CLI Reference Guide

Exinda ExOS Version 6.4

Copyright

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Document Built on Wednesday, November 6, 2013 at 1:02 PM

Using this guide

Before using this guide, become familiar with the Exinda documentation system.

- "Exinda documentation conventions" on page 7
- "Notes, Tips, Examples, and Cautions" on page 2

Notes, Tips, Examples, and Cautions

Throughout the manual the following text styles are used to highlight important points:

- **Notes** include useful features, important issues. They are identified by a light blue background.

  Note Note text

- **Tips** include hints and shortcuts. They are identified by a light blue box.

  Tip Tip text

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a light gray background.

  Example

  Text

- **Cautions** and warnings that can cause damage to the device are included when necessary, and are highlighted in yellow.

  Caution Caution text

Table of Contents

Chapter 1: Using the Command Line Interface

Many of the actions available in the Exinda Web UI can also be executed through the Command Line Interface (CLI).

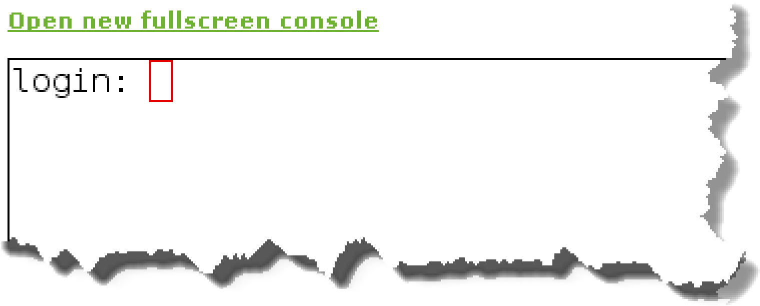
Tips	
	■ Auto complete is available by pressing the tab key after typing the first several letters of a command. Use the tab key to view available options for any of the commands. ■ Use `?` at the end of a command to view available options and descriptions. ■ Command history is available by using the up and down arrow keys. Command line editing is available, using the left and right keys to navigate. ■ Use "ctrl-w" to delete from the cursor to start of line.

Access the Command Line Interface

There are four ways of accessing the Exinda CLI (in order of preference):

1. Secure Shell (SSH) (recommended)
2. Exinda Web UI
3. Telnet
4. Serial Console Interface

Use this tool to connect to the Exinda appliance's Command Line Interface (CLI) from the Web UI. This tool connects to the appliance via the web interface and does not require SSH access.



```
login:
```

1. Click **Tools > Console**.
2. Type the appliance username and password at the prompts.
3. To enter privileged EXEC (enable) mode, at the prompt type the following command:

   ```
   hostname > enable
   ```

   The `hostname #` prompt is displayed.
4. To enter configuration (config) mode, at the prompt type the following commands:

   ```
   hostname # configure terminal
   ```

   The `hostname (config)#` prompt is displayed.

Configure command line options

Configure the command line interface to meet your needs.

1. Use the following command to set the terminal character width and number of lines:

   ```
   hostname (config)# cli session terminal width <number of characters>
   hostname (config)# cli session terminal length <number of lines>
   ```
2. Auto logout is enabled by default. To change the auto logout time use the following command:

   ```
   hostname (config)# cli default auto-logout <minutes>
   ```

   To disable auto-logout, set the minutes to `0`.
3. To enable or disable paging use the following command:

   ```
   hostname (config)# [no] cli default paging enable
   ```
4. Use the `show cli` command to see current CLI settings.
5. To save the running configuration, type `configuration write`.

Exinda documentation conventions

The Exinda documentation uses the following conventions in the documentation.

Graphical interface conventions

The following is a summary of the conventions used for graphic interfaces such as those in the Exinda Web UI and the Central Management Technical Preview UI.

Convention	Definition
bold	Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
Italics	Reference to other documents. For example: Refer to the *Exinda Application List*.
>	Separates navigation elements. For example: Select **File > Save**.

Command line conventions

The following is a summary of the syntax used for the CLI commands.

```
(config)# command <user input> keyword {list|of|options|to|select|from} [optional
parameter]
```

Convention	Definition
`monospace text`	Command line text or file names
<*courier italics*>	Arguments for which you use values appropriate to your environment.
courier bold	Commands and keywords that you enter exactly as shown.
`[x]`	Enclose an optional keyword or argument.
`{x}`	Enclose a required element, such as a keyword or argument.
`|`	Separates choices within an optional or required element.
`[x {y | z}]`	Braces and vertical lines (pipes) within square brackets indicate a required choice within an optional element.
`command with many parameters that wrap onto two lines in the documentation`	Underlined CLI commands may wrap on the page, but should be entered as a single line.

