.
Total SMB1_Read_AndX requests served locally	Number of SMB1 Read_AndX requests served locally.
Total SMB1_Read_AndX requests forwarded to file server	Number of SMB1 Read_AndX requests forwarded to the file server.
Total SMB1_Cancel requests processed	Number of SMB1 cancel requests processed.
Total SMB1_Delete Requests Processed	Number of SMB1 delete requests processed.
Total SMB1_Delete Requests Served Locally	Number of SMB1 delete requests served locally.
Total SMB1_Delete Requests Forwarded to File Server	Number of SMB1 delete requests forwarded to the file server.
Total SMB1_Delete_Dir Requests Processed	Number of SMB1 delete directory requests processed.
Total SMB1_Delete_Dir Requests Served Locally	Number of SMB1 delete directory requests served locally.
Total SMB1_Delete_Dir Requests Forwarded to File Server	Number of SMB1 delete directory requests forwarded to the file server.
Total SMB1_Create_Temp Requests Processed	Number of SMB1 create temporary directory requests processed.
Total SMB1_Check_Dir Requests Processed	Number of SMB1 check directory requests processed.
Total SMB1_Check_Dir Requests Served Locally	Number of SMB1 check directory requests served locally.
Total SMB1_Check_Dir Requests Forwarded to File Server	Number of SMB1 check directory requests forwarded to the file server.
Total SMB1_Close Requests Processed	Number of SMB1 close requests processed.
Total SMB1_Close Requests Served Locally	Number of SMB1 close requests served locally.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total SMB1_Close Requests Forwarded to File Server	Number of SMB1 close requests forwarded to the file server.
Total SMB1_Rename Requests Processed	Num ber of SMB1 rename requests processed.
Total SMB1_Rename Requests Served Locally	Number of SMB1 rename requests served locally.
Total SMB1_Rename Requests Forwarded to Server	Number of SMB1 rename requests forwarded to the file server.
Total SMB1_Session_Setup Requests Processed	Number of SMB1 session setup requests processed.
Total SMB1_Tree_Connect_AndX Requests Processed	Number of SMB1 Tree_Connect_AndX requests processed.
Total SMB1_Tree_Disconnect Requests Processed	Number of SMB1 Tree_Disconnect requests processed.
Total SMB1_Logoff Requests Processed	Number of SMB1 logoff requests processed.
Total SMB1_Negotiate Requests Processed	Number of SMB1 negotiate requests processed.
Total SMB1_Query_Path_Info Requests Processed	Number of SMB1 query path information requests processed.
Total SMB1_Query_Path_Info Requests Served Locally	Number of SMB1 query path information requests served locally.
Total SMB1_Query_Path_Info Requests Forwarded to File Server	Number of SMB1 query path information requests forwarded to the file server.
Total SMB1_Query_File_Info Requests Processed	Number of SMB1 query file information requests processed.
Total SMB1_Query_File_Info Requests Served Locally	Number of SMB1 query file information requests served locally.
Total SMB1_Query_File_Info Requests Forwarded to File Server	Number of SMB1 query file information requests forwarded to the file server.
Total SMB1_Set_Path_Info Requests Processed	Number of SMB1 set path information requests processed.
Total SMB1_Set_Path_Info Requests Served Locally	Number of SMB1 set path information requests served locally.
Total SMB1_Set_Path_Info Requests Forwarded to File Server	Number of SMB1 set path information requests forwarded to the file server.
Total SMB1_Set_File_Info Requests Processed	Number of SMB1 set file information requests processed.
Total SMB1_Set_File_Info Requests Served Locally	Number of SMB1 set file information requests served locally.
Total SMB1_Set_File_Info Requests Forwarded to File Server	Number of SMB1 set file information requests forwarded to the file server.
Total SMB1_Find_First Requests Processed	Number of SMB1 find first requests processed.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total SMB1_Find_First Requests Served Locally	Number of SMB1 find first requests served locally.
Total SMB1_Find_First Requests Forwarded to File Server	Number of SMB1 find first requests forwarded to the file server.
Total SMB1_Find_Next Requests Processed	Number of SMB1 find next requests processed.
Total SMB1_Find_Next Requests Served Locally	Number of SMB1 find next requests served locally.
Total SMB1_Find_Next Requests Forwarded to File Server	Number of SMB1 find next requests forwarded to the file server.
Total SMB1_Create_Dir Requests Processed	Number of SMB1 create directory requests processed.
Total SMB1_Trans2_Create_Dir Requests Processed	Number of SMB1 Transaction2 create directory requests processed.
Total SMB1_Query_FS_Info Requests Processed	Number of SMB1 query file share information requests processed.
Total SMB1_Query_FS_Info Requests Served Locally	Number of SMB1 query file share information requests served locally.
Total SMB1_Query_FS_Info Requests Forward to File Server	Number of SMB1 query file share information requests forwarded to the file server.
Total SMB1_Set_Security_Desc Requests Processed	Number of SMB1 set security descriptor requests processed.
Total SMB1_IOCTL Requests Processed	Number of SMB1 input/output control requests processed.
Total SMB1_OPEN_ANDX Requests Processed	Number of SMB1 Open_AndX requests processed.
Total SMB1_OPEN_ANDX Requests Served Locally	Number of SMB1 Open_AndX requests served locally.
Total SMB1_OPEN_ANDX Requests Forwarded to File Server	Number of SMB1 Open_AndX requests forwarded to the file server.
Total SMB1 Transact Notify Requests Processed	Number of SMB1 transact notify requests processed.
Total SMB1 Transact Notify Requests Served Locally	Number of SMB1 transact notify requests served locally.
Total SMB1 Transact Notify Requests Forwarded to File Server	Number of SMB1 transact notify requests forwarded to the file server.
Total SMB1 Transact Create Requests Processed	Number of SMB1 transact create requests processed.
Total SMB1 Transact Create Requests Served Locally	Number of SMB1 transact create requests served locally.
Total SMB1 Transact Create Requests Forwarded to File Server	Number of SMB1 transact create requests forwarded to the file server.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total SMB1_Locking_AndX Requests Processed	Number of SMB1 Locking_AndX requests processed.
Total SMB1_Locking_AndX Requests Served Locally	Number of SMB1 Locking_AndX requests served locally.
Total SMB1_Locking_AndX Requests Forwarded to File Server	Number of SMB1 Locking_AndX requests served locally.
Total SMB1 Transaction Requests Processed	Number of SMB1 transaction requests processed.
Total SMB1 Transaction Requests Served Locally	Number of SMB1 transacation requests served locally.
Total SMB1 Transaction Requests Forwarded to File Server	Number of SMB1 transaction requests forwarded to the file server.
Total SMB1_Set_Information Requests Processed	Number of SMB1 set information requests processed.
Total SMB1_Set_Information Requests Served Locally	Number of SMB1 set information requests served locally.
Total SMB1_Set_Information Requests Forwarded to File Server	Number of SMB1 set information requests forwarded to the file server.
Total SMB1_Set_Information2 Requests Processed	Number of SMB1 set information2 requests processed.
Total SMB1_Set_Information2 Requests Served Locally	Number of SMB1 set information2 requests served locally.
Total SMB1_Set_Information2 Requests Forwarded to File Server	Number of SMB1 set information2 requests forwarded to the file server.
Total SMB1_Query_Information Requests Processed	Number of SMB1 query information requests processed.
Total SMB1_Query_Information Requests Served Locally	Number of SMB1 query information requests served locally.
Total SMB1_Query_Information Requests Forwarded to File Server	Number of SMB1 query information requests forwarded to the file server.
Total SMB1_Query_Information2 Requests Processed	Number of SMB1 query information2 requests processed.
Total SMB1_Query_Information2 Requests Served Locally	Number of SMB1 query information2 requests served locally.
Total SMB1_Query_Information2 Requests Forwarded to File Server	Number of SMB1 query information2 requests forwarded to the file server.
Total SMB1_NTRename Requests Processed	Number of SMB1 NT rename requests processed.

Table 3-80 Field Descriptions for the show statistics accelerator smb detail Command

Field	Description
Total SMB1_FindClose2 Requests Processed	Number of SMB1 find close2 requests processed.
Total SMB1_Write Requests Processed	Number of SMB1 write requests processed.

Table 3-81 describes the fields shown in the **show statistics accelerator smb | inc Print** command display.

Table 3-81 Field Descriptions for the show statistics accelerator smb | inc Print Command

Field	Description
Total Amount of Time Saved (ms) Due to Print Optimization	Total time saved due to all the optimizations being performed on all the \spoolss pipes (one print job can open multiple \spoolss pipes) and for all the print jobs since the last time the counters were cleared.
Total SMB1 Print Open Requests Processed	The total number of calls to open (NTCreate_AndX).
Total SMB1 Print Open requests served locally	Number of SMB1 NT_Create_AndX requests for \spollss pipe served locally by the edge WAE due to cached open and delayed close optimization.
Total SMB1 Print Open requests forwarded to server	Number of SMB1 NT_Create_AndX requests for \spoolss pipe which were forwarded to the file server by the edge WAE (requests that could not be served locally).
Total SMB1 Print Close requests processed	Number of SMB1 Close requests for the \spoolss pipe seen by the edge WAE.
Total SMB1 Print Close requests served locally	Number of SMB1 Close requests for the \spoolss pipe served locally by the edge WAE as part of delayed close optimization.
Total SMB1 Print Close requests forwarded to the server	Number of SMB1 Close requests for the \spoolss pipe that were forwarded to the file server by the edge WAE (requests that could not be served locally). This total includes only the Close requests that are sent synchronously to the server (the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests first served locally and then sent to the server at a later point in time).

Table 3-81 Field Descriptions for the show statistics accelerator smb | inc Print Command

Field	Description
Print SMB1 Documents Spooled count	Number of SMB1 Transact EndDocPrinter messages for the spoolss pipe seen by the edge WAE.
Print SMB1 Pages Spooled count	Number of SMB1 Transact EndParePrinter messages for the \spoolss pipe seen by the edge WAE.
Print SMB1 Async Write count	Number of SMB1 Write_AndXmessages for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization.
Print SMB1 Async StartPagePrinter count	Number of SMB1 Transact StartPagePrinter messages (DCE-RPC opnum 18) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async EndPagePrinter count	Number of SMB1 Transact EndPagePrinter messages (DCE-RPC opnum 20) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Async WritePrinter count	Number of SMB1 Transact WritePagePrinter messages (DCE-RPC opnum 19) for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization. Note that when used with Windows 7 clients, depending on the printer driver installed, this counter may not increment because this function may be encapsulated in a different SMB command.
Print SMB1 Remote Command Count	The number of SMB1 Transact commands for the \spoolss pipe seen by the edge WAE that are not parsed and are sent to the core.

Table 3-82 describes the fields shown in the **show statistics accelerator ssl detail** command display.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command

Field	Description
Time Accelerator was started	Time stamp of when the accelerator was started. Will change if the accelerator is restarted for any reason.
Time Statistics were Last Reset/Cleared	Time stamp of when the accelerator statistics were last set to zero. This value should be the same as the Time Accelerator was started field if the **clear stat accelerator all** or **clear stat accelerator ssl** commands were never issued. Otherwise it will show the time at which the **clear stat accelerator all** or **clear stat accelerator ssl** commands were last issued.
Total Handled Connections	Number of connections that the SSL accelerator received to provide acceleration services. This includes connections that may have been accelerated successfully, as well as connections which may have experienced errors after arriving at the SSL accelerator.
Total Optimized Connections	Number of connections in which a successful SSL handshake was completed and the connection entered the data transfer phase. Connections that experienced errors during SSL handshake are not counted here. Connections that experienced errors after handshake are counted here. Connections that experienced errors during SSL re-handshake (renegotiation) are also counted here.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections that the SSL accelerator bypassed. No acceleration of these connections was done. This could be because SSL version 2 was negotiated, non-SSL traffic was detected, or SSL accelerator version and/or cipher configuration dictated that the connection should be bypassed.
Total Dropped Connections	Number of connections that the SSL accelerator ended prematurely. This could be due to verification failures, revocation check failures, errors detected during the handshake or data transfer phase of the connection, or due to internal errors. Other counters below may shed more light as to why connections were dropped.
Current Active Connections	Number of connections currently being optimized by the SSL accelerator.
Current Pending Connections	Number of connections that have been determined to be accelerated by the SSL accelerator, and have been queued to be picked up by the accelerator.
Maximum Active Connections	Maximum value ever reached by the Current Active Connections counter. This counter will be reset if the accelerator is restarted or statistics are cleared.
Total LAN Bytes Read	Number of bytes read by the SSL accelerator from the original side of the flow.
Total Reads on LAN	Number of read operations performed by the SSL accelerator on the original side of the flow.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Total LAN Bytes Written	Number of bytes written by the SSL accelerator on the original side of the flow.
Total Writes on LAN	Number of write operations performed by the SSL accelerator on the original side of the flow.
Total WAN Bytes Read	Number of bytes read by the SSL accelerator from the optimized side of the flow.
Total Reads on WAN	Number of read operations performed by the SSL accelerator on the optimized side of the flow.
Total WAN Bytes Written	Number of bytes written by the SSL accelerator on the optimized side of the flow.
Total Writes on WAN	Number of write operations performed by the SSL accelerator on the optimized side of the flow.
Total LAN Handshake Bytes Read	Number of bytes read from the original side of flows during the handshake phase of flows.
Total LAN Handshake Bytes Written	Number of bytes written to the original side of flows during the handshake phase of flows.
Total WAN Handshake Bytes Read	Number of bytes read to the optimized side of flows during the handshake phase of flows.
Total WAN Handshake Bytes Written	Number of bytes written to the optimized side of flows during the handshake phase of flows.
Total Accelerator Bytes Read	SSL accelerator internal counter. (Bytes read from original side of DRE).
Total Accelerator reads	SSL accelerator internal counter. (Read operations performed on original side of DRE).
Total Accelerator Bytes Written	SSL accelerator internal counter. (Bytes written to original side of DRE).
Total Accelerator Writes	SSL accelerator internal counter. (Write operations performed on original side of DRE).
Total DRE Bytes Read	SSL accelerator internal counter. (Bytes read from optimized side of DRE).
Total DRE Reads	SSL accelerator internal counter. (Read operations performed on the optimized side of DRE).
Total DRE Bytes Written	SSL accelerator internal counter. (Bytes read from optimized side of DRE).
Total DRE Writes	SSL accelerator internal counter. (Write operations performed on the optimized side of DRE).
Number of forward DNS lookups issued	Number of forward DNS lookups that were issued.
Number of forward DNS lookups failed	Number of forward DNS lookup failures.
Number of flows with matching host names	Number of flows where server host name matched accelerated service configuration.
Number of reverse DNS lookups issued	Number of reverse DNS lookups that were issued.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Number of reverse DNS lookups failed	Number of reverse DNS lookup failures.
Number of reverse DNS lookups cancelled	Number of reverse DNS lookups that were cancelled.
Number of flows with matching domain names	Number of flows where server domain name matched accelerated service configuration.
Number of flows with matching any IP rule	Number of flows where the server IP address matched 'IP any' rule.
Total Failed Handshakes	Number of connections that ended during the handshake phase.
Pipe-through due to cipher mismatch	Number of connections bypassed by SSL accelerator because the SSL cipher negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
Pipe-through due to version mismatch	Number of connections bypassed by SSL accelerator because the SSL version negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
Pipe-through due to non-matching domain name	Number of connections bypassed by SSL accelerator because the destination domain did not match the domains specified to be accelerated.
Pipe-through due to unknown reason	Number of connections bypassed by SSL accelerator because of unknown reasons.
Pipe-through due to detection of non-SSL traffic	Number of connections bypassed by SSL accelerator because the content of the flow did not appear to contain SSL messages.
Total SSLv3 Negotiated on LAN	Number of connections that used SSL version 3 on the original side of the flow.
Total TLSv1 Negotiated on LAN	Number of connections that used TLS version 1 on the original side of the flow.
Total SSLv3 Negotiated on WAN	Number of connections that used SSL version 3 on the optimized side of the flow.
Total TLSv1 Negotiated on WAN	Number of connections that used TLS version 1 on the optimized side of the flow.
Total SSLv3 Negotiated on Peer	Number of connections that used SSL version 3 on the control connection between WAAS devices.
Total TLSv1 Negotiated on Peer	Number of connections that used TLS version 1 on the control connection between WAAS devices.
Total renegotiations requested by server	Number of SSL “Hello Request” messages detected by the SSL accelerator.
Total SSL renegotiations performed	Number of SSL renegotiation attempts (successful and unsuccessful) detected by the SSL accelerator.
Total number of failed renegotiations	Number of unsuccessful SSL renegotiations detected by the SSL accelerator.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Flows dropped due to renegotiation timeout	Number of flows dropped due to renegotiation timeout.
[W2W-Srvr] Number of session hits	Number of times inter-WAAS SSL session resumption was successful on flows where this WAE was the Core WAE.
[W2W-Srvr] Number of session misses	Number of times inter-WAAS SSL full handshake was carried out, on flows where this WAE was the Core WAE.
[W2W-Srvr] Number of sessions timedout	Number of SSL sessions that were not reused because they were timed out.
[W2W-Srvr] Number of sessions deleted because of cache full	Number of sessions evicted from inter-WAAS session cache to make room for new sessions.
[W2W-Srvr] Number of bad sessions deleted	Number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.
[W2W-Comm] Number of sessions inserted into cache	Number of sessions inserted into the inter-WAAS session cache
[W2W-Comm] Number of sessions evicted from cache	Number of sessions evicted from the inter-WAAS session cache.
[W2W-Comm] Number of sessions in cache	Number of session currently cached in the inter-WAAS session cache.
[W2W-Clnt] Number of session hits	Number of times an inter-WAAS session resumption was successful on flows where this WAE was the Edge WAE.
[W2W-Clnt] Number of session misses	Number of times an inter-WAAS full SSL handshake was carried out, on flows where this WAE was the Edge WAE.
[W2W-Clnt] Number of sessions timedout	Number of SSL sessions that were not reused because they were timed out.
[W2W-Clnt] Number of sessions deleted because of cache full	Number of sessions evicted from inter-WAAS session cache to make room for new sessions.
[W2W-Clnt] Number of bad sessions deleted	Number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.
[C2S-Srvr] Number of session hits	Number of times a client-requested session was found in the client-facing session cache (even if eventually a full handshake had to be carried out due to session miss between Core WAE and server).
[C2S-Srvr] Number of session misses	Number of times a client-requested session was not found in the client-facing session cache.
[C2S-Srvr] Number of sessions timedout	Number of sessions in the client-facing session cache that were not reused because they were timed out.
[C2S-Srvr] Number of sessions deleted because of cache full	Number of sessions evicted from the client-facing session cache to make room for new sessions.
[C2S-Srvr] Number of bad sessions deleted	Number of sessions evicted from the client-facing session cache as they were rendered unsuitable for reuse, likely due to connection errors.

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
[C2S-Srvr] Number of sessions inserted into cache	Number of sessions inserted into the client-facing session cache.
[C2S-Srvr] Number of sessions evicted from cache	Number of sessions evicted from the client-facing session cache.
[C2S-Srvr] Number of sessions in cache	Number of sessions currently cached in the client-facing session cache.
[C2S-Clnt] Number of session hits	Number of times a Core-WAE requested session was successfully reused between the Core WAE and server.
C2S-Clnt] Number of session misses	Number of times a full SSL handshake had to be carried out between the Core WAE and server.
[C2S-Clnt] Number of sessions timedout	Number of times a session in the server-facing session cache could not be reused because it was timed out.
[C2S-Clnt] Number of sessions deleted because of cache full	Number of sessions evicted from the server-facing session cache to make room for new sessions.
[C2S-Clnt] Number of bad sessions deleted	Number of sessions evicted from the server-facing session cache as they were rendered unsuitable for reuse, likely due to connection errors.
[C2S-Clnt] Number of sessions inserted into cache	Number of sessions inserted into the server-facing session cache.
[C2S-Clnt] Number of sessions evicted from cache	Number of sessions evicted from the server-facing session cache.
[C2S-Clnt] Number of sessions in cache	Number of sessions currently cached in the server-facing session cache.
Total Successful Certificate Verifications	Number of times a certificate was successfully verified (could be client or server).
Total Failed Certificate Verifications	Number of times a certificate verification failed (could be for various reasons, other counters may indicate why).
Failed certificate verifications due to invalid certificates	Number of certificate verification attempts failed because the certificate was invalid. An inspection of the SSL accelerator errorlog may indicate the reasons.
Failed Certificate Verifications based on OCSP Check	Number of certificate verification attempts deemed unsuccessful based on results of OCSP revocation check.
Failed Certificate Verifications (non OCSP)	Number of certificate verification attempts deemed unsuccessful based on results of the certificate verification operation.
Total Failed Certificate Verifications due to Other Errors	Number of certificate verification failures due to other problems (including internal errors). An inspection of the SSL accelerator errorlog may indicate the reasons.
Total OCSP Connections Outstanding	Number of OCSP requests currently in progress.
Total OCSP Requests Processed	Number of OCSP requests completed (including successful and unsuccessful responses).

Table 3-82 Field Descriptions for the show statistics accelerator ssl detail Command (continued)

Field	Description
Maximum Concurrent OCSP Requests	Maximum value ever reached by Total OCSP Connections Outstanding counter. This will be reset if the accelerator is restarted or statistics are cleared.
Total Successful OCSP Requests	Number of OCSP requests that were completed with a valid response from the OCSP responder.
Total Successful OCSP Requests Returning OK Status	Number of OCSP request where the certificate status was OK.
Total Successful OCSP Requests with 'NONE' Revocation	Number of OCSP requests where the OCSP status was deemed OK because of fallback to method configuration: none.
Total Successful OCSP Requests Returning REVOKED Status	Number of OCSP requests where the certificate status was REVOKED.
Total Successful OCSP Requests Returning UNKNOWN Status	Number of OCSP requests where the responder did not know the status of the certificate.
Total Failed OCSP Requests	Number of OCSP requests which could not be completed successfully.
Total Failed OCSP Requests due to Other Errors	Number of OCSP requests deemed failed due to internal errors.
Total Failed OCSP Requests due to Connection Errors	Number of OCSP requests deemed failed because a connection to the OCSP responder could not be set up.
Total Failed OCSP Requests due to Connection Timeouts	Number of OCSP requests deemed failed because no response was received from the OCSP responder.
Total Failed OCSP Requests due to Insufficient Resources	Number of OCSP requests deemed failed because there was insufficient memory to carry out the revocation check.
Total OCSP Bytes Read	Number of bytes read from connections to OCSP responders.
Total OCSP Write Bytes	Number of bytes written to connections to OCSP responders.
Flows dropped due to verification check	Number of connections dropped by this WAE because verification of the client or server certificate failed.
Flows dropped due to revocation check	Number of connections dropped by this WAE because revocation check of the client or server certificate failed.
Flows dropped due to other reasons	Number of connections dropped by this WAE because of errors which may have prevented the verification check or revocation check from returning a valid result. An inspection of the SSL accelerator errorlog may indicate the reasons.

Table 3-83 describes the fields shown in the **show statistics accelerator ssl payload http** command display.

Table 3-83 Field Descriptions—show statistics accelerator ssl payload http Command

Field	Description
Total Optimized Connections	Number of connections in which a successful SSL handshake was completed and the connection entered the data transfer phase. Connections that experienced errors during SSL handshake are not counted here. Connections that experienced errors after handshake are counted here. Connections that experienced errors during SSL re-handshake (renegotiation) are also counted here.
Successful HTTP accelerator insertions	Number of connections where the SSL accelerator successfully inserted the HTTP accelerator.
Unsuccessful HTTP accelerator insertions	Number of connections where the SSL accelerator was unsuccessfully in inserting the HTTP accelerator.

Table 3-84 describes the fields shown in the **show statistics accelerator ssl payload other** command display.

Table 3-84 Field Descriptions—show statistics accelerator ssl payload other Command

Field	Description
Total Optimized Connections	Number of connections in which a successful SSL handshake was completed and the connection entered the data transfer phase. Connections that experienced errors during SSL handshake are not counted here. Connections that experienced errors after handshake are counted here. Connections that experienced errors during SSL re-handshake (renegotiation) are also counted here.

Table 3-85 describes the fields shown in the **show statistics accelerator video detail** command display.

