

# 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*

---

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

---



---

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

---

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

---

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

---

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

---

<b>Examples</b>	<p>The following example shows how to change to a directory using a relative path:</p> <pre>WAE(config)# cd local1</pre> <p>The following example shows how to change to a directory using an absolute path:</p> <pre>WAE(config)# cd /local1</pre>
-----------------	---

---

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

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

## Defaults

No default behavior or values.

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

## Command Modes

EXEC

## Device Modes

application-accelerator

## Examples

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

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

## Related Commands

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

# clear bmc

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

**clear bmc [event-log]**

<b>Syntax Description</b>	<b>event-log</b> Clears BMC system events and logs.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator appnav-controller
<b>Examples</b>	The following example shows how to clear the entries recorded in the BMC system event log on the WAAS device:  WAE# <code>clear bmc event-log</code>
<b>Related Commands</b>	<a href="#">show bmc</a>

# clear cache

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

**clear cache {dre}**

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

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

## Syntax Description

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

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator

## Usage Guidelines

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

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

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

## Examples

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

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

■ clear cache

---

Related Commands

**license add**

**show cache http-metadatacache**

**show interface**

**show license**

**show wcep**

# clear cache http-object-cache invalidate

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

**clear cache http-object-cache invalidate**

---

**Command Default** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

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

---

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

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

# clear cdp

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

**clear cdp {counters | table}**

Syntax Description	counters	Clears the CDP counters.
	table	Clears the CDP tables.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

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

```
WAE# clear cdp counters
```

**Related Commands** [license add](#)  
[show interface](#)  
[show license](#)  
[show wccp](#)



# clear connection

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

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

Syntax Description		Description
<b>client-ip</b>		Resets the connections with the specified client IP address or hostname.
<i>ip_address</i>		IP address of a client or server.
<i>hostname</i>		Hostname of a client or server.
<b>client-port</b> <i>port</i>		Resets the connections with the specified client port number. The port number is from 1 to 65535.
<b>flow-id</b> <i>id</i>		Resets the connection with the specified number identifier.
<b>server-ip</b>		Resets the connections with the specified server IP address or hostname.
<b>server-port</b> <i>port</i>		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	
<i>ip_address</i>	(Optional) IP address of a server.
<i>hostname</i>	(Optional) Hostname of a server.
<i>port</i>	(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		
<b>access-list</b>		Clears the access list statistical information.
<b>counters</b>		Clears the IP access list counters.
<i>acl-num</i>		(Optional) Counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
<i>acl-name</i>		(Optional) Counters for the specified access list, identified using an alphanumeric identifier of up to 30 characters, beginning with a letter.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

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

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

**Related Commands**

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

# clear ipv6

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

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

```
clear ipv6 neighbors virtual slot/port
```

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

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

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

**Related Commands**

- [show ipv6](#)
- [show interface](#)
- [show license](#)
- [show wccp](#)
- [clear ip](#)

# clear license

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

**clear license** [*license-name*]

<b>Syntax Description</b>	<i>license-name</i>	Name of the software license to remove. The following license names are supported: <ul style="list-style-type: none"> <li>• Transport—Enables basic DRE, TFO, and LZ optimization.</li> <li>• Enterprise—Enables the EPM, HTTP, MAPI, SSL, and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization. You cannot remove this license if the virtualization licenses are installed. You must remove both of those licenses first.</li> </ul>
---------------------------	---------------------	---

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

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

```
WAE# clear license
```

**Related Commands** [license add](#)  
[show interface](#)  
[show license](#)  
[show wccp](#)

# clear logging

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

## **clear logging**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

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

---

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

```
WAE# clear logging
```

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

---

**Related Commands** [license add](#)  
[show interface](#)  
[show license](#)  
[show wccp](#)

# clear object-cache

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

**clear object-cache [accelerator *smb*] all**

Syntax Description		
<b>accelerator</b> <i>smb</i>	(Optional) The name of the application accelerator specified, such as SMB.	
<b>all</b>	Clears all objects from the object cache. If you specify <b>all</b> , you will be prompted to confirm this action. Note that for WAAS Version 6.0, <b>all</b> is used only with accelerator SMB.	

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** The **clear object-cache** command removes all objects from the object cache, or all objects from cache that match specified criteria,

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

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

**Related Commands** [clear statistics accelerator http object-cache](#)

# 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.
	<b>appnav</b>	Clears AppNav class map and policy map counters.
	<b>waas</b>	Clears WAAS optimization class map and policy map counters.
	<b>counters</b>	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 | dre [global] | exporter | filtering | flow
  monitor type performance-monitor tcpstat-v1 | generic-gre | icmp | inline | ip | ipv6
  {internal} | 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
<b>all</b>	Clears all statistics.
<b>aoim</b>	Clears all of the application accelerator information manager statistics.
<b>appnav-controller all</b>	Clears all of the AppNav Controller statistics.
<b>authentication</b>	Clears authentication statistics.
<b>auto-discovery</b>	Clears the auto-discovery statistics.
<b>blacklist</b>	Clears the auto-discovery statistics for the blacklist.
<b>class-map</b>	Clears all class map statistics.
<b>appnav</b>	Clears all statistics for AppNav class maps.
<b>waas</b>	Clears all statistics for WAAS class maps.
<b>datamover</b>	Clears all of the data mover statistics.
<b>dre</b>	Clears the Data Redundancy Elimination (DRE) statistics.
<b>exporter</b>	Clears the exporter statistics.
<b>global</b>	(Optional) Clears the global DRE statistics.
<b>filtering</b>	Clears the filter table statistics.
<b>flow</b>	Clears the network traffic flow statistics.
<b>monitor</b>	Clears the monitor flow performance statistics.
<b>tcpstat-v1</b>	Clears the tcpstat-v1 collector statistics.
<b>generic-gre</b>	Clears the generic GRE statistics.
<b>icmp</b>	Clears the ICMP statistics.
<b>inline</b>	Clears the inline interception statistics.
<b>ip</b>	Clears the IP statistics.
<b>ipv6</b>	Clears IPv6 statistics.
<b>pass-through</b>	Clears all of the pass-through statistics.
<b>peer dre</b>	Clears all peer DRE statistics.
<b>punt</b>	Clears all the punt statistics.
<b>radius</b>	Clears the RADIUS statistics.
<b>service-insertion</b>	Clears AppNav service-insertion statistics.
<b>appnav-controller</b> <i>ip_address</i>	Clears statistics for the AppNav Controller with the specified IP address.
<b>appnav-controller-group</b> <i>data-path</i>	Clears statistics for the AppNav Controller group.
<b>data-path</b>	Clears statistics for the data path.

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

**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.

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

**Examples**

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

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

**Related Commands**

[clear statistics accelerator](#)  
[clear statistics connection](#)

# clear statistics accelerator

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

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

Syntax Description		
<b>epm</b>		Clears the statistics for the EPM application accelerator.
<b>generic</b>		Clears the statistics for generic accelerator.
<b>http</b>		Clears the statistics for the HTTP application accelerator.
<b>mapi</b>		Clears the statistics for the MAPI application accelerator.
<b>ssl</b>		Clears the statistics for the SSL application accelerator.
<b>smb</b>		Clears the statistics for the SMB application accelerator, <i>except</i> 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 <b>clear statistics accelerator generic</b> , which clears all accelerator statistics, including signed SMB bytes counters.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

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

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

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

# clear statistics accelerator http object-cache

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

**clear statistics accelerator http object-cache**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** Use this command to clear object cache statistics.

---

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

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

---

**Related Commands** [show statistics accelerator http object-cache](#)

# clear statistics connection

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

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

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

## Syntax Description

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

**clear statistics connection**

---

**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 }
```

<b>Syntax Description</b>	<b>accelerator</b>	Clears the accelerator transaction log file.
	<b>flow</b>	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		
	<b>administrative</b>	(Optional) Clears the connections (logins) of administrative users authenticated through a remote login service.
	<b>locked-out</b>	(Optional) Unlocks specified locked-out user accounts.
	<b>all</b>	Specifies all user accounts.
	<b>username</b> <i>username</i>	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		
	<b>identity</b> <i>tagName</i>	Clears identity information.
	<b>service</b> <i>spn</i>	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		
<b>read-calendar</b>		Reads the calendar and updates the system clock.
<b>set</b> <i>time day month year</i>		Sets the time and date. Current time in hh:mm:ss format (hh: 00–23; mm: 00–59; ss: 00–59). Day of the month (1–31). Month of the year (January, February, March, April, May, June, July, August, September, October, November, December). Year (1993–2035).
<b>update-calendar</b>		Updates the calendar with the system clock.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

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

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

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

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

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

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

## cms

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

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

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

Syntax Description		
<b>config-sync</b>		Sets the node to synchronize configuration with the WAAS Central Manager.
<b>deregister</b>		Removes the device registration record and its configuration on the WAAS Central Manager.
<b>force</b>		(Optional) Forces the removal of the node registration. This option is available only on WAEs and the standby Central Manager. If disk encryption is enabled, it is disabled and encrypted file systems are erased after a reload.
<b>lcm</b>		Configures local/central management on a WAAS device that is registered with the WAAS Central Manager.
<b>enable</b>		Enables synchronization of the WAAS network configuration of the device with the local CLI configuration.
<b>disable</b>		Disables synchronization of the WAAS network configuration of the device with the local CLI configuration.
<b>maintenance</b>		Cleans and reindexes the embedded database tables.
<b>full</b>		Specifies a full maintenance routine for the embedded database tables.
<b>regular</b>		Specifies a regular maintenance routine for the embedded database tables.
<b>recover</b>		Recovers the identity of a WAAS device.
<b>identity</b> <i>word</i>		Specifies the identity of the recovered device (identification key set on the Central Manager).
<b>restore</b> <i>filename</i>		Restores the database management tables using the backup local filename.
<b>validate</b>		Validates the database files.
<b>database</b>		Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
<b>backup</b>		Backs up the database management tables.
<b>config</b>		Backs up only configuration tables.
<b>create</b>		Creates the embedded database management tables.
<b>delete</b>		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	
<b>init</b>	Initializes secure store encryption on the WAE device and opens the secure store. This option is valid only on WAE devices.
<b>open</b>	<p>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 <b>cms secure-store init</b> command.</p> <p>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.</p>
<b>change</b>	<p>Changes the secure store encryption pass phrase and encryption key. On the Central Manager, this command prompts you to enter the current pass phrase, new pass phrase, and confirm the new pass phrase. The WAAS device uses the pass phrase to generate the encryption key for secure disk encryption.</p> <p>After this option is used, the Central Manager is in user-provided passphrase mode.</p> <p>This option is valid only on the primary Central Manager and WAE devices.</p>
<b>clear</b>	<p>Disables secure store encryption. This option is valid only on WAE devices.</p> <p><b>Note</b> If a Windows Domain User Account Identity has been configured on the device or the device group for encrypted-mapi acceleration, you will not be able to clear the secure store on the device. You must remove the Windows domain user account identity configuration from the device or device group before you can clear secure store.</p>
<b>reset</b>	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.
<b>mode</b>	Sets the secure store mode of opening. This option is valid only on primary Central Manager devices.
<b>user-passphrase</b>	Sets secure store to require a user-provided pass phrase to open after a reboot.
<b>auto-passphrase</b>	Sets secure store to automatically open after a reboot by using a unique system-generated pass phrase.

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

**Command Modes** EXEC

**Device Modes**

application-accelerator  
central-manager

**Usage Guidelines**

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

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

**Note**

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

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

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

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

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

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

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

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

---

## Examples

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

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

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

```
Enter new passphrase:
Confirm passphrase:
```

```
Starting cms.
```

---

**Related Commands**    [show cms secure-store](#)

# configure

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

## **configure**

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

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

**Defaults** No default behaviors or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
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 wow-recovery** {*hostname* | *ip-address*} *remotefiledir remotefilename*

Syntax Description		
<b>disk</b>		Copies a file to a local disk.
<i>hostname</i>		Hostname of the specific server.
<i>ip-address</i>		IP (IPv4/IPv6) address of the specific server.
<i>remotefiledir</i>		Directory on the FTP server where the image file to be copied is located.
<i>remotefilename</i>		Name of the file to be copied.
<i>localfilename</i>		Name of the copied file as it appears on the local disk.
<b>install</b>		Copies the file from an FTP server and installs the software release or firmware file to the local device.

**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.

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 (*/local/bios\_upgrade.txt*) for traceability. The hardware-dependent files that are downloaded from Cisco.com for the BIOS upgrade are automatically deleted from the WAAS device after the BIOS upgrade procedure has been completed.

```

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

```

#### Related Commands

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



# copy http

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

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

Syntax Description		
<b>install</b>		Copies the file from an HTTP server and installs the software release file to the local device.
<i>hostname</i>		Name of the HTTP server.
<i>ip-address</i>		IP (IPv4/IPv6) address of the HTTP server.
<i>remotefiledir</i>		Remote file directory.
<i>remotefilename</i>		Remote filename.
<b>port</b> <i>portnum</i>		(Optional) Specifies the port number (1–65535) to connect to the HTTP server (the default is 80).
<b>proxy</b> <i>proxy_portnum</i>		(Optional) Allows the request to be redirected to an HTTP proxy server. HTTP proxy server port number (1–65535).
<b>username</b> <i>username</i> <i>password</i>		(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		
<b>disk</b> <i>filename</i>		Copies the statistics in CSV format to the specified local disk file in the /local/local1 directory.
<b>ftp</b>		Copies the statistics in CSV format to the specified remote file on an FTP server.
<i>hostname</i>		Name of the FTP server.
<i>ip-address</i>		IP (IPV4/IPv6) address of the FTP server.
<i>remotefiledir</i>		Remote file directory.
<i>remotefilename</i>		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:

```
WAB# 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		
	<b>disk filename</b>	Copies the current system configuration to a disk file. Specify the name of the file to be created on a disk.
	<b>startup-config</b>	Copies the running configuration to startup configuration (NVRAM).
	<b>tftp</b>	Copies the running configuration to a file on a TFTP server.
	<i>hostname</i>	Hostname of the TFTP server.
	<i>ip-address</i>	IP (IPv4/IPv6) address of the TFTP server.
	<i>remotefilename</i>	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		
<b>disk</b>		Copies the current system configuration to a disk file.
<i>hostname</i>		Hostname of the SCP server.
<i>ip-address</i>		IP (IPv4/IPv6) address of the SCP server.
<i>remote_dir</i>		Remote directory where the system information file is to be created on the SCP server.
<i>remote_file</i>		Remote filename of the system information file to be created on the SCP server.
<i>local_file</i>		Name of the copied file as it appears on the local disk.
<b>install</b>		Copies the file from a source server and installs the software release or firmware file to the local device.
<i>hostname</i>		Hostname of the SCP server.
<i>ip-address</i>		IP address of the SCP server.
<i>remote_dir</i>		Remote directory where the system information file is to be created on the SCP server.
<i>remote_file</i>		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 username 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 2018 by damaster
Converting Manifest files ... Done
Rebuilding image based on current software ... Done
Backing up flash configuration ... Done
Reclaiming unused flash safe state sectors ...SSMGR RETURNING: 4 (Success)
Done.
Detected OE594
Installing phase3 bootloader...
Installing WAE 64-bit image.
buildsysimg: short write on /swstore/comp.basesystem: Inappropriate ioctl for device
/swstore/default_ruby_installer.sh: problem running buildsysimg
Remove /swstore/backup to free up space.
Installing system image to flash... The new software will run after you reload.
```

**Related Commands**

**install**  
**copy sysreport**  
**copy tech-support**

# copy secure-http

To securely copy configuration or image files from a source http server, use the **copy secure-http** EXEC command.

```
copy secure-http install {hostname | ip-address}
```

```
copy secure-http install usb filename
```

<b>install</b>	Copies the file from a source server and installs the software release or firmware file to the local device.
<i>hostname</i>	Hostname of the HTTP server.
<i>ip-address</i>	IP (IPv4/IPv6) address of the HTTP server.
<b>usb</b> <i>filename</i>	The filename on the USB flash drive installed in a WAVE or ENCS device.

**Defaults** No default behaviors or values.

**Command Modes** EXEC

**Device Modes**

- application-accelerator
- appnav-controller
- central-manager

**Usage Guidelines** Use the **copy secure-http install** EXEC command to copy and install a software release from a secure HTTP server on a WAAS device.

**Examples** The following example shows how to securely install the software release or firmware file from a sourcehttp server to a destination location:

```
WAE#copy secure-http install 2.43.65.21 /work/admin ruby.test.bin
```

**Related Commands**

- [install](#)
- [copy scp](#)
- [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		
<b>disk</b> <i>filename</i>		Copies the startup configuration to a disk file. Specify the name of the startup configuration file to be copied to the local disk.
<b>running-config</b>		Copies the startup configuration to running configuration.
<b>tftp</b>		Copies the startup configuration to a file on a TFTP server.
<i>hostname</i>		Hostname of the TFTP server.
<i>ip-address</i>		IP (IPv4/IPv6) address of the TFTP server.
<i>remotefilename</i>		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

<b>disk</b> <i>filename</i>	Copies system information to a disk file. Specify the name of the file to be created on a disk. Note that .tar.gz is appended to the filename that you specify.
<b>ftp</b>	Copies system information to a FTP server.
<i>hostname</i>	Hostname of the server.
<i>ip-address</i>	IP(IPV4/IPV6) address of the server.
<i>remotedirectory</i>	Remote directory where the system information file is to be created on the server.
<i>remotefilename</i>	Remote filename of the system information file to be created on the server.
<b>scp</b>	Copies system information to a SCP server.
<i>hostname</i>	Hostname of the server.
<i>ip-address</i>	IP address of the server.
<i>remotedirectory</i>	Remote directory where the system information file is to be created on the server.
<i>remotefilename</i>	Remote filename of the system information file to be created on the server.
<b>start-date</b>	(Optional) Specifies the start date of the information in the generated system report.
<i>day month</i>	Start date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.
<i>year</i>	Start date year (1993–2035).
<b>end-date</b>	(Optional) 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.
<i>day month</i>	End date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.

<i>year</i>	End date year (1993–2035).
<b>tftp</b>	Copies system information to a TFTP server.
<b>start-date</b>	(Optional) Specifies the start date of the information in the generated system report.
<i>day month</i>	Start date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.
<i>year</i>	Start date year (1993–2035).
<b>end-date</b>	(Optional) 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.
<b>usb filename</b>	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**

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

**Note**

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

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

**copy sysreport ftp** *server-ip*

- Generating the system report:

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



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

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

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

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

- Storing the completed system report:

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

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

#### Examples

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

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

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

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

#### Related Commands

**cms**  
**pwd**  
**show running-config**  
**show startup-config**  
**test**

# copy system-status

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

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

---

<b>Syntax Description</b>	<b>disk <i>filename</i></b>	Specifies the name of the file to be created on the disk.
---------------------------	-----------------------------	---

---

---

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

---

---

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

---

---

<b>Device Modes</b>	application-accelerator appnav-controller central-manager
---------------------	---

---

---

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

---

---

<b>Examples</b>	The following example shows how to copy the system status to a disk file: <pre>WAE# copy system-status disk file1</pre>
-----------------	--

---

---

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

---

# copy tech-support

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

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

## Syntax Description

<b>disk</b> <i>filename</i>	Copies system information for technical support to a disk file. Specify the name of the file to be created on disk.
<b>ftp</b>	Copies system information for technical support to an FTP server.
<i>hostname</i>	Hostname of the server.
<i>ip-address</i>	IP (IPv4/IPv6) address of the server.
<i>remotedirectory</i>	Remote directory of the system information file to be created on the server. Use the complete pathname.
<i>remotefilename</i>	Remote filename of the system information file to be created on the server.
<b>scp</b>	Copies system information for technical support to an SCP server
<i>hostname</i>	Hostname of the server.
<i>ip-address</i>	IP address of the server.
<i>remotedirectory</i>	Remote directory of the system information file to be created on the server. Use the complete pathname.
<i>remotefilename</i>	Remote filename of the system information file to be created on the server.
<b>tftp</b>	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		
<b>disk</b>		Copies an image from a TFTP server to a disk file.
<i>hostname</i>		Hostname of the TFTP server.
<i>ip-address</i>		IP (IPv4/IPv6) address of the TFTP server.
<i>remotefilename</i>		Name of the remote image file to be copied from the TFTP server. Use the complete pathname.
<i>localfilename</i>		Name of the image file to be created on the local disk.
<b>running-config</b>		Copies an image from a TFTP server to the running configuration.
<b>startup-config</b>		Copies an image from a TFTP server to the startup configuration.

**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](#)



# cpfile

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

**cpfile** *oldfilename newfilename*

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

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

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator

## Usage Guidelines

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

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



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

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

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

## Examples

The following example shows how to create an exportable self-signed certificate. The certificate file is named myfile.p12 and is created using a 2048-bit RSA modulus.

```
WAE# crypto generate self-signed-cert myfile.p12 exportable rsa modulus 2048
Generating a 2048bit RSA private key
.....+++++++
.....+++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [California]:<cr> (Press Enter to accept the default.)
Locality Name (eg, city) [San Jose]:San Jose
Organization Name (eg, company) [Cisco Systems]:
Organizational Unit Name (eg, section) [ADBU]:
Common Name (eg, YOUR name) [www.cisco.com]:
Email Address [tac@cisco.com]:

WAE#
```

## Related Commands

[crypto delete](#)  
[crypto export](#)  
[crypto import](#)

# crypto import

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

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

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

```
crypto import pcks12 { filename | admin } [exportable] [ignore-cert-chain-order] pkcs12 { disk pathname | ftp host | http host | sftp host | terminal | tftp host }
```

## Syntax Description

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

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator

central-manager

---

**Usage Guidelines**

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



---

**Note** DSA certificates and keys cannot be imported.

---

---

**Examples**

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

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

---

**Related Commands**

[crypto delete](#)

[crypto export](#)

[crypto generate](#)



# crypto pki

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

## **crypto pki managed-store initialize**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

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

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

**Related Commands**

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

# debug aaa accounting

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

**debug aaa accounting**

**undebug aaa accounting**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug aaa accounting
```

---

**Related Commands**

[show debugging](#)

# debug aaa authorization

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

**debug aaa authorization**

**undebug aaa authorization**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug aaa authorization
```

---

**Related Commands**

[show debugging](#)

# debug accelerator

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### Syntax Description

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

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



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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

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

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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



#### Note

To compress the detailed SMB accelerator logs and make the logging more optimal, you can use the **wae#debug accelerator LogShrink enable** command. To disable compression, use **wae#debug accelerator LogShrink disable** command. This command is enabled by default.

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

#### Examples

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

```
WAE# debug accelerator all
```

#### Related Commands

[show debugging](#)

# debug accelerator http object-cache

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

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

Syntax Description	all	Enable all object-cache debugging.
	<b>configuration</b>	Enable configuration debugging.
	<b>gate-keeper</b>	Enable gate keeper debugging.
	<b>logger</b>	Enable logger debugging.
	<b>preposition</b>	Enable cache prepositioning debugging.
	<b>response-headers</b>	Enable debugging headers in HTTP response.
	<b>statistics</b>	Enable statistics debugging.
	<b>traffic-plugin</b>	Enable traffic plugin debugging.

**Command Default** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

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

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

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

# debug accelerator mapi rpchttp-layer

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

**debug accelerator mapi rpchttp-layer**

**no debug accelerator mapi rpchttp-layer**

---

## Defaults

No default behavior or values.

---

## Command Modes

EXEC

---

## Device Modes

application-accelerator

---

## Usage Guidelines

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

---

## Examples

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

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

---

## Related Commands

[debug accelerator](#)

# debug all

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

**debug all**

**undebug all**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to enable all debug monitoring:

```
WAE# debug all
```

---

**Related Commands**

[show debugging](#)

# debug 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
```

<b>Syntax Description</b>	<b>access-list</b> <i>acl-name</i>	Enables access list connection debugging. Access list name is an alphanumeric identifier up to 30 characters, beginning with a letter.
---------------------------	------------------------------------	--

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

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

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

<b>Usage Guidelines</b>	<p>The ACL specified in this command is shared by the <b>monitor appnav-controller traffic</b> and <b>packet-capture</b> commands.</p> <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> </ul>
-------------------------	--

- 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		
	<b>index</b> <i>index</i>	The number of the index; the default index value is 255.
	<b>limit</b> <i>limit</i>	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 23.

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		
	<b>user</b>	Enables debugging of the user login against the system authentication.
	<b>windows-domain</b>	Enables Windows domain authentication debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

### Examples

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

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

---

Related Commands [show debugging](#)

# debug auto-discovery

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

**debug auto-discoveryconnection**

**undebug auto-discovery connection**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)

# debug buf

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

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

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

Syntax Description	all	Enables all buffer manager debugging.
	<b>dmbuf</b>	Enables only dmbuf debugging.
	<b>dmsg</b>	Enables only dmsg debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug buff all
```

---

**Related Commands**

[show debugging](#)



# debug cdp

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

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

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

Syntax Description		
	<b>adjacency</b>	Enables CDP neighbor information debugging.
	<b>events</b>	Enables CDP events debugging.
	<b>ip</b>	Enables CDP IP debugging.
	<b>packets</b>	Enables packet-related CDP debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug cdp events
```

---

**Related Commands**

[show debugging](#)

# debug cli

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

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

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

Syntax Description	all	Enables all CLI debugging.
	<b>bin</b>	Enables CLI command binary program debugging.
	<b>parser</b>	Enables CLI command parser debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug cli all
```

---

**Related Commands**

[show debugging](#)

# debug cmm

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

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

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

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug cmm all
```

---

**Related Commands**

[show debugging](#)

# debug cms

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

```
debug cms{router-config | stats}
```

```
undebug cms
```

## Syntax Description

<b>router-config</b>	Enables debug only router configuration from CM
<b>stats</b>	Enables debug only statistics

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator  
central-manager

## Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to enable CMS debug monitoring:

```
WAE# debug cms
```

---

**Related Commands**

[show debugging](#)



# debug connection

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

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

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

Syntax Description		
<b>all</b>		Enables all connection-specific debugging.
<b>access-list</b> <i>acl-name</i>		Enables access list connection debugging. Access list name is an alphanumeric identifier up to 30 characters, beginning with a letter.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug connection all
```

---

**Related Commands**

[show debugging](#)

# debug 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 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to 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.
	<b>clientlib</b>	Enables data server client library module debugging.
	<b>server</b>	Enables data server module debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug dataserver all
```

---

**Related Commands**

[show debugging](#)

# debug dhcp

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

**debug dhcp**

**undebug dhcp**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to enable DHCP debug monitoring:

```
WAE# debug dhcp
```

---

**Related Commands**

[show debugging](#)



# debug dre

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

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

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

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug dre all
```

---

**Related Commands**

[show debugging](#)

# debug egress-method

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

**debug egress-method connection**

**undebug egress-method connection**

<b>Syntax Description</b>	<b>connection</b> (Optional) Enables egress method connection debugging.
---------------------------	--

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

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

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

<b>Usage Guidelines</b>	<p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p>
-------------------------	---

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		
	<b>all</b>	Enables debugging of all encryption services components.
	<b>application-layer</b>	Enables debugging of the encryption services application layer.
	<b>cfgmgr</b>	Enables debugging of the encryption services configuration manager.
	<b>dcerpc-layer</b>	Enables debugging of the encryption services dcerpc layer.
	<b>gss</b>	Enables debugging of the encryption services gss.
	<b>io</b>	Enables debugging of the encryption services io.
	<b>secure-store</b>	Enables debugging of the encryption services secure store.
	<b>server</b>	Enables debugging of the encryption services server.
	<b>shell</b>	Enables debugging of the encryption services shell.
	<b>transport-lib</b>	Enables debugging of the encryption services transport library.
	<b>utilities</b>	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 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)

# debug fda

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

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

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

Syntax Description		
	<b>all</b>	Enables all flow distribution agent debugging.
	<b>events</b>	Enables only flow distribution agent event debugging.
	<b>infra</b>	Enables only flow distribution agent infra debugging.
	<b>messages</b>	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 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug fda all
```

---

**Related Commands**

[show debugging](#)



# debug fdm

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

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

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

Syntax Description	all	Enables all flow distribution manager debugging.
	<b>events</b>	Enables only flow distribution manager event debugging.
	<b>infra</b>	Enables only flow distribution manager infra debugging.
	<b>messages</b>	Enables only flow distribution manager message debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug fdm all
```

---

**Related Commands**

[show debugging](#)

# debug filtering

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

**debug filtering connection**

**undebug filtering connection**

Syntax Description	<b>connection</b> (Optional) Enables filtering module connection debugging.
--------------------	---

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

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

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

Usage Guidelines	<p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in <code>/local1/syslog.txt</code> or the debug log associated with the module in the file <code>/local1/errorlog/module_name-errorlog.current</code>.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <code>name-errorlog.#</code>, where <code>#</code> is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul>
------------------	--

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

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

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

---

**Examples**

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

```
WAE# debug filtering connection
```

---

**Related Commands**

[show debugging](#)

# debug flow

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

**debug flow monitor type performance-monitor tcpstat-v1**

**undebug flow monitor type performance-monitor tcpstat-v1**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)

# debug generic-gre

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

**debug generic-gre**

**undebug generic-gre**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)



# debug hw-raid

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

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

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

Syntax Description	all	Enables all hardware RAID debug commands.
	<b>cli</b>	Enables hardware RAID CLI debugging.
	<b>daemon</b>	Enables hardware RAID daemon debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)

# debug imd

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

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

```
undebug {all | cli | infra | nprm | stats}
```

Syntax Description		
	<b>all</b>	Enables all interface manager debugging.
	<b>cli</b>	Enables only interface manager cli debugging.
	<b>infra</b>	Enables only interface manager infra debugging.
	<b>nprm</b>	Enables only interface manager nprm debugging.
	<b>stats</b>	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 23.

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

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

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

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

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

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

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

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

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

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

---

### Examples

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

```
WAE# debug imd all
```

---

### Related Commands

[show debugging](#)

# debug inline

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

```
debug inline { debug | info | warn }
```

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

Syntax Description		
<b>debug</b>	Sets the debug level to debug.	
<b>info</b>	Sets the debug level to info.	
<b>warn</b>	Sets the debug level to warn.	

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug inline warn
```

---

**Related Commands**

[show debugging](#)

# debug key-manager

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

**debug key-manager**

**undebug key-manager**

Syntax Description	<b>key-manager</b> (Optional) Enables key manager debugging.
Defaults	No default behavior or values.
Command Modes	EXEC
Device Modes	central-manager (primary only)
Usage Guidelines	<p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul>

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

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

We recommend that you use the **debug** and **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	<b>all</b>	Enables all logging debugging.
--------------------	------------	--------------------------------

Defaults No default behavior or values.