Chapter 2: CLI Commands

Active Directory

To configure Active Directory (AD) settings, use the "active directory" command.

```
active directory {port|renumerate}
```

Set the listen port for the Active Directory daemon.

```
port
renumerate {all|logins|users}
```

To see the status of the active directory:

```
show service add
```

Force the AD services to re-send certain information.

```
all:   Re-fetch the entire list of users/logins.
logins: Re-fetch the entire list of logins from all clients.
users:  Re-fetch the entire list of users from all clients.
```

To manage the Active Directory service, use the "service add" command.

```
service add {stop|start|restart|enable|disable}
```

Start the service

```
start
```

Stop the service

```
stop
```

Restart the service

```
restart
```

Enable the service

```
enable
```

Disable the service

```
disable
```

Adaptive Response

To configure adaptive response settings, use the 'adaptive' command.

```
adaptive {clear|update-time|limit}
clear
```

Reset Adaptive Response network objects - clear all IPs from destination network objects.

```
update-time
```

The time interval that adaptive response evaluates the rules. By default, Adaptive Response evaluates rules every 5 minutes and adds or deletes IP addresses to dynamic network objects according to the defined rules.

```
limit <name> {amount|duration|direction|enable|network-object|except}
```

```
amount <quota>
```

Specify the quota (limit) amount (in MB).

```
duration {daily|weekly|monthly}
```

Specify the quota duration (when the quota resets).

```
direction {both|inbound|outbound}
```

Specify the direction used to count the quota.

```
enable
```

Enable this adaptive response rule.

```
network-object source <src> destination <dst>
```

Specify the source and destination network-objects. Use this command when creating a new Adaptive Response object.

```
except network-object {internal|external} <network object>
```

Specify an internal or external exception Network Object.

Alarms

To configure alarms, use the 'stats' command.

```
stats {alarm|chd|clear-all|export|sample}
```

Configure alarms based on sampled or computed statistics.

```
alarm
```

Configure computed historical data points.

```
chd
```

Clear data for all samples and CHDs, and status for all alarms.

```
clear-all
```

Export statistics to a file.

```
export
```

Configure sampled statistics.

```
sample
```

Example: Enable the interface errors alarm.

```
(config)# stats alarm if_collisions enable
```

APM

To create, modify or remove an Application Performance Metric object use the "apm" command.

To create a new apm object for a specified application:

```
apm <name> metric <metric> application <application>
```

The APM object name.

```
name
```

Specify the traffic that the APM object should monitor by Application.

```
application
```

The Application Performance Metric that this object will monitor.

```
metric
```

The following metrics are available:

network-delay	The time taken for data to traverse the network
server-delay	The time taken for a server to respond to a request
round-trip-time	The time taken for a packet to travel from a device, cross a network and return.
transaction-time	The total time for a transaction (network + server)
bytes-lost	Bytes lost due to retransmissions
tcp-connections-started	The number of TCP connections initiated
tcp-connections-aborted	A TCP connection reset after being established (RST from client or server)
tcp-connections-ignored	A TCP connection that expires in the SYN-SENT state. No response was received from the server.
tcp-connections-refused	A TCP connection that was reset before being established (RST in SYN-SENT state)

Specify an internal and/or external Network Object to filter traffic.

```
apm <name> network-object {internal|external} <network-object>
```

Enable or disable an alert when the metric rises above a configured threshold for a specified delay.

```
[no] apm <name> alert enable
```

Specify the threshold that will trigger an alert.

```
apm <name> threshold <value>
```

Specify the delay. An alert is only generated when the metric remains above the threshold for this length of time.

```
apm <name> delay {60, 300, 1800, 3600, 86400}
```

To create accurate comparisons of the network delay experienced by a transaction, the appliance must analyze packets of the same size (normalized). Specify the number of bytes used to normalize the calculation of the network delay during a transaction. The default value is 1024, and the maximum value is 1048576.

```
monitor apm transaction normalize <value>
```

Disable the normalization calculations

```
monitor apm transaction normalize 0
```

Application Groups

To create a new application group, use the 'application-group' command.

```
[no] application-group <application group name> {application}
```

To enable/disable monitoring of an application group:

```
[no] application-group <application group name> monitor
```

To clear all configuration from an application group (will leave the group empty):

```
application-group <application group name> clear
```

Example: Create an application group called 'Web' and add some applications to it.

```
(config)# application-group Web http
(config)# application-group Web https
(config)# application-group Web http-ALT
(config)# application-group Web squidproxy
```

Applications

To create a new application, use the 'application' command.

```
[no] application <application name> {network-object|port|portrange|protocol-
only|signature}
```

```
network-object <network_object_name>
```

Configure a Network Object to be attached to the application.

```
port <port number> protocol {tcp|udp}
```

Configure a port/protocol for the application.

```
portrange <port_number_low> <port_number_high> protocol {tcp|udp}
```

Configure a port range/protocol for the application.

```
protocol-only <protocol_name>
```

Configure a protocol only Application.

```
signature <l7_signature> [signature_options]
```

Configure a signature for the application. Some L7 signatures have additional options.

```
application <application name> clear
```

Remove all configuration from the application.

Example: Define an application called FTP that uses TCP ports 20 and 21, plus the L7 signature, ftp.

```
(config)# application FTP portrange 20 21 protocol tcp
(config)# application FTP signature ftp
```

APS

To create, modify or remove an Application Performance Score object use the "aps" command. To create a new aps object for a specified application:

```
aps <name> application <application>
```

To Remove an aps object:

```
no aps <name>
```

To set the aps metric thresholds:

```
aps <name> metric {network-delay|network-jitter|network-loss|norm-network-delay|norm-
server-delay|round-trip-time|server-delay} threshold <value>
```

Set the network delay threshold (ms)

```
network-delay threshold <duration (ms)>
```

Set the network-jitter threshold (ms)

```
network-jitter threshold <duration (ms)>
```

Set the network loss threshold in percentage. This is the amount of retransmitted packets (inbound or outbound)

```
network-loss threshold <percent>
```

Set the normalized network delay threshold (ms/kb)

```
norm-network-delay threshold <duration (ms/kb)>
```

Set the normalized server delay threshold (ms)

```
norm-server-delay threshold <duration (ms/kb)>
```

Set the round trip time threshold (ms)

```
round-trip-time threshold <duration (ms)>
```

To restrict traffic to a specific subnet or application server, specify an internal or external Network Object

```
aps <name> network-object {internal|external} <network-object>
```

To create an alarm (SNMP or E-Mail) that will trigger when the aps value falls below a configured value for a specified duration:

```
aps <name> alert threshold <aps-threshold>
```

Set the threshold at which the alarm should trigger. This is a value in the range [0-10].