Table 3-85 Field Descriptions—show statistics accelerator video detail Command

Field	Description
Time elapsed since “clear statistics”	Time elapsed since the statistics were last reset.
Connections handled	
Total handled	Number and percentage of connections handled.
Windows-media live accelerated	Number and percentage of accelerated connections.
Un-accelerated pipethrough	Number and percentage of connections passed through the video accelerator but not accelerated.
Un-accelerated dropped due to config	Number and percentage of connections dropped because the video accelerator detected that the connection could not be accelerated and was configured to drop unaccelerated video traffic. See the fields in the Unaccelerated Connections section for the reasons that the video accelerator cannot accelerate a connection.

Table 3-85 Field Descriptions—show statistics accelerator video detail Command (continued)

Field	Description
Error dropped connections	Number and percentage of dropped connections due to errors.
Windows-media active sessions	
Outgoing (client) sessions	Current and maximum number of active Windows Media sessions with clients.
Incoming (server) sessions	Current and maximum number of active Windows Media sessions with servers.
Unaccelerated Connections	
Total Unaccelerated	Number of unaccelerated connections.
Unsupported player	Number of unaccelerated connections due to an unsupported player.
Unsupported transport	Number of unaccelerated connections due to an unsupported transport.
Unsupported protocol	Number of unaccelerated connections due to an unsupported protocol.
Windows-media VoD	Number of unaccelerated connections due to client requesting a video on demand stream.
Max stream bitrate overload	Number of unaccelerated connections due to stream bit-rate overload.
Max aggregate bitrate overload	Number of unaccelerated connections due to aggregate bit-rate overload.
Max concurrent sessions overload	Number of unaccelerated connections due to client session overload.
Other	Number of unaccelerated connections due to other causes.
Error dropped connections	
Total errors	Total number of dropped connections due to errors.
Client timeouts	Number of client timeouts.
Server timeouts	Number of server timeouts.
Client stream errors	Number of client stream errors.
Server stream errors	Number of server stream errors.
Other errors	Number of other errors.
Windows-media byte savings	
% Bytes saved	Percentage of bytes saved by the video accelerator.
Incoming (server) bytes	Number of incoming bytes.
Outgoing (client) bytes	Number of outgoing bytes.
Windows-media aggregate bitrate	
Total bitrate	Total current and maximum bit rate, including both incoming and outgoing traffic.

Table 3-85 Field Descriptions—show statistics accelerator video detail Command (continued)

Field	Description
Outgoing (client) bitrate	Current and maximum bit rate to clients.
Incoming (server) bitrate	Current and maximum bit rate from servers.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.
Drops	Number of hits that attempted use of the video accelerator application but were dropped by the Policy Engine because it detected an overload condition and the video accelerator was configured to drop unaccelerated video traffic due to overload conditions. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.

Table 3-85 Field Descriptions—show statistics accelerator video detail Command (continued)

Field	Description
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Related Commands

show accelerator

show statistics connection closed

show statistics aoim

To display AO (accelerator) Information Manager statistics for a WAAS device, use the **show statistics aoim** EXEC command.

show statistics aoim [**local** | **peer** | **detail**]

Syntax Description

local	(Optional) Displays statistics only for all locally registered application accelerators.
peer	Displays statistics only for all peer WAAS devices encountered.
detail	Displays detailed statistics that include policy engine and auto-discovery statistics.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics aoim** command with no options to display statistical information for locally registered application accelerators and all peer WAAS devices that the local WAAS device has encountered.

Examples

Table 3-86 describes the statistics that are displayed by the **show statistics aoim** EXEC command. Only the Local AOIM Statistics section is displayed when you use the **local** option. Only the Peer AOIM Statistics section is displayed when you use the **peer** option. The Detailed AOIM Statistics section is displayed only when you use the **detail** option.

Table 3-86 Field Descriptions for the show statistics aoim Command

Field	Description
Local AOIM Statistics	
Total # Peer Syncs	Number of times that the AO Information Manager has synchronized with a peer WAAS device.
Current # Peer Syncs in Progress	Number of currently active peer synchronizations in progress.
Maximum # Peer Syncs in Progress	Historical maximum number of concurrently active peer synchronizations in progress.
AOIM DB Size	Memory size of the AO Information Management database.
Number of Peers	Number of known or encountered peer WAAS devices.

Table 3-86 Field Descriptions for the show statistics aoim Command (continued)

Field	Description
Number of Local AOs	Number of application accelerators registered on this WAAS device.
Total # of AO Handoffs & Inserts	Number of application accelerators invoked to handle a connection once a peer synchronization has completed.
AO	Name of the locally registered application accelerator.
Version	Software version of the locally registered application accelerator.
Registered	Registration status of the local application accelerator. An application accelerator may be deregistered but the AO Information Manager will still retain knowledge about it, marking it as unregistered.
# Handoffs	Number of times a connection was passed directly to the application accelerator after a peer synchronization has completed.
# Inserts	Number of times a connection was passed indirectly to the application accelerator after a peer synchronization has completed.
# Incompatible	Number of times a connection was not passed to the application accelerator due to software incompatibility with the peer application accelerator on the peer WAAS device after synchronization has completed.
Peer AOIM Statistics	
Number of Peers	Number of peer WAAS devices encountered.
PEER	MAC address of the peer WAAS device, and whether it has been formally registered with the AO Information database.
Peer Software Version	WAAS software version and build number running on the peer WAAS device. WAAS software versions prior to 4.1 do not have the AO Information Management mechanism, so they are reported as having a software version of 4.0.x.
Peer IP Address	IP address of the primary network interface of the peer WAAS device.
AO	Name of the registered application accelerator on the peer WAAS device.
VERSION	Software version of the registered application accelerator on the peer WAAS device.
COMPATIBLE	Compatibility status of the application accelerator on the peer WAAS device with a matching locally-registered application accelerator on this device. Possible values are Y (yes/compatible), N (no/incompatible), and U (unknown). The unknown state may occur if no matching local application accelerator is registered on the local WAAS device.
#CONNS	Number of incoming connections found to have a compatible application accelerator on both the local and peer WAAS devices and scheduled to be processed by the locally compatible application accelerator. Certain conditions may result in a discrepancy between a connection being scheduled to be processed by an application accelerator and being successfully processed, so this value may diverge somewhat from the number of connections that a specific local application accelerator reports.
Detailed AOIM Statistics	
Policy Engine Statistics	

Table 3-86 Field Descriptions for the show statistics aoim Command (continued)

Field	Description
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: • WAE was rebooted • Configuration change with the accelerator application enabled • Restart of the accelerator application by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.

Table 3-86 Field Descriptions for the show statistics aoim Command (continued)

Field	Description
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Related Commands

show statistics accelerator

show statistics application

To view the performance statistics for applications running on your WAAS device, use the **show statistics application** EXEC command.

show statistics application [**name** *app_name* | **savings** [**appname** *app_name*]]

Syntax Description

name *app_name*	(Optional) Statistics for the specified application.
savings	(Optional) Savings statistics applications.
appname *app_name*	(Optional) Savings statistics for the specified application.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **show statistics application** command displays statistics for all of the application traffic running on your network. To view the statistics for one specific class of applications only, use the **name** keyword.

Table 3-87 lists the valid *app_name* values you can use with the **show statistics application** EXEC command. For a description of the applications supported by WAAS, see Appendix A, "Predefined Application Policies" in the *Cisco Wide Area Application Services Configuration Guide*.

Table 3-87 app_name Variable Values for the show statistics application Command

app_name Values			
Authentication	Backup	CAD	Call-Management
CIFS	Citrix	Conferencing	Console
Content-Management	Directory-Services	Email-and-Messaging	Enterprise-Applications
File-System	File-Transfer	Instant-Messaging	Name-Services
Other	P2P	Printing	Remote-Desktop
Replication	SQL	SSH	SSL
Storage	Streaming	Systems-Management	Version-Management
VPN	Web		

Examples

Table 3-88 describes the statistics for each class of application that are displayed by the **show statistics application** EXEC command.

Table 3-88 Statistic Descriptions for the show statistics application Command

Statistic	Description
Opt TCP Plus	Optimized traffic on the WAN side, optimized at the TFO and DRE/LZ/accelerator levels.
Orig TCP Plus	Original traffic on the LAN side, optimized at the TFO and DRE/LZ/accelerator levels.
Opt Preposition	Optimized traffic on the WAN side, initiated by the WAE device for preposition purposes.
Orig Preposition	Original traffic (unoptimized) on the LAN side, initiated by the WAE device for preposition purposes.
Opt TCP Only	Optimized traffic on the WAN side, optimized at the TFO level only.
Orig TCP Only	Original traffic on the LAN side, optimized at the TFO level only.
Internal Client	Traffic initiated by the WAE device.
Internal Server	Traffic terminated by the WAE device.
PT Client	Pass-through traffic going from the client to the server.
PT Server	Pass-through traffic going from the server to the client
Opt TCP Plus	Optimized traffic on the WAN side, optimized at the TFO and DRE/LZ/accelerator levels.
Preposition	Traffic initiated by the WAE device for preposition purposes.
Opt TCP Only	Optimized traffic on the WAN side, optimized at the TFO level only.
Internal Client	Traffic initiated by the WAE device.
Internal Server	Traffic terminated by the WAE device.
Auto-Discovery	Connections in auto-discovery.
PT No Peer ...	Pass-through reasons.
PT Overall	Total passed-through traffic for all reasons.

Table 3-89 describes the result values shown for the statistics in the **show statistics application** command display.

Table 3-89 Result Value Descriptions for the show statistics application Command

Result	Description
Bytes	Amount of traffic shown as a count of the number of bytes.
Packets	Amount of traffic shown as a count of the number of packets.
Inbound	Traffic received by the WAE device.
Outbound	Traffic sent by the WAE device.
Active	The number of connections that are active.
Completed	The number of connection that have been completed.
Compression Ratio	The amount of compressed traffic compared to the amount of original, uncompressed traffic.

Related Commands show statistics

show statistics appnav-controller

To display statistics for an AppNav Controller, use the **show statistics appnav-controller** EXEC command.

show statistics appnav-controller connection [**client-ip** *ip_address* | **client-port** *port* | **server-ip** *ip_address* | **server-port** *port* | **detail** [**client-ip** *ip_address* | **client-port** *port* | **server-ip** *ip_address* | **server-port** *port*] | **summary**]

show statistics appnav-controller drop

show statistics appnav-controller flow-asymmetry

show statistics appnav-controller flow-management [**app-sess** | **appnav-controller-ip** *ip_address* | **detail** | **flow-table** | **syn**]

show statistics appnav-controller ip

show statistics appnav-controller sessions [**client-ip** *ip_address* | **server-ip** *ip_address* | **server-port** *port* | **detail** [**client-ip** *ip_address* | **server-ip** *ip_address* | **server-port** *port*]]

Syntax Description

connection	(Optional) Displays AppNav Controller connection statistics.
client-ip	(Optional) Displays the statistics for the client with the specified IP address.
ip_address	IP address of a client or server.
client-port *port*	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
server-ip	(Optional) Displays the statistics for the server with the specified IP address.
server-port *port*	(Optional) Displays the statistics for the server with the specified port number (1–65535).
detail	(Optional) Displays detailed statistics.
summary	(Optional) Displays summary statistics.
drop	(Optional) Displays statistics about dropped packets.
flow-asymmetry	(Optional) Displays statistics about asymmetric flows.
flow-management	(Optional) Displays flow learning statistics.
app-sess	(Optional) Displays application and session statistics.
appnav-controller-ip *ip_address*	(Optional) Displays flow-management statistics of the specified AppNav Controller.
flow-table	(Optional) Displays flow-table statistics.
syn	(Optional) Displays SYN statistics.
ip	(Optional) Displays IP-related statistics.
sessions	(Optional) Displays session statistics.

Defaults

No default behavior or values.

Command Modes EXEC

Device Modes appnav-controller

Related Commands **show appnav-controller flow-distribution**
show service-insertion
show statistics service-insertion

show statistics authentication

To display authentication statistics for a WAAS device, use the **show statistics authentication** EXEC command.

show statistics authentication

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show statistics authentication** command to display the number of authentication access requests, denials, and allowances recorded.

Examples

The following is sample output from the **show statistics authentication** command. It displays the statistics related to authentication on the WAAS device.

```
WAE# show statistics authentication
    Authentication  Statistics
    -------------------------------------
    Number of access requests:        115
    Number of access deny responses:  12
    Number of access allow responses: 103
```

Related Commands

(config) authentication configuration

clear arp-cache

show authentication

show statistics auto-discovery

To display Traffic Flow Optimization (TFO) auto-discovery statistics for a WAE, use the **show statistics auto-discovery** EXEC command.

show statistics auto-discovery [**blacklist**]

Syntax Description

blacklist	(Optional) Displays the blacklist server statistics.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-90 describes the result values shown for the statistics in the **show statistics application** command display.

Table 3-90 Result Value Descriptions for the show statistics auto-discovery Command

Result	Description
Auto discovery structure	
Allocation Failure	Number of auto-discovery allocation failures.
Allocation Success	Number of auto-discovery allocation successes.
Deallocations	Number of auto-discovery connections that were deallocated.
Timed Out	Number of autodiscovery allocations that timed out.
Auto discovery table	
Bucket Overflows	Number of auto-discovery table buffer overflows.
Table Overflows	Number of auto-discovery table overflows.
Entry Adds	Number of auto-discovery table option additions.
Entry Drops	Number of auto-discovery table option deletions.
Entry Count	Total number of auto-discovery table option entries.
Lookups	Number of auto-discovery table lookups performed.
Bind hash add failures	Number of hash table binds that failed.
Flow creation failures	Number of flow creation attempts that failed.
Route Lookup	
Failures	Number of route table lookups that failed.
Success	Number of route table lookups that succeeded.

Table 3-90 Result Value Descriptions for the show statistics auto-discovery Command

Result	Description
Socket	
Allocation failures	Number of socket allocations that failed.
Accept pair allocation failures	Number of socket pair allocations that failed.
Unix allocation failures	Number of Unix socket allocations that failed.
Connect lookup failures	Number of socket connection lookups that failed.
Packets	
Memory allocation failures	Number of packet memory allocations that failed.
Total Sent	Total number of auto-discovery packets sent.
Total Received	Total number of auto-discovery packets received.
Incorrect length or checksum received	Number of packets received with an incorrect length or checksum.
Invalid filtering tuple received	Number of packets received with an incorrect filtering tuple.
Received for dead connection	Number of packets received for invalid connections.
Ack dropped in synack received state	Number of acknowledgement packets dropped that were in the synchronize acknowledgement state.
Non Syn dropped in nostate state	Number on non-SYN packets dropped that were in the nostate state.
Syn-ack packets to int. client dropped	Number of synack packets dropped when being sent to internal client.
Packets dropped state already exists	Number of packets for which the dropped state already exists.
Auto discovery failure	
No peer or asymmetric route	Auto-discovery failed because no peer was found, or asymmetric routing configuration was indicated.
Insufficient option space	Auto-discovery failed because there was not enough space to add options.
Invalid option content	Auto-discovery failed because the content of an option was invalid.
Invalid connection state	Auto-discovery failed because the connection state was invalid.
Missing Ack conf	Auto-discovery failed because of missing auto discovery options that were sent from the edge WAE sends to the core WAE on the ack packet.
Intermediate device	Auto-discovery failed because a device was discovered between the WAEs.
Version mismatch	Auto-discovery failed because the WAAS software versions did not match.
Incompatible Peer AO	Auto-discovery failed because the peer accelerator is not compatible with the accelerator on this WAE.

Table 3-90 Result Value Descriptions for the show statistics auto-discovery Command

Result	Description
AOIM Sync with Peer still in progress	Auto-discovery failed because AOIM synchronization is still in progress between the peers.
Auto discovery success TO	
Internal server	Address of the internal server.
External server	Address of the external server.
Auto discovery success FOR	
Internal client	Address of the internal client.
External client	Address of the external client.
Auto discovery success SYN retransmission	
Zero retransmit	No retransmissions were required for auto-discovery SYN success.
One retransmit	One retransmission were required for auto-discovery SYN success.
Two+ retransmit	Two or more retransmissions were required for auto-discovery SYN success.
AO discovery	
AO discovery successful	Auto-discovery of an application optimizer was successful.
AO discovery failure	Auto-discovery of an application optimizer was not successful.
Auto discovery Miscellaneous	
RST received	Number of resets received.
SYNs found with our device id	Number of SYN packets received indicating WAE's device ID.
SYN retransmit count resets	Number of resets to the SYN retransmission count.
SYN-ACK sequence number resets (syncookies)	Number of SYN-ACK packets received with a sequence number reset.
SYN-ACKs found with our device id	Number of SYN-ACK packets received indicating WAE's device ID.
SYN-ACKs found with mirrored options	Number of SYN-ACK packets received with mirrored options.
Connections taken over for MAPI optimization	Number of connections taken over for MAPI acceleration from an overloaded serial cluster peer.

Related Commands

show auto-discovery

show statistics filtering

show statistics tfo

show statistics connection closed

show statistics cifs

To display the CIFS statistics information, use the **show statistics cifs** EXEC command.

show statistics cifs {**cache details** | **requests**}

Syntax Description

cache details	Specifies the statistics for the CIFS cache.
requests	Specifies the statistics for CIFS requests.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics cifs** EXEC command to view the CIFS traffic details itemized by request type. The **show statistics cifs** command is useful when you want to understand how the system is being used. For example, are requests mostly for data transfer, browsing, database activity, or for some other purpose? You might correlate these statistics with performance issues for troubleshooting purposes, or you may use them to determine what specific performance optimizations to configure.

Examples

Table 3-91 describes the fields in the **show statistics cifs requests** command display.

Table 3-91 Field Descriptions for the show statistics cifs requests Command

Field	Description
Statistics gathering period	Number of hours, minutes, seconds, and milliseconds of the statistics gathering period.
Total	Total number of CIFS requests.
Remote	Number of CIFS requests that were not handled from the local cache.
ALL_COMMANDS	Alias for all of the CIFS commands shown.
total	Total number of requests for all commands.
remote	Number of remote requests for all commands.
async	Number of async requests for all commands.
avg local	Average local request time in milliseconds for all commands.
avg remote	Average remote request time in milliseconds for all commands.
CONNECT	Connection check command.
total	Total number of requests for this command.

Table 3-91 Field Descriptions for the show statistics cifs requests Command (continued)

Field	Description
remote	Number of remote requests for this command.
async	Number of async requests for this command.
avg local	Average local request time in milliseconds for this command.
avg remote	Average remote request time in milliseconds for this command.
NB_SESSION_REQ	NetBIOS session request command.
VFN_LIVELINESS	Liveliness check command.

Related Commands show cifs

show statistics class-default

To display statistics information about the class-default class map, use the **show statistics class-default** EXEC command.

show statistics class-default top-talkers

Syntax Description		
	top-talkers	Displays the statistics for the top 10 ports with the most traffic.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Use the **show statistics class-default top-talkers** EXEC command to view statistics for traffic matched by the class-default class map. Statistics are displayed for the top 10 ports by traffic volume.

Examples

The following shows an example of output from the **show statistics class-default top-talkers** command.

```
WAE# show statistics class-default top-talkers
Rank    Port    Vol %                   Bytes                  Packets
----  -------  ------  ----------------------  ----------------------
         All  100.00             45759836065                 63801873
   1      80   94.44             43216161904                 52890647
   2     443    1.92               877275192                  4744341
   3    9182    0.00                   88010                      330
   4   34182    0.00                   87985                      324
   5   14660    0.00                   87894                      326
   6   49468    0.00                   82857                      299
   7   44180    0.00                   82746                      304
   8   29641    0.00                   82104                      292
   9   47835    0.00                   81966                      304
  10   20362    0.00                   81957                      314
```

Related Commands

clear statistics

show class-map

show statistics class-map

show statistics class-map

To display statistics information about class maps, use the **show statistics class-map** EXEC command.

show statistics class-map type {**appnav** *classmap-name* | **waas**
[**name** *classmap-name* | **summary** [**active** | **all**]]}

Syntax Description

appnav *classmap-name*	Displays statistics for the specified AppNav class map.
waas	Displays statistics for the specified WAAS optimization class map, or all class maps if no class map is specified.
name *classmap-name*	Displays statistics for the specified WAAS optimization class map.
summary	Displays summary statistics for all WAAS optimization class maps that have active and completed connections.
active	Displays summary statistics for all WAAS optimization class maps that have currently active connections.
all	Displays summary statistics for all WAAS optimization class maps.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Use the **show statistics class-map** EXEC command to view statistics for class maps.

Examples

The following is sample output from the **show statistics class-map type appnav** command.

```
WAE# show statistics class-map type appnav class-default
Class Map                        From Network to SN   From SN to Network
                                 ------------------   ------------------
class-default
  Redirected Client->Server:
    Bytes                                 5584092901           3184595397
    Packets                                 12921688             17283696
  Redirected Server->Client:
    Bytes                                  929015717            925076898
    Packets                                 12928444              9029525

Connections
-----------
    Intercepted by ANC                                          8071757
    Passed through by ANC                                        589152
    Redirected by ANC                                           7482605
    Accepted by SN                                              4351361
```

```
    Passed through by SN (on-Syn)                        3131231
    Passed through by SN (post-Syn)                      3191816


Passthrough Reasons                      Packets            Bytes
-------------------                      -------            -----
Collected by ANC:
   PT Flow Learn Failure                       0                0
   PT Cluster Degraded                         0                0
   PT SNG Overload                      12049460       2041789082
   PT AppNav Policy                            0                0
   PT Unknown                                  0                0

Indicated by SN:
   PT No Peer                           49500012      13070018416
   PT Rjct Capabilities                        0                0
   PT Rjct Resources                           0                0
   PT Rjct No License                          0                0
   PT App Config                        90563537       6966594435
   PT Global Config                            0                0
   PT Asymmetric                               0                0
   PT In Progress                              0                0
   PT Intermediate                             0                0
   PT Overload                                 0                0
   PT Internal Error                           0                0
   PT App Override                             0                0
   PT Server Black List                        0                0
   PT AD Version Mismatch                      0                0
   PT AD AO Incompatible                       0                0
   PT AD AOIM Progress                         0                0
   PT DM Version Mismatch                      0                0
   PT Peer Override                            0                0
   PT Bad AD Options                           0                0
   PT Non-optimizing Peer                      0                0
   PT SN Interception ACL                      0                0
   PT IP Fragment Unsupported                  0                0
   PT Flow Query Failure                       0                0
   PT Flow Intercept ACL deny                  0                0
                                        ------------     ------------
   PT Overall                           152113009      22078401933
```

Related Commands

show class-map

show statistics class-default

show statistics connection

To display all connection statistics for a WAAS device, use the **show statistics connection** EXEC command.

show statistics connection
client-ip {*ip_address* | *hostname*} | **client-port** *port* |
detail [**client-ip** {*ip_address* | *hostname*} | **client-port** *port* | **peer-id** *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*] |
peer-id *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*] | **conn-id** *connection_id*

Syntax Description

client-ip	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
detail	(Optional) Displays detailed connection statistics.
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).
conn-id *connection_id*	(Optional) Displays the connection statistics for the connection with the specified identifier.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The **show statistics connection** command displays the statistics for all TCP connections. This information is updated in real time.

Using the **show statistics connection** command with no options displays a summary of all the TCP connections on the WAE. To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as peer-id) show summary information and not details.

Examples

Table 3-92 describes the fields shown in the **show statistics connection** command display.

Table 3-92 Field Descriptions for the show statistics connection Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Reserved Flows	Number of connections reserved for the MAPI accelerator. It appears for all accelerators.
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
ConnID	Identification number assigned to the connection.
Source IP:Port	IP address and port of the incoming source connection.
Dest IP:Port	IP address and port of the outgoing destination connection.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, C = CIFS, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, N = NFS, S = SSL, W = WAN secure, V = video, X = signed SMB
Reduction Ratio (RR)	Relative reduction ratio (in bytes) for a particular connection.
Local IP:Port	IP address and port of the incoming local connection.
Remote IP:Port	IP address and port of the outgoing remote connection.
ConnType	Connection type (see Table 3-93).

Table 3-93 describes the possible values found in the ConnType field.

Table 3-93 Connection Types

ConnType	Description
Accelerator Non-Optimized	Connection has been initiated from an external client to an external server and is not optimized.
Accelerator Optimized	Connection has been initiated from an internal client to an external server and is optimized.