Command Modes EXEC

Device Modes application-accelerator  
central-manager

**Usage Guidelines**

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug logging all
```

---

**Related Commands**

[show debugging](#)

# debug mapi

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	<b>all</b> Enables all logging debugging.
--------------------	---

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

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

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

Usage Guidelines	<p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul>
------------------	---

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

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

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

---

**Examples**

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

```
WAE# debug logging all
```

---

**Related Commands**

[show debugging](#)



# debug monapi

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

**debug monapi**

**undebug monapi**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** central-manager (primary only)

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug monapi
```

---

**Related Commands**

[show debugging](#)

# debug nplogd

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

**debug nplogd all**

**undebug nplogd all**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application accelerator

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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



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

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

---

**Examples**

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

```
WAE# debug nplogd all
```

---

**Related Commands**

[show debugging](#)

# debug ntp

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

**debug ntp**

**undebug ntp**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to enable NTP debug monitoring:

```
WAE# debug ntp
```

---

**Related Commands**

[show debugging](#)

# debug object-cache database

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

**debug object-cache database**

**no debug object-cache database**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

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

---

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

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

---

**Related Commands** [debug object-cache existence-cache](#)  
[debug object-cache load-monitor](#)

# debug object-cache existence-cache

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

**debug object-cache existence-cache**

**no debug object-cache existence-cache**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

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

---

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

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

---

**Related Commands** [debug object-cache database](#)

# debug object-cache load-monitor

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

**debug object-cache load-monitor**

**no debug object-cache load-monitor**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

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

---

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

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

---

**Related Commands** [debug object-cache database](#)  
[debug object-cache existence-cache](#)

# debug 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		
	<b>all</b>	Enables all punt handler debugging.
	<b>module</b>	Enables only punt handler module debugging.
	<b>packets</b>	Enables only punt handler packet debugging.
	<b>socket</b>	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 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to enable all punt handler debug monitoring:

```
WAE# debug punt all
```

---

**Related Commands**

[show debugging](#)



# debug rbc

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

**debug rbc**

**undebug rbc**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

The following example shows how to enable RBCP debug monitoring:

```
WAE# debug rbc
```

---

**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 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug rmd all
```

---

**Related Commands**

[show debugging](#)

# debug rpc

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

```
debug rpc {detail | trace}
```

```
undebug rpc {detail | trace}
```

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug rpd detail
```

---

**Related Commands**

[show debugging](#)

# debug service-insertion

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

**debug service-insertion connection**

**undebug service-insertion connection**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
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 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)



# debug service-policy

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

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

**undebug service-policy type { appnav | waas }**

Syntax Description		
	<b>appnav</b>	Enables AppNav service policy debugging.
	<b>waas</b>	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 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

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

---

**Related Commands**

[show debugging](#)

# debug snmp

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

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

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

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug snmp all
```

---

**Related Commands**

[show debugging](#)

# debug standby

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

**debug standby [all]**

**undebug standby [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Enables standby debugging using all debug features.
---------------------------	---

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

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

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

<b>Usage Guidelines</b>	<p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul>
-------------------------	---

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

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

We recommend that you use the **debug** and **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		
	<b>all</b>	Enables all statistics debug commands.
	<b>ao</b>	Enables statistics acceleration debugging.
	<b>client</b>	Enables statistics client debugging.
	<b>collector</b>	Enables statistics collector debugging.
	<b>ipc</b>	Enables statistics IPC debugging.
	<b>messages</b>	Enables statistics messages/buffers debugging.
	<b>serializer</b>	Enables statistics serializer debugging.
	<b>sqm</b>	Enables statistics computation debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug statistics all
```

---

**Related Commands**

[show debugging](#)



# debug 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	<b>connection</b> Enables synq module connection debugging.
--------------------	---

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

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

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

Usage Guidelines	<p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request”</a> section on page 23.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul>
------------------	---

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

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

We recommend that you use the **debug** and **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		
<b>all</b>		Enables all TFO debugging.
<b>buffer-mgr</b>		Enables TFO data-buffer from buffer manager debugging.
<b>dre-flow</b>		Enables TFO DRE flow debugging for all connections.
<b>netio</b>		Enables TFO connection debugging for the network input/output module.
<b>scheduler</b>		Enables TFO scheduler debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug tfo all
```

---

**Related Commands**

[show debugging](#)

# debug translog

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

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

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

Syntax Description	detail	Enables transaction log detailed debugging.
	<b>export</b>	Enables transaction log FTP export debugging.
	<b>info</b>	Enables transaction log high level debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug translog detail
```

---

**Related Commands**

[show debugging](#)

# debug wafs

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

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

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

Syntax Description		
	<b>manager</b>	Sets the logging level for the Device Manager.
	<b>debug</b>	Specifies debug.
	<b>error</b>	Specifies error.
	<b>info</b>	Specifies info.
	<b>warn</b>	Specifies warn.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

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

---

**Examples**

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

```
WAE# debug wafs manager error
```

---

**Related Commands**

[show debugging](#)



# debug wccp

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

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

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

Syntax Description		
	<b>all</b>	Enables all WCCP debugging functions.
	<b>detail</b>	Enables the WCCP detail debugging.
	<b>error</b>	Enables the WCCP error debugging.
	<b>events</b>	Enables the WCCP events debugging.
	<b>keepalive</b>	Enables the debugging for WCCP keepalives that are sent to the applications.
	<b>packets</b>	Enables the WCCP packet-related information debugging.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

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

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

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

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

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

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

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

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

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

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

---

### Examples

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

```
WAE# debug wccp all
```

---

### Related Commands

[show debugging](#)

# delfile

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

**delfile** *filename*

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

# 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*]

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory to list.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager
<b>Usage Guidelines</b>	Use the <b>dir</b> EXEC command to view a detailed list of files contained within the working directory, including information about the file name, size, and time created. The <b>lls</b> EXEC command produces the same output.
<b>Examples</b>	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 23 14:40:00 2018 <DIR>   actona
    4096   Tue Mar 27 14:42:44 2018 <DIR>   core_dir
    4096   Wed Apr 11 20:23:10 2018 <DIR>   crash
    4506   Tue Apr 10 13:52:45 2018 dbupgrade.log
    4096   Wed Apr  4 22:50:11 2018 <DIR>   downgrade
    4096   Sun Apr 15 09:01:56 2018 <DIR>   errorlog
    4096   Wed Apr 11 20:23:41 2018 <DIR>   logs
   16384   Thu Feb 15 12:25:29 2018 <DIR>   lost+found
    4096   Wed Apr 11 03:26:02 2018 <DIR>   sa
   24576   Sun Apr 15 23:38:21 2018 <DIR>   service_logs
    4096   Thu Feb 15 12:26:09 2018 <DIR>   spool
  9945390   Sun Apr 15 23:38:20 2018 syslog.txt
  10026298   Fri Apr  6 12:25:00 2018 syslog.txt.1
  10013564   Fri Apr  6 12:25:00 2018 syslog.txt.2
  10055850   Fri Apr  6 12:25:00 2018 syslog.txt.3
  10049181   Fri Apr  6 12:25:00 2018 syslog.txt.4
    4096   Thu Feb 15 12:29:30 2018 <DIR>   var
    508    Sat Feb 24 13:18:35 2018 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 Fri Apr 6 12:13:50 2018 <DIR> actona
4096 Tue Mar 6 14:14:41 2018 <DIR> apache
4096 Sun Apr 15 23:36:40 2018 <DIR> emdb
4096 Thu Feb 15 11:51:51 2018 <DIR> export
  92 Wed Apr 11 20:23:20 2018 ftp_export.status
4096 Wed Apr 11 20:23:43 2018 <DIR> rpc_httpd
  0 Wed Apr 11 20:23:41 2018 snmpd.log
4096 Sun Mar 11 18:47:29 2018 <DIR> tfo
```

---

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

# disable

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

## **disable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

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

```
WAE> enable
Password:
```

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

---

**Examples** The following example shows how to enter the user-level EXEC mode from the privileged EXEC mode:

```
WAE# disable
WAE>
```

---

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

# disk

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

**disk delete-partitions** *diskname*

**disk delete-data-partitions**

**disk delete-preserve-software**

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

**disk disk-name** *diskxx* **replace**

**disk insert** *diskname*

**disk recreate-raid**

**disk scan-errors** *diskname*

Syntax Description		
<b>delete-partitions</b> <i>diskname</i>	Deletes data on the specified logical disk drive. After using this command, the WAAS software treats the specified disk drive as blank. All previous data on the drive is inaccessible.	Specify the name of the disk from which to delete partitions (disk00, disk01). For RAID-5 systems, this option is not available because only one logical drive is available.
<b>delete-data-partitions</b>	Deletes all data partitions on all logical drives. Data partitions include the CONTENT, PRINTSPOOL, and GUEST partitions. These partitions include all DRE cache files and print spool files.	
<b>delete-preserve-software</b>	Deletes all disk and data partitions and preserves current software version and CM registration details.	
<b>disk-name</b> <i>diskxx</i> <b>enable force</b>	Reenables a defunct drive (with or without removing it) that has been previously shut down.	<b>Note</b> This option is available only on RAID-5 systems.
<b>disk-name</b> <i>diskxx</i> <b>replace</b>	Shuts down the physical disk with the name <i>diskxx</i> (disk00, disk01, etc.) so that it can be replaced in the RAID-5 array.	<b>Note</b> This option is available only on RAID-5 systems.
<b>insert</b> <i>diskname</i>	Instructs the SCSI host to rescan the bus to detect and mount the newly inserted disk. Specify the name of the disk to be inserted (disk00, disk01).	<b>Note</b> This option is available only on WAE-612 models.
<b>recreate-raid</b>	Recreates the RAID-5 array.	<b>Note</b> This option is available only on RAID-5 systems.
<b>scan-errors</b> <i>diskname</i>	Scans SCSI or IDE disks for errors and remaps the bad sectors if they are unused. Specify the name of the disk to be scanned (disk00, disk01).  For RAID-5 systems, this command scans the logical RAID device for errors. On these systems, there is no <i>diskname</i> option.	



---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

- 
- Usage Guidelines**
- The WAAS software supports hot-swap functionality for both failed disk replacement and scheduled disk maintenance. On the WAE-612, use the **disk disk-name diskxx shutdown** global configuration command to shut down a disk for scheduled disk maintenance. (For the scheduled disk maintenance procedure, see the chapter “Maintaining Your WAAS System” in the *Cisco Wide Area Application Services Configuration Guide*.)
    - The disk hot-swap functionality automatically disables a failed disk if the system detects one critical disk alarm. The software removes the failed disk automatically regardless of the setting for **disk error-handling**.
    - For WAE-612 models, when you replace a failed disk that was automatically disabled by the software, use the **disk insert** EXEC command to bring the disk back into service. For all other models, see the **(config) disk disk-name** command section.
  - To identify which disks have been identified as failed or bad, use the **show disks failed-disk-id** EXEC command. Do not reinsert any disk with a serial number shown in this list.
  - Use the **disk delete-partitions** EXEC command to remove all disk partitions on a single disk drive on a WAAS device or to remove the disk partition on the logical drive for RAID-5 systems.




---

**Caution**

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

- The **disk delete-data-partitions** command deletes the DRE caches.
- After using the **disk delete-data-partitions** command, you must reload the device.




---

**Note** After using the **disk delete-data-partitions** command, you must reload the device with a cold boot. If you reload the device with a warm boot, all data is not cleared, which may prevent the device from establishing connections.

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

- When you upgrade to software version 6.1.1, and execute **disk-delete-preserve-software** command for the first time, all data and system partitions are re-created.

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

---

**Examples**

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

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

---

**Related Commands**

[\(config\) disk disk-name](#)  
[\(config\) disk error-handling](#)  
[\(config\) disk object-cache extend](#)  
[show disks](#)

# dnslookup

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

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

Syntax Description		
	<i>hostname</i>	Name of DNS server on the network.
	<i>domainname</i>	Name of domain.
	<i>ip-address</i>	IPv4 or IPv6 address

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Examples** The following example shows how the **dnslookup** command is used to resolve the hostname *myhost* to IP 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
```

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

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

# enable

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

**enable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

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

---

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

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

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

---

**Examples** The following example shows how to access privileged EXEC mode:

```
WAE> enable
WAE#
```

---

**Related Commands** [disable](#)  
[exit](#)

# exit

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

**exit**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** All modes

---

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

---

**Usage Guidelines** The **exit** EXEC command is equivalent to pressing **Ctrl-Z** or entering the **end** command. Entering the **exit** command in the user level EXEC shell terminates the console or Telnet session.

---

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

```
WAE# exit  
WAE>
```

---

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

# find-pattern

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

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

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

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

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

**Examples** The following example shows how to search a file recursively for a case-sensitive pattern:

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

```
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*

<b>Syntax Description</b>	<i>filename</i>	Specifies the name of the <i>.bin</i> file you want to install.
---------------------------	-----------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Device Modes</b>	application-accelerator appnav-controller central-manager
---------------------	---

<b>Usage Guidelines</b>	The <b>install</b> 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.
-------------------------	--



<b>Note</b>	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.



<b>Note</b>	The <b>install</b> command does not accept <i>.pax</i> files. Files should be of the type <i>.bin</i> (for example, <i>cache-sw.bin</i> ). 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 <b>install</b> command may result in a write to flash memory.
-------------	--

Close your browser and restart the browser session to the WAAS Central Manager, if you installed a new software image to the primary WAAS Central Manager.

<b>Examples</b>	The following example shows how to load the system image contained in the <i>wae512-cache-300.bin</i> file:
-----------------	---

```
WAE# install wae512-cache-300.bin
```

■ install

---

Related Commands [copy disk](#)  
[reload](#)

# less

To display a file using the Less application, use the **less** EXEC command.

**less** *file\_name*

<b>Syntax Description</b>	<i>file_name</i>	Name of the file to be displayed.
---------------------------	------------------	-----------------------------------

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Device Modes</b>	application-accelerator central-manager
---------------------	--

<b>Usage Guidelines</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Backward movement</b>—Allows you to move backward in the displayed text. Use <b>k</b>, <b>Ctrl-k</b>, <b>y</b>, or <b>Ctrl-y</b> to move backward. See the summary of Less commands for more details; to view the summary, press <b>h</b> or <b>H</b> while displaying a file in Less.</li> <li>• <b>Searching and highlighting</b>—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.</li> <li>• <b>Multiple file support</b>—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.</li> </ul>
-------------------------	---

<b>Examples</b>	<p>The following example shows how to display the text of the <i>syslog.txt</i> file using the Less application:</p> <pre>WAE# less syslog.txt</pre>
-----------------	--

<b>Related Commands</b>	<a href="#">type</a>
-------------------------	----------------------

# license add

To add a software license to a device, use the **license add** EXEC command.

**license add** *license-name*

<b>Syntax Description</b>	<i>license-name</i>	Name of the software license to add. The following license names are supported: <ul style="list-style-type: none"> <li>• Transport—Enables basic DRE, TFO, and LZ optimization.</li> <li>• Enterprise—Enables the EPM, HTTP, MAPI, SSL, and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization.</li> </ul>
<b>Defaults</b>	No default behavior or values.	
<b>Command Modes</b>	EXEC	
<b>Device Modes</b>	application-accelerator central-manager	
<b>Examples</b>	The following example shows how to install the enterprise license: WAE# <b>license add Enterprise</b>	
<b>Related Commands</b>	<a href="#">clear arp-cache license</a> <a href="#">show license</a>	

# lls

To view a long list of directory names, use the **lls** EXEC command.

**lls** [*directory*]

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory for which you want a long list of files.
---------------------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Device Modes</b>	application-accelerator central-manager
---------------------	--

<b>Usage Guidelines</b>	The <b>lls</b> command provides detailed information about files and subdirectories stored in the present working directory (including the size, date, time of creation, SYSFS name, and long name of the file). This information can also be viewed with the <b>dir</b> command.
-------------------------	---

<b>Examples</b>	The following example shows how to display a detailed list of the files in the current directory:
-----------------	---

```
WAE# lls
size          time of last change          name
-----
    4096  Fri Feb 23 14:40:00 2018 <DIR>  actona
    4096  Tue Mar 27 14:42:44 2018 <DIR>  core_dir
    4096  Wed Apr 11 20:23:10 2018 <DIR>  crash
    4506  Tue Apr 10 13:52:45 2018 dbupgrade.log
    4096  Wed Apr  4 22:50:11 2018 <DIR>  downgrade
    4096  Sun Apr 15 09:01:56 2018 <DIR>  errorlog
    4096  Wed Apr 11 20:23:41 2018 <DIR>  logs
   16384  Thu Feb 15 12:25:29 2018 <DIR>  lost+found
    4096  Wed Apr 11 03:26:02 2018 <DIR>  sa
   24576  Sun Apr 15 23:54:30 2018 <DIR>  service_logs
    4096  Thu Feb 15 12:26:09 2018 <DIR>  spool
   9951236 Sun Apr 15 23:54:20 2018 syslog.txt
  10026298 Fri Apr  6 12:25:00 2018 syslog.txt.1
    4096  Thu Feb 15 12:29:30 2018 <DIR>  var
    508   Sat Feb 24 13:18:35 2018 wdd.sh.signed
```

<b>Related Commands</b>	<a href="#">dir</a> <a href="#">lls</a> <a href="#">ls</a>
-------------------------	--

# 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*]

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory for which you want a list of files.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager
<b>Usage Guidelines</b>	Use the <b>ls</b> <i>directory</i> command to list the filenames and subdirectories within a particular directory. Use the <b>ls</b> command to list the filenames and subdirectories of the current working directory. Use the <b>pwd</b> command to view the present working directory.
<b>Examples</b>	The following example shows how to display the files and subdirectories that are listed within the root directory: <pre>WAE# ls actona core_dir crash dbupgrade.log downgrade errorlog logs lost+found sa service_logs spool syslog.txt syslog.txt.1 var wdd.sh.signed</pre>
<b>Related Commands</b>	<a href="#">dir</a> <a href="#">lls</a>

**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*

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory for which you want a list of files.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager
<b>Usage Guidelines</b>	<p>Use the <b>lsusb</b> <i>directory</i> command to list the filenames and subdirectories within a particular directory on the USB device.</p> <p>Use the <b>lsusb</b> command to list the filenames and subdirectories of the current working directory on the USB device.</p> <p>This command is available only on WAAS devices that support external USB storage devices.</p>
<b>Examples</b>	<p>The following example shows how to display the files and subdirectories that are listed within the root directory of a USB device:</p> <pre>WAE# <b>lsusb</b> directory1 afile.txt bfile.txt</pre>
<b>Related Commands</b>	<p><b>dir</b></p> <p><b>lls</b></p> <p><b>ls</b></p> <p><b>pwd</b></p>



# mkdir

To create a directory, use the **mkdir** EXEC command.

**mkdir** *directory*

---

<b>Syntax Description</b>	<i>directory</i>	Name of the directory to create.
---------------------------	------------------	----------------------------------

---

---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

---

<b>Command Modes</b>	EXEC
----------------------	------

---

<b>Device Modes</b>	application-accelerator central-manager
---------------------	--

---

<b>Examples</b>	The following example shows how to create a new directory, <i>oldpaxfiles</i> :
-----------------	---

```
WAE# mkdir /oldpaxfiles
```

---

<b>Related Commands</b>	<a href="#">cpfile</a> <a href="#">dir</a> <a href="#">lls</a> <a href="#">ls</a> <a href="#">pwd</a> <a href="#">rename</a> <a href="#">rmdir</a>
-------------------------	--

# mkfile

To create a new file, use the **mkfile** EXEC command.

**mkfile** *filename*

---

<b>Syntax Description</b>	<i>filename</i>	Name of the file that you want to create.
---------------------------	-----------------	---

---



---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

---



---

<b>Command Modes</b>	EXEC
----------------------	------

---



---

<b>Device Modes</b>	application-accelerator central-manager
---------------------	--

---



---

<b>Usage Guidelines</b>	Use the <b>mkfile</b> EXEC command to create a new file in any directory of the WAAS device.
-------------------------	--

---



---

<b>Examples</b>	The following example shows how to create a new file, <i>traceinfo</i> , in the root directory: WAE# <b>mkfile traceinfo</b>
-----------------	---

---



---

<b>Related Commands</b>	<a href="#">cpfile</a> <a href="#">dir</a> <a href="#">lls</a> <a href="#">ls</a> <a href="#">mkdir</a> <a href="#">pwd</a> <a href="#">rename</a>
-------------------------	--

---

# 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 }
```

<b>Syntax Description</b>	<b>access-list</b> <i>acl-name</i> Name of the access list that determines which flows are monitored.
	<b>disable</b> Disables flow monitoring.
<b>Defaults</b>	Monitoring is disabled.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	appnav-controller
<b>Usage Guidelines</b>	<p>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 <b>ip access-list</b> global configuration command.</p> <p>The ACL specified in this command is shared by the <b>packet-capture</b> and <b>debug appnav-controller</b> commands.</p> <p>Use the <b>show statistics monitor appnav-controller traffic</b> EXEC command to display the monitoring statistics.</p> <p>Use the <b>show monitor</b> EXEC command to display the status of traffic monitoring.</p>
<b>Examples</b>	<p>The following example shows how to enable traffic monitoring with an ACL:</p> <pre>ANC# <b>monitor appnav-controller traffic access-list myacl</b></pre>
<b>Related Commands</b>	<p><a href="#">clear statistics monitor appnav-controller traffic</a></p> <p><a href="#">show monitor</a></p> <p><a href="#">show statistics monitor appnav-controller traffic</a></p>

# 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}]
```

<b>Syntax Description</b>	<i>hostname</i>	NTP hostname.
	<i>ip-address</i>	NTP server IP (IPv4/IPv6) address.
	<b>key</b>	(Optional) Specifies to use authentication with the NTP server.
	<i>authentication-key</i>	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 all-interfaces { access-list { acl-name | acl-num } | destination-ip { hostname | ip-address } | destination-port port | source-ip { hostname | ip-address } | source-port port } [ file-size size [ number-of-files num | stop-after-num-files num ] ] | packet-size | non-encapsulated | [capture-filename]
```

```
packet-capture 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 ] ] | packet-size | non-encapsulated | [capture-filename]
```

```
packet-capture interface { GigabitEthernet slot/port | TenGigabitEthernet slot/port | PortChannel index | standby grpnumber } | virtual slot/port | { access-list { acl-name | acl-num } | destination-ip { hostname | ip-address } | destination-port port | source-ip { hostname | ip-address } | source-port port } [ file-size size [ number-of-files num | stop-after-num-files num ] ] | packet-size | non-encapsulated | [capture-filename]
```

```
packet-capture decode [ destination-ip { hostname | ip-address } | destination-port port | source-ip { hostname | ip-address } | source-port port ] [ file-size size [ number-of-files num | stop-after-num-files num ] ] | packet-size | non-encapsulated | [capture-filename]
```

```
packet-capture stop [ file-size size [ number-of-files num | stop-after-num-files num ] ] | packet-size | nonencapsulated [capture-filename]
```

## Syntax Description

<b>all-interfaces</b>	Specifies all interfaces as the source from which to capture packets.
<b>appnav-controller</b>	Capture packets on an AppNav Controller Interface Module interface.
<b>access-list</b> <i>acl-name</i>   <i>acl-num</i>	Specifies an access list for which to capture packets on the specified interface. When used with <b>packet-capture appnav-controller</b> , the <b>access-list</b> specifies an access list for which to capture packets across all AppNav Controller Interface Module interfaces. <ul style="list-style-type: none"> <li>(Optional) <i>acl-name</i>—Access list name.</li> <li>(Optional) <i>acl-num</i>—Access list numeric identifier (0–99 for standard access lists and 100–199 for extended access lists).</li> </ul>
<i>capture-filename</i>	(Optional) Specifies the name of a file to which output is saved. If no file is specified, output is sent to the console.
<b>decode</b>	Decodes captured packets.
<b>destination-ip</b> <i>hostname</i>   <i>ip-address</i>	Captures packets matching the specified destination IP address. <ul style="list-style-type: none"> <li><i>hostname</i>—The specified destination hostname.</li> <li><i>ip-address</i>—The specified destination IP address.</li> </ul>
<b>destination-port</b> <i>port</i>	Captures packets matching the specified destination port.
<b>file-size</b> <i>size</i>	(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.
<b>GigabitEthernet</b> <i>slot/port</i>	Specifies a Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).

<b>interface</b>	Specifies the source interface from which to capture packets.
<b>non-encapsulated</b>	Capture packets that are not SIA encapsulated.
<b>number-of-files</b> <i>num</i>	(Optional) Specifies the maximum number of output files to create (1–500), after which earlier files are overwritten as needed for more captured data.
<b>packet-size</b>	The maximum number of capture bytes per packet.
<b>PortChannel</b> <i>index</i>	Specifies a port channel interface (1-4).
<b>source-ip</b> <i>hostname</i>   <i>ip-address</i>	Captures packets matching the specified source IP address. <ul style="list-style-type: none"> <li>• <i>hostname</i>—The specified source hostname.</li> <li>• <i>ip-address</i>—The specified source IP address.</li> </ul>
<b>source-port</b> <i>port</i>	Capture packets matching the specified source port number.
<b>standby</b> <i>grpnumber</i>	Specifies a standby group (1-2).
<b>stop</b>	Stop automatically capturing packets.
<b>stop-after-num-files</b> <i>num</i>	(Optional) Specifies the maximum number of output files to create (1–500), after which packet capture is stopped.
<b>TenGigabitEthernet</b> <i>slot/port</i>	Specifies a 10-Gigabit Ethernet interface. The slot number and port number are separated with a forward slash character (/).
<b>Virtual</b> <i>slot/port</i>	Capture packets matching the specified virtual slot/port. The slot range is 1–2; the port range is 0.

**Defaults**

No default behavior or values.

**Command Modes**

EXEC

**Device Modes**

Note the following device mode usage for the **packet-capture** command:

- application-accelerator device mode
  - Used with **packet-capture all-interfaces**, **packet-capture interface**, **packet-capture decode**, and **packet-capture stop**.
- appnav-controller device mode
  - Used with **packet-capture all-interfaces**, **packet-capture interface**, **packet-capture appnav-controller**, **packet-capture decode**, and **packet-capture stop**.
- central-manager device mode
  - Used with **packet-capture all-interfaces**, **packet-capture interface**, **packet-capture decode**, and **packet-capture stop**.

**Usage Guidelines**

The following are usage guidelines for the packet-capture command:

- Either packet capture or debug capture can be active, but not both simultaneously.

The **packet-capture** command is preferred over the deprecated commands **tcpdump** and **tethereal**, and is required to capture data plane traffic on an AppNav Controller Interface Module interface.

- For WAAS Version 6.2.1 and later, you can run the **packet-capture** command in multiple sessions (telnet or ssh) on the same or different interfaces, up to a maximum of five sessions, that print in the WAE.

---

**Examples**

The following example shows how to capture packets on a general interface:

```
WAE(config)# ip access-list extended 100 permit tcp 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	<b>management</b>	Uses the designated management interface for the ping.
	<i>hostname</i>	Hostname of system to ping.
	<i>ip-address</i>	IP address of system to ping.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes**

- application-accelerator
- 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](#)



# ping6

To send echo packets for diagnosing basic network connectivity on IPv6 networks, use the **ping6** EXEC command.

```
ping6 {hostname | ip-address}[management]
```

Syntax Description		
	<i>hostname</i>	Hostname of system to ping.
	<i>ip-address</i>	IPv6 address of system to ping.
	<b>management</b>	Uses the designated management interface for the ping.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** To use the **ping6** command with the *hostname* argument, make sure that DNS functionality is configured on the WAAS device. To force the timeout of a nonresponsive host, or to eliminate a loop cycle, press **Ctrl-C**.

When you use a device's management interface to establish connectivity to another device, using **ping6 command**, and the management interface goes down, the communication will still succeed if the address of the end device is reachable from any other interface.

**Examples** The following example shows how to send echo packets to a machine with address 2013:1:1:10::5 to verify its availability on the network:

```
WAE# ping 2013:1:1:10::5

PING 2013:1:1:10::5(2013:1:1:10::5) 56 data bytes
64 bytes from 2013:1:1:10::5: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 2013:1:1:10::5: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 2013:1:1:10::5: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 2013:1:1:10::5: icmp_seq=4 ttl=64 time=0.029 ms
64 bytes from 2013:1:1:10::5: icmp_seq=5 ttl=64 time=0.029 ms

--- 2013:1:1:10::5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.018/0.028/0.037/0.006 ms
```

**Related Commands** [traceroute6](#)



# pwd

To view the present working directory on a WAAS device, use the **pwd** EXEC command.

## **pwd**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Examples** The following example shows how to display the current working directory:

```
WAE# pwd  
/local1
```

---

**Related Commands** [cd](#)  
[dir](#)  
[lls](#)  
[ls](#)

# reload

To halt the operation and perform a cold restart on a WAAS device, use the **reload** EXEC command.

**reload** [**force** | **in** *m* | **cancel**]

Syntax Description	
<b>force</b>	(Optional) Forces a reboot without further prompting.
<b>in</b> <i>m</i>	(Optional) Schedules a reboot after a specified interval (1-10080 minutes).
<b>cancel</b>	(Optional) Cancels a scheduled reboot.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** To reboot a WAAS device, use the **reload** command. If no configurations are saved to flash memory, you are prompted to enter configuration parameters upon a restart. Any open connections are dropped after you enter the **reload** command, and the file system is reformatted upon restart.

The **reload** command can include the option to schedule a reload of the software to take effect in a specified number of minutes. After entering this command, you are asked to confirm the reload by typing *y* and then confirm WCCP shutdown by typing *y* again (if WCCP is active).

You can use the **cancel** option to cancel a scheduled reload.

**Examples** The following example shows how to halt the operation of the WAAS device and reboot with the configuration saved in flash memory. You are not prompted for confirmations during the process.

```
WAE# reload force
```

**Related Commands** [write](#)

# rename

To rename a file on a WAAS device, use the **rename** EXEC command.

```
rename oldfilename newfilename
```

Syntax Description	<i>oldfilename</i>	Original filename.
	<i>newfilename</i>	New filename.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **rename** command to rename any SYSFS file without making a copy of the file.

**Examples** The following example shows how to rename the *errlog.txt* file to *old\_errlog.txt*:

```
WAE# rename errlog.txt old_errlog.txt
```

**Related Commands** [cpfile](#)

# restore

To restore the device to its manufactured default status by removing the user data from the disk and flash memory, use the **restore EXEC** command.

**restore { factory-default [preserve basic-config] | rollback }**

## Syntax Description

<b>factory-default</b>	Resets the device configuration and data to their manufactured default status.
<b>preserve</b>	(Optional) Preserves certain configurations and data on the device.
<b>basic-config</b>	(Optional) Selects basic network configurations.
<b>rollback</b>	Rolls back the configuration to the last functional software and device configuration.

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator  
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 100 - DAS)    140011MB(136.7GB)
disk01: Normal          (h00 c00 i01 100 - DAS)    140011MB(136.7GB)
```

```
Mounted filesystems:
```

MOUNT POINT	TYPE	DEVICE	SIZE	INUSE	FREE	USE%
/	root	/dev/root	35MB	30MB	5MB	85%
/swstore	internal	/dev/md1	991MB	333MB	658MB	33%
/state	internal	/dev/md2	3967MB	83MB	3884MB	2%
/disk00-04	CONTENT	/dev/md4	122764MB	33MB	122731MB	0%
/local/locall	SYSFS	/dev/md5	3967MB	271MB	3696MB	6%
.../locall/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) 1999-2018 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 6.4.3 (build b21 Mar 23 2018)
Version: oe612-6.4.3.340

Compiled 17:26:17 Mar 23 2018 by cnbuild

System was restarted on Mon Mar 26 15:25:02 2018.
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

<i>directory</i>	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

<b>4</b>	(Optional) Forces this command to use only IPv4 addresses.
<b>6</b>	(Optional) Forces this command to use only IPv6 addresses.
<b>B</b>	(Optional) Specifies the batch mode. In this mode, the <b>scp</b> command does not ask for passwords or passphrases.
<b>C</b>	(Optional) Enables compression. The <b>scp</b> command passes this option to the <b>ssh</b> command to enable compression.
<b>p</b>	(Optional) Preserves the following information from the source file: modification times, access times, and modes.
<b>q</b>	(Optional) Disables the display of progress information.
<b>r</b>	(Optional) Recursively copies directories and their contents.
<b>v</b>	(Optional) Specifies the verbose mode. Causes the <b>scp</b> and <b>ssh</b> commands to print debugging messages about their progress. This option can be helpful when troubleshooting connection, authentication, and configuration problems.
<b>c</b> <i>cipher</i>	(Optional) Specifies the cipher to use for encrypting the data being copied. The <b>scp</b> command directly passes this option to the <b>ssh</b> command.
<b>F</b> <i>config-file</i>	(Optional) Specifies an alternative per-user configuration file for Secure Shell (SSH). The <b>scp</b> command directly passes this option to the <b>ssh</b> command.
<b>i</b> <i>id-file</i>	(Optional) Specifies the file containing the private key for RSA authentication. The <b>scp</b> command directly passes this information to the <b>ssh</b> command.
<b>o</b> <i>ssh_option</i>	(Optional) Passes options to the <b>ssh</b> command in the format used in <i>ssh_config5</i> . See the <b>ssh</b> command for more information about the possible options.
<b>P</b> <i>port</i>	(Optional) Specifies the port to connect to on the remote host.
<b>S</b> <i>program</i>	(Optional) Specifies the program to use for the encrypted connection.
<i>user</i>	(Optional) Username.
<i>host</i>	(Optional) Hostname.
<i>file</i>	(Optional) Name of the file to copy.

## Command Modes

EXEC

## Device Modes

application-accelerator  
central-manager

---

**Usage Guidelines**

The **scp** command uses SSH for transferring data between hosts. This command is enabled by default. This command prompts you for passwords or pass phrases when needed for authentication.

---

**Related Commands**

[ssh](#)

# script

To execute a script provided by Cisco or check the script for errors, use the **script EXEC** command.

```
script {check | execute} file_name
```

Syntax Description	check	execute
	Checks the validity of the script.	Executes the script. The script file must be a SYSFS file in the current directory.
	<i>file_name</i>	Name of the script file.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **script EXEC** command opens the script utility, which allows you to execute Cisco-supplied scripts or check errors in those scripts. The script utility can read standard terminal input from the user if the script you run requires input from the user.



**Note** The script utility is designed to run only Cisco-supplied scripts. You cannot execute script files that lack Cisco signatures or that have been corrupted or modified.

**Examples** The following example shows how to check for errors in the script file *test\_script.pl*:

```
WAE# script check test_script.pl
```

# setup

To configure basic configuration settings (general settings, device network settings, interception type, disk configuration, and licenses) on the WAAS device or to complete basic configuration after upgrading to the WAAS software, use the **setup** EXEC command.

## setup

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** For instructions on using the **setup** command, see the *Cisco Wide Area Application Services Quick Configuration Guide*.  
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: <ul style="list-style-type: none"> <li>• Exec</li> <li>• Command level 0</li> <li>• Command level 15</li> <li>• System</li> </ul>
Record Event(s)	Configuration of the AAA accounting notice that is sent to the accounting server.
stop-only	WAAS device that sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.

**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: <ul style="list-style-type: none"> <li>• Command level 0</li> <li>• Command level 15</li> </ul>
Protocol	Authorization protocol that is configured.

**Related Commands** [\(config\) aaa authorization commands](#)

# show accelerator

To display the status and configuration of the application accelerators, use the **show accelerator EXEC** command.