Enable the alarm. To disable the alarm prefix the command with 'no'.

```
aps <name> alert enable
```

Set the duration (in seconds) for which the aps value should be less then the configured threshold. The values are in seconds (1 minute, 5 minutes, 30 minutes, 1 hour and 1 day)

```
aps <name> alert delay {60,300,1800,3600,86400}
```

To show all aps objects

```
show aps
```

To show details of a specific aps object

```
show aps <name>
```

To enable creating a baseline application performance metric score for an application object

```
aps <name> baseline enable
```

To specify the length of time for used for the baseline

```
aps <name> baseline period <seconds>
```

Acceptable values are 3600 seconds (1 hour), 86400 seconds (1 day), 604800 seconds (1 week).

To disable creating an automatic baseline application performance metric score for an application object

```
no aps <name> baseline
```

To create an APS for an application that sends information between the client and server at arbitrary times (non-transactional), such as Citrix XenApp servers and Microsoft Remote Desktop:

```
aps <name> non-trans-protocol
```

Bridge

The bridge command is used to enable or disable bridges. The interfaces available for a bridge are determined by the appliance model and installed expansion cards. Once enabled, an interface is created for the bridge which can used in other commands (e.g. "interface")

Enable or disable the specified bridge.

```
[no] bridge <bridge> enable
```

Specify the ageing time for this bridge.

```
bridge <bridge> ageing-time <ageing-time>
```

Specify the forwarding time for this bridge.

```
bridge <bridge> forward-time <forward time>
```

Specify the hello time for this bridge.

```
bridge <bridge> hello-time <hello time>
```

Specify the max age for this bridge.

```
bridge <bridge> max-age <max age>
```

Specify the priority for this bridge.

```
bridge <bridge> priority <priority>
```

Enable or disable the Spanning Tree Protocol for this bridge.

```
[no] bridge <bridge> spanning-tree enable
```

To show current bridge configuration use the following command:

```
show bridges
```

Set the bridge interface to provide QoS based on queue mode.

```
(config)# bridge <bridge-name> mq mode [auto-license|multi|single]
```

`auto-license`—Single- or Multi-queue is automatically selected based on the license.

`multi`—QoS uses a multi-queue network interface configuration.

`single`—QoS uses a single-queue network interface configuration.

Specify the bandwidth at which the bridge auto-license mode switches from single-queue to multi-queue.

```
(config)# bridge <bridge-name> mq switch-bandwidth <bandwidth>
```

Bypass

To configure the bypass settings use the bypass command.

```
bypass bridge {all|<bridge_name>} {auto-failover|running|failure}
auto-failover
```

Force the system to switch from the running state to the failure state in the event of a problem.

```
running {active|bypass|no-link}
```

Set the bypass mode for the running (non-failure) state. Bypass pairs can be placed into either active (normal), bypass (fail-to-wire) or no-link (ethernet cables disconnected) state.

```
failure {bypass|no-link}
```

Set the bypass mode for the failure state. Bypass pairs can be placed into either bypass (fail-to-wire) or no-link (ethernet cables disconnected) state.

Note: Depending on the hardware appliance and the type of interface cards installed, fail to wire or bypass settings may be configured globally or per bridge. Not all bypass options are available on all hardware.

To enable/disable the system watchdog (reboot the Exinda appliance in the event of failure), use the watchdog command.

```
[no] watchdog enable
```

Certificates and Keys

To import keys and certificates, use the 'crypto' command.

To import a certificate or key in PEM format - be sure to quote the PEM data:

```
(config)# crypto {certificate|key} import <name> pem data "PEM-DATA"
```

To assign a key to a certificate:

```
(config)# crypto certificate setkey <certificate_name> <key_name>
```

Clustering and HA

Use the "cluster" command to configure clustering.

Configure a Cluster Internal address. Any interface not bound to a bridge or used in another role (e.g. Mirror or WCCP) may be used. This command will need to be run on each node in the cluster, and each with a unique Cluster Internal address.

```
cluster interface <inf>
```

Next, configure the Cluster External address. This command should also be executed on all cluster nodes, using the same Cluster External address.

```
interface <inf> ip address <address> <netmask>
```

The role of the node (master or slave) is show in the CLI prompt as shown below. Once the cluster is up, configuration changes should only be made on the cluster master. Configuration changes made on the master will be sent to slave nodes.

```
exinda-091cf4 [exinda-cluster: master] (config) #
cluster master interface <inf>
cluster master address vip <address> <netmask>
```

Show a brief overview of the current cluster configuration

```
(config)# show cluster global brief
```

Control how data is synchronized between cluster members:

```
(config)# [no] cluster sync {all|acceleration|monitor|optimizer}
```

`all` - Acceleration, monitor and optimizer data are synchronized. This is disabled by default.