Table 3-93 Connection Types

ConnType	Description
App Dyn Mtch Non-Optimized	Connection has been forced through an application dynamic match and is non-optimized by an application accelerator, even though the connection may be optimized by TFO+DRE+LZ.
App Dyn Mtch Optimized	Connection has been forced through an application dynamic match to be optimized, even though the connection may be handled as pass-through.
PT AD Int Error	Connection encountered an internal error during processing by the TFO auto discovery SYN cache.
PT App Cfg	Policy action for this application is configured as pass-through.
PT App Override	Connection is pass-through because the internal application has explicitly requested that the connection not be optimized. This state would only occur if the connection would have otherwise been optimized.
PT Asym Client	Connection is pass-through due to the WAE only seeing one side of the TCP connection (where the src is the client and the dst is the server).
PT Asym Server	Connection is pass-through due to the WAE only seeing one side of the TCP connection (where the dst is the client and the src is the server).
PT Dst Cfg	Policy action for this application is configured as pass-through in the peer WAE.
PT FB Int Error	Connection encountered an internal error during processing by the filter bypass module.
PT_Glb Cfg	Global action is configured as pass-through; that is, TFO, DRE, or LZ are disabled globally on the WAE.
PT In Progress	Connection was already established when the first packet was seen by the WAE.
PT Interception ACL	Connection is pass-through due to an interception ACL denying optimization.
PT Intermediate	Connection is pass-through due to the WAE being in the middle of the best local and remote WAE's (relative to the client and server).
PT No Peer	Connection is pass-through due to no peer WAE being found during TFO auto-discovery.
PT Non-Optimizing Peer	Connection is pass-through because the only peer found is a serially clustered peer and optimization is disabled to the peer.
PT Overload	TFO application has indicated it is overloaded (that is, the maximum number of optimized connections has been exceeded). New connections not handled by an application accelerator are configured as pass-through.
PT PE Int Error	Connection encountered an internal error during processing by the policy engine.
PT Rjct Capabilities	Connection is pass-through due to auto discovery finding that the peer WAE does not have the required capabilities.

Table 3-93 Connection Types

ConnType	Description
PT Rjct Resources	Connection is pass-through due to auto discovery finding that the peer WAE does not have the required resources.
PT Server Blacklist	Connection is pass-through because the server is on the TFO blacklist as not supporting TCP Option (0x21) being present in the SYN packet.

Related Commands

clear arp-cache

show statistics accelerator

show statistics connection egress-methods

show statistics connection auto-discovery

To display auto-discovery connection statistics for a WAAS device, use the **show statistics connection auto-discovery** EXEC command.

show statistics connection auto-discovery
client-ip {*ip_address* | *hostname*} | **client-port** *port* | **peer-id** *peer_id* |
server-ip {*ip_address* | *hostname*} | **server-port** *port*

Syntax Description

auto-discovery	(Optional) Displays active connection statistics for auto-discovery connections.
client-ip	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

This command displays the statistics for auto-discovery TCP connections. This information is updated in real time.

To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as peer-id) show summary information and not details.

Examples

Table 3-94 describes the fields shown in the **show statistics connection auto-discovery** display.

Table 3-94 Field Descriptions for the show statistics connection auto-discovery Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
Local IP:Port	IP address and port of the incoming local connection.
Remote IP:Port	IP address and port of the outgoing remote connection.
PeerID	MAC address of the peer device.
O-ST	Origin state of the connection. E = Established, S = Syn, A = Ack, F = Fin, R = Reset, s = sent, r = received, O = Options, P = Passthrough
T-ST	Terminal state of the connection. E = Established, S = Syn, A = Ack, F = Fin, R = Reset, s = sent, r = received, O = Options, P = Passthrough
ConnType	Type of the connection (see Table 3-93).

Related Commands

show statistics accelerator

show statistics connection egress-methods

show statistics connection closed

To display closed connection statistics for a WAAS device, use the **show statistics connection closed** EXEC command.

show statistics connection closed
[**cifs** | **detail** | **dre** | **epm** | **http** | **mapi** | **nfs** | **ssl** | **tfo** | [**video** [**windows-media**]]
[**client-ip** {*ip_address* | *hostname*} | **client-port** *port* | **conn-id** *connection_id* |
peer-id *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port*]

Syntax Description

cifs	(Optional) Displays closed connection statistics for connections optimized by the CIFS application accelerator.
detail	(Optional) Displays detailed closed connection statistics.
dre	(Optional) Displays closed connection statistics for connections optimized by the DRE feature.
epm	(Optional) Displays closed connection statistics for connections optimized by the EPM application accelerator.
http	(Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.
mapi	(Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.
nfs	(Optional) Displays closed connection statistics for connections optimized by the NFS application accelerator.
ssl	(Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.
tfo	(Optional) Displays closed connection statistics for connections optimized by the TFO application accelerator.
video	(Optional) Displays closed connection statistics for connections optimized by the video application accelerator.
windows-media	(Optional) Displays active connection statistics for connections optimized by the video application accelerator for Windows Media streams.
client-ip	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
conn-id *connection_id*	(Optional) Displays closed connection statistics for the connection with the specified identifier.
peer-id *peer_id*	(Optional) Displays the closed connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Using the **show statistics connection closed** command with no options displays a summary of the closed TCP connections on the WAE. To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as peer-id) show summary information and not details.

Examples

Table 3-95 describes the fields shown in the **show statistics connection closed** command display.

Table 3-95 Field Descriptions for the show statistics connection closed Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
ConnID	Identification number assigned to the connection.
Source IP:Port	IP address and port of the incoming source connection.
Dest IP:Port	IP address and port of the outgoing destination connection.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, C = CIFS, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, N = NFS, S = SSL, W = WAN secure, V = video, X = signed SMB

Related Commands

clear arp-cache

show statistics accelerator
show statistics connection egress-methods

show statistics connection conn-id

To display connection ID statistics for a WAAS device, use the **show statistics connection conn-id** EXEC command.

show statistics connection conn-id *connection_id*

Syntax Description

connection_id	(Optional) Connection statistics for the connection with the specified identifier number.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The **show statistics connection conn-id** command displays the statistics for individual TCP connections. This information is updated in real time.

Examples

Table 3-91 describes the fields shown in the **show statistics connection conn-id** command display.

Table 3-96 Field Descriptions for the show statistics connection conn-id Command

Field	Description
Connection Information	
Peer ID	MAC address of the peer device.
Connection Type	Type of connection established with the peer.
Start Time	Date and time connection started.
Source IP Address	IP address of the connection source.
Source Port Number	Port number of the connection source.
Destination IP Address	IP address of the connection destination.
Destination Port Number	Port number of the connection destination.
Application Name	Name of the application traffic on the connection.
Classifier Name	Name of the application classifier on the connection.
Map Name	Name of the policy engine application map.
Directed Mode	State of directed mode: true (on) or false (off).

Table 3-96 Field Descriptions for the show statistics connection conn-id Command (continued)

Field	Description
Preposition Flow	Flow was originated by an accelerator to acquire data in anticipation of its future use: true or false.
Policy Details: Configured	Name of the configured application policy.
Policy Details: Derived	Name of the derived application policy.
Policy Details: Peer	Name of the application policy on the peer side.
Policy Details: Negotiated	Name of the negotiated application acceleration policy.
Policy Details: Applied	Name of the applied application acceleration policy.
Accelerator Details: Configured	Accelerators configured.
Accelerator Details: Derived	Accelerators derived.
Accelerator Details: Applied	Accelerators applied.
Accelerator Details: Hist	Accelerators historically used.
Original and Optimized Bytes Read/Written	Number of bytes that have been rear and written on the original (incoming) side and the optimized (outgoing) side.
DRE Stats	
Encode	Statistics for compressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for compressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for compression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
Avg Latency	Average latency (transmission delay) of the DRE traffic.
Encode Th-put	Speed of DRE traffic throughput, in kilobytes per second.
Message Size Distribution	Percentage of total messages that fall within indicated size ranges.
Connection Details	
Chunks	Number of chunks encoded, decode, and anchored (forced).
Total Messages	Total number of messages processed and the number of blocks used per message.
Ack [msg | size]	Number and size of acknowledgement messages.
Encode Bypass Due To	Reason for previous traffic encoding bypass.
Nack	Number and size of negative acknowledgement messages.
R-tx	Number of ready-to-transmit messages.
Aggregation Encode/Decode	Aggregated statistics for compressed messages.

Table 3-96 Field Descriptions for the show statistics connection conn-id Command (continued)

Field	Description
TFO Stats	
Conn-Type	Type of connection (see Table 3-93).
Policy	Policy in use on connection.
EOT State [write | req | ack | read | ack]	End of transmission state for data written and read.
Socket States	Socket states, including **read-shut**, **write-shut**, **close**, **choke**, and **envoy**.
DRE Hints [local | remote | active]	Number of DRE hints sent for the local, remote, and active connections.
Read Encode/Decode Flows	Number of encode and decode messages, and total bytes used.
Decoder Pending Queue	Size of the messages waiting in the decode queue, including maximum size, current size, average size, and the number of flow-control stop messages.
Encode/Decode	Number of calls encoded and decoded, the message latency (in ms), and the number of transmitted data/acknowledgment frames.
Writer Pending Queue	Size of the messages waiting in the write queue, including maximum size, current size, average size, and the number of flow-control stop messages.
Write	Size of the messages written, total number of messages, the average size, and the message latency (in ms).

Related Commands

clear arp-cache

show statistics accelerator

show statistics connection egress-methods

show statistics connection egress-methods

To display detailed egress method-related information about the connection segments for a WAE, use the **show statistics connection egress-methods** EXEC command.

show statistics connection egress-methods
client-ip {*ip_address* | *hostname*} | **client-port** *port* | **peer-id** *peer_id* |
server-ip {*ip_address* | *hostname*} | **server-port** *port*

Syntax Description

client-ip	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

Using the **show statistics connection egress-methods** command without options displays detailed information about each of the TFO connections for a WAE.

The **show statistics connection egress-methods** command displays egress method-related information about connection segments in an environment where the data flow from start-point to end-point is being transparently intercepted by multiple devices. A connection tuple represents one segment of an end-to-end connection that is intercepted by a WAAS device (WAE) for processing.

For example, a single client-server connection may have three segments (see Figure 3-1):

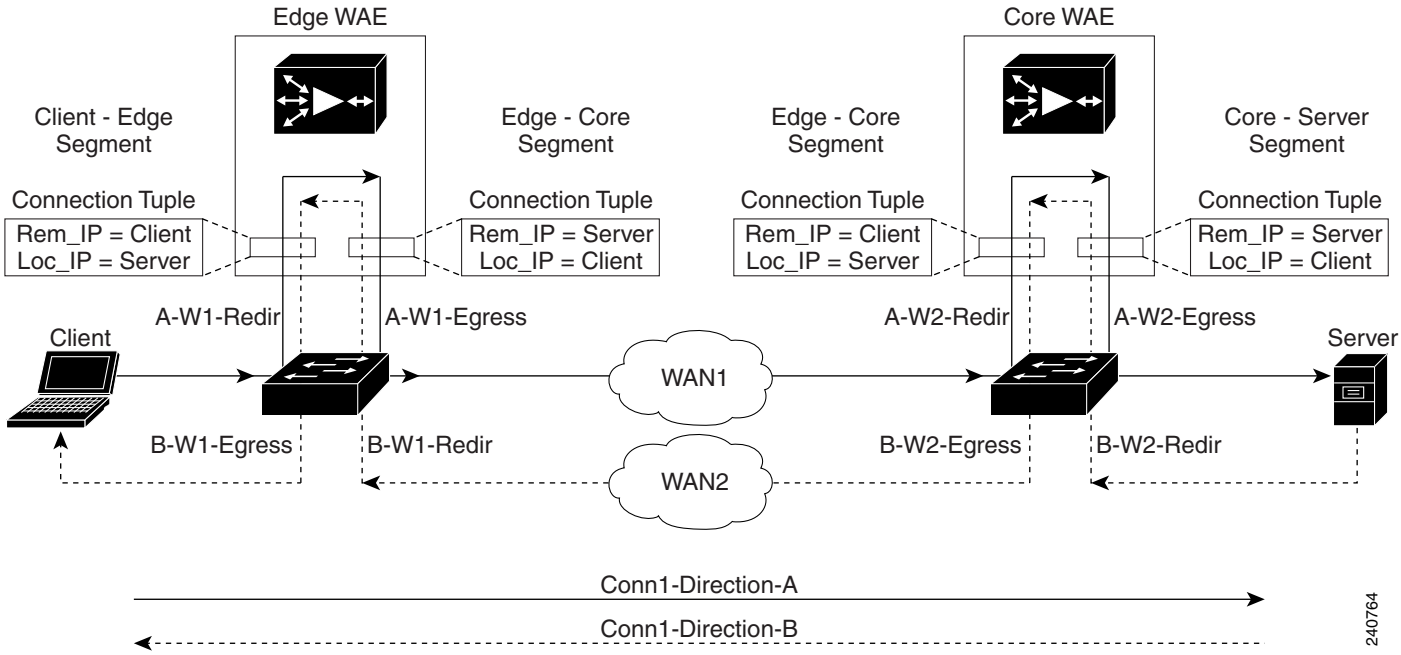
- Between the client and the Edge WAE
- Between the Edge WAE and the Core WAE
- Between the Core WAE and the server

In this example, the Edge WAE has two connection tuples for the two segments that it participates in the following:

- One connection tuple to represent the Client—Edge segment
- One connection tuple to represent the Edge—Core segment

In the **show** output, these two connection tuples appear as TUPLE and MATE. (See Table 3-97.) The important information to view is the local and remote IP address of the connection tuple and not whether it is marked as TUPLE or MATE.

Figure 3-1 Topology with Three Segments and Corresponding Connection Tuples



Because the WAAS device is transparent to both the client-end of the connection and the server-end of the connection, the local IP address for a connection tuple depends on the segment in the end-to-end topology.

For example, when WAAS intercepts a packet from the client, this packet enters the connection tuple that represents the Client—Edge segment. On this tuple, the WAAS device appears to the client as though it were the server: the local IP address in this connection tuple is the IP address of the server, while the remote IP address in this connection tuple is that of the client. Similarly, when the Edge WAE sends data to the client, the packet egresses from this connection tuple as though it were coming from the server.

When WAAS sends a packet to the server, the packet egresses from the connection tuple that represents the Edge—Core segment. On this tuple, the WAAS device appears to the server as though it were the client: the local IP address in the connection tuple is the IP address of the client, while the remote IP address in this connection tuple is that of the server. Similarly, when the Edge WAE intercepts a packet from the Core WAE, the data in this connection tuple appears to be coming from the server.

Examples

Table 3-97 describes the fields shown in the **show tfo egress-methods connection** command display.

Table 3-97 Field Descriptions for the show tfo egress-methods connection Command

Field	Description
TUPLE	
Local-IP:Port	IP address and port number of the local device in the connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the connection tuple.
MATE	
Local-IP:Port	IP address and port number of the local device in the mate connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the mate connection tuple.
Egress method	Egress method being used.
WCCP Service | Bucket	WCCP service number and bucket number for the connection tuple and mate connection tuple.
Tuple Flags	Flags for intercept method and intercept mechanism. This field may contain the following values: WCCP or NON-WCCP as the intercept method; L2 or GRE as the intercept mechanism; or PROT showing whether this tuple is receiving packets through the flow protection mechanism.
Intercepting device (ID)	
ID IP address	IP address of the intercepting device.
ID MAC address	MAC address of the intercepting device.
ID IP address updates	Number of IP address changes for the intercepting device.
ID MAC address updates	Number of MAC address changes for the intercepting device.
Memory address	Memory address.

Each time a packet enters the connection tuple, the intercepting device IP address or MAC address is recorded. The updates field in the command output indicates whether the intercepting device IP address or intercepting device MAC address has been recorded. If, for example, the ID MAC address updates field is zero (0), the MAC address was not recorded, and the ID MAC address field will be blank. The recorded intercepting device information is used when a packet egresses from the WAE.

If the egress method for the connection tuple is IP forwarding, the updates fields are always zero (0) because the intercepting device information is neither required nor recorded for the IP forwarding egress method.

If the intercept method is WCCP GRE redirect and the egress method is WCCP GRE, only the IP address field is updated and recorded. The MAC address information is neither required nor recorded because the destination address in the GRE header only accepts an IP address.

If the intercept method is WCCP L2 redirect and the egress method is WCCP GRE, both the MAC address and the IP address fields are updated and recorded because incoming WCCP L2 packets contain only a MAC header. The MAC address is recorded and the intercepting device IP address is derived from

a reverse ARP lookup and is then recorded, also. When packets egress the connection tuple in this scenario, they will have a GRE header with the destination IP address of the intercepting device that was recorded.

The updates count may be greater than 1 in certain topologies. For example, in a redundant router topology, where for the same direction of the same connection between two hosts, packets may be coming in from different intercepting routers. Each time a packet comes in, the intercepting device MAC or IP address is compared against the last recorded address. If the MAC or IP address has changed, the updates field is incremented and the new MAC or IP address is recorded.

Related Commands **show statistics tfo**

show statistics connection optimized

To display optimized connection statistics for a WAAS device, use the **show statistics connection optimized** EXEC command.

show statistics connection optimized
[**client-ip** {*ip_address* | *hostname*} | **client-port** *port* | **peer-id** *peer_id* | **server-ip** {*ip_address* | *hostname*} | **server-port** *port* |
{**cifs** | **http** | **ica** | **mapi** | **nfs** | **smb** | **ssl** | **wansecure** | **video** {**detail** | **windows-media** {**incoming** | **outgoing**} | **dre** { **all** | **savings** | {**cifs** | **http** | **ica** | **mapi** | **nfs** | **smb** | **ssl** | **video** | **wansecure**}}]

Syntax Description

optimized	(Optional) Displays active connection statistics for optimized connections.
client-ip	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	(Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).
cifs	(Optional) Displays closed connection statistics for connections optimized by the CIFS application accelerator.
http	(Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.
ica	(Optional) Displays closed connection statistics for connections optimized by the ICA application accelerator.
mapi	(Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.
nfs	(Optional) Displays closed connection statistics for connections optimized by the NFS application accelerator.
smb	(Optional) Displays the connection statistics for connections optimized by the SMB application accelerator.
ssl	(Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.
video	(Optional) Displays closed connection statistics for connections optimized by the video application accelerator.
wansecure	(Optional) Displays closed connection statistics for connections optimized by the WAN secure application accelerator.
detail	(Optional) Displays detailed closed connection statistics for connections optimized by the video application accelerator for Windows Media streams.
windows-media	(Optional) Displays active connection statistics for connections optimized by the video application accelerator for Windows Media streams.

incoming	(Optional) Displays active incoming connection statistics for connections optimized by the video application accelerator for Windows Media streams.
outgoing	(Optional) Displays active outgoing connection statistics for connections optimized by the video application accelerator for Windows Media streams.
dre	(Optional) Displays closed connection statistics for connections optimized by the DRE feature.
all	(Optional) Displays all the connection statistics for connections of the filtered type.
savings	(Optional) Displays the savings connection statistics for connections of the filtered type.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The **show statistics connection optimized** command displays the statistics for optimized TCP connections. This information is updated in real time.

Using the **show statistics connection optimized** command with no options displays a summary of all the optimized TCP connections on the WAE. To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as peer-id) show summary information and not details.

Examples

Table 3-98 describes the fields shown in the **show statistics connection optimized** command display.

Table 3-98 Field Descriptions for the show statistics connection optimized Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Active Reserved Flows	Number of reserved connections.

Table 3-98 Field Descriptions for the show statistics connection optimized Command

Field	Description
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
ConnID	Identification number assigned to the connection.
Source IP:Port	IP address and port of the incoming source connection.
Dest IP:Port	IP address and port of the outgoing destination connection.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, C = CIFS, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, N = NFS, S = SSL, W = WAN secure, V = video, X = signed SMB

Related Commands

clear arp-cache

show statistics accelerator

show statistics connection egress-methods

show statistics connection pass-through

To display pass through connection statistics for a WAAS device, use the **show statistics connection pass-through** EXEC command.

show statistics connection pass-through
client-ip {*ip_address* | *hostname*} | **client-port** *port* | **peer-id** *peer_id* |
server-ip {*ip_address* | *hostname*} | **server-port** *port*

Syntax Description

pass-through	Displays active connection statistics for pass-through connections.
client-ip	Displays the closed connection statistics for the client with the specified IP address or hostname.
ip_address	IP address of a client or server.
hostname	Hostname of a client or server.
client-port *port*	Displays the closed connection statistics for the client with the specified port number (1–65535).
peer-id *peer_id*	Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
server-ip	Displays the connection statistics for the server with the specified IP address or hostname.
server-port *port*	Displays the connection statistics for the server with the specified port number (1–65535).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The **show statistics connection pass-through** command displays the statistics for passed through TCP connections. This information is updated in real time.

Using the **show statistics connection pass-through** command with no options displays a summary of all the passed through TCP connections on the WAE. To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as peer-id) show summary information and not details.

Examples

Table 3-99 describes the fields shown in the **show statistics connection pass-through** command display.

Table 3-99 Field Descriptions for the show statistics connection pass-through Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
Local IP:Port	IP address and port of the incoming local connection.
Remote IP:Port	IP address and port of the outgoing remote connection.
PeerID	MAC address of the peer device.
ConnType	Status of the connection (see Table 3-93).

Related Commands

clear arp-cache

show statistics accelerator

show statistics connection egress-methods

show statistics crypto ssl ciphers

To display crypto SSL cipher usage statistics, use the **show statistics crypto ssl ciphers** EXEC command.

show statistics crypto ssl ciphers

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **show statistics crypto ssl ciphers** command displays the number of times each cipher was used on each segment of optimized flows.

Examples

Table 3-100 describes the fields shown in the **show statistics crypto ssl ciphers** command display.

Table 3-100 Field Descriptions for the show statistics crypto ssl ciphers Command

Field	Description
LAN	Segment between WAAS devices and client or server.
WAN	Segment between WAAS devices for data traffic.
Peering	Segment between WAAS devices for control traffic.

Related Commands

show crypto

show statistics datamover

To display statistics about the internal datamover component, use the **show statistics datamover** EXEC command.

show statistics datamover

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **show statistics datamover** command displays the statistics for the internal datamover component.

Examples

Table 3-104 describes the fields shown in the **show statistics datamover** command display.

Table 3-101 Field Descriptions for the show statistics datamover Command

Field	Description
Global Datamover Statistics	
Datamover users	Number of datamover clients (and Area blocks in the output).
Datamover container maps	Number of container_map structures allocated.
Datamover containers	Number of container structures allocated.
Datamover pages	Number of system pages used by datamover.
Datamover kmalloc areas	Number of kmalloc areas used by datamover.
Calls to cs_compact	Number of calls to cs_compact.
Container map allocation failures	Number of container_map structure allocation failures.
Container allocation failures	Number of container structure allocation failures.
Zone allocation failures	Number of zone allocation failures.
Kmem allocation failures	Number of kernel memory allocation failures.
Page allocation failures	Number of page allocation failures.
Area *n*	Name of application area. There is one Area block in the output for every datamover client.
Max Area size in pages	Total datamover size limit in pages.
Number of identifiers	Number of distinct datamover objects.

Table 3-101 Field Descriptions for the show statistics datamover Command (continued)

Field	Description
32 . . . 2048 byte areas used	Number of storage areas of each size.
Zone pages used	Number of pages used for the 32-2048 byte storage areas.
Non-zone pages used	Number of pages used for page mapping.
Cloned identifiers	Number of cloned identifiers.
Number of lookup stalls	Number of lookup stalls.
Calls to cs_compact	Number of calls to cs_compact.
Calls to cs_dup	Number of calls to cs_dup.
Calls to cs_send_bycopy	Number of calls to cs_send_bycopy.
Calls to cs_send_envoy	Number of calls to cs_send_envoy.
Calls to cs_recv_bycopy	Number of calls to cs_recv_bycopy.
Calls to cs_recv_envoy	Number of calls to cs_recv_envoy.
Identifier allocation failures	Number of identifier allocation failures.
Address allocation failures	Number of address allocation failures.
Total pages used	Number of pages used and percentage of the maximum area size used.

show statistics directed-mode

To directed mode statistics for a device, use the **show statistics directed-mode** EXEC command.

show statistics directed-mode

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-102 describes the fields shown in the **show statistics directed-mode** command display.