**show accelerator** [**detail** | **epm** | **http** [**debug**]| **ica** | **interposer-ssl** | **mapi** | **smb** | **ssl** | **wansecure**]

Syntax Description	
<b>detail</b>	(Optional) Displays the license information, configuration state, and operational state for all accelerators, and additional accelerator and policy engine configuration.
<b>epm</b>	(Optional) Displays the status for the EPM application accelerator.
<b>http</b>	(Optional) Displays the status for the HTTP application accelerator.
<b>debug</b>	(Optional) Displays more detailed status for the HTTP application accelerator.
<b>ica</b>	(Optional) Displays the status for the ICA application accelerator.
<b>mapi</b>	(Optional) Displays the status for the MAPI application accelerator.
<b>smb</b>	(Optional) Displays the status for the SMB application accelerator.
<b>ssl</b>	(Optional) Displays the status for the SSL application accelerator.
<b>wansecure</b>	(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
-----
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 mapi** command:

```

wae#sh accelerator mapi
Accelerator  Licensed  Config State  Operational State
-----
mapi        Yes      Enabled       Running

```

MAPI:

```

Accelerator Config Item  Mode  Value
-----
Read optimization        Default  enabled
Write optimization       Default  enabled
Reserved pool size max percent  Default  15%
Mapi Encryption          Default  enabled
WanSecure Mode           Default  auto
Rpc HTTP optimization    Default  enabled
Mapi over Http           Default  enabled
Mapi over Http Header Optimization  Default  enabled

Policy Engine Config Item
-----
State                    Registered
Default Action           Use Policy
Connection Limit         750
Effective Limit           740
Keepalive timeout        5.5 seconds

```

The following example displays the output for the **show accelerator smb** command:

```

wae# show accelerator smb
Accelerator  Licensed  Config State  Operational State
-----
smb          Yes      Enabled       Running

```

SMB:

```

Accelerator Config Item  Mode  Value
-----
WanSecure Mode           User  always
MultiChannel Status      User  Disabled
Encryption Status        Default  L7-opt-enable
Digital signing alarm    Default  Disabled
Change Notification size  Default  10
DRE hints                 Default  Enabled
Highest dialect           User  smb3-02
  Exceed action           Default  handoff
Matches dialect          Default  smb3-11
  Action                   Default  none
Named pipe optimization  Default  Enabled
  Resp. cache lifetime (s)  Default  20
  Sess. cache lifetime (s)  Default  30
  NamedPipe-cache size (KB)  Default  300      (default: 300
maximum: 900)

```

```

NF metadata cache opt           Default      Enabled
  Max size (MB)                 Default      32
  Aging (s)                     Default      30
  Bypass patterns               Default
SMB Print optimization          Default      Enabled
SMB Object Cache support        Default      Enabled
SMB Load-bypass support         Default      Enabled
Microsoft Office optimization  Default      Enabled
SMB2 Read-caching opt          Default      Enabled
SMB2 Guestbit opt              Default      Enabled
SMB3 Read-caching opt          Default      Enabled
Optimization bypass pattern     User         [^p]\.ini$|\\\\HCLINTON\\
\\MES\\sDOCUMENTS
  Smb2 Dir opt                   Default      Enabled
    Smb2-Dir-opt-cache size (MB) Default      55          (default: 55
maximum: 55)
    Smb2-Dir-opt-pre-fetch       Default      Enabled
  Read-ahead opt                Default      Enabled
    Buffer size (MB)              Default      110         (default: 110
maximum: 220)
  Directory listing opt          Default      Enabled
  SMB3 Async-write opt           Default      Enabled
    Quota threshold (MB)         Default      20
    Quota aging time (s)         Default      60
  SMB2 Async-write opt           Default      Enabled
    Quota threshold (MB)         Default      20
    Quota aging time (s)         Default      60
  Async-write opt                Default      Enabled
    Quota threshold (MB)         Default      20
    Quota aging time (s)         Default      60
  Metadata-opt                  Default      Enabled
    Metadata-cache size (MB)     Default      75          (default: 75
maximum: 75)
  smb2-Batch-close-opt           Default      Enabled
  smb2-Invalid-fid-opt           Default      Enabled
  smb3-Batch-close-opt           Default      Enabled
  smb3-Invalid-fid-opt           Default      Enabled
  large-pkt                      User         Enabled
  Iobuf size (MB)                Default      50          (default: 50
maximum: 100)
  Max iobuf size for 1 pkt(KB)   User         1030
  Directory aging time           Default      30
  Dynamic share                   Default
  Oplock opt                       Default      Enabled
    Client OS patterns           Default      Mac OS
  Signing opt                       Default      Enabled
    Unwrap opt                   Default      Enabled
  Debug assert                     Default      Disabled
  SMB Preposition DRE              Default      Disabled
  Symmetrickey expiry time(mins)  Default      180
  SMB202 Keyretrival              Default      Disabled
  Adm-ctrl mem-threshold           User         60
  Adm-ctrl restart-threshold       Default      60
  identity configured alarm        Default      Enabled
  Lowlatency-threshold             Default      10
  Lowlatency-interval             Default      60

Policy Engine Config Item        Value
-----
State                            Registered
Default Action                    Use Policy
Connection Limit                   750
Effective Limit                     740
Keepalive timeout                  5.5 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 epm](#)

[\(config\) accelerator http](#)

[\(config\) accelerator ica](#)

[\(config\) accelerator mapi](#)

**(config) accelerator smb**  
**(config) accelerator ssl**  
**show statistics accelerator**

# show accelerator http object-cache

To display HTTP object cache configuration and status information for a WAAS device, use the **show accelerator http object-cache EXEC** command.

## show accelerator http object-cache

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use the show accelerator http object-cache command to display HTTP object cache configuration and status information for a WAAS device.

**Examples** The following example shows output from the **show accelerator http object-cache** command:

```

HTTP Object-cache Version
-----

                                Mode      Value
                                ----      -
Object-cache                    User      Enabled
      Transparent                Default   Enabled
      Connected                  Default   Disabled
      OTT                        Default   Disabled
      Default Profile            Default   standard

      Host-profile-count         Default   0

```

**Related Commands** [show statistics accelerator http object-cache](#)

# show alarms

To display information about various types of alarms, their status, and history on a WAAS device, use the **show alarms EXEC** command.

**show alarms critical [detail [support]]**

**show alarms detail [support]**

**show alarms history** [*start\_num* [*end\_num* [**detail** [**support**]]]] | **critical** [*start\_num* [*end\_num* [**detail** [**support**]]]]

**show alarms major** [*start\_num* [*end\_num* [**detail** [**support**]]]]

**show alarms minor** [*start\_num* [*end\_num* [**detail** [**support**]]]]

**show alarms status**

**show alarms core**

**show alarms crash**

## Syntax Description

<b>critical</b>	Displays critical alarm information.
<b>detail</b>	(Optional) Displays detailed information for each alarm.
<b>support</b>	(Optional) Displays additional information about each alarm.
<b>history</b>	Displays information about the history of various alarms.
<i>start_num</i>	(Optional) Alarm number that appears first in the alarm history.
<i>end_num</i>	(Optional) Alarm number that appears last in the alarm history.
<b>major</b>	Displays information about major alarms.
<b>minor</b>	Displays information about minor alarms.
<b>status</b>	Displays the status of various alarms and alarm overload settings.
<b>core</b>	Displays all core dump files (if any)
<b>crash</b>	Displays all crash files (if any)

## 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**

The following example shows output from the show alarms core file details command:

```
vWAAS-6k#sh alarms core
```

Corefile Details:

Time	Process Name	Corefile Name
-----	-----	-----
Mon Mar 25 17:42:37 2019	waasnet	core.waasnet.bin.6.4.3b.b10.jmaddula.5146.tar.gz
Mon Mar 25 17:42:37 2019	sar	core.sar.6.2.3d.b68.cnbuild.31684.tar.gz
Mon Mar 25 17:42:37 2019	smbao64	core.smbao64.6.2.3b.b22.cnbuild.17004.tar.gz
Mon Mar 25 17:42:37 2019	nscd	core.nscd.6.4.1a.b6.cnbuild.32690.tar.gz

```
vWAAS-6k#
```

The following example shows output from the show alarms crash file details command:

```
vWAAS-6k#
vWAAS-6k#sh alarms crash
Kernel Crashfile Details:
-----
      Time                Crashfile Name
      -----
Mon Mar 25 06:32:42 2019  2019-03-18-10-05/vmcore.gz
Mon Mar 25 06:33:18 2019  2019-03-18-09-05/vmcore.gz
Mon Mar 18 12:16:03 2019  2019-03-18-12-05/vmcore.gz
```

Np Crashfile Details:

```
-----
      Time                Crashfile Name
      -----
vWAAS-6k#
```

[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.
Minor Alarms	Number of minor alarms.
Overall Alarm Status	Aggregate status of alarms.

**Table 3-5** *Field Descriptions for the show alarms status Command (continued)*

Field	Description
Device is NOT in alarm overload state.	Status of the device alarm overload state.
Device enters alarm overload state @ 999 alarms/sec.	Threshold number of alarms per second at which the device enters the alarm overload state.
Device exits alarm overload state @ 99 alarms/sec.	Threshold number of alarms per second at which the device exits the alarm overload state.
Overload detection is ENABLED.	Status of whether overload detection is enabled on the device.

**Related Commands**[\(config\) alarm overload-detect](#)[\(config\) snmp-server enable traps](#)

# show 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	
<b>client-ip</b> <i>ip_address</i>	(Optional) Displays the flow information for the client with the specified IP address.
<b>client-port</b> <i>port</i>	(Optional) Displays the flow information for the client with the specified port number (1–65535).
<b>peer-id</b> <i>peer_id</i>	(Optional) Displays the flow information for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
<b>server-ip</b> <i>ip_address</i>	(Optional) Displays the flow information for the server with the specified IP address.
<b>server-port</b> <i>port</i>	(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 Address Resolution Protocol (ARP) table for a WAAS device, use the **show arp** EXEC command.

## show arp

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **show arp** command to display the Internet-to-Ethernet address translation tables of the Address Resolution Protocol. Without flags, the current ARP entry for the host name is displayed.

On an ISR-WAAS device, no ARP entries are present for IP addresses on the same subnet as the ISR-WAAS device; there is an entry only for the defined gateway.


The ARP cache is cleared based on the `gc_stale_time`; the default time is 60 seconds.

Cache entry states, described in [Table 3-6](#), function as follows:

1. An entry in the ARP table with a Reachable state is moved to the Stale state after the ReachableTime is exceeded, or an UnsolicitedNeighbor advertisement is received.
2. After an entry in the ARP table is moved to the Stale state, it sends an ARP request and is moved to the Delay state. It remains in the Delay state until it receives an acknowledgment.
3. Depending on the next action, the entry is then moved to the Reachable state or the Probe state:
  - If the entry receives an acknowledgment on time, it is moved to the Reachable state.
  - If the entry does not receive an acknowledgment on time, it is moved to the Probe state.

**Examples** [Table 3-6](#) describes the fields shown in the **show arp** command display.

**Table 3-6** Field Descriptions for the show arp Command

Field	Description
Protocol	Type of protocol.
State	<p>Cache entry state. There are five possible cache entry states: Incomplete, Reachable, Stale, Delay, and Probe.</p> <ul style="list-style-type: none"> <li>• Incomplete—Address resolution on the cache is in progress: a Neighbor Solicitation has been sent to the solicited-mode address of the target, but the corresponding Neighbor Advertisement has not yet been received.</li> <li>• Reachable—Within the last ReachableTime milliseconds, positive confirmation has been received that the forward path to the neighbor is functioning properly. While in Reachable state, no special action occurs as packets are sent.</li> <li>• Stale—Within the last ReachableTime milliseconds, no positive confirmation has been received that the forward path to the neighbor is functioning properly. While in Stale state, no action occurs until a packet is sent.</li> </ul> <p> <b>Note</b> The Stale state is entered after an unsolicited Neighbor Discovery message is received, which updates the cached linked-layer address. Receipt of this message does <i>not</i> confirm reachability. Reachability is verified only after the entry is actually used.</p> <p>The Stale state ensures that reachability is verified quickly if the entry is actually being used.</p> <ul style="list-style-type: none"> <li>• Delay—More than the ReachableTime milliseconds has elapsed since receipt of the last positive confirmation that the forward path to the neighbor is functioning properly, and a packet was sent within the specified DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within the DELAY_FIRST_PROBE_TIME seconds of entering the Delay state, a Neighbor Solicitation is sent, and the state is changed to the Probe state.</li> <li>• Probe—Neighbor Solicitations are retransmitted every RetransTime seconds to confirm reachability, until a reachability confirmation is received.</li> </ul>
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

<b>user</b>	Displays authentication configuration for user login to the system.
<b>strict-password-policy</b>	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	Operation status of the authentication service. Values are enabled or disabled.
RADIUS	
TACACS+	
Local	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	Operation status of the authentication service. Values are enabled or disabled.  Priority status of each authentication service. Values are primary, secondary, or tertiary.
RADIUS	
TACACS+	
Local	

[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		
<b>blacklist</b>		Displays the entries in the blacklist server table.
<b>netmask</b> <i>netmask</i>		(Optional) Displays the network mask to filter the table output (A.B.C.D/).
<b>list</b>		Lists TCP flows that the WAE is currently optimizing or passing through.
		(Optional) Specifies the output modifier.
<b>begin</b> <i>regex</i>		Begins with the line that matches the regular expression. You can enter multiple expressions.
<b>exclude</b> <i>regex</i>		Excludes lines that match the regular expression. You can enter multiple expressions.
<b>include</b> <i>regex</i>		Includes lines that match the regular expression. You can enter multiple expressions.
<b>asymmetric-connections</b>		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		
	<b>info</b>	Displays the BMC information.
	<b>fru</b>	Displays the BMC Field Replaceable Unit.
	<b>event-log</b>	Displays the BMC system event log (by default, the last 10 events).
	<b>all</b>	Displays all events from the BMC system event log.
	<b>event</b>	Displays a single event number from the BMC system event log.
	<b>range</b>	Displays the range of events from the BMC system event log.
	<b>management</b>	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
```

## show bmc

```

0x04
0x1b
0x01
SEL Information
Version      : 1.5 (v1.5, v2 compliant)
Entries     : 4
Free Space  : 9136 bytes
Percent Used : 0%
Last Add Time : 05/21/2018 05:26:56
Last Del Time : 05/21/2018 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 : 05/24/2018 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        : Wed May 2 22:00:00 2018
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*

<b>Syntax Description</b>	<i>index</i> Bridge group index from 1–5.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	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.

■ show bridge

Related Commands [\(config\) bridge](#)



# show cache http-metadacache

To display HTTP metadata cache information for a WAE, use the **show cache http-metadacache EXEC** command.

```
show cache http-metadacache https { conditional-response | redirect-response |
sharepoint-prefetch | unauthorized-response }
```

```
show cache http-metadacache { all | conditional-response | redirect-response |
sharepoint-prefetch | unauthorized-response } [url]
```

## Syntax Description

<b>https</b>	Displays cache entries for HTTPS metadata cache response types, which includes the active entries only, not the URLs.
<b>conditional-response</b>	Displays cache entries for conditional responses (304).
<b>redirect-response</b>	Displays cache entries for redirect responses (301).
<b>sharepoint-prefetch</b>	Displays cache entries of the prefetched data.
<b>unauthorized-response</b>	Displays cache entries for authorization required responses (401).
<b>all</b>	Displays cache entries for all HTTP metadata cache response types.
<i>url</i>	(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-metadacache all** command display.

**Table 3-12** Field Descriptions for the show cache http-metadacache 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-metadacache all Command (continued)

Field	Description
Active HTTPS entries	Number of current HTTPS conditional cache entries.
Max Entries	Maximum number of conditional cache entries allowed.
URL	URL and expiration time (in seconds) for each conditional cache entry.
Unauthorized Cache	
Active HTTP entries	Number of current HTTP unauthorized cache entries.
Active HTTPS entries	Number of current HTTPS unauthorized cache entries.
Max Entries	Maximum number of unauthorized cache entries allowed.
URL	URL and expiration time (in seconds) for each unauthorized cache entry.

**Related Commands**

(config) accelerator http  
clear cache

# show cache object-cache

To display a list of individual objects in the cache, one per line, use the **show cache object-cache EXEC** command.

```
show cache object-cache [accelerator ao-name] {server-ip server-ip | server-host hostname | url
  path}
```

Syntax Description		
<b>accelerator</b> <i>ao-name</i>	(Optional) The name of the application accelerator specified, such as EPM or MAPI.	
<b>server-host</b> <i>hostname</i>	Displays a list of individual objects in the cache for the specified server hostname.	
<b>server-ip</b> <i>server-ip</i>	Displays a list of individual objects in the cache for the specified server IP address.	
<b>url</b> <i>path</i>	Displays a list of individual objects in the cache for the specified URL. If the URL string contains a question mark (?), it must be escaped with a preceding backslash (for example, \?).	

**Command Default** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use the **show cache object-cache** command to display a list of individual objects in the cache, one per line. You can display a list of all individual objects, or only those that match specified criteria, such as server IP address or hostname, or path of a specified URL.

**Examples** The following is sample output from the **show cache object-cache** command:

```
show cache object-cache
```

```

URL                                     Size (KB)  State
-----
http://www.sampletestdomain.com/a.jpg  10         DEL_PEND
SMB://10.1.1.1/share1/z.doc            25         COMPLETE
```

```

**** Object 1 ****
Object General information
=====
owner_ao: 15
resource_id: 253
stored_obj_id: 253
state: OC_OBJ_STATE_CREATED
url_hash: 9381385200752939448
url: /local/local1/test2.txt
server_ip: 0.0.0.1
hostname: 10.10.10.10
port: 8080
stored_offset: 9381385200752939448
stored_size: 1000
last_access_time: 16738851
hit_count: 2
flag: NODUP
Object's Protocol Related Information
=====

size: 18446744073709551615
last_modified_time: 7814
expiration_time: 18446744073709551615
protocol_req_metadata_size: 0
protocol_resp_metadata_size: 0x100
Object's Storage Related Information
=====
local_path:
/object-cache1/ocdata/smb_ao/fd/0_82316
022a7fc51b8
extent_list_size: 16
extent_list :
(0,1000)

***** END OF Object Information *****

```

# 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
<b>entry</b>	(Optional) Displays information for a specific CDP neighbor entry.
*	Specifies all neighbors.
<i>neighbor</i>	CDP neighbor entry to display.
<b>protocol</b>	(Optional) Displays the CDP protocol information.
<b>version</b>	(Optional) Displays the CDP version.
<b>interface</b>	Displays the interface status and configuration.
<b>GigabitEthernet</b> <i>slot/port</i>	(Optional) Displays the Gigabit Ethernet configuration for the designated interface.
<b>TenGigabitEthernet</b> <i>slot/port</i>	(Optional) Displays the 10-Gigabit Ethernet configuration for the designated interface.
<b>InlinePort</b> <i>slot/port</i> { <b>lan</b>   <b>wan</b> }	(Optional) Displays Inline Port configuration for the designated interface.
<b>neighbors</b>	Displays CDP neighbor entries.
<b>detail</b>	(Optional) Displays detailed information.
<b>holdtime</b>	Displays the length of time that CDP information is held by neighbors.
<b>run</b>	Displays the CDP process status.
<b>timer</b>	Displays the time when CDP information is resent to neighbors.
<b>traffic</b>	Displays CDP statistical information.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines**

The **show cdp** command displays information about how frequently CDP packets are resent to neighbors, the length of time that CDP packets are held by neighbors, the disabled status of CDP Version 2 multicast advertisements, CDP Ethernet interface ports, and general CDP traffic information. This command supports VLAN (802.1Q) tagged packets

**Note**

The CDP protocol is not supported for OVS (Open Virtual Switch) on RHEL KVM on CentOS, therefore the **show cdp** command cannot be used for vWAAS on RHEL KVM on CentOS.

**Examples**

[Table 3-13](#) 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 <b>cdp timer</b> command.
Sending a holdtime value of XX seconds	Time (in seconds) that the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the <b>cdp holdtime</b> command.
Sending CDPv2 advertisements is XX	Transmission status for sending CDP Version-2 type advertisements. Possible values are enabled or 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.

**Table 3-14** Field Descriptions for the *show cdp entry* Command (continued)

Field	Description
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
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.
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 switch, a host, an IGMP device, or a repeater.
Interface	Protocol being used by the connectivity media.
Port ID (outgoing port)	Port number of the port on the neighbor device.
Holdtime	Time, in seconds, that the current device will hold the CDP advertisement from a transmitting router before discarding it.
Version	Software version running on the neighbor device.
Copyright	Copyright information for the neighbor device.
advertisement version	Version of CDP being used for CDP advertisements.
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.

**Table 3-23** *Field Descriptions for the show cdp traffic Command (continued)*

Field	Description
Hdr syntax	(Header Syntax) Number of CDP advertisements with bad headers received by the local device.
Chksum error	(Checksum Error) Number of times that the checksum (verifying) operation failed on incoming CDP advertisements.
Encaps failed	(Encapsulations Failed) Number of times that CDP failed to transmit advertisements on an interface because of a failure caused by the bridge port of the local device.
No memory	Number of times that the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid packet	Number of invalid CDP advertisements received and sent by the local device.
Fragmented	Number of times fragments or portions of a single CDP advertisement were received by the local device instead of the complete advertisement.
CDP version 1 advertisements Output	Number of CDP Version 1 advertisements sent by the local device.
Input	Number of CDP Version 1 advertisements received by the local device.
CDP version 2 advertisements Output	Number of CDP Version 2 advertisements sent by the local device.
Input	Number of CDP Version 2 advertisements received by the local device.

**Related Commands**[\(config\) cdp](#)[\(config-if\) cdp](#)[clear arp-cache](#)[debug cdp](#)

# show class-map

To display the matching criteria configured for an AppNav or optimization class map, use the **show class-map EXEC** command.

```
show class-map type {appnav | waas} [classmap-name]
```

Syntax Description		
	<b>appnav</b>	Displays the specified AppNav class map, or all class maps if no class map is specified.
	<b>waas</b>	Displays the specified WAAS optimization class map, or all class maps if no class map is specified.
	<i>classmap-name</i>	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 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 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)
```

**show class-map**

```
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		
<b>detail</b>	(Optional) Displays detailed information; indicates the clock source (NTP) and the current summer time setting (if any).	
<b>standard-timezones</b>	(Optional) Displays information about the standard time zones.	
<b>all</b>	Displays all of the standard time zones (approximately 1500 time zones). Each time zone is listed on a separate line.	
<b>details</b> <i>timezone</i>	Displays detailed information for the specified time zone.	
<b>regions</b>	Displays the region name of all the standard time zones. All 1500 time zones are organized into directories by region.	
<b>zones</b> <i>region-name</i>	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		
<b>database</b>		Displays embedded database maintenance information.
<b>content</b>		Writes the database content to a file.
<b>dump</b> <i>filename</i>		Dumps all database content to a text file. Specifies the name of the file to be saved under local1 directory.
<b>text</b>		Writes the database content to a file in text format.
<b>xml</b>		Writes the database content to a file in XML format.
<b>info</b>		Displays CMS application information.
<b>secure-store</b>		Displays the status of the CMS secure store.
<b>device status</b> <i>name</i>		Displays status for the device or device group indicated by <i>name</i> , 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 <b>central-manager address</b> global configuration command. This address may differ from the registered address if a standby Central Manager is managing the device instead of the primary Central Manager with which the device is registered.
Registered with WAAS Central Manager	Address of the Central Manager with which the device is registered.
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. <b>Note</b> The output for primary and standby Central Manager devices is different. On a standby, the output includes the following additional information: Current WAAS Central Manager and Registered with WAAS Central Manager.
Current WAAS Central Manager	Address of the standby Central Manager as currently configured in the <b>central-manager address</b> global configuration command.
Registered with WAAS Central Manager	Address of the standby Central Manager with which the device is registered.
CMS services information	
Service cms_httpd is running	Status of the management service (running or not running). This field is specific to the Central Manager only.
Service cms_cdm is running	Status of the management service (running or not running). This field is specific to the Central Manager only.



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 <b>show cms database content text</b> command requests the management service to write its current configuration to an automatically generated file in text format.

Table 3-29 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 <b>show cms database content xml</b> command requests the management service to write its current configuration to an automatically generated file in XML format.

#### Related Commands

[cms](#)

[\(config\) cms](#)

# show cms secure-store

To display secure store status, use the **show cms secure-store** EXEC command.

**show cms secure-store**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show cms secure-store** command will display one of the following status messages ([Table 3-30](#)):

**Table 3-30** Status Messages for the show cms secure-store Command

Message	Description
WAE Messages	
<b>secure-store not initialized</b>	Secure store is not initialized.
<b>secure-store is initialized, enter pass-phrase to open store</b>	Secure store is initialized and not open.
<b>secure-store initialized and open</b>	Secure store is initialized and open.
Central Manager Messages	
<b>Secure store is in CM 'auto-generated passphrase' mode in 'Open' state.</b>	Secure store is initialized and open and in the auto-passphrase mode.
<b>Secure store is in 'User-provided passphrase' mode in 'Not Open' state. Use the command 'cms secure-store open' to open the secure store.</b>	Secure store is initialized but not open because it is in the user-passphrase mode and the passphrase has not been entered.
<b>Secure store is in 'User-provided passphrase' mode in 'Open' state.</b>	Secure store is initialized and open and the user-passphrase has been entered.

**Examples** The following is sample output from the **show cms secure-store** command:

```
WAE# show cms secure-store
Secure store is in 'User-provided passphrase' mode in 'Open' state.
```

```
***** WARNING : If Central Manager device is reloaded, you must reopen Secure St
```

ore with the correct passphrase. Otherwise disk encryption features will not operate on  
WAE(s).\*\*\*\*\*

---

**Related Commands** [cms secure-store](#)

# show crypto

To display crypto layer information, use the **show crypto** EXEC command.

```
show crypto { certificate-detail { factory-self-signed | management | admin [filename] } |
certificates | ssl services { accelerated-service service | host-service peering }
```

Syntax	Description
<b>certificate-detail</b>	Displays a certificate in detail.
<b>factory-self-signed</b>	Displays WAAS self-signed certificates in detail.
<b>management</b>	Displays WAAS management certificates in detail.
<b>admin</b>	Displays the certificate details for the Central Manager admin service certificate. This option can be used only on the Central Manager.
<i>filename</i>	Filename of the certificate to display.
<b>certificates</b>	Displays a summary of all PKI certificates. This option can be used only on the WAE.
<b>ssl services</b>	Displays status of SSL services. This option can be used only on the WAE.
<b>accelerated-service</b> <i>service</i>	Displays status of SSL accelerated service with the specified service name.
<b>host-service peering</b>	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	
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	
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**, **rbcpl**, **tfo**, **translog**, and **wccp** command options are supported in the application-accelerator device mode only. The **emdb** and **rpc** command options are supported in the central manager device mode only.

The **show debugging** command displays only the type of debugging enabled, not the specific subset of the command.

**Examples** The following is sample output from the **show debugging** command:

```
WAE# debug tfo buffer-mgr
WAE# debug tfo connection
WAE# show debugging
tfo bufmgr debugging is on
tfo compmgr debugging is on
tfo connmgr debugging is on
tfo netio debugging is on
tfo statmgr debugging is on
tfo translog debugging is on
```

In this example, the **debug tfo buffer-mgr** and the **debug tfo connection** commands coupled with the **show debugging** command display the states of **tfo buffer-mgr** and **tfo connection** debugging options.

**Related Commands** [debug all](#)

# show device-id

To display the device ID of a WAAS device, use the **show device-id** EXEC command.

## **show device-id**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Examples** This command displays the device ID, as follows:

```
WAE# show device-id  
System Device ID is: 00:1a:64:f2:22:37
```

---

**Related Commands** [\(config\) peer](#)

# show device-mode

To display the configured or current device mode of a WAAS device, use the **show device-mode EXEC** command.

**show device-mode { configured | current | profile-branch }**

Syntax Description		
	<b>configured</b>	Displays the configured device mode, which has not taken effect yet.
	<b>current</b>	Displays the current device mode.
	<b>profile-branch</b>	Displays the branch profile mode, for use with the WAVE-7571, which enables the device to function as a branch device.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** To display the configured device mode that has not yet taken effect, enter the **show device-mode configured EXEC** command. For example, if you had entered the **device mode central-manager** global configuration command on a WAAS device to change its device mode to central manager but have not yet entered the **copy run start EXEC** command to save the running configuration on the device, then if you were to enter the **show device-mode configured** command on the WAAS device, the command output would indicate that the configured device mode is central-manager.

**Examples** The following is sample output from the **show device mode** command. It displays the current mode in which the WAAS device is operating.

```
WAE# show device-mode current

Current device mode: application-accelerator
```

[Table 3-33](#) 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 disks

To view information about the WAAS device disks, use the **show disks** EXEC command.

```
show disks { cache-details | details | failed-disk-id | failed-sectors [disk_name] | tech-support
            [details | fwlogs] }
```

Syntax	Description
<b>cache-details</b>	Displays data cache details.
<b>details</b>	Displays currently effective configurations with more details.
<b>failed-disk-id</b>	Displays a list of disk serial numbers that have been identified as failed.
<b>failed-sectors</b>	Displays a list of failed sectors on all the disks.
<i>disk_name</i>	(Optional) Name of the disk for which failed sectors are displayed (disk00 or disk01).
<b>tech-support</b>	Displays 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 <b>show disk smart-info</b> EXEC command.
<b>details</b>	(Optional) Displays more detailed SMART disk monitoring information.
<b>fwlogs</b>	(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.

The following is sample output from the **show disks cache- details** command.

```

WAE# show disks cache-details
Mode # oc-weight2
Name          Default MB      Existing MB      Configured MB   Configured %
-----
Akamai        189440 MB      189440 MB      64512 MB       20.26%
Object-cache  129024 MB      129024 MB      253952 MB      79.74%
Disk cache has been configured. Please reload for the new config to take effect.

```

Table 3-36 describes the fields shown in the **show disks cache-details** command display.

**Table 3-36** Field Description for the **show disks cache-details** Command

Field	Description
Mode	Currently configured mode for data cache partitions for Akamai cache and Object cache.
Name	Name of the cache.
Default MB	Default size allotted to Akamai cache or Object cache.
Existing MB	Current size used by Akamai cache or Object cache.
Configured MB	User configured size to be used by Akamai cache or Object cache. Takes effect after a reload. After a reload the configured size and the existing size is the same.
Configured %	User configured percentage of the total available space for Akamai Cache or Object Cache.

Table 3-37 describes the fields shown in the **show disks details** command display.

**Table 3-37** Field Descriptions for the **show disks details** Command

Field	Description
Physical disk information or RAID Physical disk information	Lists the disks by number. On RAID-5 systems, this field is called RAID Physical disk information.
disk00	Availability of the disk: Present, Not present or Not responding, Not used (*), or Online (for RAID-5 disks). Disk identification number and type, for example: (h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB). Lists attributes such as serial number, the technology family(SATA/SAS) and the capacity of the SSD or HDD.
disk01	Same type of information is shown for each disk.
RAID Logical drive information	RAID-5 logical drive status and error conditions and total size. (Only shown for RAID-5 systems.)
Mounted filesystems	Table containing the following column heads:

**Table 3-37** Field Descriptions for the *show disks details* Command (continued)

Field	Description
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name “md1” indicates that the partition is a RAIDed partition and that the RAID type is RAID-1.
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].
Disk encryption feature	Indicates whether the disk encryption feature is enabled or disabled.

The following is sample output from the **show disks tech-support** command. The output shows that partition 04 and partition 05 on disks disk00 and disk01 are GOOD, and the RAIDed partitions /dev/md4 & /dev/md5 are in NORMAL OPERATION. However, the RAIDed partition /dev/md8 has an issue with one of the drives. Disk04 with partition 00 is GOOD, but the status shows ONE OR MORE DRIVES ABNORMAL because there is no pair on this partition.

```
WAE# show disks tech-support
/dev/md4      RAID-1  NORMAL OPERATION      disk00/04 [GOOD]
disk01/04 [GOOD]
/dev/md5      RAID-1  NORMAL OPERATION      disk00/05 [GOOD]
disk01/05 [GOOD]
...
/dev/md8      RAID-1  ONE OR MORE DRIVES ABNORMAL  disk04/00 [GOOD]
```

**Table 3-38** 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 3-38** 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 2018 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 3-39 describes the fields shown in the **show disks tech-support** command display for a RAID-5 appliance.

**Table 3-39** Field Descriptions for the show disks tech-support Command (RAID-5)

Field	Description
Controllers found	Number of RAID controllers found.
Controller information	
Controller Status	Functional status of the controller.
Channel description	Description of the channel transport protocols.
Controller Model	Make and model of the controller.
Controller Serial Number	Serial number of the ServeRAID controller.
Physical Slot	Slot number.
Installed memory	Amount of memory for the disk.
Copyback	Status of whether copyback is enabled or disabled.
Data scrubbing	Status of whether data scrubbing is enabled or disabled.
Defunct disk drive count	Number of defunct disk drives.
Logical drives/Offline/Critical	Number of logical drives, number of drives that are offline, and number of critical alarms.
Controller Version Information	

**Table 3-39** Field Descriptions for the *show disks tech-support* Command (RAID-5) (continued)

Field	Description
BIOS	Version number of the BIOS.
Firmware	Version number of the Firmware.
Driver	Version number of the Driver.
Boot Flash	Version number of the Boot Flash.
Controller Battery Information	
Status	Functional status of the controller battery.
Over temperature	Over temperature condition of the battery.
Capacity remaining	Percent of remaining battery capacity.
Time remaining (at current draw)	Number of days, hours, and minutes of battery life remaining based on the current draw.
Controller Vital Product Data	
VPD Assigned#	Number assigned to the controller vital product data (VPD).
EC Version#	Version number.
Controller FRU#	Number assigned to the controller field-replaceable part.
Battery FRU#	Number assigned to the battery field-replaceable part.
Logical drive information	
Logical drive number	Number identifying the logical drive to which the information applies.
Logical drive name	Name of the logical drive.
RAID level	RAID level of the logical drive.
Status of logical drive	Functional status of the logical drive.
Size	Size (in megabytes) of the logical drive.
Read-cache mode	Configuration status of read-cache mode: Enabled or Disabled.
Write-cache mode	Configuration status of write-cache mode for write-back: Enabled or Disabled.
Write-cache setting	Configuration status of the write-cache setting for write-back: Enabled or Disabled.
Partitioned	Partition state. Values are Yes or No.
Number of chunks	Number of disks participating in the RAID-5 array.
Stripe-unit size	Amount of data storage per stripe unit. The default is 256 KB per disk in the logical array. This parameter is not configurable.
Stripe order (Channel,Device)	Order in which data is striped across a group of physical drives that are grouped in a RAID array.
Bad stripes	Flag for bad stripes. Flag values are Yes or No.
Physical drive information	
Device #	Device number for which the information applies.
Device is a xxxx	Type of device.
State	State of the device: Online or Offline.

**Table 3-39** Field Descriptions for the `show disks tech-support Command (RAID-5)` (continued)

Field	Description
Supported	Status showing if the device is supported.
Transfer Speed	Device transfer speed.
Reported Channel,Device	Provides channel information for all the disks participating in the RAID-5 array.
Reported Enclosure,Slot	Device number and slot number.
Vendor	Vendor identification number.
Model	Model number.
Firmware	Firmware number.
Serial number	Serial number.
Size	Size (in megabytes) of the physical drive.
Write Cache	Status of whether the write cache is enabled.
FRU	Field Replaceable Unit number. A RAID defunct drive FRU event occurs when a specified hard disk drive with the provided FRU number fails in a RAID configuration. The default value for this field is NONE.
PFA	Predictive Failure Analysis flag. The flag default value is No. If the RAID predicts a drive failure, this field is set to Yes and a critical alarm is raised on the WAE.

[Table 3-40](#) 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 3-40** 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 2018 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.
Current Drive Temperature	Temperature of the drive in degrees Celsius.
Manufactured in week XX of year	Manufacturing details.



**Table 3-40** *Field Descriptions for the show disks tech-support details Command (continued)*

Field	Description
Current start stop count	Number of times the device has stopped or started.
Recommended maximum start stop count	Maximum recommended count used to gauge the life expectancy of the disk.
Error counter log	Table displaying the error counter log. Counters for various types of disk errors.

**Related Commands**[disk](#)[\(config\) disk error-handling](#)[show tech-support](#)

# show dre

To view DRE configuration information, use the **show dre** EXEC command.

**show dre [auto-bypass]**

Syntax Description	auto-bypass	Displays the auto bypass table entries.
--------------------	-------------	---

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	EXEC
---------------	------

Device Modes	application-accelerator appnav-controller
--------------	--

Examples	The following is sample output from the <b>show dre</b> 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	<a href="#">clear dre</a> <a href="#">(config) dre</a>
------------------	---

# 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.
<b>begin</b> <i>regex</i>	Begins with the line that matches the regular expression. You can enter multiple expressions.
<b>exclude</b> <i>regex</i>	Excludes lines that match the regular expression. You can enter multiple expressions.
<b>include</b> <i>regex</i>	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
```

## show filtering list

```

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 3-41](#) describes the fields shown in the **show flash** command display.

**Table 3-41** 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**]}

Syntax Description	<i>RecordName</i>	The name of the flow record
	<b>template</b>	The identity of the template associated with this flow record.

**Defaults** No default behavior or values.

**Device Modes** application-accelerator  
central-manager

**Command Modes** EXEC  
Device Modes  
application-accelerator  
central-manager

**Examples** The following is sample output from the **show flow record** command.