`acceleration` - Synchronize acceleration data only

`monitor` - Synchronize monitor data only

`optimizer` - Synchronize optimizer data only

Configure inline appliances to not accelerate any connections, and only perform monitoring:

```
(config)# cluster sync acceleration redirect-only
```

Display the status of all appliances:

```
(config)# show acceleration tcp connections list
```

Community

An Exinda Community is a collection of Exinda appliances in a user's network. Appliances that are part of the same community can accelerate to/from each other.

To configure Community settings, use the "community" command.

```
community {compatibility|delete-db|group|node}
```

To configure the group that this appliance belongs to:

```
community group <number>
```

Community automatically discoverers other appliances within the same group. To manually add remote appliances:

```
community node <name> address <address> port <port>
```

`name` — The name of the remote node (e.g. hostname) `address` — The IPv4 address of the remote appliance

`port` — The port to connect to.

To delete the cache of other community members:

```
community delete-db
```

To enable backward compatibility to allow appliances running ExOS version 6.4.0 and earlier in the same community:

```
community compatibility pre-v6.4.0 enable
```

Backward compatibility is enabled by default.

Configuration

The configuration set of commands are used to manipulate the configuration database. Use these commands to backup, copy, merge and view system configuration.

```
configuration copy <source filename> <destination filename>
```

Make a copy of a configuration file.

```
configuration delete <filename>
```

Delete a configuration file.

```
configuration fetch <URL or scp://username:password@hostname/path/filename>
```

Download a configuration file from a remote host using a HTTP URL or SCP.

```
configuration jump-start
```

Re-run the initial configuration wizard.

```
configuration merge <filename>
```

Merge the common settings from a given configuration file into the running configuration.

```
configuration move <source filename> <destination filename>
```

Move or rename a configuration file.

```
configuration new <filename> factory {keep-basic | keep-connect}
```

Create a new configuration file, specifying optional factory default options.

```
configuration revert
```

Revert the system configuration to a previously saved state.

```
configuration revert saved
```

Revert the running configuration to last saved configuration.

```
configuration switch-to <filename>
```

Load a configuration file and make it the active configuration.

```
configuration text fetch <URL or scp://username:password@hostname/path/filename>
```

Download a text-based configuration file from a remote host

```
configuration text file <filename>
```

Manipulate a stored text-based configuration file

```
configuration text generate {active | file <filename>}
```

Generate a new text-based configuration file from this systems configuration

```
configuration upload <filename> <URL or
scp://username:password@hostname/path/filename>
```

Upload a configuration file to a remote host.

```
configuration upload active <url>
```

Upload the active configuration file to a remote host.

```
configuration write
```

Save the running configuration (same as 'write memory').

```
configuration write local
```

Save the running configuration locally (same as 'write memory local').

```
configuration write to <filename>
```

Save running config to a new file under a different name.

```
show configuration
```

Display CLI commands to recreate the active, saved configuration.

```
show configuration files <filename>
```

Display a list of configuration files, or the contents of one.

```
show configuration full
```

Display commands to recreate the active, saved configuration and do not exclude commands that set default values.

```
show configuration running
```

Display commands to recreate the current running configuration.

```
show configuration running full
```

Display commands to recreate the current running configuration and do not exclude commands that set default values.

```
show configuration text files
```

Display names of available text-based configuration files

crypto

To import keys and certificates, use the 'crypto' command.

To import a certificate or key in PEM format - be sure to quote the PEM data:

```
(config)# crypto {certificate|key} import <name> pem data "PEM-DATA"
```

To assign a key to a certificate:

```
(config)# crypto certificate setkey <certificate_name> <key_name>
```

CSV Reports

To create a new CSV report, use the "report csv" command.

```
(report csv <name> {basic flows|frequency|email}
```

```
no report csv <name>
```

```
basic flows
```

```
Enable reporting of flow records.
```

```
frequency {on-demand|scheduled}
```

```
on-demand {last_60_minutes|last_24_hours|last_7_days|last_30_days|last_12_
months|current_hour|today|this_week|this_month|this_year|last_hour|yesterday|last_
week|last_month|last_year}
```

```
scheduled {hourly|daily|weekly|monthly}
```

```
email <email address>
```

Email address for the scheduled CSV report. Optional for on-demand CSV reports.

Note CSV reports cannot be scheduled to generate hourly.

Example: Create a daily CSV export that emails yesterday's CSV flows to test@exinda.com.

```
(config)# report csv CSV_1>
(config)# report csv CSV_1 basic flows
(config)# report csv CSV_1 email test@exinda.com
(config)# report csv CSV_1 frequency scheduled daily
```

Debug

To generate diagnostic dumps and captures, use the 'debug' command.

```
debug generate {capture|dump}
```

```
dump
```

Generate a systems diagnostic file. This file will be available for download on the Web UI or can be emailed using the "file" command - see below.

```
capture {interface|filter|timeout}
```

```
>interface: Specify an interface to capture.
```

```
>timeout: Specify the timeout (in seconds) that the capture should run for.
```

```
>filter: Specify a filter to apply to the capture.
```

To manipulate generated dumps, use the 'file' command.

```
file {debug-dump|stats|tcpdump}
```

```
debug-dump {delete|email|upload}
```

Manipulate debug dump files.

```
stats {delete|move|upload}
```

Manipulate statistics report files.

```
tcpdump {delete|upload}
```

Manipulate tcpdump output files.