Table 3-102 Field Descriptions for the show statistics directed-mode Command

Field	Description
Cumulative number of connections	Cumulative number of directed mode connections.
Total outgoing packets encapsulated	Number of outgoing packets encapsulated.
Total incoming packets de-capsulated	Number of incoming packets decapsulated.
Total RST+OPT packets received and dropped	Number of RST packets with option 33 set that are received and dropped.
Outgoing packet encapsulation failed	Number of outgoing packet encapsulation failures.
Invalid incoming packets received	Number of invalid incoming packets.
Invalid packet length received	Number of incoming packets with an invalid length.
Incoming packet pullups needed	Number of incoming packets that were fragmented and needed copying from data fragments.
Incoming packets with inner fragments	Number of incoming packets with inner fragments.

Related Commands

clear arp-cache

show directed-mode

show statistics auto-discovery

show statistics connection closed

(config) directed-mode

show statistics dre

To display Data Redundancy Elimination (DRE) general statistics for a WAE, use the **show statistics dre** EXEC command,

show statistics dre [**detail**]

Syntax Description

detail	(Optional) Specifies to show detail.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-103 describes the fields shown in the **show statistics dre detail** command display. This command shows the aggregated statistics for all connections.

Table 3-103 Field Descriptions for the show statistics dre detail Command

Field	Description
Cache	Aggregated DRE cache data statistics.
Status	Current DRE status. Status values include: Initializing, Usable, and Fail.
Oldest Data (age)	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s). For example, “1d1h” means 1 day, 1 hour.
Total usable disk size	Total disk space allocated to the DRE cache.
Used (%)	Percentage of the total DRE cache disk space being used.
Cache details	
Replaced (last hour)	Amount of cache replaced within the last hour.
Connections	
Total (cumulative)	Total cumulative connections.
Active	Number of active connections.
Encode	
Overall: msg, in, out, ratio	All messages coming to DRE components. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).

Table 3-103 Field Descriptions for the show statistics dre detail Command

Field	Description
DRE: msg, in, out, ratio	All messages handled by DRE compression. Number of DRE compressed messages, input bytes, output bytes, compression ratio (in less out, divided by in).
DRE Bypass: msg, in	Number of messages bypassed by DRE. Number of messages, number of bytes.
LZ: msg, in, out, ratio	All messages handled by LZ. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).
LZ: bypass: msg, in	Number of messages bypassed by LZ. Number of messages, number of bytes.
Avg latency: ms, Delayed msg	Average latency introduced to compress a message.
Avg msg size	Average message size.
Message size distribution	Message sizes divided into six size groups. Number of messages in each group and their distribution percentage.
Decode	
Overall: msg, in, out, ratio	All messages coming to DRE components. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).
DRE: msg, in, out, ratio	All messages handled by DRE compression. Number of DRE compressed messages, input bytes, output bytes, compression ratio (in less out, divided by in).
DRE Bypass: msg, in	Number of messages bypassed by DRE. Number of messages, number of bytes.
LZ: msg, in, out, ratio	All messages handled by LZ. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).
LZ: bypass: msg, in	Number of messages bypassed by DRE. Number of messages, number of bytes.
Avg latency: ms	Average latency introduced to compress a message.
Avg msg size	Average message size.
Message size distribution	Message sizes divided into six size groups. Number of messages in each group and their distribution percentage.
Connection details	
Encode bypass due to: last partial chunk	Number of bypassed partial chunks and total size of bypassed chunks.
Nacks: total	Total NACKs.
R-tx: total	Total number of retransmissions.
Encode LZ latency: ms per msg, avg msg size	Encoding LZ latency in milliseconds per message and average message size in bytes.
Decode LZ latency: ms per msg, avg msg size	Decoding LZ latency in milliseconds per message and average message size in bytes.

Table 3-103 Field Descriptions for the show statistics dre detail Command

Field	Description
Cache write detail	
Disk size saving due to unidirectional mode	Amount of cache disk space saved due to using unidirectional caching mode.

Related Commands show statistics peer

show statistics filtering

To display statistics about the incoming and outgoing TFO flows that the WAE currently has, use the **show statistics filtering** EXEC command.

show statistics filtering

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **show statistics filtering** command displays statistics about the TCP flows that the WAE is handling.

Examples

Table 3-104 describes the fields shown in the **show statistics filtering** command display.

Table 3-104 Field Descriptions for the show statistics filtering Command

Field	Description
Number of filtering tuples	Number of filtering tuple structures.
Number of filtering tuple collisions	Number of times creation of duplicate filtering tuples was detected and avoided.
Packets dropped due to filtering tuple collisions	Number of packet drops resulting from duplicate filtering tuple detection. Not all duplicate tuple detection results in packet drops.
Number of transparent packets locally delivered	Number of incoming packets delivered to an application on the WAE that is optimizing the connection transparently.
Number of transparent packets dropped	Number of incoming transparent packets dropped.
Packets dropped due to ttl expiry	Number of incoming packets dropped because their TTL had reached 0.
Packets dropped due to bad route	Number of outgoing packets dropped because route lookup failed.
Syn packets dropped with our own id in the options	Syn packets output by the auto-discovery module that looped back to the WAE and were dropped.
Internal client syn packets dropped	Number of syn packets generated by a process on the WAE that were dropped.

Table 3-104 Field Descriptions for the show statistics filtering Command (continued)

Field	Description
Syn packets received and dropped on estab. conn	Number of syn packets received for a connection that was in established state. In established state, the syn packet is invalid and is dropped.
Syn-Ack packets received and dropped on estab. conn	Number of syn-ack packets received on a connection that was in established state. In established state, the syn-ack packet is invalid and is dropped.
Syn packets dropped due to peer connection alive	Number of syn packets received on a partially terminated connection. In this state, the syn is invalid and is dropped.
Syn-Ack packets dropped due to peer connection alive	Number of syn-ack packets received on a partially terminated connection. In this state, the syn-ack is invalid and is dropped.
Packets recvd on in progress conn. and not handled	Number of first packets on an in-progress connection that were dropped. If the first packet seen by the WAE for a connection is not a syn, it is called an in-progress connection.
Packets dropped due to peer connection alive	Number of packets received and dropped on a partially terminated connection.
Packets dropped due to invalid TCP flags	Number of TCP packets dropped because they had an invalid combination of the syn/find/ack/rst flags set.
Packets dropped by FB packet input notifier	Number of input packets dropped.
Packets dropped by FB packet output notifier	Number of output packets dropped.
Number of errors by FB tuple create notifier	Number of packets dropped because some action that was to be taken when a connection tuple is created failed.
Number of errors by FB tuple delete notifier	Number of packets dropped because some action that was to be taken when a connection tuple is destroyed failed.
Dropped WCCP GRE packets due to invalid WCCP service	Number of incoming packets received by WCCP GRE intercept that were dropped because of invalid WCCP service information.
Dropped WCCP L2 packets due to invalid WCCP service	Number of incoming packets received by WCCP L2 intercept that were dropped because of invalid WCCP service information.
Number of deleted tuple refresh events	Number of times invalid tuples were submitted for garbage collection.
Number of times valid tuples found on refresh list	Number of times valid tuples were reclaimed from the garbage collector.
SYN packets sent with non-opt option due to MAPI	Number of syn packets sent with the non-optimizing option due to the MAPI accelerator.
Internal Server conn. not optimized due to Serial Peer	Number of server connections not optimized because this device is in a serial cluster and is passing through the connections to its serial peer.

Table 3-104 Field Descriptions for the show statistics filtering Command (continued)

Field	Description
Duplicate packets to synq dropped	Number of dropped syn packets that were retransmitted and received for a connection while it was being processed in synq (without impacting the connection).
Number of ICMP Fragmentation Needed messages sent	Number of ICMP fragmentation needed messages sent.
Incorrect length or checksum received on Syn	Number of syn packets received with incorrect length or checksum.
Dropped optimized timewait sockets	Number of sockets in the time-wait state from a previous optimized connection that were dropped due to a new connection request.
Dropped non-optimized timewait sockets	Number of sockets in the time-wait state from a previous nonoptimized connection that were dropped due to a new connection request.

Related Commands

show filtering list

show statistics auto-discovery

show statistics connection closed

show statistics flow

To display flow statistics for a WAAS device, use the **show statistics flow** EXEC command.

show statistics flow {**filters** | **monitor type performance-monitor tcpstat-v1**} | **monitor** *MonitorName* | **exporter** *ExporterName*

Syntax Description

filters	Displays flow filter statistics.
monitor type	Displays flow performance statistics.
tcpstat-v1	Displays tcpstat-v1 collector statistics.
monitor *MonitorName*	Displays statistics for a specified flow monitor.
exporter *ExporterName*	Displays statistics for a specified exporter.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-105 describes the fields shown in the **show statistics flow filters** command display.

Table 3-105 Field Descriptions for the show statistics flow filters Command

Field	Description
Number of Filters	Number of filters.
Status	Status of whether the filters are enabled or disabled.
Capture Mode	Operation of the filter. Values include FILTER or PROMISCUOUS. The promiscuous operation is not available in WAAS.
Server	IP address list of the servers for which flows are being monitored.
Flow Hits	Number of flow hits for each server.
Flags	Flags identifying the flows. CSN: Client-Side Non-Optimized (Edge) SSO: Server-Side Optimized (Edge) CSO: Client-Side Optimized (Core) SSN: Server-Side Non-Optimized (Core) PT: Pass Through (Edge/Core/Intermediate) IC: Internal Client

Table 3-106 describes the fields shown in the **show statistics flow monitor** command display.

Table 3-106 Field Descriptions for the show statistics flow monitor Command

Field	Description
Host Connection	
Configured host address	IP address of the tcpstat-v1 console for the connection.
Connection State	State of the connection.
Connection Attempts	Number of connection attempts.
Connection Failures	Number of connection failures.
Last connection failure	Date and time of the last connection failure.
Last configuration check sent	Date and time that the last configuration check was sent.
Last registration occurred	Date and time that the last registration occurred.
Host Version	Version number of the tcpstat-v1 console for the connection.
Collector Connection	
Collector host address:port	IP address and port number of the tcpstat-v1 aggregator identified through the host connection.
Connection State	State of the connection.
Connection Attempts	Number of connection attempts.
Connection Failures	Number of connection failures.
Last connection failure	Date and time of the last connection failure.
Last configuration check sent	Date and time that the last configuration check was sent.
Last update sent	Date and time that the last update was sent.
Updates sent	Number of updates sent.
Summaries discarded	Number of summaries that were discarded because disk space allocated for storage has reached its limit. The numbers in this field indicate when summaries are being collected faster than they are able to be transferred to the collector. Counters in this field generate a data_update alarm.
Last registration occurred	Date and time that the last registration occurred.
Host Version	Version number of the tcpstat-v1 aggregator for the connection.
Collection Statistics	
Collection State	State of the summary collection operation.
Summaries collected	Number of summaries collected. Summaries are packet digests of the traffic that is being monitored.
Summaries dropped	Total number of summaries dropped. This is the sum of the following subcategories.
Dropped by TFO	Number of packets that were dropped by TFO because of an error, such as not being able to allocate memory.

Table 3-106 Field Descriptions for the show statistics flow monitor Command (continued)

Field	Description
Dropped due to backlog	Number of packets that were dropped because the queue limit has been reached. This counter indicates whether the flow monitor application can keep up with the number of summaries being received.
Summary backlog	Number of packets that are waiting in the queue to be read by the collector module on the WAE.
Last drop occurred	Date and time that the last packet drop occurred.

Related Commands clear arp-cache

show statistics generic-gre

To view the GRE tunnel statistics for each intercepting router, use the **show statistics generic-gre** EXEC command.

show statistics generic-gre

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **clear statistics generic-gre** EXEC command to clear the generic GRE statistics.

Examples

Table 3-107 describes the fields shown in the **show statistics generic-gre** command display.

Table 3-107 Field Descriptions for the show statistics generic-gre Command

Field	Description
Tunnel Destination	IP address of the GRE tunnel destination.
Tunnel Peer Status	Tunnel peer status. When the egress method is not generic GRE, N/A is shown.
Tunnel Reference Count	Number of connections using the tunnel.
Packets dropped due to failed encapsulation	Number of generic GRE packets dropped due to failed encapsulation.
Packets dropped due to no route found	Number of generic GRE packets dropped due to no route found.
Packets sent	Number of generic GRE packets sent.
Packets sent to tunnel interface that is down	Number of generic GRE packets sent to a tunnel interface that is down.
Packets fragmented	Number of outgoing generic GRE packets fragmented.

Related Commands

clear arp-cache

show statistics icmp

To display ICMP statistics for a WAAS device, use the **show statistics icmp** EXEC command.

show statistics icmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-108 describes the fields shown in the **show statistics icmp** command display.

Table 3-108 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 3-108 Field Descriptions for the show statistics icmp Command (continued)

Field	Description
ICMP messages sent	Total total number of ICMP messages which this entity attempted to send. This counter includes all those counted as ICMP output errors.
ICMP messages send failed	Number of number of ICMP messages which this entity did not send because of problems discovered within ICMP, such as a lack of buffers.
Destination unreachable	Number of ICMP messages of this type sent out.
Time exceeded	Number of ICMP messages of this type sent out.
Wrong parameters	Number of ICMP messages of this type sent out.
Source quenches	Number of ICMP messages of this type sent out.
Redirects	Number of ICMP messages of this type sent out.
Echo requests	Number of ICMP messages of this type sent out.
Echo replies	Number of ICMP messages of this type sent out.
Timestamp requests	Number of ICMP messages of this type sent out.
Timestamp replies	Number of ICMP messages of this type sent out.
Address mask requests	Number of ICMP messages of this type sent out.
Address mask replies	Number of ICMP messages of this type sent out.

Related Commands clear arp-cache

show statistics ip

To display IP statistics for a WAAS device, use the **show statistics ip** EXEC command.

show statistics ip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-109 describes the fields shown in the **show statistics ip** command display.

Table 3-109 Field Descriptions for the show statistics ip Command

Field	Description
IP statistics	
Total packets in	Total number of input datagrams received from interfaces, including all those counted as input errors.
with invalid address	Number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as 0.0.0.0) and addresses of unsupported classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
with invalid header	Number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatches other format errors, time-to-live exceeded errors, and errors discovered in processing their IP options.
forwarded	Number of input datagrams for which this entity was not their final IP destination, and as a result, an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were source-routed by way of this entity, and the source-route option processing was successful.

Table 3-109 Field Descriptions for the show statistics ip Command (continued)

Field	Description
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).
Total packets out	Total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
dropped	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (such as, for lack of buffer space). This counter includes datagrams counted in the forwarded field if any such packets meet this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in the forwarded field which meet this no-route criterion, including any datagrams that a host cannot route because all of its default gateways are down.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Total number of IP datagrams that have been successfully fragmented at this entity.
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented because their Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Related Commands **clear arp-cache**

(config) ip

(config-if) ip

show ip routes

show statistics monitor appnav-controller traffic

To display traffic monitoring statistics for an AppNav Controller Interface Module, use the **show statistics monitor appnav-controller traffic** EXEC command.

show statistics monitor appnav-controller traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Examples

The following is sample output from the **show statistics monitor appnav-controller traffic** command:

```
anc# show statistics monitor appnav-controller traffic
APPNAV CONTROLLER TRAFFIC MONITOR REPORT

Monitoring Access Control List Name: myacl

                                From Network to SN   From SN to Network
                                ------------------   ------------------
  Redirected Client->Server:
    Bytes                                        0                    0
    Packets                                      0                    0
  Redirected Server->Client:
    Bytes                                        0                    0
    Packets                                      0                    0

Connections
-----------
    Intercepted by ANC                                        0
    Passed through by ANC                                     0
    Redirected by ANC                                         0
    Accepted by SN                                            0
    Passed through by SN (on-Syn)                             0
    Passed through by SN (post-Syn)                           0

Passthrough Reasons                          Packets            Bytes
-------------------                          -------            -----
Collected by ANC:
   PT Flow Learn Failure                           0                0
   PT Cluster Degraded                             0                0
   PT SNG Overload                                 0                0
   PT AppNav Policy                                0                0
   PT Unknown                                      0                0

Indicated by SN:
   PT No Peer                                      0                0
```

```
PT Rjct Capabilities                          0                0
PT Rjct Resources                             0                0
PT Rjct No License                            0                0
PT App Config                                 0                0
PT Global Config                              0                0
PT Asymmetric                                 0                0
PT In Progress                                0                0
PT Intermediate                               0                0
PT Overload                                   0                0
PT Internal Error                             0                0
PT App Override                               0                0
PT Server Black List                          0                0
PT AD Version Mismatch                        0                0
PT AD AO Incompatible                         0                0
PT AD AOIM Progress                           0                0
PT DM Version Mismatch                        0                0
PT Peer Override                              0                0
PT Bad AD Options                             0                0
PT Non-optimizing Peer                        0                0
PT SN Interception ACL                        0                0
PT IP Fragment Unsupported                    0                0
PT Cluster Member                             0                0
PT Flow Query Failure                         0                0
PT Flow Intercept ACL deny                    0                0
                                     ------------     ------------
PT Overall                                    0                0
```

Related Commands

clear statistics monitor appnav-controller traffic

monitor appnav-controller traffic

show monitor

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 3-110 describes the fields shown in the **show statistics netstat** command display.

Table 3-110 Field Descriptions for the show statistics netstat Command

Field	Description
Active Internet connections (w/o servers)	The following output prints the list of all open Internet connections to and from this WAE.
Proto	Layer 4 protocol used on the Internet connection, such as, TCP, UDP, and so forth.
Recv-Q	Amount of data buffered by the Layer 4 protocol stack in the receive direction on a connection.
Send-Q	Amount of data buffered by the Layer 4 precool stack in the send direction on a connection.
Local Address	IP address and Layer 4 port used at the WAE end point of a connection.
Foreign Address	IP address and Layer 4 port used at the remote end point of a connection.
State	Layer 4 state of a connection. TCP states include the following: ESTABLISHED, TIME-WAIT, LAST-ACK, CLOSED, CLOSED-WAIT, SYN-SENT, SYN-RCVD, SYN-SENT, SYN-ACK-SENT, and LISTEN.

show statistics pass-through

To display pass-through traffic statistics for a WAAS device, use the **show statistics pass-through** EXEC command.

show statistics pass-through

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-111 describes the fields shown in the **show statistics pass-through** command display.

Table 3-111 Field Descriptions for the show statistics pass-through Command

Field	Description
Outbound	
PT Client: Bytes	Number of bytes passed through in the client to server direction.
PT Client: Packets	Number of packets passed through in the client to server direction.
PT Server: Bytes	Number of bytes passed through in the server to client direction.
PT Server: Packets	Number of packets passed through in the server to client direction.
PT In Progress: Bytes	Number of bytes passed through in progress.
PT In Progress: Packets	Number of packets passed through in progress.
Active/Completed	
Overall	Total number of connections passed through.
No Peer	Number of connections passed through because a remote peer WAE was not found.
Rjct Capabilities	Number of connections passed through due to capability mismatch.
Rjct Resources	Number of connections passed through due to unavailability of resources.
Rjct No License	Number of connections passed through due to no license.
App Config	Number of connections passed through due to policy configuration.
Global Config	Number of connections passed through due to optimization being disabled globally.
Asymmetric	Number of connections passed through due to asymmetric routing in the network (could be an interception problem).

Table 3-111 Field Descriptions for the show statistics pass-through Command (continued)

Field	Description
In Progress	Number of connections passed through due to connections seen by the WAE mid-stream.
Intermediate	Number of connections passed through because the WAE was in between two other WAEs.
Internal Error	Number of connections passed through due to miscellaneous internal errors such as memory allocation failures, and so on.
App Override	Number of connections passed through because an application accelerator requested the connection to be passed through.
Server Black List	Number of connections passed through due to the server IP being present in the black list.
AD Version Mismatch	Number of connections passed through due to auto discovery version incompatibility.
AD AO Incompatible	Number of connections passed through due application accelerator versions being incompatible.
AD AOIM Progress	Number of connections passed through due to ongoing peer negotiations.
DM Version Mismatch	Number of connections passed through because directed mode, though enabled locally, is not supported by the peer device.
Peer Override	Number of connections passed through due to an upstream serial peer handling optimization and telling this WAE not to optimize the connection.
Bad AD Options	Number of connections passed through due to invalid auto discovery options.
Non-optimizing Peer	Number of connections passed through because the only peer found is configured as a non-optimizing serial peer.
Interception ACL	Number of connections passed through due to an interception ACL denying them.

show statistics peer

To display peer Data Redundancy Elimination (DRE) statistics for a WAE, use the **show statistics peer** EXEC command.

show statistics peer

show statistics peer dre [**context** *context-value* | **peer-id** *peer-id* | **peer-ip** *ip-address* | **peer-no** *peer-no*]

show statistics peer dre detail [**context** *context-value* | **peer-id** *peer-id* | **peer-ip** *ip-address* | **peer-no** *peer-no*]]

Syntax Description

dre	Displays the peer DRE statistics.
context *context-value*	Displays peer statistics for the specified context (0–4294967295).
peer-id *peer-id*	(Optional) Specifies the MAC address of the peer (0–4294967295).
peer-ip *ip_address*	(Optional) Specifies the IP address of the peer.
peer-no *peer-no*	(Optional) Specifies the peer number.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-112 describes the fields shown in the **show statistics peer dre detail** command display. This command shows the peer DRE device connection information.

Table 3-112 Field Descriptions for the show statistics peer dre detail Command

Field	Description
Current number of peers with active connections	Number of peer devices with active connections to this device.
Maximum number of peers with active connections	Maximum number of peer devices with active connections to this device (since reboot).
Active peer details	
Peer-No	Number assigned to the peer compression device.
Context	Context ID for the DRE debugging trace.
Peer-ID	MAC address of the peer device.
Hostname	Hostname of the peer device.
IP reported from peer	IP address reported from the peer device.

Table 3-112 Field Descriptions for the show statistics peer dre detail Command (continued)

Field	Description
Cache	DRE cache data statistics as shown by the peer.
Used disk:	Number of megabytes (MB) used on the disk for the DRE cache.
Age:	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s).
Connections:	
Total (cumulative):	Number of cumulative connections that have been processed.
Active:	Number of connections that are still open.
Concurrent connections (Last 2 min):	
max	Maximum number of concurrent connections in the last two minutes.
avg	Average number of concurrent connections in the last two minutes.
Encode	Statistics for compressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for compressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for compression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for compression.
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Decode	Statistics for decompressed messages.
Overall: [msg | in | out | ratio]	Aggregated statistics for decompressed messages. msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were decompressed.
DRE: [msg | in | out | ratio]	Number of DRE messages.
DRE Bypass: [msg | in]	Number of DRE messages that were bypassed for decompression.
LZ: [msg | in | out | ratio]	Number of LZ messages.
LZ Bypass: [msg | in]	Number of LZ messages that were bypassed for decompression.

Table 3-112 Field Descriptions for the show statistics peer dre detail Command (continued)

Field	Description
Latency (Last 3 sec): [max | avg]	Maximum time to decompress one message for both DRE and LZ in milliseconds (ms). Average time to decompress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Connection details	
Encode bypass due to: last partial chunk	Number of bypassed partial chunks and total size of bypassed chunks.
Nacks: total	Total NACKs.
R-tx: total	Total number of retransmissions.
Encode LZ latency: ms per msg, avg msg size	Encoding LZ latency in milliseconds per message and average message size in bytes.
Decode LZ latency: ms per msg, avg msg size	Decoding LZ latency in milliseconds per message and average message size in bytes.
Cache write detail	
Disk size saving due to unidirectional mode	Amount of cache disk space saved due to using unidirectional caching mode.

Related Commands **show statistics connection closed**

show statistics policy-sub-class

To display the statistics for an AppNav class map, use the **show statistics policy-sub-class** EXEC command.

show statistics policy-sub-class type appnav [**level1-class** *classmap-name* [**level2-class** *classmap-name*]]

Syntax Description

appnav	Displays statistics for all of the class maps in the active AppNav policy map.
level1-class *classmap-name*	Displays statistics for the specified class map in the top-level policy map, including all class maps in nested policies.
level2-class *classmap-name*	Displays statistics for the specified class map in a nested policy map.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Usage Guidelines

The **show statistics policy-sub-class type appnav** command displays statistics for all the class maps in the active AppNav policy map and any nested policy maps.

The **show statistics policy-sub-class type appnav level1-class** *classmap-name* command displays statistics for the specified class map in the top-level AppNav policy map, including statistics for all class maps in any nested policies. The nested policy class maps display statistics only from connections that match both the top-level and nested class maps.