```
WAE#show flow record word template
Record Name: word
Template ID: 260
Total Size : 48
      Fields          Field ID    Bytes    Offset
-----
      Source IP       8           4         0
      Destination IP  12          4         4
      Source Port     7           2         8
      Destination Port 11          2        10
      Bytes Received  36009       8        12
      Bytes Sent      36010       8        20
      Packets Received 36011       8        28
      Packets Sent    36012       8        36
      Application Name 36006       4        44
```

[Table 3-42](#) describes the fields shown in the **show flow record** command display.

**Table 3-42** *Field Descriptions for the show flow record Command*

Field	Description
Record Name	Name of a user-defined flow record.
Template ID	Unique ID of the template matching the type of NetFlow data it exports.
Total Size	?? Please provide description
Field	
Source IP	Source IP address.
Destination IP	Destination IP address.
Source Port	TCP/UDP source port number or equivalent.
Destination Port	TCP/UDP destination port number or equivalent.
Bytes Received	Number of bytes received.
Bytes Sent	Number of bytes sent.
Packets Received	Number of packets received.
Packets Sent	Number of packets sent.
Application Name	Name of the application traffic on the connection.
Field ID	??
Bytes	??
Offset	??

**Related Commands**

# 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 3-43](#) describes the fields shown in the **show hardware** command display. The display may vary depending on the hardware platform.

**Table 3-43** Field Descriptions for the show hardware Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) <i>year</i> by Cisco Systems, Inc. Cisco Wide Area Application Services (universal-k9) Software Release <i>X.X.X</i> (build <i>bnnn month day year</i> )	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 3-43** 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.
<i>Device Model Number</i>	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 3-43** 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 3-44](#) describes the fields shown in the **show hosts** command display.

**Table 3-44** *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 <b>host</b> global configuration command.

**Related Commands** [\(config\) ip hosts](#)

# show inetd

To display the status of TCP/IP services on a WAAS device, use the **show inetd** EXEC command.

## show inetd

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show inetd** EXEC command displays the enabled or disabled status of TCP/IP services on the WAAS device. You can ignore the TFTP service status because TFTP is not supported on WAAS.

**Examples** [Table 3-45](#) describes the fields shown in the **show inetd** command display.

**Table 3-45** *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
<b>GigabitEthernet</b> <i>slot/port</i>	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 (/).
<b>InlineGroup</b> <i>slot/grpnumber</i>	Displays the inline group information and the slot and inline group number for the selected interface.
<b>InlinePort</b>	Displays the inline port information and the slot and inline group number for the selected interface.
<b>lan</b>	Displays the inline port information for the LAN port.
<b>wan</b>	Displays the inline port information for the WAN port.
<b>PortChannel</b> <i>index</i>	Displays the port channel interface (1-4) device information.
<b>standby</b> <i>grpnumber</i>	Displays the standby group (1-2) information.
<b>virtual</b> <i>slot/port</i>	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.
<b>TenGigabitEthernet</b> <i>slot/port</i>	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 (/).
<b>bvi</b> <i>bridge-id</i>	Displays the bridge virtual interface (1-4) information.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**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.

**Usage Guidelines** The **show interface** command displays hardware interface information for a WAAS device, such as interface operating mode, interception statistics, packets sent, and active optimized flows.

**Note**

When you use the **show interface PortChannel index detail** command on an interface with an AppNav Controller, the output may display an error count larger than zero (0) for the Length Error Frames Received counter. The displayed error count does not impact WAAS performance: the packets will not be dropped and will undergo further processing.

**Note**

If a WAAS device is running for an extended period of time (13 hours or more) without a restart, output for the **show interface** command may erroneously show input errors for the device. To clear these statistics, reload the device, run the **show interface** command, and the input errors count will be cleared to zero.

**Examples**

The following is sample output from the **show interface** command. It displays information for GigabitEthernet interface 0 in slot 0:

```
WAE-231-03# show interface gigabitethernet 0/0
Ethernet Address           : 50:3d:e5:9c:8f:a5
Internet Address           : 2.43.65.52
Netmask                    : 255.255.255.0
IPv6 Enabled               : Yes
IPv6 Link Local Address    : fe80::4e4e:35ff:fe44:c74f
IPv6 Autoconfig Enabled    : No
IPv6 Global unicast address(es) : 2001:420:54ff:13::457:88/119
                               : 2001:1::1/64
IPv6 ND DAD attempts       : 1
Admin State                 : Up
Operation State             : Running
Maximum Transfer Unit Size : 1500
Input Errors                : 0
Input Packets Dropped       : 0
Packets Received           : 4074292
Output Errors               : 0
Output Packets Dropped      : 0
Load Interval              : 30
Input Throughput            : 12538 bits/sec, 13 packets/sec
Output Throughput           : 23235 bits/sec, 11 packets/sec
Packets Sent                : 3334662
Auto-negotiation            : On
Full Duplex                 : Yes
Speed                       : 1000 Mbps
```

[Table 3-46](#) describes the fields shown in the **show interface GigabitEthernet** command. Most of the other **show interface** command options display similar output.

**Table 3-46** 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.

**Table 3-46** Field Descriptions for the show interface GigabitEthernet command (continued)

Field	Description
Ethernet address	Layer-2 MAC address.
Internet address	Internet IP address configured for this interface.
Netmask	Netmask configured for this interface.
IPv6 Enabled	Displays yes only if IPv6 configuration is enabled for this interface.
IPv6 Link Local Address	Single link-local address for this interface.
IPv6 Global unicast address(es)	IPv6 address configured for this interface.
IPv6 ND DAD attempts	Number of Duplicate Address Detection attempts
Admin State	Administrative state.
Operational State	Administrative state.
Maximum Transfer Unit Size	Current configured MTU value.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Packets Received	Total number of packets received by this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Load Interval	Interval at which the interface is polled for statistics and to calculate throughput.
Input Throughput	Input throughput in bits per second and packets per second.
Output Throughput	Output throughput in bits per second and packets per second.
Packets Sent	Total number of packets sent from this interface.
Auto-negotiation	State of auto-negotiation for transmission speed and mode. Shown only for physical interfaces.
Full Duplex	State of full duplex transmission mode. Shown only for physical interfaces.
Speed	Configured speed. Shown only for physical interfaces.
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 3-47 describes the fields shown in the **show interface InlineGroup** command.

**Table 3-47** 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: <ul style="list-style-type: none"> <li>• Intercept—Intercepting traffic</li> <li>• Bypass—Bypassing traffic.</li> </ul>
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	<p><i>For WAAS versions earlier than 6.x:</i></p> <p>Number of non-TCP packets or other packets that the device does not want to intercept.</p> <p><i>For WAAS Version 6.x and later:</i></p> <p>All packets, including non-TCP packets or other packets, are incremented in the Packets Forwarded counter.</p>
Packets Forwarded	<p><i>For WAAS versions earlier than 6.x:</i></p> <p>Number of packets considered for optimization or pass-through, including host-generated packets.</p> <p><i>For WAAS Version 6.x and later:</i></p> <p>All packets, including non-TCP packets or other packets, are incremented in the Packets Forwarded counter.</p>
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 3-48](#) describes the fields shown in the **show inventory** command display.

**Table 3-48** *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	
<i>acl-name</i>	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
<i>acl-num</i>	(Optional) Information for a specific access list, using a numeric identifier (0–99 for standard access lists and 100–199 for extended access lists).

**Defaults** Displays information about all defined access lists.

**Command Modes** EXEC

**Device Modes** application-accelerator  
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 3-49](#) describes the fields shown in the **show ip access-list** command display.

**Table 3-49** Field Descriptions for the show ip access-list Command

Field	Description
Space available:	
XX access lists	Number of access lists remaining out of 50 maximum lists allowed.
XXX access list conditions	Number of access list conditions remaining out of 500 maximum conditions allowed.
XXX TCAM Entries	Number of remaining TCAM entries on an ANC.

**Table 3-49** 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: <i>interface slot/port</i> <i>interface direction</i> <i>access list number</i>
Application access list references	List of applications and the access lists with which they are associated, displayed in the following format: <i>application type</i> <i>access list type and number</i> <i>associated port</i>

**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	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 3-50](#) describes the fields shown in the **show ip routes** command display.

**Table 3-50** Field Descriptions for the show ip routes Command

Field	Description
Destination	Destination IP addresses for each route.
Netmask	Netmask for each route.
Gateway	Gateway address for each route.
Interface	Interface on which each route is configured.

**Related Commands** [\(config\) ip](#)  
[\(config-if\) ip](#)

# show ipv6

To display the IPv6 configuration for a WAAS device, use the **show ipv6** EXEC command.

```
show ipv6 { neighbors { virtual slot/port | GigabitEthernet [slot number/port] | Portchannel [Etherchannel index] | standby [standby index] } | routes { data | management } }
```

## Syntax Description

<b>neighbors</b>	Displays the information for IPv6 neighbors.
<i>virtual slot/port</i>	Display information for Virtual Ethernet device
<b>GigabitEthernet</b> [ <i>slot number/port</i> ]	Display information for GigabitEthernet device
<b>Portchannel</b> [ <i>Etherchannel index</i> ]	Displays information for Etherchannel device
<b>standby</b> [ <i>standby index</i> ]	Displays information for Standby interfaces
<b>routes</b>	Displays the v6 routing table.
<b>data</b>	Display ipv6 static route to send data traffic
<b>management</b>	Display ipv6 static route to send management traffic

## Defaults

Displays the neighbor details and routing table for both data and management traffic.

## Command Modes

EXEC

## Device Modes

application-accelerator  
central-manager

## Usage Guidelines

The **show ipv6** command displays the IPv6 configuration on a WAAS device. This includes the ipv6 address, local-link addresses and the default gateway of all the cached entries for the neighbor interfaces on a WAAS device. The **show ipv6 routes** command displays the IP route table, which lists all of the different routes that are configured on the WAE. The WAE uses this table to determine the next hop. This table includes routes from three sources: the WAE interfaces, any user-configured static routes, and the default gateway. The last line in the Data Routes table shows the default route

## Examples

[Table 3-51](#) describes the fields shown in the **show ipv6** command display.

**Table 3-51** Field Descriptions for the show ipv6 Command

Field	Description
IPv6 Address	Configured IPv6 address on the interface
Interface Link Layer Address	Link Local address
State	Operation State

**Table 3-51** *Field Descriptions for the show ipv6 Command*

Field	Description
Destination	Destination IP addresses for each route.
Nexthop	Netmask for each route.
Interface	Interface on which each route is configured.

---

**Related Commands**    [\(config\) ip](#)



# show kdump

To display the kernel crash dump information for a WAAS device, use the **show kdump EXEC** command.

## show kdump

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-52](#) describes the fields shown in the **show kdump** command display.

*Table 3-52 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 3-53](#) describes the fields shown in the **show kerberos** command display.

**Table 3-53** *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 3-54](#) 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 3-54** 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      11/12/2018      admin
```

**Related Commands** [clear arp-cache](#)  
[license add](#)

# show logging

To display the system message log configuration for a WAAS device, use the **show logging** EXEC command.

## show logging

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** Use the system message log to view information about events that have occurred on a WAAS device. The *syslog.txt* file is contained in the */local1* directory.

---

**Examples** The following is sample output from the **show logging** command. It displays the syslog host configuration on a WAAS device.

```
WAE# show logging
Syslog to host is disabled
Priority for host logging is set to: warning

Syslog to console is disabled
Priority for console logging is set to: warning

Syslog to disk is enabled
Priority for disk logging is set to: notice
Filename for disk logging is set to: /local1/syslog.txt

Syslog facility is set to *

Syslog disk file recycle size is set to 1000000
```

---

**Related Commands** [clear arp-cache](#)  
[\(config\) logging console](#)  
[show sysfs volumes](#)

# show memory

To display memory blocks and statistics for a WAAS device, use the **show memory** EXEC command.

## **show memory**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-55](#) describes the fields shown in the **show memory** command display.

**Table 3-55** *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

<b>Syntax Description</b>	<b>status</b> Displays the NTP status.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager
<b>Examples</b>	<a href="#">Table 3-56</a> describes the fields shown in the <b>show ntp status</b> command display.

**Table 3-56** 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 ( <b>l</b> ocal, <b>u</b> nicast, <b>m</b> ulticast, or <b>b</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 3-56** *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 } [policy-map-name]
```

Syntax Description		
	<b>appnav</b>	Displays the specified AppNav policy map, or all policy maps if no policy map is specified.
	<b>waas</b>	Displays the specified WAAS optimization policy map, or all policy maps if no policy map is specified.
	<i>classmap-name</i>	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.
	<b>all</b>	Displays detailed information for the class maps in the active AppNav policy map and any nested policy maps.
	<b>level1-class</b> <i>classmap-name</i>	Displays detailed information for the specified class map in the top-level policy map.
	<b>level2-class</b> <i>classmap-name</i>	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 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 class-default (8071757 flow-matches)
    Match tcp (8071757 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		
<b>cpu</b>	(Optional)	Displays CPU utilization.
<b>debug pid</b>	(Optional)	Prints the system call and signal traces for a specified process identifier to display system progress.
<b>memory</b>	(Optional)	Displays memory allocation processes.
<b>system</b>	(Optional)	Displays system load information in terms of updates.
<b>delay secs</b>	(Optional)	Specifies the delay between updates, in seconds (1–60).
<b>count num</b>	(Optional)	Specifies the number of updates that are displayed (1–100).

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the EXEC commands shown in this section to track and analyze system CPU utilization. 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 3-57](#) describes the fields shown in the **show processes** command display.

**Table 3-57** *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 3-58](#) describes the fields shown in the **show radius-server** command display.

**Table 3-58** 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 | wccp]**

Syntax Description		
	<b>no-policy</b>	(Optional) Does not display the policy engine configuration.
	<b>interface</b>	(Optional) Displays interface configuration.
	<b>policy</b>	(Optional) Displays policy engine configuration.
	<b>snmp</b>	(Optional) Displays SNMP configuration.
	<b>wccp</b>	(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.

```
NO-HOSTNAME-10-78-108-140#show running-config
! waas-universal-k9 version 6.4.3 (build b12 Dec 12 2018)
!
device mode central-manager
!
!hostname NO-HOSTNAME-10-78-108-140
!
!primary-interface GigabitEthernet 0/0 ipv4
!
primary-interface GigabitEthernet 0/0 ipv6
!
interface GigabitEthernet 0/0
 ip address 10.78.108.140 255.255.255.0
 ipv6 address autoconfig
 exit
interface GigabitEthernet 0/1
 shutdown
 exit
```

## ■ show running-config

```

!
ip default-gateway 10.78.108.1
!
!!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
bmc lan ip address set-to-factory-default
no bmc lan enable
no bmc serial-over-lan enable
!
!
ntp server 10.78.108.125
!
!
!
!
username admin password 1 ****
username admin privilege 15
!
!
!
!
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
inetd enable ftp
!
!
sshd enable
!
!
!
!
! End of WAAS configuration

```

**Related Commands**[configure](#)[copy running-config](#)[copy startup-config](#)

# show service-insertion

To display information about the entities (WNs, WNGs, ANCs, ANCG, and a service context) defined in an AppNav Cluster configuration and the cluster status, use the **show service-insertion EXEC** command.

```
show service-insertion { data-path mtu | pass-through offload | service-context [detail] |
  appnav-controller ip-address | appnav-controller-group | service-node [ip-address] |
  service-node-group [sngroupname]}
```

Syntax Description		
<b>data-path mtu</b>		Displays the MTU of the data path from this device to each of the other ANCs in the cluster.
<b>pass-through offload</b>		Displays the pass-through offload configuration.
<b>service-context</b>		Displays service context information. Available only on ANCs.
<b>detail</b>		Displays service context information and includes details about the ANCG, ANCs, and WNGs that are part of the service context.
<b>appnav-controller</b> <i>ip-address</i>		Displays information about the specified ANC. Available only on ANCs.
<b>appnav-controller-group</b> <b>p</b>		Displays information about the ANCG. Available only on ANCs.
<b>service-node</b> [ <i>ip-address</i> ]		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.
<b>service-node-group</b> <i>sngroupname</i>		Displays information about the specified WNG. If the group name is not specified, it shows information about all WNGs. Available only on ANCs.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
appnav-controller

**Usage Guidelines** This command returns minimal information if the entity or service context is disabled, or if the entity is not attached to the service context.

Although software version 6.x.x does not support Video and CIFS traffic acceleration, the Video and CIFS load markers have been retained in the **show service-insertion service-node** command for backward compatibility. This is to ensure that an AppNav Controller in version 5.x.x is able to forward a request for traffic acceleration to a Service Node in version 6.x.x.

**Examples** [Table 3-59](#) describes the fields shown in the **show service-insertion service-context** command display.

**Table 3-59** 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: <ul style="list-style-type: none"> <li>Operational—Stable and operational. All ANCs in the cluster have converged on a stable view of the devices in the cluster.</li> <li>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.</li> <li>Converging—Performing the convergence process due to a device change. Devices are exchanging information about each device's view of the cluster.</li> <li>Admin Disabled—Configured but not enabled.</li> <li>Initializing—Cluster is initializing.</li> <li>Internal Error—Internal error condition due to convergence failing after 5 minutes.</li> </ul>
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: <ul style="list-style-type: none"> <li>Started—Device has started to join the cluster gracefully.</li> <li>Completed—The graceful join operation completed successfully.</li> <li>Aborted—Graceful join was started and then disabled before completing.</li> <li>Not Configured—Device did not join the cluster gracefully.</li> <li>Unknown—State is unknown (default).</li> </ul>
Time joining state entered	Time the device entered the joining state.

**Table 3-59** Field Descriptions for the `show service-insertion service-context` Command

Field	Description
Cluster operational state	<p>Cluster operational state:</p> <ul style="list-style-type: none"> <li>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.)</li> <li>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.</li> </ul>
Interception Readiness State	<p>Interception readiness state of this device:</p> <ul style="list-style-type: none"> <li>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.)</li> <li>Not Ready—Not ready to intercept traffic (could be due to cluster convergence)</li> </ul>
Device Interception State	<p>Interception state of this device:</p> <ul style="list-style-type: none"> <li>Shutdown—Device is not intercepting traffic.</li> <li>Not Shutdown—Device is intercepting traffic.</li> <li>Unknown—State is unknown (default).</li> </ul>
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 3-60](#) 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 3-60** 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: <ul style="list-style-type: none"> <li>• Alive—This device can communicate with the ANC.</li> <li>• Alive (Removed from config)—This device was recently removed from the configuration but can still communicate with the ANC.</li> <li>• Dead—This device cannot communicate with the ANC.</li> <li>• 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.</li> </ul>
Time current status was reached	Time current status was reached.
Joining status of AppNav Controller	Current joining status of the ANC: <ul style="list-style-type: none"> <li>• Joining—The ANC is in the process of joining the cluster defined on the local ANC.</li> <li>• Joined—The ANC has successfully joined the cluster defined on the local ANC.</li> </ul>
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 3-60** 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: <ul style="list-style-type: none"> <li>• Alive—This device can communicate with the WN.</li> <li>• Dead—This device cannot communicate with the WN due to connectivity or not configured.</li> <li>• 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.</li> </ul>
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 3-60** 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: <ul style="list-style-type: none"> <li>• GREEN—Operating normally and accepting new flows.</li> <li>• YELLOW—Servicing existing flows but not accepting new flows due to overload, license removed, or policy engine timeout.</li> <li>• RED—Not running due to not configured, not licensed, or unresponsive.</li> </ul>
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: <ul style="list-style-type: none"> <li>• Yes—In GREEN state on at least one WN in the WNG.</li> <li>• No—In YELLOW or RED state on all WNs in the WNG.</li> </ul>
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]| status}}
```

## Syntax Description

<b>appnav</b>	Displays AppNav policy information.
<b>dynamic</b>	Displays policy information for dynamic matched flows.
<b>detail</b>	(Optional) Displays detailed policy information for dynamic matched flows.
<b>server-ip</b> <i>ip_address</i>	(Optional) Displays the policy information for dynamic matched flows for the server with the specified IP address.
<b>server-port</b> <i>port</i>	(Optional) Displays the policy information for dynamic matched flows for the server with the specified port number (1–65535).
 <b>Note</b>	The CIFS application accelerator is removed from WAAS v6.0.1, but the CIFS policy is continued for two ports: Port 139 and Port 445. For these ports only, the SMB application accelerator runs on CIFS policy. Therefore, an alarm generated by SMB on Port 139 or Port 445 is seen as a CIFS alarm.
<b>status</b>	Displays how many policy resources are in use and available.
<b>waas</b>	Displays WAAS optimization policy information.
<b>application-name</b>	Displays the configured application names on the device.
<b>app-id</b> <i>app-id</i>	Displays the policy information for dynamic matched flows for the application with the specified application number (0-1023) or the specified traffic type.
<b>mapi</b> <b>ms-ad-rep</b> <b>ms-exch-nspi</b> <b>ms-frs</b> <b>ms-frs-api</b> <b>ms-rfr</b> <b>ms-sql</b> <b>msn-messenger</b> <b>netlogon</b>	Microsoft Exchange MAPI aka Exchange Server Store EMSMDB, Microsoft Active Directory Replication (drsuapi), Microsoft Active Directory Name Service Provider (NSP), Microsoft File Replication Services (FRS), Microsoft File Replication API, Microsoft Exchange Directory RFR Interface, Microsoft SQL, Microsoft Messenger Service, Netlogon RPC
<b>dm-index</b> <i>index</i>	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 3-61](#) describes the fields shown in the **show service-policy type appnav status** command display.

**Table 3-61** *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 3-62](#) describes the fields shown in the **show service-policy type waas status** command display.

**Table 3-62** *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 3-63](#) describes the fields shown in the **show service-policy type appnav epm** command display.

**Table 3-63** *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 3-64 describes the fields shown in the **show service-policy type waas application-name** command display.

**Table 3-64** 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.

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.
	<i>port-num</i>	(Optional) Up to 8 port numbers (1–65535).
	<b>summary</b>	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		
<b>alarm-history</b>		Displays SNMP alarm history information.
<b>engineID</b>		Displays local SNMP engine identifier.
<b>event</b>		Displays events configured through the Event MIB. This keyword applies only to application-accelerator device mode.
<b>group</b>		Displays SNMP groups.
<b>stats</b>		Displays SNMP statistics.
<b>user</b>		Displays SNMP users.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show snmp alarm-history** command provides information on various SNMP variables and statistics on SNMP operations.

**Examples** [Table 3-65](#) describes the fields shown in the **show snmp alarm-history** command display.

**Table 3-65** 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 3-66 summarizes the mapping of module names to module IDs.

**Table 3-66 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 3-67 summarizes the mapping of category names to category IDs.

**Table 3-67 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 3-68 describes the fields shown in the **show snmp engineID** command display.

**Table 3-68 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 3-69 describes the fields shown in the **show snmp event** command display. The **show snmp event** command displays information about the SNMP events that were set using the **ssh** command:

**Table 3-69 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 3-69 Field Descriptions for the show snmp event Command (continued)

Field	Description
(1):	Name for the trigger. This name is locally-unique and administratively assigned. For example, this field might contain the “isValid” trigger name. Numbering indicates that this is the first management trigger listed in the <b>show</b> output.
Comment:	Description of the trigger function and use. For example: 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 <b>snmp-server trigger</b> global configuration command or by using an SNMP interface. “CLI” is the default owner.
Object:	String identifying the object.
Boolean Entry:	
Value:	Object identifier of the MIB object to sample to see whether the trigger should fire.

**Table 3-69** 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 <b>show</b> output. The fields are repeated for each instance listed in this <b>show</b> command.

[Table 3-70](#) describes the fields shown in the `show snmp group` command display.

**Table 3-70** 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 3-71](#) describes the fields shown in the `show snmp stats` command display.

**Table 3-71** *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 3-72](#) describes the fields shown in the **show snmp user** command display.

**Table 3-72** *Field Descriptions for the show snmp user Command*

Field	Description
User name	String identifying the name of the SNMP user.
Engine ID	String identifying the name of the copy of SNMP on the device.
Group Name	Name of the SNMP group, or collection of users who have a common access policy.

**Related Commands**

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server contact](#)
- [\(config\) snmp-server enable traps](#)

**(config) snmp-server group**  
**(config) snmp-server host**  
**(config) snmp-server location**  
**(config) snmp-server mib**  
**(config) snmp-server notify inform**  
**(config) snmp-server user**  
**(config) snmp-server view**  
**(config) snmp-server trigger**

# show ssh

To display the status and configuration information of the Secure Shell (SSH) service for a WAAS device, use the **show ssh** EXEC command.

## show ssh

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-73](#) describes the fields shown in the **show ssh** command display.

**Table 3-73** 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

<b>Syntax Description</b>	This command has no arguments or keywords.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager
<b>Usage Guidelines</b>	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 <b>show running-config</b> command.

## Examples

The following is sample output from the **show startup-config** command. It displays the configuration saved for use on startup of the WAAS device.

```
WAE# show startup-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname Edge-WAE1
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
ip address 10.10.10.33 255.255.255.0
exit
interface GigabitEthernet 2/0
shutdown
...
```



---

**Related Commands**[configure](#)[copy running-config](#)[show running-config](#)

# show statistics accelerator

To display application accelerator general statistics for a WAAS device, use the **show statistics accelerator EXEC** command.

**show statistics accelerator detail**

**show statistics accelerator epm [detail]**

**show statistics accelerator generic {connections {epm | http | ica | mapi | smb | ssl } | detail}**

**show statistics accelerator http [debug | detail | https]**

**show statistics accelerator ica [detail]**

**show statistics accelerator mapi [detail]**

**show statistics accelerator mapi detail rpchttp**

**show statistics accelerator smb [debug | detail | inc Print | request]**

**show statistics accelerator ssl [detail | payload {http | other}]**

**show statistics accelerator wansecure [detail]**

## Syntax Description

<b>detail</b>	(Optional) Displays detailed statistics.
<b>epm</b>	Displays statistics for the EPM application accelerator.
<b>generic</b>	Displays statistics for the generic application accelerator.
<b>connections</b>	Displays generic connection statistics.
<b>http</b>	Displays statistics for the HTTP application accelerator.
<b>ica</b>	Displays statistics for the ICA application accelerator.
<b>mapi</b>	Displays statistics for the MAPI application accelerator.
<b>mapi rpchttp</b>	Displays statistics for the MAPI RPC HTTP application accelerator.
<b>smb</b>	Displays statistics for the SMB application accelerator.
<b>request</b>	Displays SMB application accelerator statistics on requests.
<b>ssl</b>	Displays statistics for the SSL application accelerator.
<b>wansecure</b>	Displays statistics for the WAN secure application accelerator.
<b>debug</b>	(Optional) Displays debug statistics.
<b>https</b>	Displays statistics for the HTTPS application accelerator.
<b>payload</b>	(Optional) Displays the SSL payload type.
<b>other</b>	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 3-74](#) describes the fields shown in the **show statistics accelerator epm detail** command display.

**Table 3-74** Field Descriptions for the show statistics accelerator epm Command

Field	Description
Global TCP AO connection statistics	
Time Accelerator was started	Time that the accelerator was started.
Time Statistics were Last Reset/Cleared	Time that the statistics were last reset or cleared.
Total Handled Connections	Total connections handled.
Total Optimized Connections	Total optimized connections.
Total Pushed Down Connections	Total pushed down connections.
Total Dropped Connections	Total dropped connections.
Current Active Connections	Current active connections.
Current Pending Connections	Current pending connections.
Maximum Active Connections	Maximum active connections.
Total Requests	Total requests.
Total Requests Successfully Parsed	Total requests successfully parsed.
Total Request Errors	Total request errors.
Total Responses	Total responses.
Total Responses Successfully Parsed	Total responses successfully parsed.
Total Service-unavailable Responses	Total service-unavailable responses.
Total Requests for UUID not in Policy Engine Map	Total requests for UUID not in policy engine map.
Total Response Errors	Total response errors.

[Table 3-75](#) describes the fields shown in the **show statistics accelerator generic connections detail** command display. This command shows the aggregated statistics for all connections.

**Table 3-75** Field Descriptions for the show statistics accelerator generic Command

Field	Description
Time elapsed since "clear statistics"	Time that has elapsed since the statistics were last reset.
Time Accelerator was started	Local time accelerator was started or restarted.

**Table 3-75** Field Descriptions for the *show statistics accelerator generic* Command (continued)

Field	Description
Time Statistics were Last Reset/Cleared	Local time accelerator was last started or restarted, or the <b>clear statistics</b> command was executed since accelerator was last started or restarted.
Total Handled Connections	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented.  This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.  Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total Optimized Connections	Connections previously and currently optimized by the accelerator. This includes: Current Active Connections + Total Fast Connections + Fast connections initiated by peer.
Total Connections Handed-off with Compression Policies Unchanged	Connections initially accepted by accelerator, but later handed off to generic optimization without policy changes so the current negotiated policies for compression (DRE/LZ) will be used.
Total Dropped Connections	Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources).
Current Active Connections	Number of WAN side connections currently established and either in use or free for fast connection use.  WAN side connections currently established and in use can be calculated as follows: Current Active Connections - Total Active Connections Free For Fast Connection Use Not cleared using <b>clear statistics accelerator</b> 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 <b>clear statistics accelerator</b> command.
Global Generic AO Connection Statistics	
Total number of connections handled	Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented.  This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.  Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.
Total number of active connections	Total number of hits that represent either active connections using the accelerator application.

**Table 3-75** Field Descriptions for the *show statistics accelerator generic* Command (continued)

Field	Description
Total number of bytes transferred from client	Total number of bytes transferred from the client side.
Total number of bytes transferred from server	Total number of bytes transferred from the server side.
Policy Engine Statistics	
Session timeouts	Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.
Total timeouts	Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.
Last keepalive received	Amount of time since the last keepalive (seconds).
Last registration occurred	Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are as follows: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul>
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.

**Table 3-75** 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:)	<ul style="list-style-type: none"> <li>• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul>

[Table 3-76](#) describes the fields shown in the **show statistics accelerator http detail** command display.

**Table 3-76** 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 <b>clear statistics accelerator [http   all]</b> command was executed since accelerator was last started or restarted.

Table 3-76 Field Descriptions—show statistics accelerator http detail Command (continued)

Field	Description
Total Handled Connections	<p>Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented.</p> <p>This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.</p> <p>Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.</p>
Total Optimized Connections	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.	<p>Number of WAN side connections currently established and either in use or free for fast connection use.</p> <p>WAN side connections currently established and in use can be calculated as follows: Current Active Connections - Total Active Connections Free For Fast Connection Use Not cleared using <b>clear statistics accelerator [http   all]</b> command.</p>
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 <b>clear statistics accelerator [http   all]</b> 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	<p>Number of Current Active Connections that are idle and available for reuse as a fast connection. Incremented when an in-use active connection becomes idle and is available for reuse as a fast connection.</p> <p>Decrementd when an available idle active connection is reused or its idle timeout (5 secs) is reached. Not cleared using the <b>clear statistics accelerator [http   all]</b> command.</p>

**Table 3-76** Field Descriptions—*show statistics accelerator http detail* Command (continued)

Field	Description
Total Connections Handed-off	Total Pushed Down Connections + Total Connections Handed-off with Compression Policies Disabled.
Total Connections Handed-off with Compression Policies Disabled	Total number of connections handed off to generic optimization with compression policies disabled. This statistic includes handoffs for SSL CONNECT requests received by the HTTP Accelerator.
Total Connections Handed-off to SSL	Total number of connections handed off to the SSL accelerator as a result of SSL CONNECT requests received by the HTTP Accelerator.
Total Connection Hand-off Failures	Total number of connections that were attempted to be handed off but the hand off failed.
Total Fast Connection Successes	Total number of times a client side idle active WAN connection was able to be reused instead of establishing a new WAN connection.
Total Fast Connection Failures	Total number of times a client side idle active WAN connection was attempted to be reused, but the reuse failed.
Maximum Fast Connections on a Single Connection	Maximum number of times a single connection was reused. This is the “best case” of number of reuses on a single connection.  Limited to be less than maximum session reuse count (currently defined as 100 - an arbitrary max).
Total CONNECT Requests with Incomplete Message	Total number of SSL CONNECT requests with an incomplete message.
Current Active Connections with Object-cache optimization	The total number of current active connections with object-cache optimization.
Percentage of Connection Time Saved	$(\text{Total Time Saved} / (\text{Total Time Saved} + \text{Total Round Trip Time For All Connections})) * 100$ .
Object Cache Caching Type	
Object cache transactions served from cache	The total number of object cache transactions served from cache.
Object cache request bytes for cache-hit transactions	The total number of object cache request bytes for cache-hit transactions.
Object cache response bytes for cache-hit transactions	The total number of object cache response bytes for cache-hit transactions.
Object cache response time saved for cache-hit transactions	The total number of object cache response time saved for cache-hit transactions.
Avg. response time saved per cache-hit transaction (ms)	The average response time saved per cache-hit transaction, in milliseconds.
Percentage response time savings for cache-hit transactions	The total percentage response time savings for cache-hit transactions.
Avg. response time saved for connections with RTT [00-20] (ms)	The average response time saved for connections with RTT, in the range 00-20, in milliseconds.



**Table 3-76** Field Descriptions—*show statistics accelerator http detail* Command (continued)

Field	Description
Avg. response time saved for connections with RTT [20-50] (ms)	The average response time saved for connections with RTT, in the range 20-50, in milliseconds.
Avg. response time saved for connections with RTT [50-90] (ms)	The average response time saved for connections with RTT, in the range 50-90, in milliseconds.
Avg. response time saved for connections with RTT [ 90+] (ms)	The average response time saved for connections with RTT, in the range 90+, in milliseconds.
Object cache transactions requiring freshness check	The total number of object cache transactions requiring freshness check.
Object cache responses not cached	The total number of object cache responses not cached.
Object cache responses stored in cache	he total number of object cache responses stored in cache.
Object cache WAN response bytes for freshness check	The total number of object cache WAN response bytes requiring freshness check.
Object cache WAN response bytes not cached	The total number of object cache WAN response bytes not cached.
Object cache WAN response bytes stored in cache	The total number of object cache WAN response bytes stored in cache.
Object cache LAN response bytes for freshness check	The total number of object cache LAN response bytes requiring freshness check.
Object cache Percentage cache-hit transactions	The percentage of object cache cache-hit transactions.
Object cache Percentage cache-hit bytes	The percentage of object-cache cache-hit bytes.
Total Round Trip Time for All Connections (ms)	Total RTT for all WAN connections that have been established.
Total Fast Connections Initiated by Peer	Total number of times the server side WAN connection was a fast connection initiated by the client side peer.  This statistic should match the Total Fast Connections on the peer WAE.
Total SYN Timeouts	Total number of SYN timeouts because the HTTP accelerator was temporarily busy.
Total Time for Metadata Cache Miss (ms)	Total time for metadata cache misses, in milliseconds.
RTT saved by Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving redirect (301) responses, in milliseconds.
RTT saved by Authorization Redirect Metadata Cache (ms)	Round trip time saved by caching and locally serving authentication required (401) responses, in milliseconds.
RTT saved by Content Refresh Check Metadata Cache (ms)	Round trip time saved by caching and locally serving conditional (304) responses, in milliseconds.
Total Time Saved by Fast Connection Use (ms)	Total time saved by fast connection reuse, in milliseconds.
Total Locally Served Redirect Responses	Number of locally served redirect (301) responses.

**Table 3-76** Field Descriptions—*show statistics accelerator http detail* Command (continued)

Field	Description
Total Locally Served Unauthorized Responses	Number of locally served authentication required (401) responses.
Total Locally Served Conditional Responses	Number of locally served conditional (304) responses.
Total Remotely Served Redirect Responses	Number of remotely served redirect (301) responses (cache misses).
Total Remotely Served Unauthorized Responses	Number of remotely served authentication required (401) responses (cache misses).
Total Remotely Served Conditional Responses	Number of remotely served conditional (304) responses (cache misses).
Total Requests with URL Longer than 255 Characters	Number of requests not cached because the URL is longer than 255 characters.
Total Requests with HTTP Pipelining	Number of requests not cached due to HTTP pipelining.
Total Transactions Handled	Number of HTTP transactions handled.
Total Server Compression Suppression	Number of times server compression was suppressed.
Total Requests Requiring Server Content-Revalidation	Number of requests that required content to be revalidated with the origin server, as specified by a Cache-Control header.
Total Responses not to be Cached	Number of 200, 301, 304, and 401 responses not to be cached, as specified by a Cache-Control header.
Total Connections Expecting Authentication	Number of connections expecting authentication.
Total Connections with Unsupported HTTP Requests	Number of connections with unsupported HTTP requests.
Total Connections with Unsupported HTTP Responses	Number of connections with unsupported HTTP responses.
Total Hints Sent to DRE Layer to Flush Data	Number of DRE hints to flush data.
Total Hints Sent to DRE Layer to Skip LZ	Number of DRE hints to skip LZ compression.
Total Hints Sent to DRE Layer to Skip Header Information	Number of DRE hints to skip header information.
Total ACL Lookups for Subnet feature	Total number of system calls made for ACL lookup.
Total Sessions using Global enable/disable settings	Total number of sessions using global configuration for all four HTTP AO optimization features.
Total Sessions using ACL-selected settings	Total number of sessions using subnet configuration for at least one HTTP AO optimization feature.
Total sessions using SharePoint optimization	Number of sessions using SharePoint optimization feature to access objects from SharePoint server.
Total sessions using SharePoint pre-fetch optimization	Number of sessions where pre-fetch optimization for SharePoint objects ((MS Office applications) is enabled.