Example: Capture 5 seconds of traffic on Bridge br10, then upload to a server via scp

```
(config) # debug generate capture interface br10 timeout 5
Starting capture... (Press ctrl-c to end capture)
Stopping capture... Generated capture file: capture-exinda-hq-20110405-055920.tar.gz
(config) # file tcpdump upload capture-exinda-hq-20110405-055920.tar.gz \
scp://admin@foo.com/tcpdumps
```

E-Mail

To configure email settings, use the 'email' command.

```
email {auth|autosupport|dead-letter|diag-max-size|domain|mailhub|mailhub-
port|notify|return-addr|return-host|send-test}
auth {enable|password|username}
>enable - Require authentication to send email.
>password - The password used to log into the SMTP server.
>username - The username used to log into the SMTP server.
autosupport enable
```

Set handling of automatic support email.

```
dead-letter
```

Configure the behaviour for undeliverable emails.

```
>email dead-letter enable - Save undeliverable emails as dead.letter
>email dead-letter cleanup max-age 1d2h3m4s - Delete any dead.letter files older than
the specified age. The age format is: #d#h#m#s. For example, 1d2h3m4s or 3d.
>diag-max-size <size in MB>
```

Set the maximum attachment size for diagnostic emails.

```
domain <domain>
```

Override domain from which emails appear to come

```
mailhub <smtp server>
```

Set the mail relay to be used to send emails.

```
mailhub-port <snmtp port>
```

Set mail port to be used to send emails.

```
notify recipient <address> class {failure|info}
```

Set handling of events and failures via email.

```
return-addr <address>
```

Set the username in the return address for email notifications.

```
return-host <hostname>
```

Include hostname in return address for email notifications.

```
send-test
```

Send test email to all configured event and failure recipients.

Factory Default

To perform a factory default, use the "factory default" command.

```
factory default [keep-basic] [keep-connect] [keep-monitor]
```

Note: Network settings will be preserved.

Firmware Update

To install a new firmware use the image command.

```
image {fetch|install|delete|boot next}
```

Download a system image from a URL. Specify 'original' to preserve the original filename once downloaded.

```
fetch <URL or scp://username:password@hostname/path/filename> [original]
```

Install an image file onto a system partition. The name of the downloaded image "webui.img" by default. A reboot is required after the installation is complete.

```
install <image>
```

Delete an inactive system image from the hard disk.

```
delete <image>
```

Tell the appliance to boot from the "next" partition when the appliance is rebooted.

```
(config)# boot system next
```

Hostname

To configure the appliances host name, use the "hostname" command.

```
hostname <hostname>
```

Example: Set the host name of this appliance to "exinda_1".

```
(config) # hostname exinda_1
```

Interface

To configure an interface address and other IP networking settings, use the "interface" command.

Note 1 : To set global IP network settings (e.g. default gateway) use the "ip" command.

Note 2: To configure a role for an interface (e.g. Cluster, Mirror or WCCP) use associated role command (cluster, mirror or wccp)

Note 3: To configure bridge settings, use the "bridge" command.

```
[no] interface <inf> ip address <IPv4 addr> <netmask>
```

Add or remove an IPv4 address and netmask for the specified interface. The netmask can be in dotted quad format (e.g. 255.255.255.0) or a netmask length after a slash (e.g. /24)

```
[no] interface <inf> ipv6 address <IPv6 addr>/<len>
```

Add or remove an IPv6 address for the specified interface (e.g. 2001:db8:1234::5678/64)

```
[no] interface <inf> ipv6 enable
```

Enable or disable IPv6 on the specified interface.

```
[no] interface <inf> ipv6 address autoconfig [default | privacy]
```

Enable or disable IPv6 stateless address autoconfiguration (SLAAC) on the specified interface. The default option enables learning default routes. The privacy option enables autoconfiguration privacy extensions.

```
interface <inf> dhcp
```

Enable DHCP on the specified interface.

```
interface <inf> dhcp renew
```

Renew DHCP on the specified interface.

```
interface <inf> alias <alias index> ip <IPv4 addr>
```

Configure an IPv4 alias on the specified interface.

```
interface <inf> comment <comment>
```

Add a comment to this interface.

```
interface <inf> duplex {half|full|auto}
```

Configure the duplex of this interface.

```
interface <inf> mtu <mtu>
```

Configure the MTU of this interface .

```
interface <inf> shutdown
```

Disable this interface.

```
interface <inf> speed {10|100|1000|auto}
```

Configure the speed of this interface. Available options are 10,100,1000 and auto.

Example 1: Set the speed and duplex interface settings for eth2.

```
(config) # interface eth2 speed 100
(config) # interface eth2 duplex full
```

The following commands can be used to show interface running state and configuration:

```
show interfaces [<inf>]
```

Displays detailed information about the running state for all interfaces (or a specified interface).

```
show interfaces brief
```

Displays a brief running running state for all interfaces.

```
show interfaces configured
```

Displays the current configuration for all interfaces.

```
show interfaces summary
```

Displays a summary of the running state for all interfaces, including bridge and role information.

IP

To configure IP network settings use the "ip" command.

Note: To configure interface specific settings (e.g. address or speed/duplex/mtu) use the "interface" command.