The **show statistics policy-sub-class type appnav level1-class** *classmap-name* **level2-class** *classmap-name* command displays statistics for the specified class map in a nested AppNav policy map. The nested policy class map displays statistics only from connections that match both the top-level and nested class maps.

Examples

The following is sample output from the **show statistics policy-sub-class type appnav** command for a nested class map.

```
ANC# show statistics policy-sub-class type appnav level1 class-default level2 HTTP
Service-insertion service-policy : appnav_default
    Class class-map              : class-default
        service-policy           : waas_app_default
            Class                : HTTP
Class Map                         From Network to SN   From SN to Network
                                 --------------------   ------------------

HTTP
  Redirected Client->Server:
    Bytes                                 842666098           6195601143
```

```
    Packets                                 11090593             64000604
  Redirected Server->Client:
    Bytes                                179727547324           5174359780
    Packets                                126653705             10353111

Connections
-----------
    Intercepted by ANC                                          344769
    Passed through by ANC                                        11097
    Redirected by ANC                                           333672
    Accepted by SN                                              333672
    Passed through by SN (on-Syn)                                    0
    Passed through by SN (post-Syn)                             169968


Passthrough Reasons                     Packets            Bytes
-------------------                     -------            -----
Collected by ANC:
   PT Flow Learn Failure                        0                0
   PT Cluster Degraded                          0                0
   PT SNG Overload                       15033190       10912861203
   PT AppNav Policy                             0                0
   PT Unknown                                   0                0

Indicated by SN:
   PT No Peer                           256892646      194277965057
   PT Rjct Capabilities                         0                0
   PT Rjct Resources                            0                0
   PT Rjct No License                           0                0
   PT App Config                                0                0
   PT Global Config                             0                0
   PT Asymmetric                                0                0
   PT In Progress                               0                0
   PT Intermediate                              0                0
   PT Overload                                  0                0
   PT Internal Error                            0                0
   PT App Override                              0                0
   PT Server Black List                         0                0
   PT AD Version Mismatch                       0                0
   PT AD AO Incompatible                        0                0
   PT AD AOIM Progress                          0                0
   PT DM Version Mismatch                       0                0
   PT Peer Override                             0                0
   PT Bad AD Options                            0                0
   PT Non-optimizing Peer                       0                0
   PT SN Interception ACL                       0                0
   PT IP Fragment Unsupported                   0                0
   PT Cluster Member                            0                0
   PT Flow Query Failure                        0                0
   PT Flow Intercept ACL deny                   0                0
                                        ------------     ------------
   PT Overall                           271925836      205190826260
```

Related Commands

- (config) policy-map
- show class-map
- show policy-map
- show policy-sub-class

show statistics punt

To display punt statistics, use the **show statistics punt** EXEC command.

show statistics punt

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Examples

The following is sample output from the **show statistics punt** command.

```
ANC# show statistics punt
Packets received from data-plane                      : 283841
Packets sent to data-plane                            : 179872
Packets received from punt clients                    : 179872
Packets sent to punt clients                          : 283840
Packet queue size                                     : 1
Packets dropped                                       : 0
   Packets with unsupported packet type               : 0
   Packets from unknown interface                     : 0
   Packets with invalid size                          : 0
   Packets with invalid punt reason                   : 0
   Packets exceeded max size                          : 0
   Packets dropped due to insufficient memory         : 0
   Packets dropped due to insufficient recv buffer    : 0
   Packets dropped due to client unavailability       : 0
   Packets dropped due to premature closure of socket : 0
Client count                                          : 2
   DIAG PKT                                           : 1
   DUMP                                               : 0
   TRACE                                              : 0
   DUMP AND TRACE                                     : 0
   STATISTICS                                         : 1
   PUNT PKT CAPTURE                                   : 0
```

Related Commands

clear statistics

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 3-113 describes the fields shown in the **show statistics radius** command display.

Table 3-113 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 3-113 Field Descriptions for the show statistics radius Command (continued)

Field	Description
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands

clear arp-cache

(config) radius-server

show radius-server

show statistics service-insertion

To display statistics about the entities (WNs, WNGs, ANCs, ANCG, and a service context) defined in an AppNav Cluster configuration, use the **show statistics service-insertion** EXEC command.

show statistics service-insertion {**appnav-controller** *ip_address* | **appnav-controller-group** [**detail**] | **data-path** | **service-context** | **service-node** [*ip_address*] | **service-node-group** [**detail** | **name** *sng-name*]}

Syntax Description

appnav-controller *ip_address*	(Optional) Displays statistics about the specified ANC.
appnav-controller-group	(Optional) Displays ANCG statistics for the service context.
detail	(Optional) Displays detailed statistics.
data-path	(Optional) Displays data path statistics.
service-context	(Optional) Displays service context statistics.
service-node	(Optional) Displays service node (WN) statistics.
ip_address	(Optional) Displays service node statistics of the specified node.
service-node-group	(Optional) Displays statistics for all the service node groups (WNGs) in the service context.
name *sng-name*	(Optional) Displays statistics of the specified node group (WNG).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

appnav-controller

Related Commands

show statistics appnav-controller

show service-insertion

show statistics services

To display services statistics for a WAAS device, use the **show statistics services** EXEC command.

show statistics services

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-114 describes the fields shown in the **show statistics services** command display.

Table 3-114 Field Descriptions for the show statistics services Command

Field	Description
Port Statistics	Service-related statistics for each port on the WAAS device.
Port	Port number.
Total Connections	Number of total connections.

Related Commands

show services

show statistics sessions

To display the dynamic match session statistics, use the **show statistics sessions** EXEC command.

show statistics sessions [**detail**] [**app-id** {*app-id* | **mapi** | **ms-ad-rep** | **ms-exch-nspi** | **ms-frs** | **ms-frs-api** | **ms-rfr** | **ms-sql** | **msn-messenger** | **netlogon**}]

Syntax Description

detail	(Optional) Displays the detailed session statistics for all of the dynamic match sessions or for the specified traffic type.
app-id *app-id*	(Optional) Displays the session statistics for dynamic matched flows for the application with the specified application number (0-1023) or the specified traffic type.
mapi	Microsoft Exchange MAPI aka Exchange Server Store EMSMDB,
ms-ad-rep	Microsoft Active Directory Replication (drsuapi),
ms-exch-nspi	Microsoft Active Directory Name Service Provider (NSP),
ms-frs	Microsoft File Replication Services (FRS),
ms-frs-api	Microsoft File Replication API,
ms-rfr	Microsoft Exchange Directory RFR Interface,
ms-sql	Microsoft SQL,
msn-messenger	Microsoft Messenger Service,
netlogon	Netlogon RPC

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The **show statistics sessions** command displays session statistics for all the dynamic matched flows. You can optionally specify an application ID or traffic type identifier to see session statistics for only that traffic type.

The **show statistics sessions details** command displays detailed session statistics for all the dynamic matched flows. You can optionally specify an application ID or traffic type identifier to see detailed session statistics for only that traffic type.

Related Commands

(config) policy-map

show class-map

show policy-map

show policy-sub-class

show statistics snmp

To display SNMP statistics for a WAAS device, use the **show statistics snmp** EXEC command.

show statistics snmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-115 describes the fields shown in the **show statistics snmp** command display.

Table 3-115 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 3-115 Field Descriptions for the show statistics snmp Command (continued)

Field	Description
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Related Commands

show snmp

(config) snmp-server user

(config) snmp-server view

show statistics synq

To display the cumulative statistics for the SynQ module, use the **show statistics synq** EXEC command.

show statistics synq

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics synq** command to display statistics for the SynQ module.

Examples

The following is sample output from the **show statistics synq** command:

```
WWAE# show statistics synq
Synq structures allocations success:                    0
Synq structures allocations failure:                    0
Synq structures deallocations:                          0
Synq table entry adds:                                  0
Synq table entry drops:                                 0
Synq table entry lookups:                               0
Synq table overflows:                                   0
Synq table entry count:                                 0
Packets received by synq:                               0
Packets received with invalid filtering tuple:          0
Non-syn packets received:                               0
Locally originated/terminating syn packets received:    0
Retransmitted syn packets received while in Synq:       0
Synq user structure allocations success:                0
Synq user structure allocations failure:                0
Synq user structure deallocations:                      0
Invalid packets received 0
```

Related Commands

show synq list

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 3-116 describes the fields shown in the **show statistics tacacs** command display.

Table 3-116 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 3-116 Field Descriptions for the show statistics tacacs Command (continued)

Field	Description
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands

clear arp-cache

(config) tacacs

show tacacs

show statistics tcp

To display TCP statistics for a WAAS device, use the **show statistics tcp** EXEC command.

show statistics tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-117 describes the fields shown in the **show statistics tcp** command display.

Table 3-117 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 3-117 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
Segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Bad segments received	Number of bad segments received.
Segments retransmitted	Total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
TCP memory usage (KB)	TCP memory usage.
TCP extended statistics	
Sync cookies sent	Number of SYN-ACK packets sent with SYN cookies in response to SYN packets.
Sync cookies received	Number of ACK packets received with the correct SYN cookie that was sent in the SYN-ACK packet by the device.
Sync cookies failed	Number of ACK packets received with the incorrect SYN cookie that was sent in the SYN-ACK packet by the device.
Embryonic connection resets	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state, the SYN-SENT state, or the SYN-ACK-SENT state.
Prune message called	Number of times that the device exceeded the memory pool allocated for the connection.
Packets pruned from receive queue	Number of packets dropped from the receive queue of the connection because of a memory overrun.
Out-of-order-queue pruned	Number of times that the out-of-order queue was pruned because of a memory overrun.
Out-of-window Icmp messages	Number of ICMP packets received on a TCP connection that were out of the received window.
Lock dropped Icmp messages	Number of ICMP packets dropped because the socket is busy.
Arp filter	Number of ICMP responses dropped because of the ARP filter.
Time-wait sockets	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets recycled	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets killed	Number of times that the TCP connection made a transition to the CLOSED state from TIME-WAIT state.
PAWS passive	Number of incoming SYN packets dropped because of a PAWS check failure.
PAWS active	Number of incoming SYN-ACK packets dropped because of a PAWS check failure.
PAWS established	Number of packets dropped in ESTABLISHED state because of a PAWS check failure.
Delayed acks sent	Number of delayed ACKs sent.

Table 3-117 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
Delayed acks blocked by socket lock	Number of delayed ACKs postponed because the socket is busy.
Delayed acks lost	Number of delayed ACKs lost.
Listen queue overflows	Number of incoming TCP connections dropped because of a listening server queue overflow.
Connections dropped by listen queue	Number of incoming TCP connections dropped because of an internal error.
TCP packets queued to prequeue	Number of incoming TCP packets prequeued to a process.
TCP packets directly copied from backlog	Number of incoming TCP packets copied from the backlog queue directly to a process.
TCP packets directly copied from prequeue	Number of incoming TCP packets copied from the prequeue directly to a process.
TCP prequeue dropped packets	Number of packets removed from the TCP prequeue.
TCP header predicted packets	Number of TCP header-predicted packets.
Packets header predicted and queued to user	Number of TCP packets header-predicted and queued to the user.
TCP pure ack packets	Number of ACK packets received with no data.
TCP header predicted acks	Number of header-predicted TCP ACK packets.
TCP Reno recoveries	Number of TCP Reno recoveries.
TCP SACK recoveries	Number of TCP SACK recoveries.
TCP SACK reneging	Number of TCP SACK reneging.
TCP FACK reorders	Number of TCP FACK reorders.
TCP SACK reorders	Number of TCP SACK reorders.
TCP Reno reorders	Number of TCP Reno reorders.
TCP TimeStamp reorders	Number of TCP TimeStamp reorders.
TCP full undos	Number of TCP full undos.
TCP partial undos	Number of TCP partial undos.
TCP DSACK undos	Number of TCP DSACK undos.
TCP loss undos	Number of TCP loss undos.
TCP losses	Number of TCP losses.
TCP lost retransmit	Number of TCP lost retransmit.
TCP Reno failures	Number of TCP Reno failures.
TCP SACK failures	Number of TCP SACK failures.
TCP loss failures	Number of TCP loss failures.
TCP fast retransmissions	Number of TCP fast retransmissions.
TCP forward retransmissions	Number of TCP forward retransmissions.
TCP slowstart retransmissions	Number of TCP slow start retransmissions.
TCP Timeouts	Number of TCP timeouts.

Table 3-117 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
TCP Reno recovery fail	Number of TCP Reno recovery failures.
TCP Sack recovery fail	Number of TCP Sack recovery failures.
TCP scheduler failed	Number of TCP scheduler failures.
TCP receiver collapsed	Number of TCP receiver collapsed failures.
TCP DSACK old packets sent	Number of TCP DSACK old packets sent.
TCP DSACK out-of-order packets sent	Number of TCP DSACK out-of-order packets sent.
TCP DSACK packets received	Number of TCP DSACK packets received.
TCP DSACK out-of-order packets received	Number of TCP DSACK out-of-order packets received.
TCP connections abort on sync	Number of TCP connections aborted on sync.
TCP connections abort on data	Number of TCP connections aborted on data.
TCP connections abort on close	Number of TCP connections aborted on close.
TCP connections abort on memory	Number of TCP connections aborted on memory.
TCP connections abort on timeout	Number of TCP connections aborted on timeout.
TCP connections abort on linger	Number of TCP connections aborted on linger.
TCP connections abort failed	Number of TCP connections abort failed.
TCP memory pressures	Number of times the device approaches the allocated memory pool for the TCP stack.

Related Commands

clear arp-cache

show tcp

(config) tcp

show statistics tfo

To display Traffic Flow Optimization (TFO) statistics for a WAE, use the **show statistics tfo** EXEC command.

show statistics tfo [**connection** | **detail**]

show statistics tfo peer [**peer-id** *peer-id* | **peer-ip** *peer-ip* | **peer-no** *peer-no*]

Syntax Description

connection	(Optional) Displays aggregated TFO connection statistics.
detail	(Optional) Displays detailed TFO statistics.
peer	(Optional) Displays DRE peer statistics.
peer-id *peer-id*	(Optional) Displays peer statistics for peer ID.
peer-ip *peer-ip*	(Optional) Displays peer statistics for peer IP.
peer-no *peer-no*	(Optional) Displays peer statistics for peer number.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

Table 3-118 describes the fields shown in the **show statistics tfo** command. The Policy Engine Statistics and Auto-Discovery Statistics sections are displayed only when you use the **detail** option.

Table 3-118 Field Descriptions for the show statistics tfo Command

Field	Description
Total number of connections	Total number of TCP connections that were optimized since the last TFO statistics reset.
No. of active connections	Total number of TCP optimized connections.
No. of pending (to be accepted) connections	Number of TCP connections that will be optimized but are currently in the setup stage.
No. of bypass connections	Number of connections using TFO only, with no DRE or LZ.
No. of normal closed connections	Number of optimized connections closed without any issues using TCP FIN.
No. of reset connections	Number of connections closed with one of the following errors.
Socket write failure	Failed to write on a socket (either on the LAN or WAN side).
Socket read failure	Failed to read from a socket (either LAN or WAN side).
WAN socket close while waiting to write	Socket between two WAEs (WAN socket) closed before completing writing into it.
AO socket close while waiting to write	Socket between the WAE and the client/server (LAN socket) closed before completing writing into it.

Table 3-118 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
WAN socket error close while waiting to read	Socket between two WAEs (WAN socket) closed before completing reading from it.
AO socket error close while waiting to read	Socket between the WAE and the client/server (LAN socket) closed before completing reading from it.
DRE decode failure	DRE internal error while decoding data. (Should not happen.)
DRE encode failure	DRE internal error while encoding data. (Should not happen.)
Connection init failure	Failed to setup the connection although auto-discovery finished successfully.
WAN socket unexpected close while waiting to read	Socket between two WAEs (WAN socket) closed before completing reading from it.
Exceeded maximum number of supported connections	Connection closed ungracefully because the WAE reached its scalability limit.
Buffer allocation or manipulation failed	Internal memory allocation failure. (Should not happen.)
Peer received reset from end host	TCP RST sent by the server or client. (Can be normal behavior and does not necessarily indicate a problem.)
DRE connection state out of sync	DRE internal error. (Should not happen.)
Memory allocation failed for buffer heads	Internal memory allocation failure. (Should not happen.)
Unoptimized packet received on optimized side	Unoptimized packet received by the WAE when it expected an optimized packet.
Data buffer usages	Data buffer usage statistics for allocated (Used) and cloned buffers. The first column indicates the size of the data stored in the buffers; the second column indicates the size of the buffers; and the third column indicates the number of memory blocks used.
Buffer Control	Buffer control statistics for encode and decode queue buffers. The first column indicates the size of the buffers; the second column indicates the number of slow reads issued to control the queue size; and the third column indicates the number of stop reads issued to control the queue size.
AckQ Control	Shows the total and current number of connections blocked due to a full ack queue.
Scheduler	Scheduler queue sizes and number of jobs processed by each queue.
Policy Engine Statistics	
Session timeouts	Number of times the TFO component did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the TFO component within the Policy Engine.

Table 3-118 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
Total timeouts	Total number of times the TFO component did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the TFO component registered with the Policy Engine (seconds). Most likely causes are as follows: • WAE was rebooted • Configuration change with TFO enabled • Restart of the TFO component by the Node Manager
Hits	Number of connections that had a configured policy that specified the use of TFO.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the TFO component.
Active Connections	Number of hits that represent either active connections using the TFO component or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the TFO component and have completed.
Drops	Number of hits that attempted use of the TFO component but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.
Rejected Connection Counts Due To: (Total:)	• Number of all of the reject reasons that represent hits that were not able to use TFO. Reject reasons include the following: • Not registered • Keepalive timeout • No license • Load level not within range • Connection limit exceeded • Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window) • Minimum TFO not available • Resource manager (minimum resources not available) • Global config optimization disabled • TFO limit exceeded (systemwide connection limit reached) • Server-side invoked • DM deny (Policy Engine dynamic match deny rule matched) • No DM accept was matched

Table 3-118 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
Auto-Discovery Statistics	
Total connections queued for accept	Total number of connections added to the TFO connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the TFO connection accept queue due to a failure. The failure could possibly be due to queue overflow.
AO discovery successful	Number of times TFO discovery was successful.
AO discovery failure	Number of times TFO discovery failed.

Related Commands **show statistics connection closed**

show statistics udp

To display User Datagram Protocol (UDP) statistics for a WAAS device, use the **show statistics udp** EXEC command.

show statistics udp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-119 describes the fields shown in the **show statistics udp** command display.

Table 3-119 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 vn-service vpath

To display VPATH interception statistics for your vWAAS device, use the **show statistics vn-service vpath** EXEC command.

show statistics vn-service vpath

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics vn-service vpath** EXEC command to display statistics about VPATH interception on your vWAAS device.

Note Only one type of interception can be enabled at a time on a vWAAS device (VPATH or WCCP).

Examples

Table 3-120 describes the fields shown in the **show statistics vn-service vpath** command display.

Table 3-120 Field Descriptions for the show statistics vn-service vpath

Field	Description
VPATH Enabled	Indicates if VPATH interception is enabled on the WAAS device.
VPATH Packet received	Number of packets received through VPATH interception.
Optimized TCP Packets VPATH returned	Number of Optimized TCP packets returned through VPATH interception.
WAAS Bypassed VPATH packets returned	Number of packets that bypassed WAAS returned through VPATH interception.
VPATH encapsulated IP pkts(excluding TCP) returned	Number of encapsulated IP packets (excluding TCP) returned through VPATH interception.
VPATH encapsulated Non-IP packets returned	Number of encapsulated non-IP packets (excluding TCP) returned through VPATH interception.
VPATH Fragments received	Number of fragments received through VPATH interception.

Table 3-120 Field Descriptions for the show statistics vn-service vpath (continued)

Field	Description
VPATH Fragments returned	Number of Fragments returned through VPATH interception.
VPATH Packets returned when VPATH not configured	Number of packets returned when VPATH interception is not configured.
Non-VPATH Packets received	Number of packets returned when VPATH interception is not configured.
Error Statistics	Displays the error statistics.
VPATH intercepted packets dropped	Number of intercepted packed dropped due to errors.
VPATH Packet CRC failures	Number of packets CRC failures.
VPATH packets with unsupported Version	Number of packets with unsupported version intercepted through VPATH.
VPATH packets with wrong request type	Number of packets with wrong request type intercepted through VPATH.
VPATH packets with wrong destination MAC	Number of packets with wrong destination MAC address.

Related Commands

(config) vn-service vpath

clear statistics vn-service vpath

show statistics wccp

To display WCCP statistics for a WAE, use the **show statistics wccp** EXEC command.

show statistics wccp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Usage Guidelines

The output of this command differs depending on the device mode of the WAE.

Examples

Table 3-121 describes the fields shown in the **show statistics wccp gre** command display for an application accelerator device.

Table 3-121 Field Descriptions for the show statistics wccp Command on a WAE

Field	Description
Transparent GRE packets received	Total number of GRE packets received by the WAE, regardless of whether or not they have been intercepted by WCCP. GRE is a Layer 3 technique that allows packets to reach the WAE, even if there are any number of routers in the path to the WAE.
Transparent non-GRE packets received	Number of non-GRE packets received by the WAE, either using the traffic interception and redirection functions of WCCP in the router hardware at Layer 2 or Layer 4 switching (a Content Switching Module [CSM]) that redirects requests transparently to the WAE.
Transparent non-GRE non-WCCP packets received	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.

Table 3-121 Field Descriptions for the show statistics wccp Command on a WAE (continued)

Field	Description
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the IP header of the redirected packet has a zero TTL.
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.

Table 3-121 Field Descriptions for the show statistics wccp Command on a WAE (continued)

Field	Description
Packets failed encapsulated reassembly	Number of reassembled GRE encapsulated packets that were dropped because they failed the reassembly sanity check. Reassembled GRE encapsulated packets are composed of two or more GRE encapsulated fragments. This field is related to the previous statistic.
Packets failed GRE encapsulation	Number of GRE packets that are dropped by the WAE because they could not be redirected due to problems while encapsulating the packet with a GRE header.
Packets dropped due to invalid fwd method	Number of GRE packets that are dropped by the WAE because it was redirected using GRE but the WCCP service was configured for Layer 2 redirection.
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.
Packets due to clean wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
Packets dropped due to received on loopback	Number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined to a local address of the device. There is no valid or usable route for the packet.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.
Packets dropped due to received on loopback	Number of packets that are dropped by the WAE because they were received on the loopback interface.

Table 3-121 Field Descriptions for the show statistics wccp Command on a WAE (continued)

Field	Description
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).
Packets fragmented for bypass	Number of bypass GRE packets that do not contain enough data to hold an IP header.
Packets fragmented for egress	Number of egress GRE packets that do not contain enough data to hold an IP header.
Packet pullups needed	Number of times a packet had to be consolidated as part of its processing. Consolidation is required when a packet is received as fragments and the first fragment does not contain all the information needed to process it.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.
WCCP Loop Packets detected	Number of WCCP loop packets detected.
WCCP Loop Packets dropped	Number of WCCP loop packets dropped.

Table 3-122 describes the fields shown in the **show statistics wccp** command display for an ANC device.

Table 3-122 Field Descriptions for the show statistics wccp Command on an ANC

Field	Description
WCCP Stats for Router	Router address. This section appears for each WCCP router.
Packets Received from Router	Packets received from the router.
Bytes Received from Router	Bytes received from the router.
Packets Transmitted to Router	Packets sent to the router.
Bytes Transmitted to Router	Bytes sent to the router
Pass-thru Packets sent to Router	Pass-through packets sent to the router.
Pass-thru Bytes sent to Router	Pass-through bytes sent to the router.
Redirect Packets sent to SN	Redirect packets sent to WAAS nodes (WNs) for optimization.
Redirect Bytes sent to SN	Redirect bytes sent to WNs.
Cummulative WCCP Stats	Cumulative statistics for all WCCP routers.
Total Packets Received from all Routers	Total packets received from all routers.
Total Bytes Received from all Routers	Total bytes received from all routers.
Total Packets Transmitted to all Routers	Total packets sent to all routers.
Total Bytes Transmitted to all Routers	Total bytes sent to all routers.

Table 3-122 Field Descriptions for the show statistics wccp Command on an ANC

Field	Description
Total Pass-thru Packets sent to all Routers	Total pass-through packets sent to all routers.
Total Pass-thru Bytes sent to all Routers	Total pass-through bytes sent to all routers.
Total Redirect Packets sent to SN	Total redirect packets sent to all WNs.
Total Redirect Bytes sent to SN	Total redirect bytes sent to all WNs.