**Table 3-76** 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.
<b>Policy Engine Statistics</b>	
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: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul>
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.

Table 3-76 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:)	<ul style="list-style-type: none"> <li>• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul>
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.
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 3-77 describes the fields shown in the **show statistics accelerator http debug** command display.

**Table 3-77** 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 3-77** 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 3-77** *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 3-77** 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 3-78 describes the fields shown in the **show statistics accelerator http https** command display.

**Table 3-78** 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	<p>HTTPS connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted. Never decremented.</p> <p>This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.</p> <p>Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.</p>
Total 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 3-78** 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 milliseconds.
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 3-78** 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 3-79](#) describes the fields shown in the **show statistics accelerator ica detail** command display.

**Table 3-79** Field Descriptions—*show statistics accelerator ica detail* Command

Field	Description
Global Statistics	
Time Accelerator was started	Time that the accelerator was started.
Time statistics were Last Reset/Cleared	Time that the statistics were last reset.
Total Handled Connections	Number of connections handled since the accelerator was started.
Total Optimized Connections	Number of connections optimized since the accelerator was started, from start to finish.
Total Connections Handed-off with Compression Policies Unchanged	Total number of connections received by the accelerator but to which only generic optimizations were done (no acceleration).
Total Dropped Connections	Total number of connections dropped for reasons other than client/server socket errors or close.
Current Active Connections	Total number of current active connections being handled by the ICA accelerator.
Current Pending Connections	Total number of connections pending to be accepted.
Maximum Active Connections	Maximum number of active connections handled by the accelerator.

**Table 3-79** Field Descriptions—*show statistics accelerator ica detail* Command (continued)

Field	Description
Current Active SSL Connections	Total number of SSL connections currently being handled by the accelerator.
Current Active Non-SSL Connections	Total number of non-SSL connections currently being handled by the accelerator
Current Active CGP Connections	Total number of CGP (Common Gateway Protocol) connections currently being handled by the accelerator.
Current Active ICA Connections	Total number of ICA connections currently being handled by the accelerator.
Total SSL Connections	Total number of SSL connections.
Total non-SSL Connections	Total number of non-SSL connections.
Total CGP Connections	Total number of CGP connections.
Total ICA Connections	Total number of ICA connections being handled by the accelerator.
Total CGP Reconnections	Total number of CGP reconnections being handled by the accelerator.
Total Sessions Client Version 13.1	Total number of ICA sessions with client version (Citrix Receiver) 13.1.
Total Sessions Client Version 13.0	Total number of ICA sessions with client version (Citrix Receiver) 13.0.
Total Sessions Client Version 12.1	Total number of ICA sessions with client version (online plugin) 12.1.
Total Sessions Client Version 12.0	Total number of ICA sessions with client version (online plugin) 12.0.
Total Sessions Client Version 11.2	Total number of ICA sessions with client version (online plugin) 11.2.
Total Sessions Client Version 11.0	Total number of ICA sessions with client version (online plugin) 11.0.
Total Sessions Other Client Versions	Total number of ICA sessions with other client versions.
Total Sessions with No Encryption	Total number of ICA sessions with no encryption.
Total Sessions with Basic Encryption	Total number of ICA sessions with basic encryption.
Total Sessions with RC5_40 Encryption	Total number of ICA sessions with RC5 40-bit encryption.
Total Sessions with RC5_56 Encryption	Total number of ICA sessions with RC5 56-bit encryption.
Total Sessions with RC5_128 Encryption	Total number of ICA sessions with RC5 128-bit encryption.
Total Sessions with RC5_128 Logon-Only Encryption	Total number of ICA sessions with RC5 128-bit logon-only encryption.
Connections Handed Off Because of Unrecognized Protocol	Total number of ICA connections handed off because of unrecognized protocol.

**Table 3-79** Field Descriptions—*show statistics accelerator ica detail* Command (continued)

Field	Description
Connections Handed Off Because of Unsupported Client Version	Total number of ICA connections handed off because of unsupported client version.
Connections Handed Off Because of Unknown CGP Session ID	Total number of ICA connections handed off because of unknown CGP session ID.
Connections Handed Off Because of Client on Denied List	Total number of ICA connections handed off because of client on Denied list.
Connections Handed Off Because of Resource Limit	Total number of ICA connections handed off because of resource limit.
Connections Handed Off Because of Other Reasons	Total number of ICA connections handed off because of other reasons.
Connections Disconnected Because of Unsupported Client Version	Total number of ICA connections disconnected because of unsupported client version.
Connections Disconnected Because of I/O Error	Total number of ICA connections disconnected because of I/O error.
Connections Disconnected Because of Parsing Error	Total number of ICA connections disconnected because of parsing error.
Connections Disconnected Because of Resource Limit	Total number of ICA connections disconnected because of resource limit.
Connections Disconnected Because of Session in Use	Total number of ICA connections disconnected because of session in use.
Connections Disconnected Because of Other Reasons	Total number of ICA connections disconnected because of other reasons.
Active MSI Very High Connections	Number of active MSI very high priority connections.
Active MSI High Connections	Number of active MSI high priority connections.
Active MSI Medium Connections	Number of active MSI medium priority connections.
Active MSI Low Connections	Number of active MSI low priority connections.
Active non-MSI Connections	Number of active non-MSI connections.
Total MSI Very High Connections	Total number of MSI very high priority connections.
Total MSI High Connections	Total number of MSI high priority connections.
Total MSI Medium Connections	Total number of MSI medium priority connections.
Total MSI Low Connections	Total number of MSI low priority connections.
Total non-MSI Connections	Total number of non-MSI connections.
LAN bandwidth (kb/s)	LAN bandwidth speed, in kilobytes per second.

[Table 3-80](#) describes the fields shown in the **show statistics accelerator mapi detail** command display.

**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command

Field	Description
Global Statistics	
Time Accelerator was started	Time that the accelerator was started.
Time statistics were Last Reset/Cleared	Time that the statistics were last reset.
Total Handled Connections	Number of connections handled since the accelerator was started.
Total Optimized Connections	Number of connections handled since the accelerator was started, from start to finish.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections received by the accelerator but to which only generic optimizations were done (no acceleration).
Total Dropped Connections	Number of connections dropped for reasons other than client/server socket errors or close.
Current Active Connections	Number of connections currently being handled by the accelerator.
Current Pending Connections	Number of connections pending to be accepted.
Maximum Active Connections	Maximum number of simultaneous connections handled by the accelerator.
Total Secured Connections	Number of connections to Outlook clients that use encryption. Such connections are not accelerated by the MAPI accelerator but are passed through.
Number of Synch Get Buffer Requests	Number of MAPI SyncGetBuffer calls made. Each call downloads a chunk of data from a cached folder.
Minimum Synch Get Buffer Size (bytes)	Minimum chunk size downloaded by the MAPI SyncGetBuffer call.
Maximum Synch Get Buffer Size (bytes)	Maximum chunk size downloaded by the MAPI SyncGetBuffer call.
Average Synch Get Buffer Size (bytes)	Average chunk size downloaded by the MAPI SyncGetBuffer call.
Number of Read Stream Requests	Number of MAPI ReadStream calls made. Each call downloads a chunk of data from a noncached folder.
Minimum Read Stream Buffer Size (bytes)	Minimum chunk size downloaded by the MAPI ReadStream call.
Maximum Read Stream Buffer Size (bytes)	Maximum chunk size downloaded by the MAPI ReadStream call.
Average Read Stream Buffer Size (bytes)	Average chunk size downloaded by the MAPI ReadStream call.
Minimum Accumulated Read Ahead Data Size (bytes)	Minimum data size for MAPI read ahead.
Maximum Accumulated Read Ahead Data Size (bytes)	Maximum data size for MAPI read ahead.

**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command (continued)

Field	Description
Average Accumulated Read Ahead Data Size (bytes)	Average data size for MAPI read ahead.
Local Response Count	Number of local MAPI command responses sent to the client without waiting for a response from the peer WAE.
Average Local Response Time (usec)	Average time used for local responses, in microseconds.
Remote Response Count	Number of MAPI commands forwarded to the Exchange server for a response.
Average Remote Response Time (usec)	Average time used for remote responses, in microseconds.
Number of Write Stream Requests	Number of write stream requests.
Minimum Async Write Stream Buffer Size (bytes)	Minimum size of the asynchronous request stub sent on the WAN, calculated from the minimum stub size across all sessions.
Maximum Async Write Stream Buffer Size (bytes)	Maximum size of the asynchronous request stub sent on the WAN, calculated from the maximum stub size across all sessions.
Average Async Write Stream Buffer Size (bytes)	Average size of the asynchronous request stub sent on the WAN, calculated by taking the average of the stub size across all sessions.
Current 2000 Accelerated Sessions	Number of accelerated sessions to Outlook 2000 clients. Sessions (users), not TCP connections.
Current 2003 Accelerated Sessions	Number of accelerated sessions to Outlook 2003 clients. Sessions (users), not TCP connections.
Current 2007 Accelerated Sessions	Number of accelerated sessions to Outlook 2007 clients. Sessions (users), not TCP connections.
Current 2010 Accelerated Sessions	Number of accelerated sessions to Outlook 2010 clients. Sessions (users), not TCP connections.
Current 2013 Accelerated Sessions	Number of accelerated sessions to Outlook 2013 clients. Sessions (users), not TCP connections.
Current 2016 Accelerated Sessions	Number of accelerated sessions to Outlook 2016 clients. Sessions (users), not TCP connections.
Current Exchange to Exchange Accelerated Sessions	Number of accelerated sessions between the exchange servers.
Current 2003 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2003 clients.
Current 2007 Accelerated Secured Sessions	Number of accelerated secured sessions to Outlook 2007 clients.
Current 2010 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2010 clients.
Current 2013 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2013 clients.

**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command (continued)

Field	Description
Current 2016 Accelerated Secured Session	Number of accelerated secured sessions to Outlook 2016 clients.
Lower than 2000 Sessions	Number of sessions to clients using a version of Outlook lower than Outlook 2000. Such connections are not accelerated by the MAPI accelerator but are passed through.
Unsupported Higher Client Version Sessions	Number of sessions to clients using a version of Outlook higher than that supported. Such connections are not accelerated by the MAPI accelerator but are passed through.
<b>Async Write Optimization Statistics</b>	
Current Number Of Async Write Stubs On WAN	Current number of asynchronous requests on the WAN.
Current Number Of Requests Queued Due To Flow Control	Current number of client session flows that were blocked due to threshold limit.
Current Number Of Requests Queued Due To RopBackOff	Current number of client session flows that were blocked due to ropbackoff response.
Total Number Of RopBackOff Response Received	Total number of ropbackoff responses received across all connections.
Total RopBackOff Duration (msec)	Cumulative time of ropbackoff durations across all connections, in milliseconds.
Total Wait Time Of Requests Queued Due To FlowControl (msec)	Cumulative wait time of requests queued due to flow control across all connections, in milliseconds.
Total Wait Time Of Requests Queued Due To RopBackOff (msec)	Cumulative wait time of requests queued due to ropbackoff across all connections, in milliseconds.
Connection Hand-Off Reasons	Number of connections handed off from the MAPI accelerator to the generic accelerator for various reasons.
Total Handled RPC TCP Connections	The total handled RPC TCP connections handled during this session.
Total Handled RPCH HTTP Connections	The total handled RPCH HTTP connections handled since the accelerator was started or its statistics last reset.
Total Handled RPCH HTTPS Connections	The total handled RPCH HTTPS connections handled since the accelerator was started or its statistics last reset.
Total Handled MAPI-HTTPS Connections	The total handled MAPI HTTPS connections handled since the accelerator was started or its statistics last reset.
Total Optimized RPC TCP Connections	The total optimized RPC TCP connections.
Total Optimized RPCH HTTP Connections	The total optimized RPCH HTTP connections.
Total Optimized RPCH HTTPS Connections	The total optimized RPCH HTTPS connections.
Total Handled RPCH Virtual Sessions	The total handled RPCH virtual sessions.
Total Optimized RPCH Virtual Sessions	The total optimized RPCH virtual sessions,
Total Pipe-Through Virtual Sessions	The total pipe-through virtual sessions.

**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command (continued)

Field	Description
Total Optimized MAPI-HTTPS Connections	The total number of optimized MAPI HTTPS connections.
Total Pipe-Through MAPI-HTTPS Connections	The total number of MAPI- HTTPS connections that are handed over from the MAPI accelerator.
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.
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.



**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command (continued)

Field	Description
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.
Exchange Server Error Statistics	Number of errors of various types that were returned by the Exchange server.
<b>Policy Engine Statistics</b>	
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: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul>
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.

**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command (continued)

Field	Description
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.
Rejected Connection Counts Due To: (Total:)	<ul style="list-style-type: none"> <li>• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul>
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.
<b>Auto-Discovery Statistics</b>	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.

**Table 3-80** Field Descriptions—*show statistics accelerator mapi detail* Command (continued)

Field	Description
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.
AO discovery successful	For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.
AO discovery failure	Number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.

Table 3-81 describes the fields shown in the *show statistics accelerator mapi detail rpchttp* command display.

**Table 3-81** Field Descriptions for the *show statistics accelerator mapi detail rpchttp* Command

Field	Description
Number of active IN channels	Count of current active IN channel RPCHTTP(S) connections.
Number of active OUT channels	Count of current active OUT channel RPCHTTP(S) connections.
Number of active optimized sessions	Count of current active RPCHTTP(S) Virtual sessions. This count is equal to the current active IN/OUT channel count.
Number of active RPC HTTP(S) clients	Number of outlook clients currently optimized for RPCHTTP(S).
Number of RPC HTTP connections optimized since uptime	Total count of the RPCHTTP(S) connections optimized. This count is the total of the IN and OUT channels optimized. This count is equal to 2 times the 'Number of Optimized RPCH Virtual Sessions' counter.
Number of Handled RPCH Virtual Sessions	Total count of the RPCHTTP(S) virtual session handled by MAPI AO.
Number of Optimized RPCH Virtual Sessions	Total count of the RPCHTTP(S) virtual sessions optimized. This counter is half of the 'Number of RPC HTTP connections optimized since uptime' counter.
Number of Pipe-through Virtual Sessions	Total number of RPCHTTP(S) sessions handed over without optimization. This counter is equal to 'Number of Handled RPCH Virtual Sessions' - 'Number of Optimized RPCH Virtual Sessions'

Table 3-82 describes the fields shown in the **show statistics accelerator smb detail** command display.

**Table 3-82** 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 policy changes so the current negotiated policies for compression (DRE/LZ) will be used.
Total Dropped Connections	Number of connections dropped.
Total Active Connections	Number of connections currently being optimized by the SMB accelerator.
Current Pending Connections	Number of connections that have been determined to be accelerated by the SMB accelerator, and have been queued to be picked up by the accelerator.
Maximum Active Connections	Maximum value reached by the Current Active Connections counter. This counter will be reset if the accelerator is restarted or statistics are cleared.
Total Number of SMB1 Sessions Optimized	Total number of SMB1 sessions optimized by the accelerator.
Total Number of SMB1 Signed Sessions (L4 Opt)	Total number of SMB1 signed sessions (Layer 4 optimization).
Total Number of SMB1 Sessions Not Optimized	Total number of SMB1 sessions not optimized by the accelerator.
Total Number of SMB2 Sessions Not Optimized (handoff on request)	Total number of SMB2 sessions not optimized by the accelerator.
Total Number of SMB2 Sessions (L4 optimization, handoff on request)	Total number of SMB2 sessions optimized (Layer 4 optimization)
Total Number of SMB2_0 Sessions Optimized	Total number of SMB2 sessions optimized.
Total Number of SMB2_0 Signed Sessions (L4 Opt)	Number of SMB2_0 signed sessions (Layer 4 optimization)
Total Number of SMB2_0 Signed Sessions (L7Opt)	Number of SMB2_0 signed sessions (Layer 7 optimization)
Total Number of SMB2_0 Sessions Not Optimized	Number of SMB2_1 session optimized.
Total Number of SMB2_1 Sessions Optimized	Number of SMB2_1 sessions optimized.
Total Number of SMB3_11 Sessions Optimized	Number of SMB3_11 sessions optimized.

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
Total Number of SMB2_1 Signed Sessions (L4 Opt)	Number of SMB2_1 signed sessions (Layer 4 optimization)
Total Number of SMB2_1 Signed Sessions (L7 Opt)	Number of SMB2_1 signed sessions (Layer 7 optimization)
Total Number of SMB2_1 Sessions Not Optimized	Number of SMB2_1 sessions not optimized.
Total Number of SMB3_0 Sessions Optimized:	Total number of SMB3 sessions optimized.
Total Number of SMB3_0 Sessions Not Optimized:	Total number of SMB3 sessions not optimized by the accelerator.
Total Number of SMB3_11 Sessions Not Optimized	Total number of SMB3 sessions not optimized by the accelerator.
Total Number of SMB3_0 Sessions Optimized (L4 Opt)	Number of SMB3_0 sessions (Layer 4 optimization).
Total Number of SMB3_0 Sessions Not Optimized	Total number of SMB3 sessions not optimized by the accelerator.
Total Number of Signed SMB3_0 Signed Sessions Optimized	Number of optimized signed SMB3_0 sessions.
Total Number of Signed SMB3_0 Signed Sessions (L4/Not Optimized)	Number of signed SMB3_0 sessions not optimized. (Layer 4)
Total Number of Signed SMB3_02 Signed Sessions Optimized	Number of optimized signed SMB3_02 sessions.
Total Number of Signed SMB3_02 Signed Sessions (L4/Not Optimized)	Number of signed SMB3_02 sessions not optimized. (Layer 4)
Total Number of SMB3_02 Signed Sessions (L7 opt)	Number of signed SMB3_02 signed sessions optimized. (Layer 7)
Total Number of SMB3_02 Encrypted Sessions not optimized	Number of encrypted SMB3_02 sessions not optimized.
Total Number of SMB3_0 Encrypted Sessions (L4 opt)	Total number of SMB 3_0 encrypted sessions using Layer 4 optimization.
Total Number of SMB3_0 Encrypted Sessions (L7 opt)	Total number of SMB 3_0 encrypted sessions using Layer 7 optimization.
Total Number of SMB3_02 Encrypted Sessions (L4 opt)	Total number of SMB 3_02 encrypted sessions using Layer 4 optimization.
Total Number of SMB3_02 Encrypted Sessions (L7 opt)	Total number of SMB 3_02 encrypted sessions using Layer 7 optimization.
Total Number of Requests Processed	Number of requests processed (including successful and unsuccessful responses).
Total Number of Signed Requests Processed	Number of signed requests processed (including successful and unsuccessful responses).
Total Number of Encrypted Requests Processed	Number of encrypted requests processed (including successful and unsuccessful responses)

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
Total Number of Requests Served Locally	Number of requests served locally by the WAAS device.
Total Number of Signed Requests Served Locally	Number of signed requests served locally by the WAAS device.
Total Number of Encrypted Requests Served Locally	Number of encrypted requests served locally by the WAAS device.
Total Number of Requests Sent to File Servers	Number of requests sent to file servers.
Total Number of Signed Requests Sent to File Servers	Number of signed requests sent to file servers.
Total Number of Encrypted Requests Sent to File Servers	Number of encrypted requests sent to file servers.
Total Number of SMB1 Requests Processed	Number of SMB1 requests processed (including successful and unsuccessful responses).
Total Number of SMB2 Requests Processed	Number of SMB2 requests processed (including successful and unsuccessful responses).
Total Number of SMB2 Signed Requests Processed	Number of signed SMB2 requests processed (including successful and unsuccessful responses).
Total Number of VFN Requests Processed	Number of VFN requests processed (including successful and unsuccessful responses).
Total Number of Active Requests	Number of active SMB requests.
Total Number of Open Files	Number of open files on the WAE. The SMB accelerator performs below the optimum level if there are too many open files. The maximum value of the open-file count is platform-dependent. Use ( <b>config</b> ) <b>threshold-monitor</b> to configure monitoring thresholds.
Total Number of Bytes Read from Cache	Number of bytes read from cache.
Total Number of Bytes Written to Cache	Number of bytes written to the cache.
Total SMB Object Cache Read bytes	Number of SMB Object Cache read bytes.
Total SMB Object Cache Write bytes	Number of SMB Object Cache write bytes.
Object cache load bypass read	Total number of read request that were sent to server because of object cache load.
Object cache load bypass write	Total number of write requests which are not cached in object cache because of load
Object cache load bypass read bytes	Total number of read bytes that went to the server because of object cache load
Object cache load bypass write byte	Total number of write bytes which are not written to object cache because of object cache load.
Total Number of Bytes Written to LAN (Original)	Number of unoptimized bytes written to the LAN.
Total Number of Bytes Read from LAN (Original)	Number of unoptimized bytes read from the LAN.

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
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.
SMB preposition gain %	Gain percent when a file is served locally from cache because it was previously cached using preposition.
Total Number of Signed SMB Bytes Read from LAN (Original)	Number of unoptimized signed SMB bytes read from the LAN.
Total Number of Signed SMB Bytes Written to LAN (Original)	Number of unoptimized signed SMB bytes written to the LAN.
Total Number of Signed SMB Bytes Read from WAN (L4 Optimized)	Number of Layer 4 optimized signed SMB bytes read from the WAN.
Total Number of Signed SMB Bytes Written to WAN (L4 Optimized)	Number of Layer 4 optimized signed SMB bytes written to the WAN.
Total Number of Encrypted SMB Bytes read from LAN (Original):	Number of unoptimized encrypted bytes read from the LAN.
Total Number of Encrypted SMB Bytes written to LAN (Original)	Number of unoptimized encrypted bytes written to the LAN.
Total Number of Encrypted SMB Bytes read from WAN (L4 Optimized)	Number of encrypted optimized bytes read from the WAN.
Total Number of Encrypted SMB Bytes Written to WAN(L4 Optimized)	Number of encrypted optimized bytes written to the WAN.
Average Response Time (ms) for Requests Served Locally	Average response time for requests served locally, in milliseconds.
Average Signed Response Time (ms) for Requests Served Locally	Average response time for signed requests served locally, in milliseconds
Average Response Time (ms) for Requests Sent to File Servers	Average response time for requests sent to file servers, in milliseconds.
Average Signed Response Time (ms) for Requests Sent to File Servers	Average response time for signed requests sent to file servers, in milliseconds.
Total Round Trip Time (ms) for All Requests	Total round trip time for all requests, in milliseconds.
Total Amount of Time Saved (ms) Due to Optimization	Total time saved due to optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Read-ahead	Total time saved due to read-ahead, in milliseconds.
Total Amount of Time Saved (ms) Due to Metadata Optimization	Total time saved due to metadata optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Microsoft Optimization	Total time saved due to Microsoft optimization, in milliseconds.
Total Amount of Time Saved (ms) Due to Not-found-metadata Cache	Total time saved due to not-found metadata cache, in milliseconds.

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
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	Current allocated memory usage of not-found metadata cache.
Number of Entries in Not-found Metadata Cache	Number of entries in not-found metadata cache.
Not-found Metadata Cache Hit Count	Number of not-found metadata cache hits.
Not-found Metadata Cache Access Attempts Count	Number of not-found metadata cache access attempts.
Not-found Metadata Cache Allowed Access Count	Number of not-found metadata cache allowed accesses.
Not-found Metadata Cache Update Attempts Count	Number of not-found metadata cache update attempts.
Not-found Metadata Cache Allowed Updates Count	Number of not-found metadata cache allowed updates.
Not-found Metadata Cache Hash Bucket Count	Number of not-found metadata cache hash buckets. <b>Note</b> 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.



**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
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 metadata 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 locally.
Total Number of Other Requests Served Locally	Number of other requests served locally.
Total Number of Metadata Cached Resources	Number of metadata cached references.
Total SMB1 Named Pipe Open Requests Processed	Number of SMB1 NT_Create_AndX requests for non \spoolss pipe seen by the edge WAE.
Total SMB1 Named Pipe Open Requests Served Locally	Number of SMB1 NT_Create_AndX requests for non \spoolss pipe served locally by the edge WAE, due to cached-open and delayed-close optimization.
Total SMB1 Named Pipe Open Requests Forward to Server	Number of SMB1NT_Create_AndX requests for non \spoolss pipe that were forwarded to the server by the edge WAE (requests that could not be served locally).
Total SMB1 Named Pipe Close requests processed	Number of SMB1 Close requests for non \spoolss pipe seen 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 edge 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.

**Table 3-82** Field Descriptions for the `show statistics accelerator smb detail` Command

Field	Description
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.
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 <i>synchronously</i> to the server (the client is waiting for a response from the server). It does not include the Close requests that are sent <i>asynchronously</i> (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_AndX messages for the \spoolss pipe, for which the edge WAE does an asynchronous reply optimization.

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
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.
Total Number of Read Requests with Office Optimization	Number of read requests with Microsoft Office optimization.
Total Number of Write Requests with Office Optimization	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.

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
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.
Total SMB1_Close Requests Forwarded to File Server	Number of SMB1 close requests forwarded to the file server.
Total SMB1_Rename Requests Processed	Number 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.

**Table 3-82** *Field Descriptions for the show statistics accelerator smb detail Command*

Field	Description
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.
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.

**Table 3-82** Field Descriptions for the *show statistics accelerator smb detail* Command

Field	Description
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.
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 transaction 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.

**Table 3-82** *Field Descriptions for the show statistics accelerator smb detail Command*

Field	Description
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.
Total SMB1_FindClose2 Requests Processed	Number of SMB1 find close2 requests processed.
Total SMB1_Write Requests Processed	Number of SMB1 write requests processed.
Total SMB2_Read requests Processed	Number of SMB2 read requests processed.
Total SMB2_Write requests Processed	Number of SMB2 write requests processed.
Directory-Browsing Active nodes	Number of active directory browsing created directory browsing active files being served from the WAAS device's RAM.
Directory-Browsing Total nodes	Total number of directory browsing files that can be created in the WAAS device's RAM.
Directory-Browsing Total Size used in Bytes	Total RAM memory (in bytes) used by directory browsing requests.
Directory-Browsing Nodes Evicted	Total number of directories/files removed because they were not being used to free up limited memory space.
Total SMB2_Query_Directory requests processed	Number of SMB2 query directory requests processed
Total SMB2_Query_Directory requests served locally	Number of SMB2 query directory requests served locally from the WAAS device RAM infrastructure.

**Table 3-82** Field Descriptions for the `show statistics accelerator smb detail` Command

Field	Description
Total SMB2_Query_Directory forwarded to file server	Number of SMB2 query directory requests that could not be served locally from the WAAS device and were forwarded to the file server.
Total SMB2_Compound requests served locally	Number of SMB2 compound query requests (2) served locally from the WAAS device RAM infrastructure.
Total SMB3_11 TreeConnects passed through	Number of SMB 3_11 connection) packets related to a specific Tree that are passed through
Pushdown--> SMB_311	Number of connections not handled by SMBAO (pushed down) and handed down to L4 layer that receive only TDL optimization
Total SMB3_11 connections passed through	Number of SMB3_11 complete connections passed through the accelerator but are not optimized.
Total Number of SMB3_11 Encrypted Sessions (L4 opt)	Number of SMB 3_11 encrypted sessions for L4 optimization.
Total Number of SMB3_11 Encrypted Sessions (L7 opt)	Number of SMB 3_11 encrypted sessions for L7 optimization.
Total Number of SMB3_11 Signed Sessions (L4 opt)	Number of SMB3_11 signed sessions for L4 optimization.
Total Number of SMB3_11 Signed Sessions (L7 opt)	Number of SMB3_11 signed sessions for L7 optimization.
Total Number of SMB3_11 Encrypted Sessions not optimized	Number of SMB3_11 encrypted sessions that were not optimized.

Table 3-83 describes the fields shown in the `show statistics accelerator smb debug` command display.

**Table 3-83** Field Descriptions for the `show statistics accelerator smb debug` Command (continued)

Field	Description
<b>Total SMB Object Cache Open calls</b>	Total number of SMB Object open calls made by the SMB Acceleration Accelerator to the Object Cache (OC) API.
<b>Total SMB Object Cache Open success</b>	Total number of SMB Object Cache calls that were successfully answered by the object cache API.
<b>Total SMB Object Cache Open failure</b>	Total number of SMB Object Cache calls that failed to be answered by the object cache API
Total SMB Object Cache Open No Create	
<b>Total SMB Object Cache Open failure due to load bypass</b>	Total number of SMB Object Cache calls that failed to be answered by the object cache API due to network latency.



Field	Description
<b>Total SMB Object Cache Read success</b>	The total number of successful read requests sent to the OC.
<b>Total SMB Object Cache Read calls</b>	The total number of read requests sent to the OC.
<b>Total SMB Object Cache Read failure</b>	The total number of failed read requests.
<b>Total SMB Object Cache Read failure due to load bypass</b>	The total number of failed read requests due to network latency.
<b>Total SMB Object Cache Read failure due to version check</b>	The total number of failed read requests due to version mismatch.
<b>Total SMB Object Cache Write success</b>	Total number of SMB data that has been successfully written to object cache
<b>Total SMB Object Cache Write calls</b>	Total number of write requests sent to OC.
<b>Total SMB Object Cache Write failure</b>	Total number of write requests that could not be written to OC.
<b>Total SMB Object Cache Write failure due to load bypass</b>	Total number of write requests that failed due to network latency.
<b>Total SMB Object Cache Write issued with overwrite flag set</b>	Total number of calls to object cache write with differentiator as the overwriteflag, so that it overwrites existing data or writes to offset.
<b>Total SMB Object Cache Write issued when load bypass was set</b>	Total number of object cache writes issued with load bypass flag.
<b>Total SMB Object Cache Duplicate calls</b>	Total number of duplicate calls to open object in object cache.
<b>Total SMB Object Cache Duplicate success</b>	Total number of successful duplicate calls to open object in object cache.
<b>Total SMB Object Cache Duplicate failure</b>	Total number of unsuccessful duplicate calls to open object in object cache.
<b>Total SMB Object Cache Close calls</b>	Total number of close file requests sent to OC.
<b>Total SMB Object Cache Close success</b>	Total number of successful close file request done by OC.
<b>Total SMB Object Cache Close failure</b>	Total number of files that could not be successfully closed by the OC.
<b>Total SMB Object Cache Delete calls</b>	Total number of delete file requests sent to the OC.
<b>Total SMB Object Cache Delete success</b>	Total number of files that were successfully deleted from the OC after receiving a response from the server.
<b>Total SMB Object Cache Delete failure</b>	Total number of files that were could not be deleted from the OC even after receiving a response from the server.
<b>Total SMB Object Cache SetMetaData calls</b>	Total number of object meta-data set calls sent to object cache.
<b>Total SMB Object Cache SetMetaData success</b>	Total number of successful object meta-data set calls sent to object cache.
<b>Total SMB Object Cache SetMetaData failure</b>	Total number of unsuccessful object meta-data set calls sent to object cache.

Field	Description
<b>Total SMB Object Cache Rename calls</b>	Total number of requests made to the server for renaming the files.
<b>Total SMB Object Cache Rename success</b>	Total number of files that were successfully renamed by the OC.
<b>Total SMB Object Cache Rename failure</b>	Total number of files that could not be renamed by the OC because of no response from the server.
<b>Total SMB Object Cache GetNextHole calls</b>	Total number of get next hole calls sent to object cache to see if there is any hole in the data after the offset. This enables to understand what to read next in read ahead from server after the offset.
<b>Total SMB Object Cache GetNextHole success</b>	Total number of successful get next hole calls sent to object cache.
<b>Total SMB Object Cache GetNextHole failure</b>	Total number of unsuccessful get next hole calls sent to object cache.
<b>Total SMB Object Cache GetNextHole that returned no hole</b>	Total number of get next hole calls sent to object cache for which no holes were identified.
<b>Total SMB Object Cache GetNextHole that returned hole</b>	Total number of get next hole calls sent to object cache for which holes were identified.
<b>Total SMB Object Cache GetNextData calls</b>	Total number of get next data calls sent to object cache to look for next available data in the object cache after offset. This enables to return the data after offset and finds the length of data that is available.
<b>Total SMB Object Cache GetNextData success</b>	Total number of successful get next data calls sent to object cache to look for next available data in the object cache after offset.
<b>Total SMB Object Cache GetNextData failure</b>	Total number of unsuccessful get next data calls sent to object cache to look for next available data in the object cache after offset.
<b>Total SMB Object Cache GetNextData that returned no data</b>	Total number of get next data calls sent to object cache to look for next available data in the object cache after offset that did not find the next available object.
<b>Total SMB Object Cache GetNextData that returned data</b>	Total number of get next data calls sent to object cache to look for next available data in the object cache after offset and that returned the next available object.
OCLite: Number of Document Open Requests Processed	Total Number of document open requests processed by OCLite.
OCLite: Number of Document Open Requests Failed	Total number of document open requests that failed in OCLite.
OCLite: Average Open time taken:	Average time taken to open a document by OCLite.
OCLite: Total Open time taken	Total time taken to open a document by OCLite.
OCLite: Maximum Open time taken	Maximum time taken to open a document by OCLite.
OCLite: Number of Document Dup Requests Processed	Total number of document duplicate requests that were processed by OCLite.

Field	Description
OCLite: Number of Document Dup Requests Failed	Total number of duplicate document duplicate requests that failed in OCLite.
OCLite: Total Dup time taken	Total time taken to process Duplicate requests from OCLite.
OCLite: Average Dup time taken	Average time taken to process Duplicate requests from OCLite.
OCLite: Maximum Dup time taken	Maximum time taken to process Duplicate requests from OCLite.
OCLite: Number of document Delete Requests Processed	Total number of delete document requests processed by OCLite.
OCLite: Number of document Delete Requests Failed	Total number of delete document requests that failed in the OCLite library.
OCLite: Total Delete time taken	Total time taken for delete document requests.
OCLite: Average Delete time taken	Average time taken for delete document requests.
OCLite: Maximum Delete time taken:	Maximum time taken for delete document requests.
OCLite: Number of document close Requests Processed:	Total number of close document requests processed by OCLite.
OCLite: Number of document Close Requests Failed	Total number of close document requests that failed in the OCLite library.
OCLite: Total Close time taken	Total time taken for close document requests.
OCLite: Average Close time taken	Average time taken for close document requests.
OCLite: Maximum Close time taken	Maximum time taken for close document requests.
OCLite: Number of document Rename Requests Processed	Total number of rename document requests processed by OCLite.
OCLite: Number of document Rename Requests Failed	Total number of rename document requests that failed in the OCLite library.
OCLite: Total Rename time taken	Total time taken for rename document requests.
OCLite: Average Rename time taken	Average time taken for rename document requests.
OCLite: Maximum Rename time taken	Maximum time taken for rename document requests.
OCLite: Number of document Invalidate Requests Processed	Total number of invalidate document requests processed by OCLite. This request invalidates the existing cache including the RAM cache.
OCLite: Number of document Invalidate Requests Failed	Total number of invalidate document requests that failed in the OCLite library.
OCLite: Total Invalidation time taken	Total time taken to process invalidate requests.
OCLite: Average Invalidation time taken	Average time taken to process invalidate requests.
OCLite: Maximum Invalidation time taken	Maximum time taken to process invalidate requests.
OCLite: Number of document Read Requests Processed	Total number of read document requests processed by OCLite.
OCLite: Number of document Read Requests Failed	Total number of read document requests that failed in the OCLite library.