Note: Use the "ipv6" command to change IPv6 settings.

```
ip default-gateway <IPv4 address>
```

Configure a default IPv4 gateway.

```
ip name-server <IPv4 or IPv6 address>
```

Configure a DNS server.

```
ip neighbour size <size>
```

Configure the kernel neighbour table size.

```
ip map-hostname
```

Ensure a static host mapping for the current hostname.

```
ip domain-list
```

Add a domain name to use when resolving hostnames.

```
ip route <network prefix> <netmask> <next hop IP address or interface name>
```

Add a static IPv4 route.

```
ip dhcp
```

Configure global DHCP settings.

```
ip dhcp default-gateway yeild-to-static
```

Do not install a default gateway from DHCP if there is already a statically configured one

```
ip dhcp send-hostname
```

Allow the DHCP client to send a hostname during negotiation

```
ip dhcp hostname <hostname>
```

Specify the hostname the DHCP will send during negotiation (if send-hostname is enabled)

```
ip dhcp primary-intf <interface>
```

Set the interface from which non-interface-specific configuration (resolver, routes) will be accepted from DHCP

```
ip flow-export
```

Configure netflow export. See Netflow

Example: Configure eth1 with address 192.168.0.98 /24, gateway 192.168.0.1 and Bridge br1 enabled

```
(config)# interface eth1 ip address 192.168.0.98 /24
(config)# ip default-gateway 192.168.0.1
(config)# bridge br1 enable
```

Example: Enable IPv6 autoconfig (SLAAC) on interface eth1

```
(config)# interface eth1 ipv6 address autoconfig
```

Example: Configure a DNS server

```
(config) # ip name-server 192.168.0.1
```

IPMI

The IPMI commands configure access to the appliances baseboard management controller (BMC). When access is configured, an IPMI client may be used to remote power on / off the appliance, query sensors and access the serial-over-lan console.

```
[no] ipmi enable
```

Enable or disable IPMI access.

```
[no] ipmi ip address <IPv4 address> <netmask>
[no] ipmi ip default-gateway <IPv4 address>
```

Configure a static IPMI IPv4 address, netmask and default gateway. A netmask can be specified in long (e.g. 255.255.254.0) or short (e.g /23) format. If no netmask is specified a default of /24 is used.

```
[no] ipmi dhcp
```

Enable or disable DHCP on the IPMI interface.

```
ipmi username <user> password <password>
```

Configure IPMI authentication.

```
[no] ipmi sel enable
```

Enable or disable sending BMC System Event Log (SEL) events to the appliance log.

```
[no] ipmi seltime enable
```

Enable or disable synchronising SEL time with the appliance on startup.

To show the current IPMI configuration use the following command:

```
show ipmi
```

To control the power of a remote appliance which has enabled IPMI access as above, use the "ipmi power" command.

```
ipmi power address <address> username <username> password <password> \
 control {on|off|cycle|reset|status}


on: Power on the chassis
off: Power off the chassis - no clean shutdown of the OS
cycle: Power off for a minimum of 1 second, and then power on
```

```
reset: Hard reset of the appliance
status: Display the power status of the chassis
```

IPv6

To configure IPv6 specific settings, use the "ipv6" command.

```
[no] ipv6 enable
```

Enable or disable IPv6 for the entire system.

```
[no] ipv6 default-gateway <IPv6 address or interface>
```

Add or remove an IPv6 default gateway.

```
[no] ipv6 route <network prefix> <next hop IPv6 address or interface>
```

Add or remove an IPv6 static route.

```
[no] ipv6 host <hostname> <IPv6 address>
```

Add or remove a static hostname/IPv6 address mapping

```
[no] ipv6 map-hostname
```

Add or remove a static IPv6 hostname mapping for the current hostname.

```
[no] ipv6 neighbor <IPv6 address> <interface> <MAC address>
```

Configure a static IPv6 neighbor MAC (link layer) address mapping.

LDAP

LDAP authentication allows you to configure the Exinda appliance to authenticate user login attempts with a remote LDAP (including Active Directory) server.

```
(config) # ldap {base-dn|bind-dn|bind-password|group-attribute|group-dn|host|login-
attribute|port|referrals|scope|ssl|timeout-bind|timeout-search|version}
```

Configure the LDAP user search base.

```
(config) # ldap base-dn <string>
```

Configure the DN (distinguished name) to bind to the server.

```
(config) # ldap bind-dn <string>
```

Specify the password for bind DN.

```
(config) # ldap base-dn <string>
```

Specify the name of the group membership attribute.

```
(config) # ldap group-attribute {<string>|member|uniqueMember}
```

Specify the DN of the group required for authentication.

```
(config) # ldap group-dn <string>
```

Specify the hostname or IP address of the LDAP server. IPv4 and IPv6 addresses can be used.

```
(config) # ldap host <hostname or IP address>
```

Specify the attribute that contains the login name.

```
(config) # ldap login-attribute {<string>|uid|sAMAccountName}
```

Specify the port of the LDAP server.

```
(config) # ldap port
```

Enable LDAP referrals.

```
(config) # ldap referrals
```

Specify whether the scope of the LDAP search is the object's immediate children (`one-level`) or all descendants (`subtree`).

```
(config) # ldap scope {one-level|subtree}
```

Configure the SSL and TSL settings.

```
(config) # ldap ssl {cert-verify|mode|ssl-port}
```

Specify the number of seconds before LDAP times out for binding to a server.

```
(config) # ldap timeout-bind <seconds>
```

Specify the number of seconds before a search for user infomation on the LDAP server times out.

```
(config) # ldap timeout-search <seconds>
```

Configure the version of LDAP that is supported.

```
(config) # ldap version {2|3}
```

License

To show currently installed licenses use the following command:

```
show licences
```

Use the "license" command to add, delete or change the auto license feature:

```
license {fetch|install|delete|auto}
```

```
fetch
```

Download and install the latest license key over the Internet from the Exinda licensing server.

```
install <license key>
```

Install a new license.

```
delete <license id>
```

Delete an existing license. Licenses are identified by their ID which can be found with the "show licenses" command.

```
[no] auto enable
```

Enable or disable the auto-license feature. When enabled, the appliance will automatically fetch and install any new available licenses. It checks every 24 hours and is enabled by default.