Related Commands

(config) wccp access-list

(config) wccp flow-redirect

(config) wccp router-list

(config) wccp shutdown

(config) wccp tcp-promiscuous service-pair

show statistics windows-domain

To display Windows domain server information for a WAAS device, use the **show statistics windows-domain** EXEC command.

show statistics windows-domain

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show statistics windows-domain** EXEC command to view the Windows domain server statistics, then clear the counters for these statistics by entering the **clear statistics windows-domain** EXEC command.

Examples

Table 3-123 describes the fields shown in the **show statistics windows-domain** command display.

Table 3-123 Field Descriptions for the show statistics windows-domain Command

Field	Description
Windows Domain Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.
Number of authorization success responses	Number of authorization success responses.

Table 3-123 Field Descriptions for the show statistics windows-domain Command (continued)

Field	Description
Accounting	
Number of accounting requests	Number of accounting requests.
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands **windows-domain**

(config) windows-domain

show statistics windows-print requests

To display Windows print acceleration statistics for a WAE using a CIFS application accelerator, use the **show statistics windows-print requests** EXEC command.

show statistics windows-print requests

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show statistics windows-print requests** command to view the Windows print traffic details for a WAE using a CIFS application accelerator.

To display print acceleration statistics for a WAE using an SMB application accelerator, use the **show statistics accelerator SMB** EXEC command.

Note For Windows 7 clients, depending on the printer driver installed, the EndPagePrinter, StartPagePrinter, and WritePrinter counters may not increment because these functions may be encapsulated in a different SMB command.

Examples

Table 3-124 describes the fields shown in the **show statistics windows-print requests** command display.

Table 3-124 Field Descriptions for the show statistics windows-print requests Command

Field	Description
Statistics gathering period	Number of hours, minutes, seconds, and milliseconds of the statistics gathering period.
Documents spooled	Number of documents spooled.
Pages spooled	Number of pages spooled.
Total commands	Total number of print commands.
Remote commands	Number of print commands that were not handled from the local cache.
ALL_COMMANDS	All the print commands combined.
total	Total number of requests for all commands.

Table 3-124 Field Descriptions for the show statistics windows-print requests Command

Field	Description
remote	Number of remote requests for all commands.
async	Number of async requests for all commands.
avg local	Average local request time in milliseconds for all commands.
avg remote	Average remote request time in milliseconds for all commands.
Bind, ClosePrinter, EnumJobs, and so on	Statistics for individual print commands. Each has the same fields as the ALL_COMMANDS section.

Related Commands **(config) accelerator windows-print**

show synq list

To display the connections for the SynQ module, use the **show synq list** EXEC command.

show synq list [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}] [| {**begin** *regex* [*regex*] | **exclude** *regex* [*regex*] | **include** *regex* [*regex*]}]

Syntax Description

|	(Optional) Specifies the output modifier.
begin *regex*	Begins with the line that matches the regular expression. You can enter multiple expressions.
exclude *regex*	Excludes lines that match the regular expression. You can enter multiple expressions.
include *regex*	Includes lines that match the regular expression. You can enter multiple expressions.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show synq list** command to list connections that are currently being tracked in the SynQ module.

Examples

The following is sample output from the **show synq list** command:

```
WAE# show synq list
Src-IP:Src-Port      Dest-IP:Dest-Port     Timeout(msec)   Rexmit cnt
```

Related Commands

show statistics synq

show sysfs volumes

To display system file system (sysfs) information for a WAAS device, use the **show sysfs volumes** EXEC command.

show sysfs volumes

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The system file system (sysfs) stores log files, including transaction logs, syslogs, and internal debugging logs. It also stores system image files and operating system files.

Examples

Table 3-125 describes the fields shown in the **show sysfs volumes** command display.

Table 3-125 Field Descriptions for the show sysfs volumes Command

Field	Description
sysfs 00–04	System file system and disk number.
/local/local1–5	Mount point of the volume.
nnnnnnKB	Size of the volume in kilobytes.
nn% free	Percentage of free space in the SYSFS partition.

Related Commands

disk

(config) disk error-handling

show tacacs

To display TACACS+ authentication protocol configuration information for a WAAS device, use the **show tacacs** EXEC command.

show tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-126 describes the fields shown in the **show tacacs** command display.

Table 3-126 Field Descriptions for the show tacacs Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for authorization or configuration authentication.
TACACS+ Configuration	TACACS+ server parameters.
TACACS+ Authentication	Indicates whether TACACS+ authentication is enabled on the the WAAS device.
Key	Secret key that the WAE uses to communicate with the TACACS+ server. The maximum length of the TACACS+ key is 32 characters.
Timeout	Number of seconds that the WAAS device waits for a response from the specified TACACS+ authentication server before declaring a timeout.
Retransmit	Number of times that the WAAS device is to retransmit its connection to the TACACS+ if the TACACS+ timeout interval is exceeded.
Password type	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.
Server	Hostname or IP address of the TACACS+ server.

Table 3-126 Field Descriptions for the show tacacs Command (continued)

Field	Description
Port	Port number of the TACACS+ server.
Status	Indicates whether server is the primary or secondary host.

Related Commands

clear arp-cache

show statistics tacacs

show tacacs

(config) tacacs

show tcp

To display TCP configuration information for a WAAS device, use the **show tcp** EXEC command.

show tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-127 describes the fields shown in the **show tcp** command display. This command displays the settings configured with the **tcp** global configuration command.

Table 3-127 Field Descriptions for the show tcp Command

Field	Description
TCP Configuration	
TCP keepalive timeout XX sec	Length of time that the WAAS device is set to keep a connection open before disconnecting.
TCP keepalive probe count X	Number of times the WAAS device will retry a connection before the connection is considered unsuccessful.
TCP keepalive probe interval XX sec	Length of time (in seconds) that the WAAS device is set to keep an idle connection open.
TCP explicit congestion notification disabled	Configuration status of the TCP explicit congestion notification feature. Values are enabled or disabled.
TCP cwnd base value X	Value (in segments) of the send congestion window.
TCP initial slowstart threshold value X	Threshold (in segments) for slow start.
TCP increase (multiply) retransmit timer by X	Number of times set to increase the length of the retransmit timer base value.
TCP memory_limit	
Low water mark	Lower limit (in MB) of memory pressure mode, below which TCP enters into normal memory allocation mode.
High water mark (pressure)	Upper limit (in MB) of normal memory allocation mode, beyond which TCP enters into memory pressure mode.
High water mark (absolute)	Absolute limit (in MB) on TCP memory usage.

Related Commands

clear arp-cache

show statistics tcp

(config) tcp

show tech-support

To view information necessary for Cisco TAC to assist you, use the **show tech-support** EXEC command.

show tech-support [**page**]

Syntax Description

page	(Optional) Displays command output page by page.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **show tech-support** command to view system information necessary for Cisco TAC to assist you with a WAAS device. We recommend that you log the output to a disk file. (See the **(config) logging console** command.)

Examples

The following is sample output from the **show tech-support** command:

Note Because the **show tech-support** command output can be long, excerpts are shown in this example.

```
WAE# show tech-support
------------------ version and hardware --------------------

Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
...
Version: ce510-4.0.0.180

Compiled 18:08:17 Feb 16 2006 by cnbuild

System was restarted on Fri Feb 17 23:09:53 2006.
The system has been up for 5 weeks, 3 days, 2 hours, 9 minutes, 49 seconds.

CPU 0 is GenuineIntel Intel(R) Celeron(R) CPU 2.40GHz (rev 2) running at 2401MHz
.
Total 1 CPU.
512 Mbytes of Physical memory.
...
BIOS Information:
Vendor                          : IBM
Version                         : -[PLEC52AUS-C.52]-
Rel. Date                       : 05/19/03
...
```

```
List of all disk drives:
Physical disk information:

  disk00: Normal                (IDE disk)                 76324MB( 74.5GB)
  disk01: Normal                (IDE disk)                 76324MB( 74.5GB)


Mounted filesystems:

  MOUNT POINT       TYPE       DEVICE           SIZE    INUSE     FREE USE%
  /                 root       /dev/root         31MB     26MB      5MB  83%
  /sw               internal   /dev/md0         991MB    430MB    561MB  43%
  /swstore          internal   /dev/md1         991MB    287MB    704MB  28%
  /state            internal   /dev/md2        3967MB     61MB   3906MB   1%
  /disk00-04        CONTENT    /dev/md4       62539MB     32MB  62507MB   0%
  /local/local1     SYSFS      /dev/md5        3967MB    197MB   3770MB   4%
  .../local1/spool  PRINTSPOOL /dev/md6         991MB     16MB    975MB   1%


Software RAID devices:

  DEVICE NAME  TYPE     STATUS                 PHYSICAL DEVICES AND STATUS
  /dev/md0     RAID-1   NORMAL OPERATION       disk00/00[GOOD]  disk01/00[GOOD]
  /dev/md1     RAID-1   NORMAL OPERATION       disk00/01[GOOD]  disk01/01[GOOD]
/dev/md0     RAID-1   NORMAL OPERATION       disk00/00[GOOD]  disk01/00[GOOD]
  /dev/md1     RAID-1   NORMAL OPERATION       disk00/01[GOOD]  disk01/01[GOOD]
  /dev/md2     RAID-1   NORMAL OPERATION       disk00/02[GOOD]  disk01/02[GOOD]
...
Currently content-filesystems RAID level is not configured to change.


------------------ running configuration -------------------

! WAAS version 4.0.0
!
!
...
------------------ processes --------------------

CPU average usage since last reboot:
   cpu: 0.00% User,  1.79% System,  3.21% User(nice),  95.00% Idle
------------------------------------------------------------------------
 PID  STATE PRI User T  SYS T        COMMAND
----- ----- --- ------ ------ --------------------
    1     S   0  20138  21906 (init)
    2     S   0      0      0 (migration/0)
    3     S  19      0      0 (ksoftirqd/0)
    4     S -10      0      0 (events/0)
    5     S -10      0      0 (khelper)
   17     S -10      0      0 (kacpid)
   93     S -10      0      0 (kblockd/0)
...
```

Related Commands

show version

show hardware

show disks details

show running-config

show processes

show processes memory
show memory
show interface
show cdp entry
show cdp neighbors
show statistics wccp
show alarms all
show statistics auto-discovery
show statistics ip
show statistics icmp
show statistics netstat
show statistics peer
show statistics tfo
show disks SMART-info
show disks SMART-info details
show disks failed-sectors

show telnet

To display Telnet services configuration for a WAAS device, use the **show telnet** EXEC command.

show telnet

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

The following is sample output from the **show telnet** command. It shows whether or not Telnet is enabled on the WAAS device.

```
WAE# show telnet
telnet service is enabled
```

Related Commands

telnet

(config) telnet enable

(config) exec-timeout

show tfo tcp

To display global Traffic Flow Optimization (TFO) TCP buffer information for a WAE, use the **show tfo tcp** EXEC command.

show tfo tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

The following is sample output from the **show tfo tcp** command. It displays TCP buffer information for the WAE.

```
WAE# show tfo tcp
Maximum Segment Size:
   Configured:
         Optimized MSS                     : 1432 bytes
         Original MSS                      : 1432 bytes
   Default:
         Optimized MSS                     : 1432 bytes
         Original MSS                      : 1432 bytes

Buffer Sizing Status:
   Configured:
      Adaptive buffer sizing               : enabled
         Maximum receive buffer size       : 8192 KB
         Maximum orig side receive buf size : 256 KB (capped)
         Maximum send buffer size          : 8192 KB
      Fixed buffer sizing                  : disabled
         Optimized side receive buffer size : 2048 KB
         Optimized side send buffer size    : 2048 KB
         Original side receive buffer size  : 32 KB
         Original side send buffer size     : 32 KB
   Default:
      Adaptive buffer sizes                :
         Maximum receive buffer size       : 8192 KB
         Maximum send buffer size          : 8192 KB
      Fixed buffer sizes:
         Optimized side receive buffer size : 32 KB
         Optimized side send buffer size    : 32 KB
         Original side receive buffer size  : 32 KB
         Original side send buffer size     : 32 KB

TFO Status:
   Adaptive buffer sizing is enabled
```

Related Commands

show statistics tfo

show statistics auto-discovery

show statistics connection closed

show statistics filtering

(config) tfo tcp adaptive-buffer-sizing

show transaction-logging

To display the transaction log configuration settings and a list of archived transaction log files for a WAE, use the **show transaction-logging** EXEC command.

show transaction-logging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show transaction-logging** EXEC command to display information about the current configuration of transaction logging on a WAE. Transaction log file information is displayed for TFO transactions and video accelerator transactions.

Note For security reasons, passwords are never displayed in the output of the **show transaction-logging** EXEC command.

Examples

The following is sample output from the **show transaction-logging** command. It lists information about the current configuration of transaction logging on a WAE.

```
WAAE# show transaction-logging
Flow transaction log configuration:
---------------------------------------
Flow Logging is disabled.
Flow Archive interval: every-day every 1 hour
Flow Maximum size of archive file: 2000000 KB

Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour
Accelerator video windows-media transaction log configuration:
-------------------------------------------------------------
Accelerator video windows-media logging is disabled.
Accelerator video windows-media archive interval: every-day every 1 hour
Accelerator video windows-media maximum size of archive file: 2000000 KB

Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour
```

Related Commands

clear arp-cache

transaction-log

(config) transaction-logs

show user

To display user identification number and username information for a particular user of a WAAS device, use the **show user** EXEC command.

show user {**uid** *number* | **username** *name*}

Syntax Description

uid *number*	Displays user information based on the identification number of the user (0–65535).
username *name*	Displays user information based on the name of the user.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-128 describes the fields shown in the **show user** command display.

Table 3-128 Field Descriptions for the show user Command

Field	Description
Uid	User ID number.
Username	Username.
Password	Login password. This field does not display the actual password.
Privilege	Privilege level of the user.
Configured in	Database in which the login authentication is configured.

Related Commands

clear arp-cache

show users administrative

(config) username

show users administrative

To display users with administrative privileges to the WAAS device, use the **show users administrative** EXEC command.

show users administrative [**history** | **locked-out** | **logged-in**]

Syntax Description

administrative	Displays a list of users defined on the device.
history	(Optional) Displays a historical list of user log-ins.
locked-out	(Optional) Displays a list of locked out users.
logged-in	(Optional) Displays a list of users that are logged in.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-129 describes the fields shown in the **show users administrative history** command display.

Table 3-129 Field Descriptions for the show users administrative history Command

Field	Description
Username	Users that have logged in to this appliance CLI during the historical period. When windows domain authentication is enabled, a space in the windows domain username is replaced by the "+" symbol in the output.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that logged in to this appliance.
Loggin details	Day of the week, month, date, time, and whether or not the user is still logged in.

Table 3-130 describes the fields shown in the **show users administrative logged-in** command display.

Table 3-130 Field Descriptions for the show users administrative logged-in Command

Field	Description
Username	Users currently logged in to the appliance CLI. When windows domain authentication is enabled, a space in the windows domain username is replaced by the "+" symbol in the output.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that is logged in to this appliance.
Loginn details	Day of week, month, date, and time that each user logged in.

Related Commands

clear arp-cache

(config) username

show version

To display version information about the WAAS software that is running on the WAAS device, use the **show version** EXEC command.

show version [**last** | **pending**]

Syntax Description

last	(Optional) Displays the version information for the last saved image.
pending	(Optional) Displays the version information for the pending upgraded image.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Examples

Table 3-131 describes the fields shown in the **show version** command display.

Table 3-131 Field Descriptions for the show version Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) *year* by Cisco Systems, Inc. Cisco Wide Area Application Services (universal-k9) Software Release XXX (build b*XXX* month day year)	Software application, copyright, release, and build information. Displays universal-k9 for the full software image, accelerator-k9 for the accelerator only software image, and universal-npe-k9 or accelerator-npe-k9 for the NPE versions of those images. The NPE image versions have the disk encryption feature disabled for use in countries where disk encryption is not permitted.
Version	Version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Compiled information for the software build.
Device Id	Hardware device ID.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for	Length of time the system has been running since the last reboot.

show virtual-blade

To display virtual blade information on your WAE device, use the **show virtual-blade** EXEC command.

show virtual-blade [*virtual-blade-number* [**blockio | interface** {**1 | 2**}] **| detail | vmstat**]

Syntax Description

virtual-blade-number	Individual virtual blade for which to view detailed information.
blockio	(Optional) Displays statistics information for disk devices on a virtual blade.
**interface 1	2**	(Optional) Displays statistics information for a bridged network interface on a virtual blade.
detail	(Optional) Displays detailed information about all virtual blades.
vmstat	(Optional) Displays virtual machine statistics information for all virtual blades.

Command Default

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following is sample output from the **show virtual-blade** command. It displays general virtual blade information for all virtual blades.

```
WAE# show virtual-blade
Virtual-blade resources:
  VB Memory: 1000MiB configured, 3072MiB available.
  VB Disk space: 40GiB configured, 180GiB available.
  VB Image space /local1/vbs: 128MiB used, 125644MiB available
  CPU(s) assigned: 2
Virtual-blade(s) state:
  virtual-blade 1 is running
```

The following is sample output from the **show virtual-blade detail** command. It displays detailed information for all virtual blades.

```
WAE# show virtual-blade detail
*** virtual blade 1 ***
virtual-blade 1
config:
 description Windows 2008 Server
 device cpu qemu64
 device nic rtl8139
 device disk IDE
 device keyboard us
 cpu-list 1 2
 memory 1000
 disk 40
 no boot fd-image
 boot cd-image /local1/vbs/WoW_1.0.2.iso
```

```
 boot from cd-rom
 interface 1 bridge GigabitEthernet 1/0 mac-address 00:16:3E:97:6F:84
 no vnc
 autostart
state:
 running
 serial console session inactive
 vnc server disabled
 current cd /local1/vbs/WoW_1.0.2.iso
 current floppy [not inserted]
```

Table 3-132 describes the fields shown in the general **show virtual-blade** display.

Table 3-132 Field Descriptions for the General show virtual-blade Command

Field	Description
VB Memory	Amount of WAAS system memory assigned to all virtual blades, and the amount of memory remaining.
VB Disk Space	Amount of WAAS system disk space assigned to all virtual blades, and the amount of disk space remaining.
VB Image space	Location and amount of virtual blade image space assigned to the virtual blade, and the amount of disk space remaining.
CPU(s) Assigned	CPU numbers of the CPUs assigned for use by virtual blades. (For example, if 2 is shown, that means that CPU number 2 is assigned for use by virtual blades.)
Virtual Blade State	State of each defined virtual blade (running or stopped).

Table 3-133 describes the fields shown in the **show virtual-blade detail** command display for each virtual blade.

Table 3-133 Field Descriptions for the show virtual-blade detail Command

Field	Description
virtual blade	Virtual blade number.
description	Description of the virtual blade.
device	Device emulation parameters used by the virtual blade.
cpu-list	CPUs allocated to the virtual blade.
memory	Memory allocated to the virtual blade, in MB.
disk	Disk space allocated to the virtual blade, in GB.
no boot fd-image	Floppy disk image from which the virtual blade is configured to boot. In this case, it shows that the virtual blade is not configured to boot from the floppy disk image.
boot cd-image	CD-ROM image from which the virtual blade is configured to boot. Appears only if boot cd-image is configured.
boot from	Boot source location.
interface	Interface bridging configuration.
no vnc	Shows that the VNC server is disabled. (This line does not appear when the VNC server is enabled.)

Table 3-133 Field Descriptions for the show virtual-blade detail Command (continued)

Field	Description
autostart	Shows that the virtual blade is configured to start automatically.
state	State of the virtual blade (running or stopped) and other runtime information.

Related Commands

virtual-blade

(config) virtual-blade

(config-vb) autostart

(config-vb) boot

(config-vb) cpu-list

(config-vb) description

(config-vb) device

(config-vb) disk

(config-vb) interface

(config-vb) memory

(config-vb) vnc

show wccp

To display Web Cache Connection Protocol (WCCP) information for a WAE, use the **show wccp** EXEC command.

show wccp clients

show wccp egress

show wccp flows tcp-promiscuous [**summary**]

show wccp masks tcp-promiscuous

show wccp routers [**detail**]

show wccp services [**detail**]

show wccp statistics

show wccp status

Syntax Description

clients	Displays which WAEs are seen by which routers.
egress	Displays WCCP egress methods.
flows	Displays WCCP packet flows. This option is not available on ANCs
tcp-promiscuous	Displays TCP-promiscuous service information.
summary	(Optional) Displays summarized information about TCP-Promiscuous caching service packet flows.
masks	Displays WCCP mask assignments for a given service.
routers	Displays routers seen and not seen by this WAE.
services	Displays WCCP services configured.
detail	(Optional) Displays details of routers or services.
statistics	Displays WCCP generic routing encapsulation packet-related information.
status	Displays the enabled state of WCCP and the configured service IDs.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

Examples

Table 3-134 describes the fields shown in the **show wccp statistics** command display.

Table 3-134 Field Descriptions for the show wccp statistics Command

Field	Description
Transparent GRE packets received	Total number of GRE packets received by the WAE, regardless of whether or not they have been intercepted by WCCP. GRE is a Layer 3 technique that allows packets to reach the WAE, even if there are any number of routers in the path to the WAE.
Transparent non-GRE packets received	Number of non-GRE packets received by the WAE, either using the traffic interception and redirection functions of WCCP in the router hardware at Layer 2 or Layer 4 switching (a Content Switching Module [CSM]) that redirects requests transparently to the WAE.
Transparent non-GRE non-WCCP packets received	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the IP header of the redirected packet has a zero TTL.
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. **Note** A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts on non-owned bucket	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.

Table 3-134 Field Descriptions for the show wccp statistics Command (continued)

Field	Description
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
GRE packets sent to router (not bypass)	Number of GRE packets that are sent back from the WAE to the router from which the request was redirected, and are not bypass traffic.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.
Packets failed encapsulated reassembly	Number of reassembled GRE encapsulated packets that were dropped because they failed the reassembly sanity check. Reassembled GRE encapsulated packets are composed of two or more GRE encapsulated fragments. This field is related to the previous statistic.
Packets failed GRE encapsulation	Number of GRE packets that are dropped by the WAE because they could not be redirected due to problems while encapsulating the packet with a GRE header.
Packets dropped due to invalid fwd method	Number of GRE packets that are dropped by the WAE because it was redirected using GRE but the WCCP service was configured for Layer 2 redirection.
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.

Table 3-134 Field Descriptions for the show wccp statistics Command (continued)

Field	Description
Connections bypassed during wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
L2 Bypass packets destined for loopback	Number of packets that were bypassed by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined to a local address of the device.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.
Packets dropped due to received on loopback	Number of packets that are dropped by the WAE because they were received on the loopback interface.
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the **wccp access-list** command).
Packets fragmented for bypass	Number of bypass GRE packets that do not contain enough data to hold an IP header.
Packets fragmented for egress	Number of egress GRE packets that do not contain enough data to hold an IP header.
Packet pullups needed	Number of times a packet had to be consolidated as part of its processing. Consolidation is required when a packet is received as fragments and the first fragment does not contain all the information needed to process it.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.
WCCP Loop Packets detected	Number of WCCP loop packets detected.
WCCP Loop Packets dropped	Number of WCCP loop packets dropped.