Field	Description
OCLite: Number of document Read Bytes Requested	Number of document read bytes requested from OCLite.
OCLite: Number of document Read Bytes Served	Number of document read bytes served from OCLite cache.
OCLite: Total time taken for Read Requests	Total time taken for serving read requests.
OCLite: Average read time per request	Average time taken for serving read requests.
OCLite: Maximum read time	Maximum time taken for serving read requests.
OCLite: Average read time per byte	Average time taken for serving read requests per byte.
OCLite: Number of document Write Requests Processed	Number of document write requests processed by OCLite.
OCLite: Number of document Write Requests Failed	Number of document write requests that failed in the OCLite library.
OCLite: Number of document Write Bytes Requests	Number of document write bytes requested from OCLite.
OCLite: Number of document Write Bytes Served	Number of document write bytes served from OCLite.
OCLite: Total time taken for Write Requests	Total time taken for serving write requests.
OCLite: Average write time per request	Average time taken for serving write requests.
OCLite: Maximum write time	Maximum time taken for serving write requests.
OCLite: Average write time per byte	Average time taken for serving write requests per byte.
OCLite: Hash Table Insert Attempts	Number of attempts made to insert a document in to the hash table.
OCLite: Hash table Insert Failed	Number of times a new document name could not be inserted into the Hash Table.
OCLite: Hash Table Delete Attempts	Number of attempts made to delete a document from the hash table.
OCLite WAG: Write From Iovec Attempts	Number of attempts made to write from I/O vector to Write Aggregation Buffer.
OCLite WAG: Write From Iovec Successful	Number of attempts made to write from I/O vector to Write Aggregation Buffer that succeeded.
OCLite WAG: Write From Iovec Copy Iovec Failures	Number of attempts made to write from I/O vector to Write Aggregation Buffer that failed during copying.
OCLite WAG: Write From Iovec - Disk Write Failures	Number of attempts made to write from I/O vector to Write Aggregation Buffer that failed during write to disk.
OCLite WAG: Write From Buffer Attempts	Number of attempts made to write from RAM buffer to Write Aggregation Buffer.
OCLite WAG: Write From Buffer Success	Number of attempts made to write from RAM buffer to Write Aggregation Buffer that succeeded.
OCLite WAG: Write From Buffer Failed - RAM flag not set	Number of attempts made to write from RAM buffer to Write Aggregation Buffer that failed due to RAM flag not being set.

Field	Description
OCLite WAG: Write From Buffer Failed - RAM address not set	Number of attempts made to write from RAM buffer to Write Aggregation Buffer that failed due to RAM address not set.
OCLite WAG: Write From Buffer Failed - Disk Write Field	Number of attempts made to write from RAM buffer to Write Aggregation Buffer that failed due to disk write failed.
OCLite WAG: Merge attempts	Number of merge attempts to Write Aggregation Buffer.
OCLite WAG: Merge successful	Number of merge attempts to Write Aggregation Buffer that succeeded.
OCLite WAG: Merge failed - WAG flag not set	Number of merge attempts to Write Aggregation (WAG) buffer failed due to WAG flag not set.
OCLite WAG: Merge failed - Copy Iovec Failed	Number of merge attempts to Write Aggregation(WAG) buffer failed due to copy from I/O vector failed.
OCLite WAG: Read attempts	Number of attempts made to read from Write Aggregation buffer.
OCLite WAG: Read success	Number of times read from Write Aggregation buffer succeeded.
OCLite WAG: Read failed	Number of times read from Write Aggregation buffer failed.
OCLite WAG: Get buffer attempts	Number of attempts made to get Write Aggregation buffer.
OCLite WAG: Get buffer successful	Number of times get Write Aggregation buffer was successful.
OCLite WAG: Get buffer failed - Magic Mismatch	Number of times get Write Aggregation buffer failed due to magic mismatch.
OCLite WAG: Write to Disk attempts	Number of attempts made to write from Write aggregation to disk.
OCLite WAG: Write to Disk successful	Number of times write from Write aggregation buffer to disk succeeded.
OCLite WAG: Write to Disk Failed	Number of times write from Write aggregation buffer to disk failed.
OCLite WAG: Force invoke GC attempts	Number of times garbage collector was invoked forcibly.
OCLite WAG: Force invoke GC successful	Number of times force invocation of garbage collector succeeded.
OCLite WAG: Force invoke GC Failed	Number of times force invocation of garbage collector failed.
OCLite WAG: GC Timer Stop Failed	Number of times garbage collector timer stop failed to operate.
OCLite RAM Cache: Number of Blocks Accessed	Number of data blocks accessed from RAM Cache.
OCLite RAM Cache: Number of bytes accessed	Total Bytes of data accessed from RAM Cache.

Field	Description
OCLite RAM Cache: Number of Blocks evicted	Number of data blocks evicted from RAM Cache.
OCLite RAM Cache: Number of bytes evicted	Total Bytes of data evicted from RAM Cache.
OCLite RAM Cache: Number of Blocks invalidated	Number of blocks of data that were invalidated in the RAM cache.
OCLite RAM Cache: Number of bytes invalidated	Number of bytes of data that were invalidated in the RAM cache.
OCLite RAM Cache: Number of Blocks in Use	Number of data blocks used in RAM cache.
OCLite RAM Cache: Number of bytes used	Total Bytes of data used in RAM Cache.
OCLite RAM Cache: Number of Leaked blocks	Number of data blocks currently leaked from RAM Cache.
OCLite RAM Cache: Null Node Received	Total number of Null Node received for processing
OCLite RAM Cache: Null Node sent for Adding to List	Total number of Null Node received for adding to RAM LRU List
OCLite RAM Cache: Null Node sent for Deleting from List	Total number of Null Node received for deleting from RAM LRU List
OCLite RAM Cache: Empty List encountered	Total number of times empty LRU List encountered
OCLite RAM Cache: Node is Busy with other operation	Total number of times node is busy with other operation
OCLite RAM Cache: LRU List Overflow	Total number of times LRU List Overflow
OCLite RAM Cache: Initialization Failed	Total number of times RAM Cache Initialization failed
OCLite RAM Cache: Memory Free failed	Total Number of times memory deallocation failed
OCLite RAM Cache: Free Node Allocation Failed	Total Number of times free node allocation failed
OCLite RAM Cache: Node Updation Failed	Total Number of times RAM Cache Node updation failed
OCLite RAM Cache: Node evicted from disk	Total number of times Node evicted from disk while processing
OCLite RAM Cache: Null tree node in Disk Read List	Total number of times null tree node received in Disk Read List
OCLite RAM Cache: Disk Read List is empty	Total number of times empty Disk Read List received
OCLite RAM Cache: Node deletion failed	Total number of times RAM Cache Node deletion failed
OCLite RAM Cache: Tree Node Pointer is Corrupted	Total number of times tree node pointer is corrupted
OCLite Disk: Partition Magic Version Match	Number of times OCLite disk version matched with previous version
OCLite Disk: Serialize Timer Cb Called	Number of times serialization timer callback is called

Field	Description
OCLite Disk: Deserialization Partially Failed	Number of times deserialization failed partially
OCLite Disk: Serialize Doc Wrong Param	Number of times serialization triggered with invalid parameters
OCLite Disk: Node Beyond Disk Size	Number of nodes found beyond disk size during deserialization
OCLite Disk: Serialization Exceeding Di	Number of times, the directory size was not sufficient to serialize the nodes
OCLite Disk: Pwrite Intermitently Failed	Number of times the pwrite failed intermittently
OCLite Disk: Pwritev Intermitently Failed	Number of times the pwritev failed intermittently
OCLite Disk: Copy Inbetween Uint Serialize	Number of times an integer is split between pages during serialization
OCLite Disk: Copy Inbetween String Serialize	Number of times a string is split between pages during serialization
OCLite Disk: Copy Endof Uint Serialize	Number of times an integer copy fills a page during serialization
OCLite Disk: Copy Endof String Serialize	Number of times a string copy fills a page during serialization
OCLite Disk: Read Inbetween Uint Deserialize	Number of times an integer is split between pages during deserialization.
OCLite Disk: Pread Intermitently Failed	Number of times the pread failed intermittently.
OCLite Disk: Read Inbetween String Deserialize	Number of times a string is split between pages during deserialization.
OCLite Disk: Read Endof Uint Deserialize	Number of times an integer copy fills a page during deserialization.
OCLite Disk: Read Endof String Deserialize	Number of times a string copy fills a page during deserialization.
OCLite Disk: Documents Serialized	Number of documents serialized.
OCLite Disk: Documents Deserialized	Number of documents deserialized.
OCLite Disk: Document Nodes Serialized	Number of document nodes serialized.
OCLite Disk: Document Nodes Deserialized	Number of document nodes deserialized.
OCLite Disk: Dir1 Serializations Attempted	Number of serializations attempted into 1st directory.
OCLite Disk: Dir2 Serializations Attempted	Number of serializations attempted into 2nd directory.
OCLite Disk: Serializations Completed	Number of serializations completed.
OCLite Disk: Dir1 Deserializations Attempted	Number of deserializations attempted with 1st directory.
OCLite Disk: Dir2 Deserializations Attempted	Number of deserializations attempted with 2nd directory.
OCLite Disk: Deserializations Completed	Number of deserializations completed successfully.

Field	Description
OCLite Disk: Write Pointer Wrap	Number of times Disk is filled to the end.
OCLite Disk: Unexpected Write Pointer	Number of times a wrong write pointer is returned.
OCLite Disk: GC Read Success	Number of times garbage collector disk reads succeeded.
OCLite Disk: GC Read Wrong Params	Number of times garbage collector passed wrong parameters during disk read.
OCLite Disk: Read Success	Number of times disk reads succeeded.
OCLite Disk: Read Wrong Params	Number of times wrong parameters are passed to disk read.
OCLite Disk: Write Success	Number of times disk writes succeeded.
OCLite Disk: Write Wrong Params	Number of times wrong parameters are passed to disk write.
OCLite Disk: Write Metadata Success	Number of times metadata disk writes were successful.
OCLite Disk: Write Metadata Wrong Params	Number of times wrong parameters are passed to metadata disk write.
OCLite Disk: Writev Success	Number of times disk writev succeeded.
OCLite Disk: Writev Wrong Params	Number of times wrong parameters are passed to disk writev.
OCLite Disk: Node Delete Success	Number of times node delete by disk module succeeded.
OCLite Disk: Node Delete Failed	Number of times node delete by disk module failed.
OCLite Disk: URL Hash Update Success	Number of times an existing cached document could be successfully updated in the directory table.
OCLite Disk: URL Hash Update Failed	Number of times an existing cached document could not be successfully updated in the directory table.
OCLite Disk: Integrity Check Success	Number of times checksum validation succeeded during disk read.
OCLite Disk: Integrity Check Failed	Number of times checksum validation failed during disk read.
OCLite Disk: Number Of Blocks Incremented	Number of times the cache disk size is incremented.
OCLite Disk: Partition Magic Version Match Failed	Number of times OCLT disk version failed to match with previous version.
OCLite Disk: Aligned Alloc Failed	Number of times aligned alloc failed.
OCLite Disk: Ftruncate Failed	Number of times Ftruncate failed.
OCLite Disk: Pwrite Failed	Number of times the pwrite failed.
OCLite Disk: Pread Failed	Number of times the pread failed.
OCLite Disk: Pwritev Failed	Number of times the pwritev failed
OCLite Disk: Deserializations Not Attempted	Number of times deserializations not attempted
OCLite Disk: Deserialization Failed	Number of times deserialization failed.
OCLite Disk: Document Serialization Skipped	Number of times document serialization is skipped



Field	Description
OCLite Disk: Node Serialization Skipped	Number of times a document node serialization is skipped.
OCLite Disk: Invalid Dir1 Sequence Number	Number of times 1st directory deserialization skipped because of invalid sequence number
OCLite Disk: Invalid Dir2 Sequence Number	Number of times 2nd directory deserialization skipped because of invalid sequence number
OCLite Disk: Number of Blocks Decremented	Number of times the cache disk size is decremented.
OCLite Disk: Average Write Time	Average time taken for the pwrite call.
OCLite Disk: Average Read Time	Average time taken for the pread call.
OCLite Disk: Maximum Write Time	Maximum time taken for a pwrite call.
OCLite Disk: Latest Write Time	Time taken for the latest pwrite call.
OCLite Disk: Maximum Metadata Write Time	Maximum time taken for a pwrite call for writing metadata.
OCLite Disk: Latest Metadata Write Time	Time taken for the latest pwrite call for writing metadata.
OCLite Disk: Average Metadata Write Time	Average time taken for the pwrite call for writing metadata.
OCLite Disk: Maximum Read Time	Maximum time taken for a pread call.
OCLite Disk: Latest Read Time	Time taken for the latest pread call.
OCLite Disk: Maximum Garbage Collector Read Time	Maximum time taken for a garbage collector pread call.
OCLite Disk: Latest Garbage Collector Read Time	Latest time taken for a garbage collector pread call.
OCLite Disk: Average Garbage Collector Read Time	Average time taken for a garbage collector pread call.
OCLite Disk: Deserialization Time	Time taken for deserialization.
OCLite Disk: Average Serialization Time	Average time taken for serialization.
OCLite Disk: Maximum Serialization Time	Maximum time taken for a serialization.
OCLite Disk: Latest Serialization Time	Time taken for latest serialization.
OCLite GC: Timer Callback Called	Number of times garbage collector timer is called.
OCLite GC: Timer callback returned without processing	Number of times garbage collector returned without processing.
OCLite GC: Nodes deleted successfully	Number of nodes deleted by garbage collector
OCLite GC: Nodes delete failed	Number of nodes that couldn't be deleted by garbage collector.
OCLite GC: Number of Blocks freed	Number of disk blocks freed by garbage collector.
OCLite GC: Disk read failures during GC read	Number of times disk read failed during garbage collector operation.
OCLite GC: Block Magic validation failed	Number of times block magic validation failed during garbage collector operation.

Field	Description
OCLite GC: Number of times GC returned with less free blocks	Number of times garbage collector returned with less number of free blocks.
OCLite Util: Copy from Iovec Attempts	Number of attempts made to copy from I/O vector.
OCLite Util: Copy from Iovec Successful	Number of times copy from I/O vector succeeded.
OCLite Util: Copy from Iovec Failed	Number of times copy from I/O vector failed.
OCLite Util: Copy to Iovec Attempts	Number of attempts made to copy to I/O vector.
OCLite Util: Copy to Iovec Successful	Number of times copy from I/O vector succeeded.
OCLite Util: Copy to Iovec Failed	Number of times copy from I/O vector failed.
Invalid Doc Offset	Number of times copy to I/O vector failed due to invalid document offset.
WAG flush	Number of times copy to I/O vector failed due to WAG flush to disk.
Invalid Length	Number of times copy to I/O vector failed due to invalid length.
RAM node evicted	Number of times copy to I/O vector failed due to RAM node evicted.
Incorrect Flag	Number of times copy to I/O vector failed due to incorrect flag.
OCLite: Number of work items in state machine	Number of requests currently running in the state machine.
OCLite: Max number of items in state machine	Maximum number of requests observed in the state machine.
OCLite: Number of work items in scheduler	Number of requests currently in the scheduler queue.
OCLite: Max number of items in scheduler	Maximum number of requests observed in the scheduler.

Table 3-84 describes the fields shown in the **show statistics accelerator smb | inc Print** command display.

**Table 3-84** 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 \spoolss pipe served locally by the edge WAE due to cached open and delayed close optimization.

**Table 3-84** Field Descriptions for the *show statistics accelerator smb | inc Print Command*

Field	Description
Total SMB1 Print Open requests forwarded to server	Number of SMB1 NT_Create_AndX requests for \spoolss pipe which were forwarded to the file server by the edge WAE (requests that could not be served locally).
Total SMB1 Print Close requests processed	Number of SMB1 Close requests for the \spoolss pipe seen by the edge WAE.
Total SMB1 Print Close requests served locally	Number of SMB1 Close requests for the \spoolss pipe served locally by the edge WAE as part of delayed close optimization.
Total SMB1 Print Close requests forwarded to the server	Number of SMB1 Close requests for the \spoolss pipe that were forwarded to the file server by the edge WAE (requests that could not be served locally).  This total includes only the Close requests that are sent synchronously to the server (the client is waiting for a response from the server). It does not include the Close requests that are sent asynchronously (the Close requests first served locally and then sent to the server at a later point in time).
Print SMB1 Documents Spooled count	Number of SMB1 Transact EndDocPrinter messages for the spoolss pipe seen by the edge WAE.
Print SMB1 Pages Spooled count	Number of SMB1 Transact EndPagePrinter 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.

**Table 3-84** Field Descriptions for the `show statistics accelerator smb | inc Print` Command

Field	Description
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 3-85](#) describes the fields shown in the `show statistics accelerator ssl detail` command display.

**Table 3-85** Field Descriptions for the `show statistics accelerator ssl detail` Command

Field	Description
Time Accelerator was started	Time stamp of when the accelerator was started. Will change if the accelerator is restarted for any reason.
Time Statistics were Last Reset/Cleared	Time stamp of when the accelerator statistics were last set to zero. This value should be the same as the Time Accelerator was started field if the <b>clear stat accelerator all</b> or <b>clear stat accelerator ssl</b> commands were never issued. Otherwise it will show the time at which the <b>clear stat accelerator all</b> or <b>clear stat accelerator ssl</b> commands were last issued.
Total Handled Connections	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.

**Table 3-85** Field Descriptions for the *show statistics accelerator ssl detail* Command (continued)

Field	Description
Total Dropped Connections	Number of connections that the SSL accelerator ended prematurely. This could be due to verification failures, revocation check failures, errors detected during the handshake or data transfer phase of the connection, or due to internal errors. Other counters below may shed more light as to why connections were dropped.
Current Active Connections	Number of connections currently being optimized by the SSL accelerator.
Current Pending Connections	Number of connections that have been determined to be accelerated by the SSL accelerator, and have been queued to be picked up by the accelerator.
Maximum Active Connections	Maximum value ever reached by the Current Active Connections counter. This counter will be reset if the accelerator is restarted or statistics are cleared.
Total LAN Bytes Read	Number of bytes read by the SSL accelerator from the original side of the flow.
Total Reads on LAN	Number of read operations performed by the SSL accelerator on the original side of the flow.
Total LAN Bytes Written	Number of bytes written by the SSL accelerator on the original side of the flow.
Total Writes on LAN	Number of write operations performed by the SSL accelerator on the original side of the flow.
Total WAN Bytes Read	Number of bytes read by the SSL accelerator from the optimized side of the flow.
Total Reads on WAN	Number of read operations performed by the SSL accelerator on the optimized side of the flow.
Total WAN Bytes Written	Number of bytes written by the SSL accelerator on the optimized side of the flow.
Total Writes on WAN	Number of write operations performed by the SSL accelerator on the optimized side of the flow.
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).

**Table 3-85** Field Descriptions for the `show statistics accelerator ssl detail` Command (continued)

Field	Description
Total Accelerator Bytes Written	SSL accelerator internal counter. (Bytes written to original side of DRE).
Total Accelerator Writes	SSL accelerator internal counter. (Write operations performed on original side of DRE).
Total DRE Bytes Read	SSL accelerator internal counter. (Bytes read from optimized side of DRE).
Total DRE Reads	SSL accelerator internal counter. (Read operations performed on the optimized side of DRE).
Total DRE Bytes Written	SSL accelerator internal counter. (Bytes read from optimized side of DRE).
Total DRE Writes	SSL accelerator internal counter. (Write operations performed on the optimized side of DRE).
Number of forward DNS lookups issued	Number of forward DNS lookups that were issued.
Number of forward DNS lookups failed	Number of forward DNS lookup failures.
Number of flows with matching host names	Number of flows where server host name matched accelerated service configuration.
Number of reverse DNS lookups issued	Number of reverse DNS lookups that were issued.
Number of reverse DNS lookups failed	Number of reverse DNS lookup failures.
Number of reverse DNS lookups cancelled	Number of reverse DNS lookups that were cancelled.
Number of flows with matching domain names	Number of flows where server domain name matched accelerated service configuration.
Number of flows with matching any IP rule	Number of flows where the server IP address matched 'IP any' rule.
Total Failed Handshakes	Number of connections that ended during the handshake phase.
Pipe-through due to cipher mismatch	Number of connections bypassed by SSL accelerator because the SSL cipher negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
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.

**Table 3-85** Field Descriptions for the *show statistics accelerator ssl detail* Command (continued)

Field	Description
Total SSLv3 Negotiated on LAN	Number of connections that used SSL version 3 on the original side of the flow.
Total TLSv1 Negotiated on LAN	Number of connections that used TLS version 1 on the original side of the flow.
Total SSLv3 Negotiated on WAN	Number of connections that used SSL version 3 on the optimized side of the flow.
Total TLSv1 Negotiated on WAN	Number of connections that used TLS version 1 on the optimized side of the flow.
Total SSLv3 Negotiated on Peer	Number of connections that used SSL version 3 on the control connection between WAAS devices.
Total TLSv1 Negotiated on Peer	Number of connections that used TLS version 1 on the control connection between WAAS devices.
Total renegotiations requested by server	Number of SSL “Hello Request” messages detected by the SSL accelerator.
Total SSL renegotiations performed	Number of SSL renegotiation attempts (successful and unsuccessful) detected by the SSL accelerator.
Total number of failed renegotiations	Number of unsuccessful SSL renegotiations detected by the SSL accelerator.
Flows dropped due to renegotiation timeout	Number of flows dropped due to renegotiation timeout.
[W2W-Srvr] Number of session hits	Number of times inter-WAAS SSL session resumption was successful on flows where this WAE was the Core WAE.
[W2W-Srvr] Number of session misses	Number of times inter-WAAS SSL full handshake was carried out, on flows where this WAE was the Core WAE.
[W2W-Srvr] Number of sessions timedout	Number of SSL sessions that were not reused because they were timed out.
[W2W-Srvr] Number of sessions deleted because of cache full	Number of sessions evicted from inter-WAAS session cache to make room for new sessions.
[W2W-Srvr] Number of bad sessions deleted	Number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.
[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-CInt] Number of session hits	Number of times an inter-WAAS session resumption was successful on flows where this WAE was the Edge WAE.
[W2W-CInt] Number of session misses	Number of times an inter-WAAS full SSL handshake was carried out, on flows where this WAE was the Edge WAE.

**Table 3-85** *Field Descriptions for the show statistics accelerator ssl detail Command (continued)*

Field	Description
[W2W-Clnt] Number of sessions timedout	Number of SSL sessions that were not reused because they were timed out.
[W2W-Clnt] Number of sessions deleted because of cache full	Number of sessions evicted from inter-WAAS session cache to make room for new sessions.
[W2W-Clnt] Number of bad sessions deleted	Number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.
[C2S-Srvr] Number of session hits	Number of times a client-requested session was found in the client-facing session cache (even if eventually a full handshake had to be carried out due to session miss between Core WAE and server).
[C2S-Srvr] Number of session misses	Number of times a client-requested session was not found in the client-facing session cache.
[C2S-Srvr] Number of sessions timedout	Number of sessions in the client-facing session cache that were not reused because they were timed out.
[C2S-Srvr] Number of sessions deleted because of cache full	Number of sessions evicted from the client-facing session cache to make room for new sessions.
[C2S-Srvr] Number of bad sessions deleted	Number of sessions evicted from the client-facing session cache as they were rendered unsuitable for reuse, likely due to connection errors.
[C2S-Srvr] Number of sessions inserted into cache	Number of sessions inserted into the client-facing session cache.
[C2S-Srvr] Number of sessions evicted from cache	Number of sessions evicted from the client-facing session cache.
[C2S-Srvr] Number of sessions in cache	Number of sessions currently cached in the client-facing session cache.
[C2S-Clnt] Number of session hits	Number of times a Core-WAE requested session was successfully reused between the Core WAE and server.
C2S-Clnt] Number of session misses	Number of times a full SSL handshake had to be carried out between the Core WAE and server.
[C2S-Clnt] Number of sessions timedout	Number of times a session in the server-facing session cache could not be reused because it was timed out.
[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.



**Table 3-85** Field Descriptions for the *show statistics accelerator ssl detail* Command (continued)

Field	Description
Total Successful Certificate Verifications	Number of times a certificate was successfully verified (could be client or server).
Total Failed Certificate Verifications	Number of times a certificate verification failed (could be for various reasons, other counters may indicate why).
Failed certificate verifications due to invalid certificates	Number of certificate verification attempts failed because the certificate was invalid. An inspection of the SSL accelerator errorlog may indicate the reasons.
Failed Certificate Verifications based on OCSP Check	Number of certificate verification attempts deemed unsuccessful based on results of OCSP revocation check.
Failed Certificate Verifications (non OCSP)	Number of certificate verification attempts deemed unsuccessful based on results of the certificate verification operation.
Total Failed Certificate Verifications due to Other Errors	Number of certificate verification failures due to other problems (including internal errors). An inspection of the SSL accelerator errorlog may indicate the reasons.
Total OCSP Connections Outstanding	Number of OCSP requests currently in progress.
Total OCSP Requests Processed	Number of OCSP requests completed (including successful and unsuccessful responses).
Maximum Concurrent OCSP Requests	Maximum value ever reached by Total OCSP Connections Outstanding counter. This will be reset if the accelerator is restarted or statistics are cleared.
Total Successful OCSP Requests	Number of OCSP requests that were completed with a valid response from the OCSP responder.
Total Successful OCSP Requests Returning OK Status	Number of OCSP request where the certificate status was OK.
Total Successful OCSP Requests with 'NONE' Revocation	Number of OCSP requests where the OCSP status was deemed OK because of fallback to method configuration: none.
Total Successful OCSP Requests Returning REVOKED Status	Number of OCSP requests where the certificate status was REVOKED.
Total Successful OCSP Requests Returning UNKNOWN Status	Number of OCSP requests where the responder did not know the status of the certificate.
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.

**Table 3-85** Field Descriptions for the `show statistics accelerator ssl detail` Command (continued)

Field	Description
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 3-86](#) describes the fields shown in the `show statistics accelerator ssl payload http` command display.

**Table 3-86** 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 3-87](#) describes the fields shown in the `show statistics accelerator ssl payload other` command display.

**Table 3-87** Field Descriptions—`show statistics accelerator ssl payload other` Command

Field	Description
Total Optimized Connections	Number of connections in which a successful SSL handshake was completed and the connection entered the data transfer phase. Connections that experienced errors during SSL handshake are not counted here. Connections that experienced errors after handshake are counted here. Connections that experienced errors during SSL re-handshake (renegotiation) are also counted here.

Related Commands

[show accelerator](#)

[show statistics connection closed](#)

# show statistics accelerator http object-cache

To display object cache statistics for a WAAS device, use the **show statistics accelerator http object-cache** EXEC command.

## show statistics accelerator http object-cache

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use **show statistics accelerator http object-cache** to display a summary of the number of HTTP transactions to the specified host. The top hosts list is always displayed after the cache-type statistics, and contains between 0-10 hosts. This same information can be displayed in graphics form in the Monitor > Caching > Akamai Connect section of the WCM.



**Note** Depending on which cache types are enabled and what traffic is seen, the output may show statistics for any or all of the following cache types: bypass, standard, advanced, connected cache, OTT-youtube, OTT-generic, or unknown.

**Examples** The following example shows sample output from the **show statistics accelerator http object-cache** command:

```
HTTP:
  Object Cache Statistics
  -----

Object Cache Caching Type:                                ott-youtube
  Object cache transactions served from cache:            7
  Object cache request bytes for cache-hit transactions:   5560
  Object cache response bytes for cache-hit transactions:  962534
  Object cache transactions requiring freshness check:     1
  Object cache responses not cached:                       43
  Object cache responses stored in cache:                  295
Object Cache Caching Type:                                standard
  Object cache transactions served from cache:             31
```

```

Object cache request bytes for cache-hit transactions:          10770
Object cache response bytes for cache-hit transactions:        50235
Object cache response time savings for cache-hit transactions:  5546
Average response time saved per cache-hit transactions (ms)    5
Percentage response time saving for cache-hit transactions:    60
Object cache transactions requiring freshness check:           3
Object cache responses not cached:                             364
Object cache responses stored in cache:                         65

Object cache top hosts ordered by:                               hit count

Object cache host name:
au.download.windowsupdate.com
    Object cache transaction count:                             197
    Object cache WAN response bytes:                           54245680
    Object cache LAN response bytes:                            54260258
Object cache host name:
r13---sn-hp576ne7.googlevideo.com
    Object cache transaction count:                             123
    Object cache WAN response bytes:                           40209279
    Object cache LAN response bytes:                            41180077
Object cache host name:                                         s.youtube.com
    Object cache transaction count:                             102
    Object cache WAN response bytes:                           43160
    Object cache LAN response bytes:                            54551
Object cache top hosts ordered by:                               Total Response Time Savings

Object cache host name:                                         www.carnival.com
    Object cache transaction count:                             31
    Object cache WAN response bytes:                           15
    Object cache WAN response bytes:                           329919
    Object cache LAN response bytes:                            1706503
    Object cache response time savings (ms):                    6565476

```

**Related Commands** [show statistics accelerator](#)

# show statistics accelerator http preposition

To display preposition task status information for a WAAS device, use the **show statistics accelerator http preposition EXEC** command.

## show statistics accelerator http preposition

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use **show statistics accelerator http preposition** to display task status information for a WAAS device.

**Examples** The following example shows output from the **show statistics accelerator http preposition** command:

```
Preposition Task                               mytask1
  Status                                       COMPLETE
  Error                                       None
  Start Time:                               2018-11-23 14:53:00
  End Time:                                   2018-11-23 14:53:03
  Transaction Count:                         1
  Byte count:                                2229
  Refresh object count:                      0
  Refresh object bytes                       0
  Cache store object count                   1
  Cache store object bytes                   2229
  Uncacheable object count                   0
  Uncacheable object bytes                   0
```

# show statistics aoim

To display AO (accelerator) Information Manager statistics for a WAAS device, use the **show statistics aoim EXEC** command.

**show statistics aoim [local | peer | detail]**

Syntax Description	local	(Optional) Displays statistics only for all locally registered application accelerators.
	<b>peer</b>	Displays statistics only for all peer WAAS devices encountered.
	<b>detail</b>	Displays detailed statistics that include policy engine and auto-discovery statistics.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use the **show statistics aoim** command with no options to display statistical information for locally registered application accelerators and all peer WAAS devices that the local WAAS device has encountered.

**Examples** [Table 3-88](#) 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 3-88** 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 3-88** 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 3-88** *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: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul>
Hits	Number of connections that had a configured policy that specified the use of the accelerator application.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.
Active Connections	Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the accelerator application and have completed.
Drops	Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.

**Table 3-88** Field Descriptions for the `show statistics aoim` Command (continued)

Field	Description
Rejected Connection Counts Due To: (Total:)	<ul style="list-style-type: none"> <li>• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul>
Auto-Discovery Statistics	
Connections queued for accept	Number of connections added to the accelerator connection accept queue by auto discovery.
Accept queue add failures	Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.
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

<b>name</b> <i>app_name</i>	(Optional) Statistics for the specified application.
<b>savings</b>	(Optional) Savings statistics applications.
<b>appname</b> <i>app_name</i>	(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 3-89](#) lists the valid *app\_name* values you can use with the **show statistics application** EXEC command. For a description of the applications supported by WAAS, see Appendix A, “Predefined Application Policies” in the *Cisco Wide Area Application Services Configuration Guide*.



### Note

If the HTTP connection to the client aborts while the file transfer is in progress, the **show statistics application** command output may display a higher total for optimized traffic than for original traffic. This is because the HTTP cache always caches the complete file, even if the connection to the client is aborted before the file transfer has completed.

**Table 3-89** *app\_name* Variable Values for the show statistics application Command

app_name Values			
Authentication	Backup	CAD	Call-Management
Citrix	Conferencing	Console	Content-Management
Directory-Services	Email-and-Messaging	Enterprise-Applications	File-System
File-Transfer	Instant-Messaging	Name-Services	Other
P2P	Printing	Remote-Desktop	Replication
SQL	SSH	SSL	Storage

**Table 3-89** *app\_name Variable Values for the show statistics application Command*

app_name Values			
Streaming	Systems-Management	Version-Management	VPN
Web			

**Examples**

[Table 3-90](#) describes the statistics for each class of application that are displayed by the **show statistics application EXEC** command.

**Table 3-90** *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 3-91](#) describes the result values shown for the statistics in the **show statistics application** command display.

**Table 3-91** *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

<b>connection</b>	(Optional) Displays AppNav Controller connection statistics.
<b>client-ip</b>	(Optional) Displays the statistics for the client with the specified IP address.
<i>ip_address</i>	IP address of a client or server.
<b>client-port</b> <i>port</i>	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
<b>server-ip</b>	(Optional) Displays the statistics for the server with the specified IP address.
<b>server-port</b> <i>port</i>	(Optional) Displays the statistics for the server with the specified port number (1–65535).
<b>detail</b>	(Optional) Displays detailed statistics.
<b>summary</b>	(Optional) Displays summary statistics.
<b>drop</b>	(Optional) Displays statistics about dropped packets.
<b>flow-asymmetry</b>	(Optional) Displays statistics about asymmetric flows.
<b>flow-management</b>	(Optional) Displays flow learning statistics.
<b>app-sess</b>	(Optional) Displays application and session statistics.
<b>appnav-controller-ip</b> <i>ip_address</i>	(Optional) Displays flow-management statistics of the specified AppNav Controller.
<b>flow-table</b>	(Optional) Displays flow-table statistics.
<b>syn</b>	(Optional) Displays SYN statistics.
<b>ip</b>	(Optional) Displays IP-related statistics.
<b>sessions</b>	(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]**

<b>Syntax Description</b>	<b>blacklist</b> (Optional) Displays the blacklist server statistics.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator

**Examples** [Table 3-92](#) describes the result values shown for the statistics in the **show statistics application** command display.

**Table 3-92** 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 3-92** 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 3-92** Result Value Descriptions for the *show statistics auto-discovery* Command

Result	Description
AOIM Sync with Peer still in progress	Auto-discovery failed because AOIM synchronization is still in progress between the peers.
Auto discovery success TO	
Internal server	Address of the internal server.
External server	Address of the external server.
Auto discovery success FOR	
Internal client	Address of the internal client.
External client	Address of the external client.
Auto discovery success SYN retransmission	
Zero retransmit	No retransmissions were required for auto-discovery SYN success.
One retransmit	One retransmission were required for auto-discovery SYN success.
Two+ retransmit	Two or more retransmissions were required for auto-discovery SYN success.
AO discovery	
AO discovery successful	Auto-discovery of an application optimizer was successful.
AO discovery failure	Auto-discovery of an application optimizer was not successful.
Auto discovery Miscellaneous	
RST received	Number of resets received.
SYNs found with our device id	Number of SYN packets received indicating WAE's device ID.
SYN retransmit count resets	Number of resets to the SYN retransmission count.
SYN-ACK sequence number resets (syncookies)	Number of SYN-ACK packets received with a sequence number reset.
SYN-ACKs found with our device id	Number of SYN-ACK packets received indicating WAE's device ID.
SYN-ACKs found with mirrored options	Number of SYN-ACK packets received with mirrored options.
Connections taken over for MAPI optimization	Number of connections taken over for MAPI acceleration from an overloaded serial cluster peer.