Link State Mirroring

Use the following commands to configure link state mirroring. If link state mirroring is enabled bridge port states will be synchronized. For example, if one port is link down the other port will be manually forced into the link down state.

If link state mirroring is enabled it applies to all bridge interfaces.

To enable or disable link state mirroring:

```
[no] link-state enable
```

To set the delay in ms before an interface is forced into the down state:

```
link-state down-delay <duration_ms>
```

To set the delay in ms before a link is returned to the up state:

```
link-state up-delay <duration_ms>
```

To show the current link state configuration:

```
show link-state
```

Logging

Configure logging parameters and show the system logs. The appliance will log what it is doing to a set of files.

View the complete log file.

```
(config)# show log
```

View the log file as it gets updated.

```
(config)# show log continuous
```

View new log messages that match a given regular expression.

```
(config)# show log continuous {matching|not matching} <regex>
```

View the contents of the current log file based on a regular expression.

```
(config)# show log {matching|not matching} <regex>
```

View the contents of a saved log file.

```
(config)# show log files <file>
```

View the contents of the file based on the regular expression.

```
(config)# show log files <file> {matching| not matching} <regex>
```

Rotate log files on a fixed time-based schedule.

```
(config)# logging files rotation criteria frequency {daily|weekly|monthly}
```

Rotate log files when they pass a size threshold.

```
(config)# logging files rotation criteria size <megabytes>
```

Rotate logs when they surpass a specified percentage of disk.

```
(config)# logging files rotation criteria size-pct <percentage>
```

Specify the maximum number of old log files to keep.

```
(config)# logging files rotation max-num <number>
```

Delete log files.

```
(config)# logging files delete {current|oldest}
```

Specify minimum severity level for this class.

```
(config)# logging local override class <class> priority
```

Allow syslog messages to be received from remote hosts.

```
(config)# logging receive
```

Include the number of seconds since the epoch in the logs.

```
(config)# logging fields seconds {enable|fractional-digits|whole-digits}
```

Select the format of the log files.

```
(config)# logging format {standard|welf}
```

Select the severity of log entries recorded for select CLI commands

```
(config)# logging level cli commands
{none|emerg|alert|crit|err|warning|notice|info|debug}
```

Specify the hostname or IP address of a remote syslog server to send log files to.

```
(config)# logging <hostname or IPv4 address>
```

Set the minimum severity of log messages sent to syslog servers.

```
(config)# logging trap {none|emerg|alert|crit|err|warning|notice|info|debug}
```

Example: Show log messages containing the string 'httpd'.

```
(config)# show log continuous matching httpd
```

MAPI

Accelerate email traffic being sent to and from a Microsoft Exchange server.

Enable MAPI acceleration.

```
acceleration mapi enable
```

Disable MAPI acceleration.

```
no acceleration mapi enable
```

Display the state of MAPI acceleration.

```
show acceleration mapi
```

Display MAPI acceleration configuration.

```
show acceleration mapi config
```

Accelerate MAPI traffic using only basic header marking. With basic header marking, only the top level RPC header of each message is ignored when the traffic is accelerated. When basic header marking is enabled, performance is good, but there is less reduction in MAPI traffic.

```
acceleration mapi basic-header-marking-only
```

Disables acceleration of MAPI traffic using only basic header marking. With basic header marking disabled, performance is slower, but provides better reduction by decoding lower levels of the protocol. This is the default setting.

```
no acceleration mapi basic-header-marking-only
```

Mirror

```
[no] mirror interface <inf>
```

Assign an interface to use as a mirror port. Mirror ports are typically used in Clustered environments.

More information can be found in the Topologies Guide.

Monitor

To configure monitoring settings, use the "monitor" command.

```
(config) # monitor {apm|bit-torrent|clear|display|edonkey|host-resolution|ignore-
internal|layer7|linklocal|openvpn|sensitivity|skype}
```

Display the monitoring configuration:

```
(config) # show monitor setup
```

Display the diagnostic configuration, such as graphing format, Layer 7 monitoring, host resolution, and monitoring database status:

```
(config) # show monitor diagnostics
```

To create accurate comparisons of the network delay experienced by a transaction, the appliance must analyze packets of the same size (normalized). Specify the number of bytes used to normalize the calculation of the network delay during a transaction. The default value is 1024, and the maximum value is 1048576.

```
(config) # monitor apm transaction normalize <value>
```

Set bit-torrent monitoring sensitivity.

```
(config) # monitor bit-torrent {high|med|low}
```

Clear monitoring data.

```
(config) # monitor clear
{all|apm|appliance|appsubnet|aps|interface|monitor|network|optimizer|reduction|sla}
```

Adjust various monitoring display settings.

```
(config) # monitor display {chart-size|graphing|real-time|sort-subnets-by-name|subnet-
pie|show-app-by-subnet-other|table-size|url-size}
```

`chart-size`: Number of chart items. Acceptable values are 1-10.