The following is sample output from the **show wccp clients** command:

```
WAE# show wccp clients
Wide Area Engine List for Service: 61
Number of WAE's in the Cache farm: 2
        IP address = 10.75.152.131       Lead WAE = NO   Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226

        IP address = 10.75.152.130       Lead WAE = YES  Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226

Wide Area Engine List for Service: 62
Number of WAE's in the Cache farm: 2
        IP address = 10.75.152.131       Lead WAE = NO   Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226

        IP address = 10.75.152.130       Lead WAE = YES  Weight = 0
        Routers seeing this Wide Area Engine(1)
                10.75.152.226
```

The following is sample output from the **show wccp services** command:

```
WAE# show wccp services
Services configured on this File Engine
        TCP Promiscuous 61
        TCP Promiscuous 62
```

The following is sample (partial) output from the **show wccp services detail** command:

```
WAE# show wccp services detail
Service Details for TCP Promiscuous 61 Service
        Webcache ID                         : 10.43.65.52
        Service Enabled                     : Yes
        Service Priority                    : 34
        Service Protocol                    : 6
        Service Flags (in Hex)              : 501
        Weight for this Web-CE              : 0
        Redirect method                     : GRE
        Assignment method                   : MASK
        Return method (Auto Negotiated)  :GRE
       Egress method                       : IP-Forwarding
        Negotiated HIA interval             : 2.00 second(s)
        Negotiated failure-detection timeout  : 30.00 second(s)
        Negotiated RA timeout               : 15.00 second(s)
        Values configured:
        Source IP mask (in Hex)             : f00
        Destination IP mask (in Hex)        : 0
        Last Received Assignment Key IP address: 0.0.0.0
        Last Received Assignment Key Change Number: 0
        Flow Protection Enabled: NO
        Flow Protection Timeout: 0 secs
        Join Alarm Raised for service: NO
        Mask Mismatch Alarm Raised for service: NO
        Missing Assignment Alarm Raised for service: NO
        Farm Incompatible Alarm Raised for service: NO


Service Details for TCP Promiscuous 62 Service
        Webcache ID                         : 10.43.65.52
        Service Enabled                     : Yes
        Service Priority                    : 34
```

```
        Service Protocol                    : 6
        Service Flags (in Hex)              : 502
        Weight for this Web-CE              : 0
        Redirect method                     : L2
        Assignment method                   : MASK
       Return method (Auto Negotiated)  : L2
        Egress method                       : L2
        Negotiated HIA interval             : 2.00 second(s)
        Negotiated failure-detection timeout  : 30.00 second(s)
        Negotiated RA timeout               : 15.00 second(s)
        Values configured:
        Source IP mask (in Hex)             : 0
        Destination IP mask (in Hex)        : f00
        Last Received Assignment Key IP address: 0.0.0.0
        Last Received Assignment Key Change Number: 0
        Flow Protection Enabled: NO
        Flow Protection Timeout: 0 secs
        Join Alarm Raised for service: NO
        Mask Mismatch Alarm Raised for service: NO
        Missing Assignment Alarm Raised for service: NO
        Farm Incompatible Alarm Raised for service: NO
```

The following is sample output from the **show wccp routers** command:

```
WAE# show wccp routers
Router Information for Service Id: 61
        Routers Seeing this Wide Area Engine(1)
        Router Id       Sent To
        10.43.228.165    10.43.228.65
        Routers not Seeing this Wide Area Engine
        10.10.10.45    -Redirect Method Mismatch-
        Routers Notified of from other WAE's
                -NONE-

Router Information for Service Id: 62
        Routers Seeing this Wide Area Engine(1)
        Router Id       Sent To
        10.43.228.165    10.43.228.65
        Routers not Seeing this Wide Area Engine
        10.10.10.45    -Redirect Method Mismatch
        Routers Notified of from other WAE's
                -None-
```

The following is sample output from the **show wccp routers detail** command:

```
WAE# show wccp routers detail
Router Information for Service Id: 61

        Routers Seeing this Wide Area Engine(1)

  Router Id         Sent To         Recv ID  KeyIP           KeyCN    MCN

  10.75.152.226      10.75.152.129    03456469 10.75.152.130    1        233
        Transmit timer (ms): 0/0        Timer Scale: (0/0),(0/0)
        Last ISU received: 1/19/2012 00:09:51
        Output Interface IP Address: 10.75.152.130       Interface State: UP
        MAC Addr: 00:24:97:7a:d0:30

        Routers not Seeing this Wide Area Engine
                -NONE-

        Routers Notified of from other WAE's
                -NONE-
```

```
Router Information for Service Id: 62

        Routers Seeing this Wide Area Engine(1)

  Router Id         Sent To         Recv ID  KeyIP           KeyCN    MCN

  10.75.152.226      10.75.152.129    03433645 10.75.152.130    1        229
        Transmit timer (ms): 0/0        Timer Scale: (0/0),(0/0)
        Last ISU received: 1/19/2012 00:09:51
        Output Interface IP Address: 10.75.152.130       Interface State: UP
        MAC Addr: 00:24:97:7a:d0:30

        Routers not Seeing this Wide Area Engine
                -NONE-

        Routers Notified of from other WAE's
                -NONE-
```

The following is sample output from the **show wccp status** command:

```
WAE# show wccp status
WCCP Interception :
Configured State :  Enabled
Operational State : Enabled

Services Enabled on this WAE:
        TCP Promiscuous 61
        TCP Promiscuous 62
```

The Configured State refers to the state configured. The Operational State refers to the actual system state, which could differ from the configured state. For example, if an ANC is converging due to a cluster change, the system disables WCCP until convergence is completed.

The following is sample output from the **show wccp egress** command:

```
WAE# show wccp egress

        TCP Promiscuous Service : 61
        Egress Method in Use: L2

        TCP Promiscuous Service : 62
        Egress Method in Use: L2
```

Related Commands

(config) wccp access-list

(config) wccp flow-redirect

(config) wccp router-list

(config) wccp shutdown

(config) wccp tcp-promiscuous service-pair

show windows-domain

To display Windows domain configuration information for a WAAS device, use the **show windows-domain** EXEC command.

show windows-domain

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Device Modes

application-accelerator

central-manager

Examples

Table 3-135 describes the fields shown in the **show windows-domain** command display.

Table 3-135 Field Descriptions for the show windows-domain Command

Field	Description
Login Authentication for Console/Telnet Session:	Status of the primary login authentication method for the session: enabled or disabled.
Configuration Authentication for Console/Telnet Session: enabled (secondary)	Status of the secondary login authentication method for the session:enabled or disabled.
Windows domain Configuration:	Shows the Windows domain configuration settings.
Workgroup	Workgroup identification string.
Comment	Comment line.
Net BIOS	Windows NetBIOS name for the WAE.
Realm	Kerberos Realm (similar to the Windows domain name, except for Kerberos).
WINS Server	IP address of the WINS server.
Password Server	Kerberos server DNS name.
Security	Type of authentication configured, either “Domain” for NTLM or “ADS” for Kerberos.
Administrative groups	
Super user group	Active Directory(AD) group name. Users in this group have administrative rights.
Normal user group	AD group name. Users in this group have the normal/default privilege level in the WAE.

Related Commands windows-domain

(config) windows-domain

show windows-domain encrypted services

To display Windows domain encrypted services information for a WAAS device, use the **show windows-domain encrypted services** EXEC command.

show windows-domain encrypted services { identity [detail] | blacklist identity | status | keylist user }

Syntax Description

identity	Identity tag of the encryption service.
identity detail	Identity details including identity tag, account type, account name, domain, realm, status, and match domains.
blacklist identity	Identity tag, blacklist reason, and domain name.
status	Service name, configuration state (enabled or disabled), and operational state (running or
keylist user	Number of keys, maximum retrieval time (in milliseconds), average retrieval time (in milliseconds), and domain name.

Defaults

No default behavior or values.

Device Modes

application-accelerator

central-manager

Related Commands

windows-domain

(config) windows-domain

shutdown

To shut down the WAAS device, use the **shutdown** EXEC command.

shutdown [**poweroff**]

Syntax Description		
	poweroff	(Optional) Turns off the power after closing all applications and operating system.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

A controlled shutdown refers to the process of properly shutting down a WAAS device without turning off the power on the device. With a controlled shutdown, all of the application activities and the operating system are properly stopped on a WAE, but the power remains on. Controlled shutdowns of a WAAS device can help you minimize the downtime when the WAAS device is being serviced.

Caution If a controlled shutdown is not performed, the WAAS file system can be corrupted. Rebooting the WAAS device takes longer if it was not properly shut down.

Note A WAAS device cannot be powered on again through the WAAS software after a software poweroff. You must press the power button once on a WAAS device to bring it back online.

The **shutdown** EXEC command facilitates a proper shutdown for WAAS device, and is supported on all WAE hardware models. The **shutdown poweroff** command is also supported by all of the WAE hardware models as they support the ACPI.

The **shutdown** command closes all applications and stops all system activities, but keeps the power on. The fans continue to run and the power LED is on, indicating that the device is still powered on. The device console displays the following menu after the shutdown process is completed:

```
================= SHUTDOWN SHELL =================
System has been shut down.


You can
0. Power down system by pressing and holding power button
1. Reload system by software
2. Power down system by software
[1-2]?
```

The **shutdown poweroff** command closes all applications and the operating system, stops all system activities, and turn off the power. The fans stop running and the power LED starts flashing, indicating that the device has been powered off.

Note If you use the **shutdown** or **shutdown poweroff** commands, the device does not perform a file system check when you power on and boot the device the next time.

Table 3-136 describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

Table 3-136 Description of the shutdown Command Operations

Activity	Process
User performs a shutdown operation on the WAE	Shutdown poweroff `WAE# shutdown poweroff`
User intervention to bring WAE back online	After a shutdown poweroff, you must press the power button once to bring the WAAS device back online.
File system check	Is *not* performed after you turn the power on again and reboot the WAAS device.

You can enter the **shutdown** EXEC command from a console session or from a remote session (Telnet or SSH version 2) to shut down a WAAS device.

To shut down a WAAS device, enter the **shutdown** EXEC command as follows:

```
WAE# shutdown
```

When you are asked if you want to save the system configuration, enter **yes**.

```
System configuration has been modified. Save?[yes]:yes
```

When you are asked if you want to proceed with the shutdown, press **Enter** to proceed with the shutdown operation.

```
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
```

A message appears, reporting that all services are being shut down on this WAE.

```
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

After the system is shut down (the system has halted), a WAAS software shutdown shell displays the current state of the system (for example, “System has been shut down”) on the console. You are asked whether you want to perform a software power off (the **Power down system by software** option), or if you want to reload the system through the software.

```
================= SHUTDOWN SHELL =================
System has been shut down.
You can either
   Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

To power down the WAAS device, press and hold the power button on the WAAS device, or use one of the following methods to perform a shutdown poweroff:

- From the console command line, enter **2** when prompted, as follows:

```
================= SHUTDOWN SHELL =================
System has been shut down.
You can either
   Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

- From the WAAS CLI, enter the **shutdown poweroff** EXEC command as follows:

```
WAE# shutdown poweroff
```

When you are asked if you want to save the system configuration, enter **yes**.

```
System configuration has been modified. Save?[yes]:yes
```

When you are asked to confirm your decision, press **Enter**.

```
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

Examples

The following example shows how to close all applications and stop all system activities using the **shutdown** command:

```
WAE1# shutdown
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

The following example shows how to close all applications, stop all system activities, and then turn off power to the WAAS device using the **shutdown poweroff** command:

```
WAE2# shutdown poweroff
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

snmp trigger

To configure thresholds for a user-selected MIB object for monitoring purposes on a WAAS device, use the **snmp trigger** EXEC command.

snmp trigger {**create** *mibvar* [**wildcard**] [*wait-time*
[**absent** [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] |

equal [**absolute** *value* [[*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] |

falling [**absolute** *value* [*LINE* | **mibvar1** *mibvar*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] |

greater-than [**absolute** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] |

less-than [**absolute** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] |

on-change [[*LINE* | **mibvar1** *mibvar1*][*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]] |

present [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] |

rising [**absolute** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*] | **delta** *value* [*LINE* | **mibvar1** *mibvar1*] [*LINE* | **mibvar2** *mibvar2*] [*LINE* | **mibvar3** *mibvar3*] [*LINE*]]]]}

snmp trigger delete *mibvar*

Syntax Description

create *mibvar*	Configures a threshold for a MIB object. Specifies the name of the MIB object that you want to monitor or the MIB object for which you want to remove a monitoring threshold.
wildcard	(Optional) Treats the specified MIB variable name as having a wildcard.
wait-time	(Optional) Number of seconds, 60–600, to wait between trigger samples.
absent	(Optional) Applies the absent existence test.
LINE	(Optional) Description of the threshold being created.
mibvar1 *mibvar1*	(Optional) Adds a MIB object to the notification.
mibvar2 *mibvar2*	(Optional) Adds a MIB object to the notification.
mibvar3 *mibvar3*	(Optional) Adds a MIB object to the notification.
equal	Applies the equality threshold test.
absolute *value*	(Optional) Specifies an absolute value sample type.

delta *value*	Specifies a delta sample type.
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** EXEC command, you can define additional SNMP traps for other MIB objects of interest to your particular configuration. You can select any MIB object from any of the support MIBs for your trap. The trap can be triggered based on a variety of tests:

- absent—A specified MIB object that was present at the last sampling is no longer present as of the current sampling.
- equal—The value of the specified MIB object is equal to the specified threshold.
- falling—The value of the specified MIB object has fallen below the specified threshold value. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value rises above the threshold value and then falls below the falling threshold value again.
- greater-than—The value of the specified MIB object is greater than the specified threshold value.
- less-than—The value of the specified MIB object is less than the specified threshold value.
- on-change—The value of the specified MIB object has changed since the last sampling.
- present—A specified MIB object is present as of the current sampling that was not present at the previous sampling.
- rising—The value of the specified MIB object has risen above the specified threshold. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value falls below the threshold value and then rises above the rising threshold value again.

The threshold value can be based on an *absolute* sample type or on a *delta* sample type. An absolute sample type is one in which the test is evaluated against a fixed integer value between zero and 4294967295. A delta sample type is one in which the test is evaluated against the change in the MIB object value between the current sampling and the previous sampling.

After you configure SNMP traps, you must use the **snmp-server enable traps event** global configuration command for the event traps you just created to be generated. Also, to preserve SNMP trap configuration across a system reboot, you must configure event persistence using the **snmp-server mib persist event** global configuration command, and save the MIB data using the **write mib-data** EXEC command.

Note You can create valid triggers only on read-write and read-only MIB objects. If you try to create a trigger on a read-create MIB object, you receive an error message.

Examples

The following example shows how to create a threshold for the MIB object *esConTabIsConnected* so that a trap is sent when the connection from the Edge WAE to the Core WAE is lost:

```
WAE# snmp trigger create esConTabIsConnected ?
  <60-600>  The number of seconds to wait between trigger sample
  wildcard  Option to treat the MIB variable as wildcarded
WAE# snmp trigger create esConTabIsConnected wildcard 600 ?
  absent        Absent existence test
  equal         Equality threshold test
  falling       Falling threshold test
  greater-than  Greater-than threshold test
  less-than     Less-than threshold test
  on-change     Changed existence test
  present       Present present test
  rising        Rising threshold test
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling ?
  absolute Absolute sample type
  delta   Delta sample type
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute ?
  <0-4294967295>  Falling threshold value
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 ?
  LINE     Trigger-comment
  mibvar1  Optional mib object to add to the notification
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 "Lost the
connection with the core server."
WAE# configure
WAE(config)# snmp-server enable traps event
```

Once you have configured the WAE to send SNMP traps, you can view the results of these newly created traps using the **show snmp events** EXEC command.

You can also delete user-created SNMP traps. The following example shows how to delete the trap set for *esConTabIsConnected* that we created in the previous example.

```
WAE# snmp trigger delete esConTabIsConnected
```

Related Commands

show snmp

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

write

ssh

To allow secure encrypted communications between an untrusted client machine and a WAAS device over an insecure network, use the **ssh** EXEC command.

ssh *options* [**management**]

Syntax Description

options	Options to use with the **ssh** EXEC command. For more information about the possible options, see RFC 4254 at http://www.rfc-archive.org/getrfc.php?rfc=4254.
management	Uses the designated management interface for the SSH operation.

Defaults

By default, the Secure Shell (SSH) feature is disabled on a WAAS device.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

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.

Examples

The following example shows how to log in to a WAAS device using the SSH client:

```
WAE# ssh 10.11.55.2
```

Related Commands

telnet

(config) sshd

(config) ssh-key-generate

tcpdump

To dump network traffic, use the **tcpdump** EXEC command.

tcpdump [*LINE*]

Syntax Description

LINE	(Optional) Dump options. For more information see the "Usage Guidelines" section.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

TCPdump is a utility that allows a user to intercept and capture packets passing through a network interface, making it useful for troubleshooting network applications.

Note In WAAS version 5.0, TCPdump cannot capture data plane traffic on an AppNav Controller Interface Module interface; only control plane traffic is captured. Instead, use the **packet-capture** EXEC command to capture data plane traffic.

During normal network operation, only the packets which are addressed to a network interface are intercepted and passed on to the upper layers of the TCP/IP protocol layer stack. Packets which are not addressed to the interface are ignored. In Promiscuous mode, the packets which are not intended to be received by the interface are also intercepted and passed on to the higher levels of the protocol stack. TCPdump works by putting the network interface into promiscuous mode. TCPdump uses the free libpcap (packet capture library).

Use the *-h* option to view the options available, as shown in the following example:

```
WAE# tcpdump -h
tcpdump version 3.8.1 (jlemon)
libpcap version 0.8
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
                [ -E algo:secret ] [ -F file ] [ -i interface ] [ -r file ]
                [ -s snaplen ] [ -T type ] [ -w file ] [ -y datalinktype ]
                [ expression ]
```

You can use either linux interface port names (for example, eth0) or WAAS port names (for example, GigabitEthernet 1/0 port 80, or InlinePort 1/0 lan) to designate the interface from which you want to capture packets. You cannot specify an inlineGroup.

Examples

The following example shows how to start a network traffic dump to a file named *tcpdump.txt*:

```
WAE# tcpdump -w tcpdump.txt
```

Related Commands

less

packet-capture

ping

tethereal

traceroute

telnet

To log in to a WAAS device using the Telnet client, use the **telnet** EXEC command.

telnet {*hostname* | *ip-address*} [*portnum*] [**management**]

Syntax Description

hostname	Hostname of the network device.
ip-address	IP address of the network device.
portnum	(Optional) Port number (1–65535). The default port number is 23.
management	Uses the designated management interface for the Telnet operation.

Defaults

The default port number is 23.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

UNIX shell functions such as escape and the **suspend** command are not available in the Telnet client. Multiple Telnet sessions are also not supported. This Telnet client allows you to specify a destination port.

Examples

The following example shows how to log in to a WAAS device using the Telnet client in several ways:

```
WAE# telnet cisco-wae
WAE# telnet 10.168.155.224
WAE# telnet cisco-wae 2048
WAE# telnet 10.168.155.224 2048 management
```

Related Commands

ssh

(config) telnet enable

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal** EXEC command.

terminal {**length** *length* | **monitor** [**disable**]}

Syntax Description

length *length*	Sets the length of the display on the terminal (0–512). Setting the length to 0 means there is no pausing.
monitor	Copies the debug output to the current terminal.
disable	(Optional) Disables monitoring at this specified terminal.

Defaults

The default is 24 lines.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

When 0 is entered as the *length* parameter, the output to the screen does not pause. For all nonzero values of *length*, the -More- prompt is displayed when the number of output lines matches the specified *length* number. The -More- prompt is considered a line of output. To view the next screen, press the **Spacebar**. To view one line at a time, press the **Enter** key.

The **terminal monitor** command allows a Telnet session to display the output of the **debug** commands that appear on the console. Monitoring continues until the Telnet session is terminated.

For proper display of the **setup** command, leave the terminal length set to the default value of 24 lines.

Examples

The following example shows how to set the number of lines to display to 20:

```
WAE# terminal length 20
```

The following example shows how to configure the terminal for no pausing:

```
WAE# terminal length 0
```

Related Commands

All **show** commands.

test

To perform authentication and diagnostic tests for the Radius/Tacacs/Windows users, use the **test** EXEC command.

test aaa {**radius** | **tacacs** | **windows**} *username password*

test self-diagnostic [**system** | **basic** | **connectivity** | **interfaces** | **application-security** | **tfo** | **wccp** | **inline**] | **all**

Syntax Description

aaa	Performs authentication tests for the users trying to access the WAAS Central Manager or WAE.
radius	Uses the RADIUS server for authentication purposes.
tacacs	Uses the TACACS server for authentication purposes.
windows	Uses the Windows domain for authentication purposes.
username	Username for authentication.
password	Password for authentication.
self-diagnostic	Performs self-diagnostics tests.
system	(Optional) Checks the device status, presence of core files, and alarms.
basic	(Optional) Checks the device network configuration.
connectivity	(Optional) Checks if the external hosts required for device operation are reachable by sending ICMP ping packets.
interfaces	(Optional) Checks the operation of physical or virtual interfaces, including ports on the Cisco WAE Inline Network Adapter and Cisco Interface Module.
application-security	(Optional) Checks for potentially malicious (XSS) entries.
tfo	(Optional) Checks the traffic optimization configuration settings and operation. (Applies only to application accelerator devices.)
wccp	(Optional) Checks the WCCP configuration settings and operation. (Applies only to application accelerator devices.)
inline	(Optional) Checks the inline group configuration settings and operation. (Applies only to application accelerator devices that have a Cisco WAE Inline Network Adapter or Cisco Interface Module installed.)
all	Runs all of the diagnostic tests.

Defaults

No default behavior or values.

Command Modes

EXEC mode

Device Modes

application-accelerator

central-manager

Usage Guidelines

If you use the **test self-diagnostic** command with the **all** option, all applicable tests are performed. You can specify one or more test options to perform just those tests.

The last diagnostic test report is stored on the device in the following file: /local1/diagnostic_report.txt.

Examples

The following example shows how to perform the basic, connectivity, interfaces, and WCCP tests:

```
WAE# test self-diagnostic basic connectivity interfaces wccp
```

Table 3-137 describes the error messages that can be returned by the **test self-diagnostics** command.

Table 3-137 Error Codes Returned by the test self-diagnostics Command

Test	Error Code	Description
system	HAS_COREDUMP	Core files are present.
	HAS_ALARM	Critical or major alarms are pending.
basic	NO_PRIM_IFACE	The primary interface is not configured.
	NO_PRIM_ADDR	The primary interface has no IP address configured.
	NO_HOSTNAME	The hostname is not configured.
	NO_NAMESERVER	The name servers are not configured.
	NO_DOMAIN	The domain name is not configured.
	NO_DEFAULT_GW	The default gateway is not configured.
	NO_CM_ADDR	The WAAS Central Manager IP address is not configured.
	NO_NTP_CFG	The NTP server is not configured.
connectivity	UNREACHABLE	The default gateway, name servers, NTP servers, authentication servers (RADIUS, TACACS, or Windows domain), or WAAS Central Manager are unreachable.
	UNRESOLVABLE	The fully qualified domain name of the device cannot be resolved.
	WINS_UNAVAILABLE	The WINS server is unreachable or not operational and cannot resolve the device netbios name.
interfaces	IFACE_DOWN	The interface is in shutdown mode. If all interfaces are shut down, the test will fail.
	IFACE_BW	The interface is configured or negotiated to use 10-MB speed instead of a faster speed.
	IFACE_HD	The interface is configured or negotiated to use half duplex instead of full duplex.
	IFACE_ERRORS	The interface has packet errors on more than 1 percent of received or sent packets.
	IFACE_COLLISIONS	The interface has packet collisions on more than 1 percent of sent packets.
tfo	TFO_DISABLED	TFO is disabled.
	TFO_NO_DRE	DRE is disabled.
	TFO_NO_LZ	Compression is disabled.
	TFO_NOAOACCL	An application accelerator in the policy engine is not enabled to accelerate traffic.
	PE_OTHER	Unclassified traffic is configured to pass through.
	TFO_NOPT	Traffic that is configured to be optimized is being passed through.

Table 3-137 Error Codes Returned by the test self-diagnostics Command (continued)

Test	Error Code	Description
wccp	NO_RTRCFG	WCCP is enabled but TCP promiscuous mode is not configured.
	NO_RTRLIST	The router list specified in WCCP configuration is not configured.
	UNREACHABLE	Configured WCCP routers are unreachable or other WAEs in the WCCP farm are unreachable.
	NO_WCCP_RTRS	The WAE and WCCP routers cannot communicate with each other.
	NO_INTERCEPT	The WAE is not receiving intercepted traffic.
inline	INLINE_NO_INT	Traffic interception is not configured on the inlineGroup interface.
	INLINE_SHUTDOWN	The inlineGroup interface is shut down.
	INLINE_BYPASS	The inlineGroup interface is in bypass mode.
	INLINE_INTRCPT	The inlineGroup interface is not intercepting traffic.

tethereal

To analyze network traffic from the command line, use the **tethereal** EXEC command.

tethereal [*LINE*]

Syntax Description

LINE	(Optional) Options. For more information see the "Usage Guidelines" and "Examples" sections.

Defaults

No default behavior values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Tethereal is the command-line version of the network traffic analyzer tool Ethereal. Like TCPdump, it also uses the packet capture library (libpcap). Aside from network traffic analysis, Tethereal also provides facilities for decoding packets.