**Related Commands**

[show auto-discovery](#)  
[show statistics filtering](#)  
[show statistics tfo](#)  
[show statistics connection closed](#)

# show statistics class-default

To display statistics information about the class-default class map, use the **show statistics class-default EXEC** command.

## show statistics class-default top-talkers

<b>Syntax Description</b>	<b>top-talkers</b>	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	
<b>appnav</b> <i>classmap-name</i>	Displays statistics for the specified AppNav class map.
<b>waas</b>	Displays statistics for the specified WAAS optimization class map, or all class maps if no class map is specified.
<b>name</b> <i>classmap-name</i>	Displays statistics for the specified WAAS optimization class map.
<b>summary</b>	Displays summary statistics for all WAAS optimization class maps that have active and completed connections.
<b>active</b>	Displays summary statistics for all WAAS optimization class maps that have currently active connections.
<b>all</b>	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
```

## show statistics class-map

```

    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

```

auto-discovery{ client-ip [ ip_address | hostname ] | client-port port | peer-id peer_id |
server-ip { ip_address | hostname } | server-port port } |
client-ip { ip_address | hostname } | client-port port |
closed |
detail [client-ip { ip_address | hostname } | client-port port | peer-id peer_id | server-ip
{ ip_address | hostname } | server-port port] |
egress methods |
optimized |
pass-through |
peer-id peer_id |
server-ip { ip_address | hostname } |
server-port port] |
conn-id connection_id

```

Syntax	Description
<b>auto-discovery</b>	Displays currently active auto-discovery connections
<b>client-ip</b>	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
<b>client-port</b> <i>port</i>	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
<b>closed</b>	Displays closed connections for client, server and peer along with their details.
<b>detail</b>	(Optional) Displays detailed connection statistics.
<b>peer-id</b> <i>peer_id</i>	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
<b>server-ip</b>	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
<b>server-port</b> <i>port</i>	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).
<b>egress-methods</b>	Displays detailed information on the egress-methods
<b>optimized</b>	Displays currently active optimized connections.
<b>pass-through</b>	Display currently active pass-through connections.
<b>conn-id</b> <i>connection_id</i>	(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.

Consider the following guidelines for the **show statistics connection** command:

- 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.
- Pass-through entries
  - A new connection immediately replaces an old connection. If a connection termination takes less than 10 seconds, then the new connection replaces it. However, WAAS has pass-through connection entry for both new and old connections (connections lasting 10 seconds or more). Therefore, in a scenario where pass-through entries take 10 seconds or more to expire, the output from **show statistics connection** will show totals for both old and new connections.
  - Unlike optimized flow, WAAS does not inspect each packet at TCP level to confirm when the connection got reset. Therefore, when there is no activity for 10 seconds, the pass-through flow entry get removed. The pass-through flows are then a count of pass-through flows seen in less than 10 seconds.
- Calculating the reduction in traffic (the total reduction ratio:
  - a. Use the **show statistics connection conn-id connection id** to compare optimized traffic packet level bytes calculation (the amount of traffic that went across the WAN) with original traffic (the amount of traffic that went out the WAN) for a specific identifier.

**Example output:**

	<b>Original</b>	<b>Optimized</b>
Bytes Read	78,7408	92,939
Bytes Written	<u>40,1764</u>	<u>117,657</u>
	1,189,172	210,596

- b. For this single connection, the amount of bytes that went across the WAN (210,596) is significantly less than the amount of bytes that went out the WAN (1,189,172).
- c. To calculate the reduction in traffic use this formula:  
**1 - (total optimized bytes/total original bytes)**
- d. In this example, the calculation is:  
**1 - (210596/1189172) = .82290535 or 82.291%**



- e. If the amount of optimized bytes is greater than the amount of original bytes, you see a total reduction ratio of 0.00%.

Table 3-93 describes the fields shown in the **show statistics connection** command display.

**Table 3-93** 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, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, S = SSL, W = WAN secure, X = signed SMB
Reduction Ratio (RR)	Relative reduction ratio (in bytes) for a particular connection.
Local IP:Port	IP address and port of the incoming local connection.
Remote IP:Port	IP address and port of the outgoing remote connection.
ConnType	Connection type (see Table 3-94).

Table 3-94 describes the possible values found in the ConnType field.

**Table 3-94** 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 3-94 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 3-94** *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
<b>auto-discovery</b>	(Optional) Displays active connection statistics for auto-discovery connections.
<b>client-ip</b>	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
<b>client-port</b> <i>port</i>	(Optional) Displays the connection statistics for the client with the specified port number (1–65535).
<b>peer-id</b> <i>peer_id</i>	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
<b>server-ip</b>	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
<b>server-port</b> <i>port</i>	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).

**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 3-95](#) describes the fields shown in the **show statistics connection auto-discovery** display.

**Table 3-95** *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 <a href="#">Table 3-94</a> ).

**Related Commands**[show statistics accelerator](#)[show statistics connection egress-methods](#)

# show statistics connection closed

To display closed connection statistics for a WAAS device, use the **show statistics connection closed** EXEC command.

## show statistics connection closed

```
[detail | dre | epm | http | mapi | ssl | tfo | [client-ip {ip_address | hostname} |
client-port port | conn-id connection_id | peer-id peer_id | server-ip {ip_address | hostname}
| server-port port]
```

Syntax	Description
<b>detail</b>	(Optional) Displays detailed closed connection statistics.
<b>dre</b>	(Optional) Displays closed connection statistics for connections optimized by the DRE feature.
<b>epm</b>	(Optional) Displays closed connection statistics for connections optimized by the EPM application accelerator.
<b>http</b>	(Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.
<b>mapi</b>	(Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.
<b>ssl</b>	(Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.
<b>tfo</b>	(Optional) Displays closed connection statistics for connections optimized by the TFO application accelerator.
<b>client-ip</b>	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
<b>client-port</b> <i>port</i>	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
<b>conn-id</b> <i>connection_id</i>	(Optional) Displays closed connection statistics for the connection with the specified identifier.
<b>peer-id</b> <i>peer_id</i>	(Optional) Displays the closed connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
<b>server-ip</b>	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
<b>server-port</b> <i>port</i>	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).

**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 3-96 describes the fields shown in the **show statistics connection closed** command display.

**Table 3-96** Field Descriptions for the **show statistics connection closed** Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
ConnID	Identification number assigned to the connection.
Source IP:Port	IP address and port of the incoming source connection.
Dest IP:Port	IP address and port of the outgoing destination connection.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, S = SSL, W = WAN secure, X = signed SMB

### Related Commands

[clear arp-cache](#)

[show statistics accelerator](#)

[show statistics connection egress-methods](#)

# show statistics connection conn-id

To display connection ID statistics for a WAAS device, use the **show statistics connection conn-id EXEC** command.

**show statistics connection conn-id** *connection\_id*

<b>Syntax Description</b>	<i>connection_id</i> (Optional) Connection statistics for the connection with the specified identifier number.
---------------------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Device Modes</b>	application-accelerator appnav-controller
---------------------	--

<b>Usage Guidelines</b>	The <b>show statistics connection conn-id</b> command displays the statistics for individual TCP connections. This information is updated in real time.
-------------------------	---

<b>Examples</b>	<a href="#">Table 3-97</a> describes the fields shown in the <b>show statistics connection conn-id</b> command display.
-----------------	---

**Table 3-97** Field Descriptions for the **show statistics connection conn-id** Command

Field	Description
<b>Connection Information</b>	
Peer ID	MAC address of the peer device.
Connection Type	Type of connection established with the peer.
Start Time	Date and time connection started.
Source IP Address	IP address of the connection source.
Source Port Number	Port number of the connection source.
Destination IP Address	IP address of the connection destination.
Destination Port Number	Port number of the connection destination.
Application Name	Name of the application traffic on the connection.
Classifier Name	Name of the application classifier on the connection.
Map Name	Name of the policy engine application map.
Directed Mode	State of directed mode: true (on) or false (off).



**Table 3-97** 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 read and written on the original (incoming) side and the optimized (outgoing) side.
<b>DRE Stats</b>	
Encode	Statistics for compressed messages.
Overall: [msg   in   out   ratio]	Aggregated statistics for compressed messages. 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.
<b>Connection Details</b>	
Chunks	Number of chunks encoded, decode, and anchored (forced).
Total Messages	Total number of messages processed and the number of blocks used per message.
Ack [msg   size]	Number and size of acknowledgement messages.
Encode Bypass Due To	Reason for previous traffic encoding bypass.
Nack	Number and size of negative acknowledgement messages.
R-tx	Number of ready-to-transmit messages.
Aggregation Encode/Decode	Aggregated statistics for compressed messages.

**Table 3-97** Field Descriptions for the *show statistics connection conn-id* Command (continued)

Field	Description
<b>TFO Stats</b>	
Conn-Type	Type of connection (see <a href="#">Table 3-94</a> ).
Policy	Policy in use on connection.
EOT State [write   req   ack   read   ack]	End of transmission state for data written and read.
Socket States	Socket states, including <b>read-shut</b> , <b>write-shut</b> , <b>close</b> , <b>choke</b> , and <b>envoy</b> .
DRE Hints [local   remote   active]	Number of DRE hints sent for the local, remote, and active connections.
Read Encode/Decode Flows	Number of encode and decode messages, and total bytes used.
Decoder Pending Queue	Size of the messages waiting in the decode queue, including maximum size, current size, average size, and the number of flow-control stop messages.
Encode/Decode	Number of calls encoded and decoded, the message latency (in ms), and the number of transmitted data/acknowledgment frames.
Writer Pending Queue	Size of the messages waiting in the write queue, including maximum size, current size, average size, and the number of flow-control stop messages.
Write	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
<b>client-ip</b>	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
<b>client-port port</b>	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
<b>peer-id peer_id</b>	(Optional) Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
<b>server-ip</b>	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
<b>server-port port</b>	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).

**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](#)):

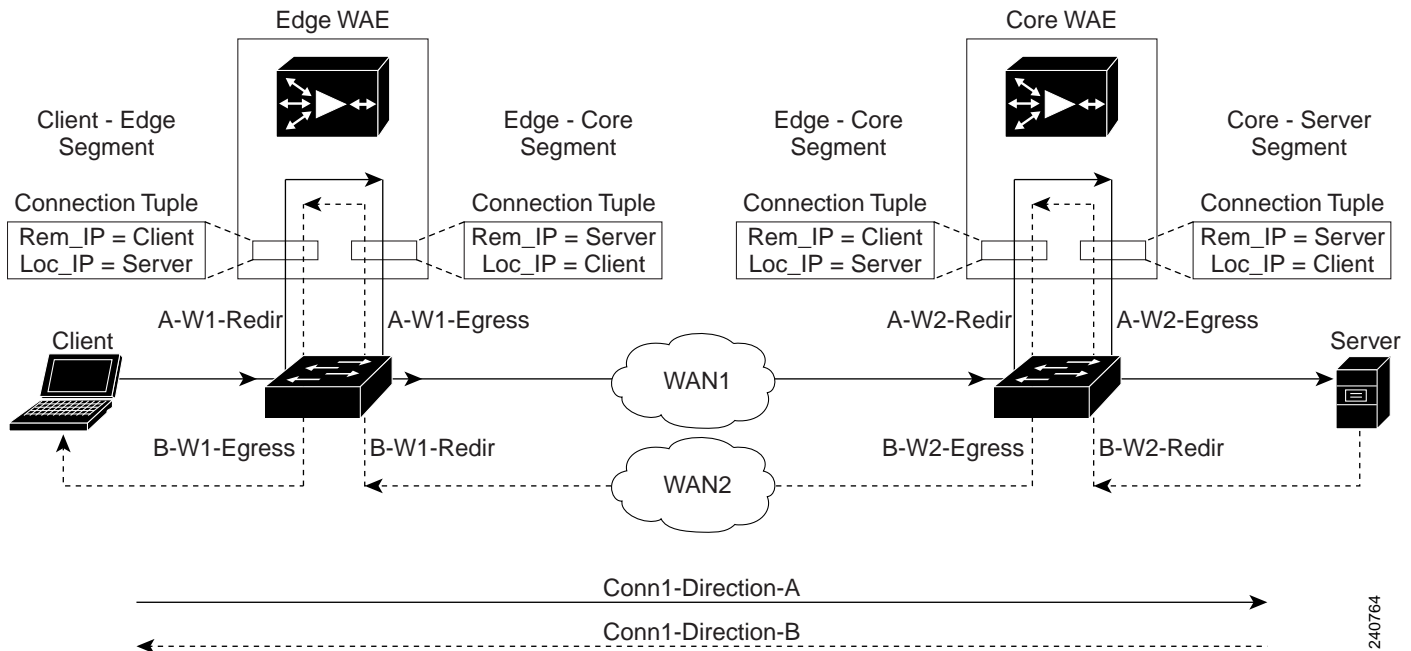
- Between the client and the Edge WAE
- Between the Edge WAE and the Core WAE
- Between the Core WAE and the server

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 3-98](#).) 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 3-98](#) describes the fields shown in the **show tfo egress-methods connection** command display.

**Table 3-98** Field Descriptions for the show tfo egress-methods connection Command

Field	Description
TUPLE	
Local-IP:Port	IP address and port number of the local device in the connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the connection tuple.
MATE	
Local-IP:Port	IP address and port number of the local device in the mate connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the mate connection tuple.
Egress method	Egress method being used.
WCCP Service   Bucket	WCCP service number and bucket number for the connection tuple and mate connection tuple.
Tuple Flags	Flags for intercept method and intercept mechanism. This field may contain the following values: WCCP or NON-WCCP as the intercept method; L2 or GRE as the intercept mechanism; or PROT showing whether this tuple is receiving packets through the flow protection mechanism.
Intercepting device (ID)	
ID IP address	IP address of the intercepting device.
ID MAC address	MAC address of the intercepting device.
ID IP address updates	Number of IP address changes for the intercepting device.
ID MAC address updates	Number of MAC address changes for the intercepting device.
Memory address	Memory address.

Each time a packet enters the connection tuple, the intercepting device IP address or MAC address is recorded. The updates field in the command output indicates whether the intercepting device IP address or intercepting device MAC address has been recorded. If, for example, the ID MAC address updates field is zero (0), the MAC address was not recorded, and the ID MAC address field will be blank. The recorded intercepting device information is used when a packet egresses from the WAE.

If the egress method for the connection tuple is IP forwarding, the updates fields are always zero (0) because the intercepting device information is neither required nor recorded for the IP forwarding egress method.

If the intercept method is WCCP GRE redirect and the egress method is WCCP GRE, only the IP address field is updated and recorded. The MAC address information is neither required nor recorded because the destination address in the GRE header only accepts an IP address.

If the intercept method is WCCP L2 redirect and the egress method is WCCP GRE, both the MAC address and the IP address fields are updated and recorded because incoming WCCP L2 packets contain only a MAC header. The MAC address is recorded and the intercepting device IP address is derived from

a reverse ARP lookup and is then recorded, also. When packets egress the connection tuple in this scenario, they will have a GRE header with the destination IP address of the intercepting device that was recorded.

The updates count may be greater than 1 in certain topologies. For example, in a redundant router topology, where for the same direction of the same connection between two hosts, packets may be coming in from different intercepting routers. Each time a packet comes in, the intercepting device MAC or IP address is compared against the last recorded address. If the MAC or IP address has changed, the updates field is incremented and the new MAC or IP address is recorded.

---

Related Commands [show statistics tfo](#)

# show statistics connection optimized

To display optimized connection statistics for a WAAS device, use the **show statistics connection optimized** EXEC command.

## show statistics connection optimized

```
[client-ip {ip_address | hostname} | client-port port | peer-id peer_id | server-ip {ip_address
| hostname} | server-port port |
{http | ica | mapi | smb | ssl | wansecure} | {detail | dre { all | savings | {http | ica | mapi | smb
| ssl | wansecure}}}]
```

Syntax	Description
<b>optimized</b>	(Optional) Displays active connection statistics for optimized connections.
<b>client-ip</b>	(Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
<b>client-port port</b>	(Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).
<b>peer-id peer_id</b>	(Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.
<b>server-ip</b>	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
<b>server-port port</b>	(Optional) Displays the connection statistics for the server with the specified port number (1–65535).
<b>http</b>	(Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.
<b>ica</b>	(Optional) Displays closed connection statistics for connections optimized by the ICA application accelerator.
<b>mapi</b>	(Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.
<b>smb</b>	(Optional) Displays the connection statistics for connections optimized by the SMB application accelerator.
<b>ssl</b>	(Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.
<b>wansecure</b>	(Optional) Displays closed connection statistics for connections optimized by the WAN secure application accelerator.
<b>dre</b>	(Optional) Displays closed connection statistics for connections optimized by the DRE feature.
<b>all</b>	(Optional) Displays all the connection statistics for connections of the filtered type.
<b>savings</b>	(Optional) Displays the savings connection statistics for connections of the filtered type.

## Defaults

No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
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 3-99](#) describes the fields shown in the **show statistics connection optimized** command display.

**Table 3-99** Field Descriptions for the show statistics connection optimized Command

Field	Description
Current Active Optimized Flows	Number of current active optimized TCP connections of all types.
Current Active Optimized TCP Plus Flows	Number of current active connections using DRE/LZ optimization or handled by an accelerator.
Current Active Optimized TCP Only Flows	Number of current active connections using TFO optimization only.
Current Active Optimized TCP Preposition Flows	Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.
Current Active Auto-Discovery Flows	Number of current active connections in the auto-discovery state.
Current Active Reserved Flows	Number of reserved connections.
Current Active Pass-Through Flows	Number of current active pass-through connections.
Historical Flows	Number of closed TCP connections for which statistical data exists.
ConnID	Identification number assigned to the connection.
Source IP:Port	IP address and port of the incoming source connection.
Dest IP:Port	IP address and port of the outgoing destination connection.
PeerID	MAC address of the peer device.
Accel	Types of acceleration in use on the connection. D = DRE, L = LZ, T = TCP optimization, A = AOIM, E = EPM, G = generic, H = HTTP, I = ICA, M = MAPI, S = SSL, W = WAN secure, X = signed SMB

**Related Commands** [clear arp-cache](#)



**show statistics accelerator**

**show statistics connection egress-methods**

# show statistics connection pass-through

To display pass through connection statistics for a WAAS device, use the **show statistics connection pass-through EXEC** command.

## show statistics connection pass-through

```
client-ip {ip_address | hostname} | client-port port | peer-id peer_id |
server-ip {ip_address | hostname} | server-port port
```

Syntax	Description
<b>pass-through</b>	Displays active connection statistics for pass-through connections.
<b>client-ip</b>	Displays the closed connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
<b>client-port port</b>	Displays the closed connection statistics for the client with the specified port number (1–65535).
<b>peer-id peer_id</b>	Displays the connection statistics for the peer with the specified identifier. The peer ID is from 0 to 4294967295 identifying a peer.
<b>server-ip</b>	Displays the connection statistics for the server with the specified IP address or hostname.
<b>server-port port</b>	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 3-100](#) describes the fields shown in the **show statistics connection pass-through** command display.

**Table 3-100** 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 <a href="#">Table 3-94</a> ).

**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 3-101](#) describes the fields shown in the **show statistics crypto ssl ciphers** command display.

**Table 3-101** *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 3-102](#) describes the fields shown in the **show statistics datamover** command display.

**Table 3-102** Field Descriptions for the show statistics datamover Command

Field	Description
Global Datamover Statistics	
Datamover users	Number of datamover clients (and Area blocks in the output).
Datamover container maps	Number of container_map structures allocated.
Datamover containers	Number of container structures allocated.
Datamover pages	Number of system pages used by datamover.
Datamover kmalloc areas	Number of kmalloc areas used by datamover.
Calls to cs_compact	Number of calls to cs_compact.
Container map allocation failures	Number of container_map structure allocation failures.
Container allocation failures	Number of container structure allocation failures.
Zone allocation failures	Number of zone allocation failures.
Kmem allocation failures	Number of kernel memory allocation failures.
Page allocation failures	Number of page allocation failures.
Area <i>n</i>	Name of application area. There is one Area block in the output for every datamover client.
Max Area size in pages	Total datamover size limit in pages.
Number of identifiers	Number of distinct datamover objects.

**Table 3-102** Field Descriptions for the *show statistics datamover* Command (continued)

Field	Description
32 . . . 2048 byte areas used	Number of storage areas of each size.
Zone pages used	Number of pages used for the 32-2048 byte storage areas.
Non-zone pages used	Number of pages used for page mapping.
Cloned identifiers	Number of cloned identifiers.
Number of lookup stalls	Number of lookup stalls.
Calls to cs_compact	Number of calls to cs_compact.
Calls to cs_dup	Number of calls to cs_dup.
Calls to cs_send_bycopy	Number of calls to cs_send_bycopy.
Calls to cs_send_envoy	Number of calls to cs_send_envoy.
Calls to cs_recv_bycopy	Number of calls to cs_recv_bycopy.
Calls to cs_recv_envoy	Number of calls to cs_recv_envoy.
Identifier allocation failures	Number of identifier allocation failures.
Address allocation failures	Number of address allocation failures.
Total pages used	Number of pages used and percentage of the maximum area size used.

# show statistics dre

To display Data Redundancy Elimination (DRE) general statistics for a WAE, use the **show statistics dre** EXEC command.

**show statistics dre [detail]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Specifies to show detail.
---------------------------	--

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

## Examples

### Example 1

[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.

**Example 2**

The following example shows output from the `show statistics dre` command.

```
Cache:
  Status: Usable, Oldest Data (age): 14d16h
  Total usable disk size: 77822 MB, Used: 96.69%
WAE-337-06#sh statistics dre

Cache:
  Status: Usable, Oldest Data (age): 14d17h
  Total usable disk size: 77822 MB, Used: 96.69%

Connections: Total (cumulative): 9 Active: 9

Encode:
  Overall: msg:      1398, in:   2586 KB, out:   2318 KB, ratio:  10.38%
          DRE: msg:      1389, in:   2549 KB, out:   2381 KB, ratio:   6.57%
DRE Bypass: msg:      1398, in:   38235 B
          LZ: msg:      1347, in:   2384 KB, out:   2253 KB, ratio:   5.49%
  LZ Bypass: msg:       51, in:   35814 B
  Avg latency:      0.334 ms, Avg msg size:   1894 B
  Message size distribution:
    0-1K=7% 1K-5K=88% 5K-15K=3% 15K-25K=0% 25K-40K=0% >40K=0%

Decode:
  Overall: msg:      27, in:  14140 B, out:  29223 B, ratio:  51.61%
          DRE: msg:      27, in:  29770 B, out:  29079 B, ratio:   0.00%
DRE Bypass: msg:      27, in:    144 B
          LZ: msg:      27, in:  14140 B, out:  30076 B, ratio:  52.99%
  LZ Bypass: msg:       0, in:     0 B
  Avg latency:      0.061 ms, Avg msg size:   1082 B
```

**Example 3**

The following example shows sample output using the `cwoDre` parameter. The output provides two types of MIB DRE statistics—DRE cache statistics and DRE performance statistics:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsStatus.0 = STRING: Usable
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsAge.0 = STRING: 14d17h
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsTotal.0 = Counter64: 77822 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 96 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitUsage.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrDataUnit.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitAge.0 = STRING: 0s
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockUsage.0 = Counter64: 1695 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrSigblock.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockAge.0 = STRING: 14d17h
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeCompressionRatio.0 = Gauge32: 9 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeCompressionLatency.0 = Counter64: 0 ms
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeAvgMsgSize.0 = STRING: 1991 B
```

■ show statistics dre

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeCompressionRatio.0 = Gauge32: 51 percent  
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeCompressionLatency.0 = Counter64: 0 ms  
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeAvgMsgSize.0 = STRING: 1082 B
```

---

**Related Commands**

[show statistics peer](#)

# show statistics encryption-services

To display encryption-services general statistics for a WAE, use the **show statistics encryption-services EXEC** command,

```
show statistics encryption-services {interposer-ssl (detail) | sake}
```

Syntax Description	interposer-ssl	Displays interposer-ssl statistics
	sake	Displays sake statistics

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

## Examples

### Example 1

[Table 3-104](#) describes the fields shown in the **show statistics interposer-ssl detail** command.

**Table 3-104** Field Descriptions for the show statistics interposer-ssl detail Command

Field	Description
Time Accelerator was started	Local time accelerator was started or restarted.
Time Statistics were Last Reset/Cleared	Local time accelerator was last started or restarted, or the clear statistics accelerator [interposer-ssl   all] command was executed since accelerator was last started or restarted.
Total Handled Connections	Total number of handled connections by the Interposer.
Total Optimized Connections	Total number of optimized connections by the Interposer.
Total Connections Handed-off	Connections initially accepted by Interposer accelerator, but later handed off to generic optimization without policy changes
Total Dropped Connections	Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources)
Current Active Connections	Number of WAN side connections currently established
Maximum Active Connections	Highest number of active connections since accelerator was last started/restarted.
Number of flows with matching IP	Number of connection that flows with the matching ip i.e configured in accelerated service.

**Table 3-104** Field Descriptions for the *show statistics interposer-ssl detail* Command

Field	Description
Number of flows with matching SNI	Number of connection that flows with the matching server name.
Total requests to SAKE	Total number of requests sent to the SAKE server
Total responses from SAKE	Total number of responses from the SAKE server
Total Failed Certification Validations	Total Number of Failed Certificate validation.
Total Connections Dropped due to OCSP failures	Total Number of connection pushdown due OCSP failures.
Interposer SSL Detailed Statistics	
Total Pushdown Flows	Total number of flows that were pushed down due to various reasons.
Pushdown due to cipher mismatch	Number of connections pushed down by Interposer- SSL accelerator because the SSL cipher negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
Pushdown due to unsupported SSL version	Number of connections pushed down by Interposer- SSL accelerator because the SSL version negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.
Pushdown due to detection of non-SSL traffic	Number of connections pushed down by the Interposer- SSL accelerator because the content of the flow did not appear to contain SSL messages.
Pushdown due to ASVC not found	Number of connections pushed down by the Interposer- SSL accelerator because no matching accelerated service was found for the content of the flow.
Pushdown due to unknown reason	Number of connections pushed down by the Interposer- SSL accelerator because of unknown reasons.
Total Handled Flows	
Total SSLv3	Total number of connection that are negotiated with the SSL version SSLv3.
Total TLS	
Total TLS1.0	Total number of connection that are negotiated with the SSL version TLS1.0 in Handshakes
Total TLS 1.1	Total number of connection that are negotiated with the SSL version TLS1.1 in Handshakes
Total TLS1.2	Total number of connection that are negotiated with the SSL version TLS1.2 in Handshakes
SSL Handshake classification	
Total SSL Handshakes	Total number of all handshakes seen by the WAE since the last reset.

**Table 3-104** Field Descriptions for the *show statistics interposer-ssl detail* Command

Field	Description
Total Full SSL Handshakes	Total number of connections that performed a full handshake exchanging cryptographic information.
Total SSL Resumptions	Total number of connections that perform a resumption (either with session-id or session-ticket) handshake.
Session-Id	Number of SSL Handshakes with Resumption with Session-Id.
Session-Ticket	Number of SSL Handshakes with Resumption with Session-Ticket
Fallback to Full SSL Handshakes	Total number of resumption failures that result in a fallback to full handshake.
Total SSL renegotiations	Total number of renegotiated SSL handshakes.
Total number of failed renegotiations	Total number of renegotiation handshakes that resulted in failures.
<b>Certificate Validation</b>	
Total Certificate Validation Requests	Total number of client and server certificate validation attempted by SMART-SSL accelerator. Total Number of Certificate Validation Requests without OCSP revocation check
Total Successful Certificate Validations	Total Number of successful Certificate Validation done by the SMART-SSL accelerator without OCSP revocation check.
Total Trusted Certificate Store Refresh	Total number of times CA trusted pool is updated. In other words, total number of trusted certificate store refresh.
<b>OCSP</b>	
Total OCSP validation requests initiated	Number of OCSP validation requests that were initiated by the SMART-SSL accelerator based on configuration settings.
Total OCSP validation responses completed	Number of OCSP validation requests that were completed with a valid response from the OCSP responder.
Total OCSP requests that timed out	Number of OCSP requests deemed failed because no response was received from the OCSP responder.
Total Successful OCSP requests with GOOD status	Number of OCSP requests where the OCSP certificate status was "GOOD"
Total Successful OCSP requests with NONE status	Number of OCSP requests where the OCSP status was deemed OK because of fallback to method configuration: NONE.
Total Successful OCSP requests with REVOKED status	Number of OCSP requests where the OCSP certificate status was REVOKED.
Total Successful OCSP requests with UNKNOWN status	Number of OCSP requests where the responder did not know the status of the certificate.
Total OCSP requests pending	Number of OCSP requests currently in progress.
Total OCSP requests with a corrupted certificate	Number of OCSP requests where certificate verification attempts failed because the certificate was corrupted.

**Table 3-104** Field Descriptions for the `show statistics interposer-ssl detail` Command

Field	Description
Total OCSP requests with failed certificate verification	Number of OCSP requests where certificate verification attempts failed.
Total OCSP requests that encountered internal error	Number of OCSP requests deemed failed due to internal errors.

[Table 3-105](#) describes the fields shown in the `show statistics sake detail` command.

**Table 3-105** Field Descriptions for the `show statistics sake detail` Command

Field	Description
SAKE Server Statistics	
Time Accelerator was started	Local time accelerator was started or restarted.
Time Statistics were Last Reset/Cleared	Local time accelerator was last started or restarted, or the clear statistics accelerator [interposer-ssl   all] command was executed since accelerator was last started or restarted.
ASVC Config Channel	This indicates that the SMART-SSL accelerator is ready to receive the configuration from CLI or CM.
Number of ISM Connected	Total number of Interposer Session Manager participating in the SSL handshake.
Accelerated Service Count	Number of configured accelerated services.
Number of Sake Requests Received	Total number of Accelerated services configured on SAKE server.
Number of Sake Pending Requests	Total number of SAKE requests pending to be served.
Number of Sake Success Responses	Total number of successful SAKE responses.
Number of flows with matching SNI	The total number of connections requests that matched the SNI (Service Name Indicator) to find the right accelerated service.
Number of Sake Error Responses	Total number of requests that resulted in errors.
SAKE Server Detailed Statistics	
Number of requests per Crypto	Total number of crypto requests serviced by SAKE server.
DHE key exchange	Number of SAKE Requests that originates from DHE Handshakes.
ECDHE Key exchange	Number of SAKE Request that is carried with ECDHE algorithm at the time of the connection between interposer and sake.
RSA key exchange	Number of SAKE Request that is carried with RSA algorithm at the time of the connection between interposer and sake.
Client Authentication	Number of SAKE Request when server asks for the client Authentication

**Table 3-105** *Field Descriptions for the show statistics sake detail Command*

Field	Description
Number of requests per ASVC	Number of connection that flows to that particular Accelerated Service.
ASVC-ngssl	Number of requests to SAKE from a particular Accelerated Service.

■ show statistics encryption-services



# 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 3-106](#) describes the fields shown in the **show statistics filtering** command display.

**Table 3-106** 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 3-106** 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 3-106** 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		
	<b>filters</b>	Displays flow filter statistics.
	<b>monitor type</b>	Displays flow performance statistics.
	<b>tcpstat-v1</b>	Displays tcpstat-v1 collector statistics.
	<b>monitor</b> <i>MonitorName</i>	Displays statistics for a specified flow monitor.
	<b>exporter</b> <i>ExporterName</i>	Displays statistics for a specified exporter.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** [Table 3-107](#) describes the fields shown in the **show statistics flow filters** command display.

**Table 3-107** 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 3-108 describes the fields shown in the **show statistics flow monitor** command display.

**Table 3-108** Field Descriptions for the **show statistics flow monitor** Command

Field	Description
<b>Host Connection</b>	
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.
<b>Collector Connection</b>	
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.
<b>Collection Statistics</b>	
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 3-108** *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 3-109](#) describes the fields shown in the **show statistics generic-gre** command display.

**Table 3-109** 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 3-110](#) describes the fields shown in the **show statistics icmp** command display.

**Table 3-110** 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 3-110** Field Descriptions for the *show statistics icmp* Command (continued)

Field	Description
ICMP messages sent	Total total number of ICMP messages which this entity attempted to send. This counter includes all those counted as ICMP output errors.
ICMP messages send failed	Number of number of ICMP messages which this entity did not send because of problems discovered within ICMP, such as a lack of buffers.
Destination unreachable	Number of ICMP messages of this type sent out.
Time exceeded	Number of ICMP messages of this type sent out.
Wrong parameters	Number of ICMP messages of this type sent out.
Source quenches	Number of ICMP messages of this type sent out.
Redirects	Number of ICMP messages of this type sent out.
Echo requests	Number of ICMP messages of this type sent out.
Echo replies	Number of ICMP messages of this type sent out.
Timestamp requests	Number of ICMP messages of this type sent out.
Timestamp replies	Number of ICMP messages of this type sent out.
Address mask requests	Number of ICMP messages of this type sent out.
Address mask replies	Number of ICMP messages of this type sent out.

**Related Commands**[clear arp-cache](#)

# show statistics icmp6

To display ICMP statistics for a WAAS device, use the **show statistics icmp** EXEC command.

## show statistics icmp

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-111](#) describes the fields shown in the **show statistics icmp6** command display.

**Table 3-111** Field Descriptions for the show statistics icmp6 Command

Field	Description
ICMP6 messages received	Total number of Internet Control Message Protocol (ICMP) messages which the entity received, including all those counted as ICMP6 input errors.
ICMP6 messages receive failed	Number of ICMP6 messages which the entity received but determined as having ICMP-specific errors, such as bad ICMP checksums, bad length, and so forth.
Destination unreachable	Number of ICMP6 messages that can not be delivered to its destination address for reasons other than congestion.
Large packets	Number of ICMP6 messages that have packets larger than the MTU size specified.
Timeout in transit	Number of ICMP6 messages that failed to reach its destination due to extra time taken during transit, than the set limit.
Wrong parameters	Number of ICMP6 messages with erroneous parameters in its header etc.
Echo requests	Number of echo requests sent during the ping request to check and confirm the connectivity to the neighbor device.
Echo replies	Number of echo replies generated in response to the echo request.
Group member queries	Number of groups who would want to receive the ICMP6 packets

**Table 3-111** Field Descriptions for the *show statistics icmp6* Command (continued)

Field	Description
Group member responses	Number of groups who would want to receive the ICMP6 packets
Group member reductions	
Router solicits	Number of router solicitations messages sent by host in order to prompt routers to generate router advertisements
Router advertisements	Number of periodic router advertisement messages or in response to a router solicitation.
Neighbor solicits	Neighbor solicitation messages to request the link-layer address of a target device while also providing their own link-layer address to the target.
Neighbor advertisements	Number of neighbor advertisements in response to neighbor solicitations.
Redirects	Number of neighbor redirect messages of this type received.
MLDv2 reports	Type of Multicast Listener Discovery v2 message.
Type 134	Number of advertisement messages sent out.
ICMP6 messages sent	Total total number of ICMP6 messages which this entity attempted to send. This counter includes all those counted as ICMP output errors.
Destination unreachable	Number of ICMP6 sent messages that can not be delivered to its destination address for reasons other than congestion.
Large packets	Number of ICMP6 messages that have packets larger than the MTU size specified.
Time exceeded	Number of ICMP messages of this type sent out.
Wrong parameters	Number of ICMP messages of this type sent out.
Echo requests	Number of echo requests sent during the ping request it to check and confirm the connectivity to the neighbor device.
Echo replies	Number of echo replies generated in response to the echo request.
Group member queries	Number of ICMP messages of this type sent out.
Group member responses	Number of ICMP messages of this type sent out.
Group member reductions	Number of ICMP messages of this type sent out.
Router solicits	Number of ICMP messages of this type sent out.
Router advertisements	Number of ICMP reply Packet from the device to neighbor.
Neighbor solicits	Number of ICMP request to the neighbor device.
Neighbor advertisements	Number of responses from the device against the request coming from the client device.
Redirects	Number of neighbor redirect messages of this type received.
MLDv2 reports	Type of Multicast Listener Discovery v2 message.
Type 133	Number of Neighbor advertisement message sent out.