Note In WAAS version 5.0, Tethereal cannot capture data plane traffic on an AppNav Controller Interface Module interface; only control plane traffic is captured. Instead, use the **packet-capture** EXEC command to capture data plane traffic.

When using the **-a** option to print heavy traffic to the screen, it can take significantly longer than the autostop duration to display the information on the screen. Wait for the command to finish. Displaying output to the console can take significantly longer than through telnet or SSH, therefore console display is not recommended.

When using the **-f** option with the host or not host filter expression, the wrong traffic may be captured with WCCP GRE encapsulated or VLAN traffic. With WCCP GRE traffic, tethereal sees only the outermost IP address, not the original IP address inside the encapsulated packets. Add the **proto 47** keyword into the **-f** filter expression to capture the correct traffic (protocol 47 is GRE traffic). Additionally, for VLAN traffic, add the **vlan** keyword into the **-f** filter expression so that VLAN traffic is parsed correctly.

When using the **-a** filesize option together with the **-R** option, tethereal may stop unexpectedly and print the message "Memory limit is reached" before reaching the specified autostop file size. In this case, the maximum memory limit for the command was reached before the autostop file size limit.

You can use either Linux interface port names (for example, eth0) or WAAS port names (for example, GigabitEthernet 1/0 port 80, or InlinePort 1/0 lan) to designate the interface from which you want to capture packets. You cannot specify an inlineGroup.

Examples

The following example shows how to display the options available with the WAAS **tethereal** command:

```
WAE# tethereal -h
tethereal: Setting virtual memory limit to 209715200
TShark 1.0.0
Dump and analyze network traffic.
See http://www.wireshark.org for more information.

Copyright 1998-2008 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Usage: tshark [options] ...

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
Capture output:
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
                           filesize:NUM - switch to next file after NUM KB
                              files:NUM - ringbuffer: replace after NUM files
Input file:
  -r <infile>              set the filename to read from (no pipes or stdin!)

Processing:
  -R <read filter>         packet filter in Wireshark display filter syntax
  -n                       disable all name resolutions (def: all enabled)
  -N <name resolve flags>  enable specific name resolution(s): "mntC"
  -d <layer_type>==<selector>,<decode_as_protocol> ...
                           "Decode As", see the man page for details
                           Example: tcp.port==8888,http
Output:
  -w <outfile|->           set the output filename (or '-' for stdout)
  -C <config profile>      start with specified configuration profile
  -F <output file type>    set the output file type, default is libpcap
                           an empty "-F" option will list the file types
  -V                       add output of packet tree        (Packet Details)
  -S                       display packets even when writing to a file
  -x                       add output of hex and ASCII dump (Packet Bytes)
  -T pdml|ps|psml|text|fields
                           format of text output (def: text)
  -e <field>               field to print if -Tfields selected (e.g. tcp.port);
                           this option can be repeated to print multiple fields
  -E<fieldsoption>=<value> set options for output when -Tfields selected:
     header=y|n            switch headers on and off
     separator=/t|/s|<char> select tab, space, printable character as separator
     quote=d|s|n           select double, single, no quotes for values
  -t ad|a|r|d|dd|e         output format of time stamps (def: r: rel. to first)
  -l                       flush standard output after each packet
  -q                       be more quiet on stdout (e.g. when using statistics)
  -X <key>:<value>         eXtension options, see the man page for details
  -z <statistics>          various statistics, see the man page for details
```

```
Miscellaneous:
  -h                       display this help and exit
  -v                       display version info and exit
  -o <name>:<value> ...    override preference setting
```

Related Commands

packet-capture

tcpdump

top

To view the current top CPU activities, use the **top** EXEC command.

top -hv | -cisS -d *delay* **-n** *iterations* **[-u** *user* **| -U** *user***] -p** *pid* **[,***pid* **...]**

Syntax Description

-h	Prints help information and exits.
-v	Prints version information and exits.
-c	Displays the command line instead of the command name only.
-i	Suppresses the display of any idle or zombie processes.
-s	Tells top to run in secure mode. This option disables the potentially dangerous interactive commands.
-S	(Optional) Specifies cumulative mode, where each process is listed with the CPU time it has spent. It also lists the CPU time of the dead children for each process.
-d *delay*	Specifies the delay between screen updates.
-n *iterations*	Specifies the number of iterations. Update the display this number of times and then exit.
-u *user*	Monitors only processes with the specified effective UID or username.
-p *pid*	(Optional) Monitors only those processes with the given process id. This option can be given up to twenty times. This option is not available interactively.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **top** command is a system-defined alias for the Linux **top** command, which displays and updates information about the top CPU processes. It provides a real-time view of the processor activity. It lists the most CPU-intensive tasks on the system, and provides an interactive interface for manipulating processes. It can sort the tasks by CPU usage, memory usage, and runtime.

The command runs in an interactive environment and you can interact with the output by pressing various keys. Press h or ? to display the following help for interactive commands:

```
Help for Interactive Commands - procps version 3.2.5
Window 1:Def: Cumulative mode Off.  System: Delay 3.0 secs; Secure mode Off.

  Z,B       Global: 'Z' change color mappings; 'B' disable/enable bold
  l,t,m     Toggle Summaries: 'l' load avg; 't' task/cpu stats; 'm' mem info
  1,I       Toggle SMP view: '1' single/separate states; 'I' Irix/Solaris mode
```

```
  f,o     . Fields/Columns: 'f' add or remove; 'o' change display order
  F or O  . Select sort field
  <,>     . Move sort field: '<' next col left; '>' next col right
  R       . Toggle normal/reverse sort
  c,i,S   . Toggle: 'c' cmd name/line; 'i' idle tasks; 'S' cumulative time
  x,y     . Toggle highlights: 'x' sort field; 'y' running tasks
  z,b     . Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
  u       . Show specific user only
  n or #  . Set maximum tasks displayed

  k,r       Manipulate tasks: 'k' kill; 'r' renice
  d or s    Set update interval
  W         Write configuration file
  q         Quit
          ( commands shown with '.' require a visible task display window )
Press 'h' or '?' for help with Windows,
any other key to continue
```

Examples

The following example shows how to display the options available with the WAAS **top** command:

```
WAE# top -h
    top: procps version 3.2.5
usage:  top -hv | -bcisS -d delay -n iterations [-u user | -U user] -p pid [,pid ...]
```

Note The **-b** option is not supported.

The following example shows an example of the interactive command output:

```
WAE# top
top - 17:54:02 up 9 days,  6:09,  1 user,  load average: 0.05, 0.17, 0.19
Tasks: 992 total,   1 running, 991 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.7% us,  2.3% sy,  4.0% ni, 91.1% id,  1.7% wa,  0.0% hi,  0.3% si
Mem:   1939124k total,  1528440k used,   410684k free,   159720k buffers
Swap:  2037624k total,      812k used,  2036812k free,   554824k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
28359 admin     20   0  2544 1584  808 R  1.3  0.1   0:00.29 top
 7694 admin     30  10 1448m 105m  15m S  0.7  5.6  19:33.74 java
 9312 admin     30  10  494m 173m  20m S  0.7  9.2   2:47.23 java
 6950 admin     30  10  684m 204m 4876 S  0.3 10.8  28:31.64 so_dre
 7702 admin     30  10  955m 121m  18m S  0.3  6.4   3:07.97 java
 8782 admin     30  10 1448m 105m  15m S  0.3  5.6   3:32.04 java
 8802 admin     30  10 1448m 105m  15m S  0.3  5.6   0:49.17 java
    1 admin     20   0  1488  540  468 S  0.0  0.0   0:06.78 init
    2 admin     15  -5     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 admin     RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 admin     15  -5     0    0    0 S  0.0  0.0   0:09.07 ksoftirqd/0
    5 admin     RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
```

Related Commands

show processes

traceroute

To trace the route between a WAAS device to a remote host, use the **traceroute** EXEC command.

traceroute [**management**] {*hostname* | *ip-address*} [**tcp-syn**]

Syntax Description

management	(Optional) Uses the designated management interface for the traceroute.
hostname	Name of remote host.
ip-address	IP address of remote host.
tcp-syn	(Optional) Sends TCP-SYN packets for trace routing instead of UDP

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Traceroute is a widely available utility on most operating systems. Much like ping, it is a valuable tool for determining connectivity in a network. Ping allows the user to find out if there is a connection between two end systems. Traceroute does this as well, but also lists the intermediate routers between the two systems. Users can therefore see the possible routes packets can take from one system to another. Use **traceroute** to find the route to a remote host, when either the hostname or the IP address is known.

Examples

The following example shows how to trace the route between the WAAS device and a device with an IP address of 10.0.0.0:

```
WAE# traceroute 10.0.0.0
traceroute to 10.0.0.0 (10.0.0.0), 30 hops max, 38 byte packets
 1  sblab2-rtr.abc.com (192.168.10.1)  0.959 ms  0.678 ms  0.531 ms
 2  192.168.1.1 (192.168.1.1)  0.665 ms  0.576 ms  0.492 ms
 3  172.24.115.66 (172.24.115.66)  0.757 ms  0.734 ms  0.833 ms
 4  sjc20-sbb5-gw2.abc.com (192.168.180.93)  0.683 ms  0.644 ms  0.544 ms
 5  sjc20-rbb-gw5.abc.com (192.168.180.9)  0.588 ms  0.611 ms  0.569 ms
 6  sjce-rbb-gw1.abc.com (172.16.7.249)  0.746 ms  0.743 ms  0.737 ms
 7  sj-wall-2.abc.com (172.16.7.178)  1.505 ms  1.101 ms  0.802 ms
 8  * * *
 9  * * *
 . . .
```

Related Commands

ping

waas-tcptrace

transaction-log

To force the exporting or the archiving of the transaction log, use the **transaction-log** EXEC command.

transaction-log force {**archive** | **export**} {**flow** | **accelerator video windows-media**}

Syntax Description

archive	Forces the archiving of the transaction log file.
export	Forces the archived transaction log files to be exported.
flow	Forces the archiving or exporting of the Traffic Flow Optimization (TFO) transaction log file.
accelerator video windows-media	Forces the archiving or exporting of the video accelerator transaction log file.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example shows how to force the archiving of the TFO transaction log file on the WAE:

```
WAE# transaction-log force archive flow
```

The following example shows how to force the exporting of the video transaction file on the WAE:

```
WAE# transaction-log force export accelerator video windows-media
```

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 the **type** command to display the contents of a file within any file directory on a WAAS device. The **type** command may be used to monitor features such as transaction logging or system logging (syslog).

Examples

The following example shows how to display the contents of the *syslog.txt* file:

```
WAE# type /local1/syslog.txt
```

Related Commands

cpfile

dir

lls

ls

pwd

rename

type-tail

To view a specified number of lines of the end of a log file, to view the end of the file continuously as new lines are added to the file, to start at a particular line in the file, or to include or exclude specific lines in the file, use the **type-tail** EXEC command.

type-tail *filename* [*line* | **follow** | | {**begin** *LINE* | **exclude** *LINE* | **include** *LINE*}]

Syntax Description

filename	File to be examined.
line	(Optional) Number of lines from the end of the file to be displayed (1–65535).
follow	(Optional) Displays the end of the file continuously as new lines are added to the file.
|	(Optional) Displays contents of the file according to the **begin**, **exclude**, and **include** output modifiers.
begin *LINE*	Identifies the line at which to begin file display. Specifies a regular expression to match in the file.
exclude *LINE*	Indicates lines that are to be excluded from the file display. Specifies a regular expression to match in the file.
include *LINE*	Indicates lines that are to be included in the file display. Specifies a regular expression to match in the file.

Defaults

The last ten lines are shown.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

The **type-tail** command allows you to monitor a log file by letting you view the end of the file. You can specify the number of lines at the end of the file that you want to view, or you can follow the last line of the file as it continues to log new information. To stop the last line from continuously scrolling as with the **follow** option, use the key sequence **Ctrl-C**.

You can further indicate the type of information to display using the output modifiers. These allow you to include or exclude specific lines or to indicate where to begin displaying the file.

Examples

The following example shows how to looks for a list of log files in the */local1* directory and then displays the last ten lines of the *syslog.txt* file. In this example, the number of lines to display is not specified, so the default of ten lines is used:

```
WAE# ls /local1
actona
core_dir
crash
```

```
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed

WAE# type-tail /local1/syslog.txt
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get https
equest throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/ftp connection 5
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/ftp' from dataserver
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get ftp-ov
r-http request throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: setValues getMethod
all ...
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: setValues found...
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/http/perf/throughput/requests/sum connection 5
Apr 17 00:21:48 edge-wae-11java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/http/perf/throughput/requests/sum' from dataserver
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: unable to get http r
quest throughput stats(error 4)
Apr 17 00:23:20 edge-wae-11 java: %CE-TBD-3-100000: WCCP_COND_ACCEPT: TU
LE DELETE conditional accept tuple {Source IP [port] = 0.0.0.0 [0]   Destinatio
 IP [port] = 32.60.43.2 [53775]  }returned error: -1 errno 9
```

The following example shows how to follow the *syslog.txt* file as it grows:

```
WAE# type-tail /local1/syslog.txt follow
```

virtual-blade

To change the virtual blade CD-ROM, save or delete the memory state, reset, or start and stop a virtual blade, use the **virtual-blade** EXEC command.

virtual-blade [*bladenumber*] {**cd** {**cd-rom** | **disk** *pathname* | **eject**} | **kill-save-state** | **reset** | **save** | **session** [**clear**] | **start** [*delay*] | **stop** [*timeout*]}

Syntax Description

bladenumber	(Optional) Number of the virtual blade. Valid values depend on the hardware capabilities. If you do not specify a number, the command is applied to all virtual blades.
cd	Changes the virtual blade CD-ROM.
cd-rom	Uses the WAE CD-ROM drive.
disk *pathname*	Specifies a CD-ROM image file located on the WAE hard drive This file is located in the */local1/vbs* directory.
eject	Ejects the disk from the WAE CD-ROM drive.
kill-save-state	Deletes the saved virtual blade memory state.
reset	Resets the virtual blade immediately.
save	Saves the current memory state of the virtual blade.
session	Opens a telnet session to the remote host/port.
clear	(Optional) Cancels the telnet session to the remote host/port.
start	Starts the specified virtual blade.
delay	(Optional) Startup delay for the virtual blade being started. Valid values are 1 through 60 seconds.
stop	Stops the specified virtual blade.
timeout	(Optional) Shutdown timeout delay for the virtual blade being stopped. Valid values are 0 through 900 seconds. Specify 0 to force immediate shutdown of the virtual blade (not a clean shutdown).

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **virtual-blade** EXEC command is used to execute general operations on a virtual blade. The **virtual-blade** *n* **cd** command changes the source of the virtual blade operating system image or ejects the CD. The **virtual-blade** *n* **save** command saves a snapshot of the current virtual blade memory state and saves it to /local1/vbs. The **virtual-blade** *n* **kill-save-state** command deletes the memory snapshot.

The **virtual-blade** *n* **reset** command immediately resets the virtual blade operating system, similar to pressing the reset button on a real computer. Because this is not a clean shutdown, you are prompted to confirm this command.

The **virtual-blade** *n* **start** and **virtual-blade** *n* **stop** commands allow you to activate and deactive the virtual blade. Each command has an optional delay.

When you use the **virtual-blade** *n* **stop** command, it sends a power down command to the virtual blade so that the guest OS can shut down cleanly. If the guest OS does not respond within the specified timeout, the virtual blade is not shut down. You may want to cleanly shut down the guest OS from the VNC console. You can specify a timeout of 0 to force an immediate unclean shutdown of the guest OS; you are also prompted to confirm this command.

Examples

The following example shows how to start virtual blade 1 immediately:

```
WAE# virtual-blade 1 start
```

The following example shows how to stop virtual blade 1 after a 3 minute timeout period:

```
WAE# virtual-blade 1 stop 180
```

The following example shows how to eject the CD in the WAE CD-ROM drive:

```
WAE# virtual-blade 1 cd eject
```

Related Commands

show virtual-blade

(config) virtual-blade

(config-vb) boot

(config-vb) device

(config-vb) disk

(config-vb) interface

(config-vb) memory

vm

To initialize the virtual machine after the VMware cloning operation, or to configure the host clock sync setting, use the **vm** EXEC command.

vm {{**clock-sync** {**disable** | **enable** | **status**} | **init**}

Syntax Description

clock-sync	Manually changes the host clock sync setting.
disable	Disables VM clock sync to host.
enable	Enables VM clock sync to host.
status	Displays the status of the VM clock sync to host setting.
init	Initializes the VM after the VMware cloning operation.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **vm** for vWAAS virtual machine operations. To speed up vWAAS deployments, you can create a clone of the vWAAS virtual machine. However, since the clone is an exact copy of the original vWAAS VM, you must use the **vm init** command to remove the certificate hash and the device registration information before the new vWAAS VM will register with the Central Manager.

You must reload the device after running **vm init**.

Use the **vm clock-sync** command to manually change the host clock sync setting without configuring NTP.

Examples

The following example shows how to initialize the virtual machine after the VMware cloning operation:

```
WAE# vm init
This command performs the following actions:
 - remove any network interface IP addresses,
 - deregister this device from CM, and
 - delete the machine's unique certificate hash.

Reload is REQUIRED to generate a new certificate hash
Continue?  (yes|no) [no]? yes
Interface Virtual 1/0 -> no ip address 2.1.6.116 255.255.255.0
Init complete.Reload the device to generate new certificate hash.
WAE#
```

Related Commands cms

waas-tcptrace

To list all the WAAS devices in the path to a destination host, use the **waas-tcptrace** EXEC command.

waas-tcptrace *ip-address port*

Syntax Description

ip-address	IP address of the destination host.
port	Port to connect to on the destination host.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Use **waas-tcptrace** to list all the WAAS devices in the path between the device on which this command is run and the specified destination host. The path is traversed in both directions.

This command returns the configured application accelerators, system policy, and effective system policy for each WAAS device found in the path, as well as the overall system policy for the connection.

You can use this command to find the overall policy applied to the connection and to find asymmetric paths.

Examples

The following example shows how to trace the route between the WAAS device and a destination host with an IP address of 2.75.227.50 on port 80:

```
WAE# waas-tcptrace 2.75.227.50 80
Response recieved from 2.75.227.137 on path TO destination...
Response recieved from 2.75.227.137 on path FROM destination ....

********************************************************************************
*****************************
Number of WAAS devices on the path TO 2.75.227.50 = 1
--------------------------------------------------------------------------------
------------------------------
 IP               MAC                AD Ver  Packet    Position  Device  Configured AO
Configured TFO    Derived TFO
--------------------------------------------------------------------------------
------------------------------
 2.75.227.137      0:21:5e:28:e1:34    4      Regular   1         SN      HTTP
Optimize Full     Optimize Full
--------------------------------------------------------------------------------
------------------------------
Number of WAAS devices on the path FROM 2.75.227.50 = 1
```

```
-------------------------------------------------------------------------------------------
------------------------------
 IP               MAC                 AD Ver  Packet    Position  Device  Configured AO
Configured TFO    Derived TFO
-------------------------------------------------------------------------------------------
------------------------------
 2.75.227.137      0:21:5e:28:e1:34    4      Regular   1         SN      HTTP
Optimize Full     Optimize Full
-------------------------------------------------------------------------------------------
------------------------------
The derived TFO policy for this connection is Passthrough (No Peer)
*******************************************************************************************
*****************************
```

Related Commands traceroute

whoami

To display the username of the current user, use the **whoami** EXEC command.

whoami

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **whoami** command to display the username of the current user.

Examples

The following example shows how to display your username:

```
WAE# whoami
admin
```

Related Commands

pwd

windows-domain

To join or leave a Windows domain or access the Windows domain utilities on a WAAS device, use the **windows-domain** EXEC command.

windows-domain join domain-name *domain* **[organization-unit** *org_unit*] **user** *username* [**debug**]

windows-domain leave [**user** *username*]

windows-domain diagnostics
{**domain-controller** {**list** | **status** | **time** [**domain-name** *domain_name*]} |
encryption-service {**get-key** *fqdn domain_name*} | **getent** |
group {**gid** *gid_no* | **groupname** *groupname* | **username** *username*} | **machine-account-info** |
user [**sid** *sid_name* | **uid** *user_no* | **username** *username*] | **verify join**}

Syntax Description

join	Joins a Windows domain.
domain-name *domain*	Specifies the domain to join.
organization-unit *org_unit*	(Optional) Specifies the organization unit of the domain.
user *username*	Specifies a user that has the permission to create a machine account on the domain controller.
debug	(Optional) Logs the domain join operation to the following file: /local1/logs/windows_domain_join.log
leave	Leaves a Windows domain.
diagnostics	Enables the selection of Windows domain diagnostic utilities.
domain-controller	Displays domain controller status information.
list	Displays information about all available domain controllers.
status	Displays the status of the currently joined domain controller.
time	Displays the time of the currently joined domain controller.
domain-name *domain_name*	(Optional) Displays the time of the domain controller specified.
encryption-service	Displays encryption service status information.
get-key *fqdn domain_name*	Displays the key retrieval information of the fully qualified domain name (for example, *machine-name*.cisco.com) and domain name.
getent	Displays the utility to get unified list of local users, PDC users, and groups.
group	Displays the diagnostic information of all groups or a particular group on Active Directory. In the output, a space in the group name is replaced by the "+" symbol.
gid *gid_no*	Displays group-related diagnostics information that corresponds to the group ID number specified.
groupname *groupname*	Displays group-related diagnostic information of a particular group.
username *username*	Displays group-related diagnostics information of a user.
machine-account-info	Displays the machine account-related information.

user	Displays the diagnostic information of all users or a particular user on Active Directory. In the output, a space in the username is replaced by the "+" symbol.
sid *sid_name*	(Optional) Displays the diagnostic information of a user based on the SID of the user specified.
uid *user_no*	(Optional) Displays the diagnostic information of a user based on the UID specified.
username *username*	(Optional) Display the diagnostic information of a user on Active Directory based on the username.
verify join	Displays the domain join status.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator

appnav-controller

central-manager

Usage Guidelines

Use the **windows-domain** command to join or leave a Windows domain or activate the selected Windows domain diagnostic utility.

When you use the **windows-domain join** command, it automatically discovers the windows domain configuration parameters and prompts you to approve the changes. You can respond with **yes** to approve the changes, **quit** to do nothing and exit the command, or **no** to enter interactive edit mode where you can edit any of the parameters before submitting the change.

If you do not specify the password as part of the command, you are prompted for the password and it is not shown on the console when you enter it.

Examples

The following example shows how to join a Windows domain and includes the interactive output:

```
WAE# windows-domain join domain-name waaslab.com user Administrator
Joining to AD Domain: WAASLAB.COM
With Computer DNS Name: wae.waaslab.com

administrator@WAASLAB.COM's password:
SUCCESS
```

The following example shows how to leave a Windows domain:

```
WAE# windows-domain leave user myname
```

Note In version 5.1.1, although the **windows-domain leave** operation disables the machine account on Active Directory (AD), it does not delete it.

The following example shows how to display the options available for the Get Entity utility:

```
WAE# windows-domain diagnostics getent --help
Usage: getent [OPTION...] database [key ...]
getent - get entries from administrative database.

  -s, --service=CONFIG       Service configuration to be used
  -?, --help                 Give this help list
      --usage                Give a short usage message
  -V, --version              Print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

Supported databases:
aliases ethers group hosts netgroup networks passwd protocols rpc
services shadow
```

Related Commands **(config) windows-domain**

write

To save startup configurations on a WAAS device, use the **write** EXEC command.

write [**erase** | **memory** | **mib-data** | **terminal**]

Syntax Description

erase	(Optional) Erases startup configuration from NVRAM.
memory	(Optional) Writes the configuration to NVRAM. This is the default location for saving startup information.
mib-data	(Optional) Saves MIB persistent configuration data to disk.
terminal	(Optional) Writes the configuration to a terminal session.

Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **write** command to either save running configurations to NVRAM or to erase memory configurations. Following a **write erase** command, no configuration is held in memory, and a prompt for configuration specifics occurs after you reboot the WAAS device.

Use the **write terminal** command to display the current running configuration in the terminal session window. The equivalent command is **show running-config**.

Examples

The following example shows how to save the current startup configuration to memory:

```
WAE# write memory
```

Related Commands

copy running-config

copy startup-config

show running-config

show startup-config