*Table 3-111 Field Descriptions for the show statistics icmp6 Command (continued)*

Field	Description
Type 135	Number of Neighbor solicits message sent out.
Type 143	Number of Home Agent Address Discovery message send out

**Related Commands** [clear arp-cache](#)

# show statistics ip

To display IP statistics for a WAAS device, use the **show statistics ip** EXEC command.

## show statistics ip

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-112](#) describes the fields shown in the **show statistics ip** command display.

**Table 3-112** 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 3-112** Field Descriptions for the show statistics ip Command (continued)

Field	Description
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).
Total packets out	Total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
dropped	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (such as, for lack of buffer space). This counter includes datagrams counted in the forwarded field if any such packets meet this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in the forwarded field which meet this no-route criterion, including any datagrams that a host cannot route because all of its default gateways are down.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Total number of IP datagrams that have been successfully fragmented at this entity.
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented because their Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

**Related Commands**

**clear arp-cache**  
**(config) ip**

**(config-if) ip**  
**show ip routes**

# show statistics ipv6

To display IPv6 statistics for a WAAS device, use the **show statistics ipv6** EXEC command.

## show statistics ipv6 internal

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-113](#) describes the fields shown in the **show statistics ipv6 internal** command display.

**Table 3-113** Field Descriptions for the show statistics ipv6 Command

Field	Description
IPv6 statistics internal	
Total packets in	Total number of input datagrams received from interfaces, including all those counted as input errors.
with invalid address	Number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as 0.0.0.0) and addresses of unsupported classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
with large errors	Number of error messages sent by the device.
with invalid headers	Number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatches other format errors, time-to-live exceeded errors, and errors discovered in processing their IP options.
dropped (no route)	Number of packets dropped on device without knowing the destination device.
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
truncated packets	Number of modified packet without any acknowledgment.



**Table 3-113** Field Descriptions for the *show statistics ipv6* Command (continued)

Field	Description
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).
multicast packets	Total number of multicast packets.
octets	Total number of octets
multicast octets	Total number of multicast octets in the IPv6 packet.
broadcast octets	Total number of broadcast octets in the IPv6 packet
Total packets out forwarded	Total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
requests	Total number of requests received of the above type.
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
dropped (no route)	Number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in the forwarded field which meet this no-route criterion, including any datagrams that a host cannot route because all of its default gateways are down.
multicast packets	Total number of multicast packets out forwarded.
octets	Total number of octets out forwarded.
multicast octets	Total number of multicast octets in the out forwarded packets.
broadcast octets	Total number of broadcast octets in the out forwarded packets.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Total number of IP datagrams that have been successfully fragmented at this entity.

**Table 3-113** Field Descriptions for the show statistics ipv6 Command (continued)

Field	Description
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented because their Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

---

**Related Commands**    [\(config\) ip](#)

# show statistics 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
```

---

**show statistics monitor appnav-controller traffic**

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 3-114](#) describes the fields shown in the **show statistics netstat** command display.

**Table 3-114** *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 3-115](#) describes the fields shown in the **show statistics pass-through** command display.

**Table 3-115** 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 3-115** 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		
<b>dre</b>		Displays the peer DRE statistics.
<b>context</b> <i>context-value</i>		Displays peer statistics for the specified context (0–4294967295).
<b>peer-id</b> <i>peer-id</i>	(Optional)	Specifies the MAC address of the peer (0–4294967295).
<b>peer-ip</b> <i>ip_address</i>	(Optional)	Specifies the IP address of the peer.
<b>peer-no</b> <i>peer-no</i>	(Optional)	Specifies the peer number.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** [Table 3-116](#) describes the fields shown in the **show statistics peer dre detail** command display. This command shows the peer DRE device connection information.

**Table 3-116** 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 3-116** 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 3-116** 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	Parameter	Description
	<b>appnav</b>	Displays statistics for all of the class maps in the active AppNav policy map.
	<b>level1-class</b> <i>classmap-name</i>	Displays statistics for the specified class map in the top-level policy map, including all class maps in nested policies.
	<b>level2-class</b> <i>classmap-name</i>	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
```

**show statistics policy-sub-class**

```

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 3-117](#) describes the fields shown in the **show statistics radius** command display.

**Table 3-117** 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 3-117** *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
<b>appnav-controller</b> <i>ip_address</i>	(Optional) Displays statistics about the specified ANC.
<b>appnav-controller-group</b>	(Optional) Displays ANCG statistics for the service context.
<b>detail</b>	(Optional) Displays detailed statistics.
<b>data-path</b>	(Optional) Displays data path statistics.
<b>service-context</b>	(Optional) Displays service context statistics.
<b>service-node</b> <i>ip_address</i>	(Optional) Displays service node (WN) statistics. (Optional) Displays service node statistics of the specified node.
<b>service-node-group</b>	(Optional) Displays statistics for all the service node groups (WNGs) in the service context.
<b>name</b> <i>sng-name</i>	(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 3-118](#) describes the fields shown in the **show statistics services** command display.

**Table 3-118** *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		
<b>detail</b>	(Optional) Displays the detailed session statistics for all of the dynamic match sessions or for the specified traffic type.	
<b>app-id</b> <i>app-id</i>	(Optional) Displays the session statistics for dynamic matched flows for the application with the specified application number (0-1023) or the specified traffic type.	
<b>mapi</b>	Microsoft Exchange MAPI aka Exchange Server Store EMSMDB,	
<b>ms-ad-rep</b>	Microsoft Active Directory Replication (drsuapi),	
<b>ms-exch-nspi</b>	Microsoft Active Directory Name Service Provider (NSP),	
<b>ms-frs</b>	Microsoft File Replication Services (FRS),	
<b>ms-frs-api</b>	Microsoft File Replication API,	
<b>ms-rfr</b>	Microsoft Exchange Directory RFR Interface,	
<b>ms-sql</b>	Microsoft SQL,	
<b>msn-messenger</b>	Microsoft Messenger Service,	
<b>netlogon</b>	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 3-119](#) describes the fields shown in the **show statistics snmp** command display.

**Table 3-119** 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 3-119** 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 system cpu

To display the detailed parameters of the cpu utilization, use the **show statistics system cpu** EXEC command.

## show statistics system cpu

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use the **show statistics system cpu** command to display statistics for the system cpu utilization.

**Examples** The following is sample output from the **show statistics system cpu** command:

```
WAE# show statistics system cpu
CPU overload protection params:
State:                               Normal
CPU utilization:
  samples average:                     8%
  current probe:                       8%
Config thresholds:
  high:                                98%
  low:                                  90%
Config sampling window:                4 samples
Sampling intervals in secs:
  current:                              10
  config (normal state):                10
  config (overload state):              30
```

### Table

Field	Description
State	The current system-level state-- normal, overloaded or disabled. When the CPU utilization percentage is lower than the threshold used, it is in the normal state; otherwise it is overloaded. When this functionality is disabled through its CLI "no threshold-monitor system cpu enable", this state would become disabled.
CPU utilization	

Field	Description
samples average	The reading obtained from Linux during last sampling time by the system.
current probe	The reading taken right after executing this show command. When the sampling window is wide, this reading shows the value between the sampling instances.
Config thresholds	
high	The configured high threshold above which the system goes into the overloaded state when it is normal. But in the overloaded state, it doesn't go back to the normal state until the CPU utilization goes below the low threshold.
low	The configured low threshold below which the system goes into the normal state when it is overloaded. But in the normal state, it doesn't transition into the overloaded state until the CPU utilization goes above the high threshold.
Config sampling window	The configured sampling window size for the moving average. The number of the most recent CPU utilization samples taken in calculating the latest CPU utilization percentage. The result is the average of the given number of samples.
Sampling intervals in secs	
current	When the show command is issued, usually the Sysload is in the inactive state between sampling moments. The current sample rate determines the duration of the current inactive state. The duration can be different from the configured sampling rate, if the configured values are changed between sampling instances before the current inactive state expires.
config (normal state)	The configured sampling rate for the normal state.
config (overload state)	The configured sampling rate for the overloaded state.

# show statistics tacacs

To display TACACS+ authentication and authorization statistics for a WAAS device, use the **show statistics tacacs EXEC** command.

## show statistics tacacs

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** [Table 3-120](#) describes the fields shown in the **show statistics tacacs** command display.

**Table 3-120** 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 3-120** *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 3-121](#) describes the fields shown in the **show statistics tcp** command display.

**Table 3-121** 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 3-121** 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 3-121** 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 renegeing	Number of TCP SACK renegeing.
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 3-121** 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

<b>connection</b>	(Optional) Displays aggregated TFO connection statistics.
<b>detail</b>	(Optional) Displays detailed TFO statistics.
<b>peer</b>	(Optional) Displays DRE peer statistics.
<b>peer-id</b> <i>peer-id</i>	(Optional) Displays peer statistics for peer ID.
<b>peer-ip</b> <i>peer-ip</i>	(Optional) Displays peer statistics for peer IP.
<b>peer-no</b> <i>peer-no</i>	(Optional) Displays peer statistics for peer number.

## Command Modes

EXEC

## Device Modes

application-accelerator

## Examples

[Table 3-122](#) 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 3-122** 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 3-122 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 3-122** 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: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with TFO enabled</li> <li>• Restart of the TFO component by the Node Manager</li> </ul>
Hits	Number of connections that had a configured policy that specified the use of TFO.
Updated Released	Number of hits that were released during Auto-Discovery and did not make use of the TFO component.
Active Connections	Number of hits that represent either active connections using the TFO component or connections that are still in the process of performing Auto-Discovery.
Completed Connections	Number of hits that have made use of the TFO component and have completed.
Drops	Number of hits that attempted use of the TFO component but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.
Rejected Connection Counts Due To: (Total:)	<ul style="list-style-type: none"> <li>• Number of all of the reject reasons that represent hits that were not able to use TFO. Reject reasons include the following: <ul style="list-style-type: none"> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> </li> </ul>



**Table 3-122** 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 3-123](#) describes the fields shown in the **show statistics udp** command display.

**Table 3-123** 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 3-124](#) describes the fields shown in the **show statistics vn-service vpath** command display.

**Table 3-124** 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 3-124** 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 3-125](#) describes the fields shown in the **show statistics wccp gre** command display for an application accelerator device.

**Table 3-125** 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 3-125** 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.  <b>Note</b> A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.
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 3-125** 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 3-125** 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 <b>wccp access-list</b> 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 3-126](#) describes the fields shown in the **show statistics wccp** command display for an ANC device.

**Table 3-126** 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 3-126** 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 3-127](#) describes the fields shown in the **show statistics windows-domain** command display.

**Table 3-127** 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 3-127** 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 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.
<b>begin</b> <i>regex</i>	Begins with the line that matches the regular expression. You can enter multiple expressions.
<b>exclude</b> <i>regex</i>	Excludes lines that match the regular expression. You can enter multiple expressions.
<b>include</b> <i>regex</i>	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)  Rermit 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 3-128](#) describes the fields shown in the **show sysfs volumes** command display.

**Table 3-128** *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 3-129](#) describes the fields shown in the **show tacacs** command display.

**Table 3-129** 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 3-129 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 3-130](#) describes the fields shown in the **show tcp** command display. This command displays the settings configured with the **tcp** global configuration command.

**Table 3-130** 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 satellite	Configuration status of the TCP satellite connection. Disabled by default.
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.



**Table 3-130** *Field Descriptions for the show tcp Command (continued)*

Field	Description
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]**

<b>Syntax Description</b>	<b>page</b> (Optional) Displays command output page by page.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager
<b>Usage Guidelines</b>	Use the <b>show tech-support</b> command to view system information necessary for Cisco TAC to assist you with a WAAS device. We recommend that you log the output to a disk file. (See the <a href="#">(config) logging console</a> command.)

**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) 1999-2018 by Cisco Systems, Inc.
...
Version: ce510-6.4.3.180

Compiled 18:08:17 Feb 15 2018 by cnbuild

System was restarted on Fri Feb 16 23:09:53 2018.
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-file-systems 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 wecp**  
**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.



### Note

For security reasons, passwords are never displayed in the output of the **show transaction-logging** EXEC command.

**Examples** The following is sample output from the **show transaction-logging** command. It lists information about the current configuration of transaction logging on a WAE.

```
WAAE# show transaction-logging
Flow transaction log configuration:
-----
Flow Logging is disabled.
Flow Archive interval: every-day every 1 hour
Flow Maximum size of archive file: 2000000 KB

Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour
-----
Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour
```

**Related Commands** [clear arp-cache](#)  
[transaction-log](#)



# show user

To display user identification number and username information for a particular user of a WAAS device, use the **show user** EXEC command.

**show user** { **uid** *number* | **username** *name* }

Syntax Description	Parameter	Description
	<b>uid</b> <i>number</i>	Displays user information based on the identification number of the user (0–65535).
	<b>username</b> <i>name</i>	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 3-131](#) describes the fields shown in the **show user** command display.

**Table 3-131** *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 3-132](#) describes the fields shown in the **show users administrative history** command display.

**Table 3-132** 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.
Login details	Day of the week, month, date, time, and whether or not the user is still logged in.

[Table 3-133](#) describes the fields shown in the **show users administrative logged-in** command display.

**Table 3-133** *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.
	<b>pending</b>	(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 3-134](#) describes the fields shown in the **show version** command display.

**Table 3-134 Field Descriptions for the show version Command**

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) <i>year</i> by Cisco Systems, Inc. Cisco Wide Area Application Services (universal-k9) Software Release XXX (build bXXX month day year)	Software application, copyright, release, and build information. Displays universal-k9 for the full software image, accelerator-k9 for the accelerator only software image, and universal-npe-k9 or accelerator-npe-k9 for the NPE versions of those images. The NPE image versions have the disk encryption feature disabled for use in countries where disk encryption is not permitted.
Version	Version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Compiled information for the software build.
Device Id	Hardware device ID.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for	Length of time the system has been running since the last reboot.

# show wccp

To display Web Cache Connection Protocol (WCCP) information for a WAE, use the **show wccp EXEC** command.

**show wccp clients**

**show wccp egress**

**show wccp flows tcp-promiscuous [summary]**

**show wccp masks tcp-promiscuous**

**show wccp routers [detail]**

**show wccp services [detail]**

**show wccp statistics**

**show wccp status**

Syntax	Description
<b>clients</b>	Displays which WAEs are seen by which routers.
<b>egress</b>	Displays WCCP egress methods.
<b>flows</b>	Displays WCCP packet flows. This option is not available on ANCs
<b>tcp-promiscuous</b>	Displays TCP-promiscuous service information.
<b>summary</b>	(Optional) Displays summarized information about TCP-Promiscuous caching service packet flows.
<b>masks</b>	Displays WCCP mask assignments for a given service.
<b>routers</b>	Displays routers seen and not seen by this WAE.
<b>services</b>	Displays WCCP services configured.
<b>detail</b>	(Optional) Displays details of routers or services.
<b>statistics</b>	Displays WCCP generic routing encapsulation packet-related information.
<b>status</b>	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 3-135](#) describes the fields shown in the **show wccp statistics** command display.

**Table 3-135** 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.  <b>Note</b> A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts 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 3-135** 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 3-135** 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 <b>wccp access-list</b> 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: 1/14/2019 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: 1/14/2019 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 3-136](#) describes the fields shown in the **show windows-domain** command display.

**Table 3-136** 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		
	<b>identity</b>	Identity tag of the encryption service.
	<b>identity detail</b>	Identity details including identity tag, account type, account name, domain, realm, status, and match domains.
	<b>blacklist identity</b>	Identity tag, blacklist reason, and domain name.
	<b>status</b>	Service name, configuration state (enabled or disabled), and operational state (running or
	<b>keylist user</b>	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]**

<b>Syntax Description</b>	<b>poweroff</b> (Optional) Turns off the power after closing all applications and operating system.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator 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 3-137](#) describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

**Table 3-137** Description of the shutdown Command Operations

Activity	Process
User performs a shutdown operation on the WAE	Shutdown poweroff WAE# <b>shutdown poweroff</b>
User intervention to bring WAE back online	After a shutdown poweroff, you must press the power button once to bring the WAAS device back online.
File system check	Is <i>not</i> performed after you turn the power on again and reboot the WAAS device.

You can enter the **shutdown EXEC** command from a console session or from a remote session (Telnet or SSH version 2) to shut down a WAAS device.

To shut down a WAAS device, enter the **shutdown EXEC** command as follows:

```
WAE# shutdown
```

When you are asked if you want to save the system configuration, enter **yes**.

```
System configuration has been modified. Save? [yes] :yes
```

When you are asked if you want to proceed with the shutdown, press **Enter** to proceed with the shutdown operation.

```
Device can not be powered on again through software after shutdown.
Proceed with shutdown? [confirm]
```

A message appears, reporting that all services are being shut down on this WAE.

```
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

After the system is shut down (the system has halted), a WAAS software shutdown shell displays the current state of the system (for example, “System has been shut down”) on the console. You are asked whether you want to perform a software power off (the **Power down system by software** option), or if you want to reload the system through the software.

```
===== SHUTDOWN SHELL =====
System has been shut down.
You can either
    Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```



To power down the WAAS device, press and hold the power button on the WAAS device, or use one of the following methods to perform a shutdown poweroff:

- From the console command line, enter **2** when prompted, as follows:

```
===== SHUTDOWN SHELL =====
System has been shut down.
You can either
    Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

- From the WAAS CLI, enter the **shutdown poweroff EXEC** command as follows:

```
WAE# shutdown poweroff
```

When you are asked if you want to save the system configuration, enter **yes**.

```
System configuration has been modified. Save?[yes]:yes
```

When you are asked to confirm your decision, press **Enter**.

```
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

## Examples

The following example shows how to close all applications and stop all system activities using the **shutdown** command:

```
WAE1# shutdown
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

The following example shows how to close all applications, stop all system activities, and then turn off power to the WAAS device using the **shutdown poweroff** command:

```
WAE2# shutdown poweroff
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

# ssh

To allow secure encrypted communications between an untrusted client machine and a WAAS device over an insecure network, use the **ssh** EXEC command.

**ssh options [management]**

<b>Syntax Description</b>	<i>options</i>	Options to use with the <b>ssh</b> EXEC command. Options include the following: <ul style="list-style-type: none"> <li>• 3des-cbc</li> <li>• 3des</li> <li>• blowfish</li> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> <li>• blowfish</li> <li>• blowfish-cbc</li> <li>• des</li> <li>• arcfour</li> <li>• cast128-cbc</li> </ul> <p>For more information about SSH, see <a href="#">RFC 4254</a>. For more information on SSH and ciphers, see <a href="#">RFC 4253</a>.</p>
	<b>management</b>	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. The SSH client accepts both IPv4 and IPv6 addresses.



**Note**

The Telnet daemon can still be used with the WAAS device. SSH does not replace Telnet.

---

**Examples**

The following example shows how to log in to a WAAS device using the SSH client:

```
WAE# ssh 10.11.55.2
```

---

**Related Commands**

[telnet](#)

[\(config\) sshd](#)

[\(config\) ssh-key-generate](#)

# tcpdump

To dump network traffic, use the **tcpdump** EXEC command.

**tcpdump** [*LINE*]

<b>Syntax Description</b>	<i>LINE</i> (Optional) Dump options. For more information see the “Usage Guidelines” section.
---------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Device Modes</b>	application-accelerator central-manager
---------------------	--

<b>Usage Guidelines</b>	TCPdump is a utility that allows a user to intercept and capture packets passing through a network interface, making it useful for troubleshooting network applications.
-------------------------	--



**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 [-aAdDeflLnNOPqRStuUvxxX] [-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](#)  
[tetherreal](#)  
[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

<i>hostname</i>	Hostname of the network device.
<i>ip-address</i>	IP address (IPv4 or IPv6) of the network device.
<i>portnum</i>	(Optional) Port number (1–65535). The default port number is 23.
<b>management</b>	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 <i>length</i>	monitor [disable]
	Sets the length of the display on the terminal (0–512). Setting the length to 0 means there is no pausing.	Copies the debug output to the current terminal.
		(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
<b>aaa</b>	Performs authentication tests for the users trying to access the WAAS Central Manager or WAE.
<b>radius</b>	Uses the RADIUS server for authentication purposes.
<b>tacacs</b>	Uses the TACACS server for authentication purposes.
<b>windows</b>	Uses the Windows domain for authentication purposes.
<i>username</i>	Username for authentication.
<i>password</i>	Password for authentication.
<b>self-diagnostic</b>	Performs self-diagnostics tests.
<b>system</b>	(Optional) Checks the device status, presence of core files, and alarms.
<b>basic</b>	(Optional) Checks the device network configuration.
<b>connectivity</b>	(Optional) Checks if the external hosts required for device operation are reachable by sending ICMP ping packets.
<b>interfaces</b>	(Optional) Checks the operation of physical or virtual interfaces, including ports on the Cisco WAE Inline Network Adapter and Cisco Interface Module.
<b>application-security</b>	(Optional) Checks for potentially malicious (XSS) entries.
<b>tfo</b>	(Optional) Checks the traffic optimization configuration settings and operation. (Applies only to application accelerator devices.)
<b>wccp</b>	(Optional) Checks the WCCP configuration settings and operation. (Applies only to application accelerator devices.)
<b>inline</b>	(Optional) Checks the inline group configuration settings and operation. (Applies only to application accelerator devices that have a Cisco WAE Inline Network Adapter or Cisco Interface Module installed.)
<b>all</b>	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 3-138](#) describes the error messages that can be returned by the **test self-diagnostics** command.

**Table 3-138** 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 3-138** 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.

# tetherreal

To analyze network traffic from the command line, use the **tetherreal** EXEC command.

**tetherreal** [*LINE*]

<b>Syntax Description</b>	<i>LINE</i> (Optional) Options. For more information see the “Usage Guidelines” and “Examples” sections.
<b>Defaults</b>	No default behavior values.
<b>Command Modes</b>	EXEC
<b>Device Modes</b>	application-accelerator central-manager

**Usage Guidelines** Tetherreal 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, Tetherreal also provides facilities for decoding packets.



**Note**

In WAAS version 5.0, Tetherreal 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, tetherreal 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, tetherreal 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 **tetherreal** command:

```
WAE# tetherreal -h
tetherreal: Setting virtual memory limit to 209715200
TShark 1.0.0
Dump and analyze network traffic.
See http://www.wireshark.org for more information.

Copyright 1998-2019 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

<b>-h</b>	Prints help information and exits.
<b>-v</b>	Prints version information and exits.
<b>-c</b>	Displays the command line instead of the command name only.
<b>-i</b>	Suppresses the display of any idle or zombie processes.
<b>-s</b>	Tells top to run in secure mode. This option disables the potentially dangerous interactive commands.
<b>-S</b>	(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.
<b>-d delay</b>	Specifies the delay between screen updates.
<b>-n iterations</b>	Specifies the number of iterations. Update the display this number of times and then exit.
<b>-u user</b>	Monitors only processes with the specified effective UID or username.
<b>-p pid</b>	(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](#)

# tracert

To trace the route between a WAAS device to a remote host, use the **tracert** EXEC command.

```
tracert [management] {hostname | ip-address} [tcp-syn]
```

Syntax Description	management	(Optional) Uses the designated management interface for the tracert.
	<i>hostname</i>	Name of remote host.
	<i>ip-address</i>	IP (v4) address of remote host.
	<b>tcp-syn</b>	(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** Tracert 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. Tracert 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 **tracert** 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# tracert 10.0.0.0

tracert to 10.0.0.0 (10.0.0.0), 30 hops max, 38 byte packets
 1 sblab2-rtr.abc.com (192.168.10.1)  0.959 ms  0.678 ms  0.531 ms
 2 192.168.1.1 (192.168.1.1)  0.665 ms  0.576 ms  0.492 ms
 3 172.24.115.66 (172.24.115.66)  0.757 ms  0.734 ms  0.833 ms
 4 sjc20-sbb5-gw2.abc.com (192.168.180.93)  0.683 ms  0.644 ms  0.544 ms
 5 sjc20-rbb-gw5.abc.com (192.168.180.9)  0.588 ms  0.611 ms  0.569 ms
 6 sjce-rbb-gw1.abc.com (172.16.7.249)  0.746 ms  0.743 ms  0.737 ms
 7 sj-wall-2.abc.com (172.16.7.178)  1.505 ms  1.101 ms  0.802 ms
 8 * * *
 9 * * *
 . . .
```



---

**Related Commands**[ping](#)[ping6](#)[traceroute6](#)[waas-tptrace](#)

# tracert6

To trace the route between a WAAS device to a remote host with an IPv6 address, use the **tracert6** EXEC command.

```
tracert6 [management] {hostname | ip-address}
```

Syntax Description	<b>management</b>	(Optional) Uses the designated management interface for the tracert6.
	<i>hostname</i>	Name of remote host.
	<i>ip-address</i>	IP v6 address of remote host.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Tracert6 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. Tracert6 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 **tracert6** to find the route to a remote host, when either the hostname or the IP address is known.

If a device's management interface is used to trace the route between two end systems using **tracert6** and the management interface goes down, the communication will still succeed if the end device's address is reachable from any other interface.

**Examples** The following example shows how to trace the route between the WAAS device and a device with an IP address of 2013:1:1:2::4:

```
WAE# tracert6 2013:1:1:2::4
tracert6 to 2013:1:1:2::4 (2013:1:1:2::4) from 2013:1:1:10::5, 30 hops max, 24 byte
packets
 1 2013:1:1:10::1 (2013:1:1:10::1) 0.326 ms 0.341 ms 0.313 ms
 2 2013:1:1:1::1 (2013:1:1:1::1) 0.461 ms 0.255 ms 0.277 ms
 3 2013:1:1:2::4 (2013:1:1:2::4) 0.569 ms 0.59 ms 0.389 ms
```

**Related Commands** [ping](#)  
[ping6](#)  
[tracert6](#)  
[waas-tcptrace](#)

# transaction-log

To force the exporting or the archiving of the transaction log, use the **transaction-log EXEC** command.

**transaction-log force { archive | export | flow }**

Syntax Description	archive	Forces the archiving of the transaction log file.
	<b>export</b>	Forces the archived transaction log files to be exported.
	<b>flow</b>	Forces the archiving or exporting of the Traffic Flow Optimization (TFO) transaction log file.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** The following example shows how to force the archiving of the TFO transaction log file on the WAE:

```
WAE# transaction-log force archive flow
```

**Related Commands** [show transaction-logging](#)

# type

To display a file, use the **type** EXEC command.

**type** *filename*

---

<b>Syntax Description</b>	<i>filename</i>	Name of file.
---------------------------	-----------------	---------------

---



---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

---

<b>Command Modes</b>	EXEC
----------------------	------

---

<b>Device Modes</b>	application-accelerator central-manager
---------------------	--

---

<b>Usage Guidelines</b>	Use the <b>type</b> command to display the contents of a file within any file directory on a WAAS device. The <b>type</b> command may be used to monitor features such as transaction logging or system logging (syslog).
-------------------------	---

---

<b>Examples</b>	The following example shows how to display the contents of the <i>syslog.txt</i> file: WAE# <b>type /local1/syslog.txt</b>
-----------------	---

---

<b>Related Commands</b>	<b>cpfile</b> <b>dir</b> <b>lls</b> <b>ls</b> <b>pwd</b> <b>rename</b>
-------------------------	---

# type-tail

To view a specified number of lines of the end of a log file, to view the end of the file continuously as new lines are added to the file, to start at a particular line in the file, or to include or exclude specific lines in the file, use the **type-tail** EXEC command.

```
type-tail filename [line | follow | | {begin LINE | exclude LINE | include LINE}]
```

Syntax Description	
<i>filename</i>	File to be examined.
<i>line</i>	(Optional) Number of lines from the end of the file to be displayed (1–65535).
<b>follow</b>	(Optional) Displays the end of the file continuously as new lines are added to the file.
	(Optional) Displays contents of the file according to the <b>begin</b> , <b>exclude</b> , and <b>include</b> output modifiers.
<b>begin</b> LINE	Identifies the line at which to begin file display. Specifies a regular expression to match in the file.
<b>exclude</b> LINE	Indicates lines that are to be excluded from the file display. Specifies a regular expression to match in the file.
<b>include</b> 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 look for a list of log files in the */local1* directory and then displays the last ten lines of the *syslog.txt* file. In this example, the number of lines to display is not specified, so the default of ten lines is used:

```
WAE# ls /local1
actona
core_dir
crash
```

```

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 dataservert
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get ftp-ov
er-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 dataservert
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] Destinati
o IP [port] = 32.60.43.2 [53775] }returned error: -1 errno 9

```

The following example shows how to follow the *syslog.txt* file as it grows:

```
WAE# type-tail /local1/syslog.txt follow
```

## vm

To initialize the virtual machine after the VMware cloning operation, or to configure the host clock sync setting, use the **vm EXEC** command.

```
vm {{ clock-sync {disable | enable | status} | init }
```

Syntax Description	clock-sync	Manually changes the host clock sync setting.
	<b>disable</b>	Disables VM clock sync to host.
	<b>enable</b>	Enables VM clock sync to host.
	<b>status</b>	Displays the status of the VM clock sync to host setting.
	<b>init</b>	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#
```

■ vm

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	<i>ip-address</i>	IP address of the destination host.
	<i>port</i>	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		
<b>join</b>		Joins a Windows domain.
<b>domain-name</b> <i>domain</i>		Specifies the domain to join.
<b>organization-unit</b> <i>org_unit</i>		(Optional) Specifies the organization unit of the domain.
<b>user</b> <i>username</i>		Specifies a user that has the permission to create a machine account on the domain controller.
<b>debug</b>		(Optional) Logs the domain join operation to the following file: /local1/logs/windows_domain_join.log
<b>leave</b>		Leaves a Windows domain.
<b>diagnostics</b>		Enables the selection of Windows domain diagnostic utilities.
<b>domain-controller</b>		Displays domain controller status information.
<b>list</b>		Displays information about all available domain controllers.
<b>status</b>		Displays the status of the currently joined domain controller.
<b>time</b>		Displays the time of the currently joined domain controller.
<b>domain-name</b> <i>domain_name</i>		(Optional) Displays the time of the domain controller specified.
<b>encryption-service</b>		Displays encryption service status information.
<b>get-key</b> <i>fqdn domain_name</i>		Displays the key retrieval information of the fully qualified domain name (for example, <i>machine-name.cisco.com</i> ) and domain name.
<b>getent</b>		Displays the utility to get unified list of local users, PDC users, and groups.
<b>group</b>		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.
<b>gid</b> <i>gid_no</i>		Displays group-related diagnostics information that corresponds to the group ID number specified.
<b>groupname</b> <i>groupname</i>		Displays group-related diagnostic information of a particular group.
<b>username</b> <i>username</i>		Displays group-related diagnostics information of a user.
<b>machine-account-info</b>		Displays the machine account-related information.

<b>user</b>	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.
<b>sid</b> <i>sid_name</i>	(Optional) Displays the diagnostic information of a user based on the SID of the user specified.
<b>uid</b> <i>user_no</i>	(Optional) Displays the diagnostic information of a user based on the UID specified.
<b>username</b> <i>username</i>	(Optional) Display the diagnostic information of a user on Active Directory based on the username.
<b>verify join</b>	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.

**Note**

When you use the command `windows-domain diagnostics encryption-service get-key user username domain-name domain_name` to configure WAAS as an identity server, you must execute this command two times to ensure that the key retrieval process is complete.

As shown below, the first time you execute this command an in-progress message is displayed, and the second time a completion message is displayed.

```
WAE# windows-domain diagnostics encryption-service get-key user username domain-name domain_name
WAE# Key retrieval in progress.
WAE# windows-domain diagnostics encryption-service get-key user username domain-name domain_name
WAE# The key for the user username is now in the cache.
```

**Examples**

The following example shows how to join a Windows domain and includes the interactive output:

```
WAE# windows-domain join domain-name waaslab.com user Administrator
Joining to AD Domain: WAASLAB.COM
With Computer DNS Name: wae.waaslab.com

administrator@WAASLAB.COM's password:
SUCCESS
```

The following example shows how to leave a Windows domain:

```
WAE# windows-domain leave user myname
```


**Note**


---

In version 5.1.1, although the **windows-domain leave** operation disables the machine account on Active Directory (AD), it does not delete it.

---

The following example shows how to display the options available for the Get Entity utility:

```
WAE# windows-domain diagnostics getent --help
Usage: getent [OPTION...] database [key ...]
getent - get entries from administrative database.

-s, --service=CONFIG      Service configuration to be used
-?, --help                Give this help list
--usage                   Give a short usage message
-V, --version              Print program version
```

Mandatory or optional arguments to long options are also mandatory or optional for any corresponding short options.

Supported databases:  
aliases ethers group hosts netgroup networks passwd protocols rpc  
services shadow

---

Related Commands [\(config\) windows-domain](#)

# write

To save startup configurations on a WAAS device, use the **write EXEC** command.

**write** [**erase** | **memory** | **mib-data** | **terminal**]

Syntax Description		
	<b>erase</b>	(Optional) Erases startup configuration from NVRAM.
	<b>memory</b>	(Optional) Writes the configuration to NVRAM. This is the default location for saving startup information.
	<b>mib-data</b>	(Optional) Saves MIB persistent configuration data to disk.
	<b>terminal</b>	(Optional) Writes the configuration to a terminal session.

**Defaults** The configuration is written to NVRAM by default.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **write** command to either save running configurations to NVRAM or to erase memory configurations. Following a **write erase** command, no configuration is held in memory, and a prompt for configuration specifics occurs after you reboot the WAAS device.

Use the **write terminal** command to display the current running configuration in the terminal session window. The equivalent command is **show running-config**.

**Examples** The following example shows how to save the current startup configuration to memory:

```
WAE# write memory
```

**Related Commands**

- [copy running-config](#)
- [copy startup-config](#)
- [show running-config](#)
- [show startup-config](#)

# zzdebugshell

To enter debug shell mode, use the **zzdebugshell** EXEC command. To exit from the shell environment, use the **exit** command.

**Caution**

---

The **zzdebugshell** command can only be used by Cisco support personnel during a live support session. The **zzdebugshell** command requires both administrative WAAS user credentials and a special authentication token from Cisco TAC personnel. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.

---

---

**Syntax Description**

This command has no arguments or keywords.

---

**Defaults**

No default behavior or values.

---

**Command Modes**

EXEC

---

**Usage Guidelines**

As highlighted in the above Caution note, the **zzdebugshell** command can only be used by Cisco support personnel during a live support session. The **zzdebugshell** command requires both administrative WAAS user credentials and a special authentication token from Cisco TAC personnel. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 23.