`graphing`: Flash or non-flash.

`real-time`: Default real-time window refresh time interval. Available values are 10, 20, 30, 40, 50, 60 seconds.

`sort-subnets-by-name`: Subnet names included in reports are sorted by name.

`subnet-pie`: Display the applications per subnet chart as a pie chart.

`show-app-by-subnet-other`: Display the remaining application traffic, that is, all traffic minus the top applications, on the applications for a subnet chart when displayed as a time series chart.

`table-size`: Number of lines of data displayed in report tables. Acceptable values are 1-1000.

`url-size`: Limit the number of characters used when displaying a URL.

Display the applications per subnet chart as a time series chart.

```
(config) # no monitor display subnet-pie
```

Display only the top applications (don't show the remaining application traffic) on the applications for a subnet time series chart.

```
(config) # no monitor display show-app-by-subnet-other
```

Set eDonkey monitoring sensitivity.

```
(config) # monitor edonkey {high|med|low}
```

Set host resolution method. Rank from 1-4.

```
(config) # monitor host-resolution {DNS|IP|Netbios|Network_Object}
```

Enable ignore internal to internal traffic.

```
(config) # monitor ignore-internal
```

Enable layer7 monitoring.

```
(config) # monitor layer7
```

Enable IPv6 link local traffic monitoring.

```
(config) # monitor linklocal
```

Specify the sensitivity of the openvpn traffic monitoring.

```
(config) # monitor openvpn sensitivity [aggressive|safe]
```

Set monitoring sensitivity. Acceptable values are 1-10, with 10 being the lowest sensitivity.

```
(config) # monitor sensitivity <sensitivity>
```

Set Skype monitoring sensitivity.

```
(config) # monitor skype {high|med}
```

To configure Application Specific Analysis Modules (ASAM) settings, use the `asam` command. This command enables/disables drill-down monitoring capabilities for the specified application.

```
(config) # [no] asam {anonymousproxy|apm|asymm-
route|citrix|dcerpc|http|ssl|urllog|voip} enable
```

Disable collecting statistics for applications by network objects or subnets.

```
(config) # no monitor statistics network-object-application enable
```

Enable collecting statistics for applications by network objects or subnets.

```
(config) # monitor statistics network-object-application enable
```

Netflow

Netflow allows the Exinda appliance to export flow records to 3rd party applications. Use the following CLI commands to configure netflow export.

To set the destination address and port (UDP) of the device that will receive netflow records:

```
ip flow-export destination <IPv4 address> <udp-port>
```

To configure which information is sent:

```
[no] ip flow-export export {application|aps|bytes-long|direction|extra-info|
 interfaces|lost-bytes|network-delay|network-jitter|output-counts|
 packets-long|packets-size|payload-size|policy|rtt|server-delay|tos|
 traffic-class|ttl|usernames|vlan|voip}
```

```
application
```

Application identification

```
aps
```

aps score

```
bytes-long
```

Use 64 bit values for byte counters

```
direction
```

Flow direction (inbound|outbound)

```
extra-info
```

Extra details (e.g. hostnames, codecs)

```
interfaces
```

SNMP input and output interfaces

```
lost-bytes
```

Lost bytes count

```
network-delay
```

aps network delay

```
network-jitter
```

aps network-jitter

```
output-counts
```

packet and byte counts

```
packets-long
```

Use 64 bits for packet counters

```
packets-size
```

Minimum and maximum packet sizes

```
payload-size
```

Set the maximum netflow packet payload size in bytes.

```
policy
```

policy identification

```
rtt
```

Round trip time

```
server-delay
```

aps server delay

```
tos
```

minimum and maximum TOS

```
traffic-class
```

traffic class

```
ttl
```

minimum and maximum TTL

```
usernames
```

Username details (see Active Directory and Static Users)

```
vlan
```

VLAN identifier

```
voip
```

Voice over IP details

To control refresh settings for export of options:

```
ip flow-export options {refresh-rate|timeout-rate|usernames}
refresh-rate <packet_count>
```

Sets the maximum number of packets allowed between options export

```
timeout-rate <duration_sec>
```

Sets the maximum number of seconds between options export

```
usernames expiry-rate <duration_hours>
```

Set the maximum number of hours to remember inactive usernames

```
usernames timeout-rate <duration_min>
```

Set the maximum number of minutes between export of username options

To control refresh settings for export of templates:

```
ip flow-export template {refresh-rate|timeout-rate}
refresh-rate <packet_count>
```

Set the maximum number of packets before template export

```
timeout-rate <duration_sec>
```

Set the maximum number of seconds before template export

To control how often netflow records are exported:

```
ip flow-export timeout active
```

```
active <duration_min>
```

How often to export active flow information

To show the current flow-export settings:

```
show ip flow-export config
```

To show currently configured netflow destinations:

```
show ip flow-export collectors
```

To show netflow template details

```
show ip flow-export templates {appid|appgroupid|appgroups|ipv4|ipv4voip|ipv4aps}
```

Network Objects

To create a new network object or modify the properties of an existing network object use the 'network-object' command.

```
[no] network-object <name> subnet <IPv4 or IPv6 address> <dotted quad mask (IPv4) or
mask length (IPv4 or IPv6)>
```

Add or remove a subnet to a network object. This command creates a network object if it does not already exist.

To remove a network object:

```
no network-object <name>
```

To set the the location of the network object with respect to the appliance

```
network-object <name> location {internal, external, inherit}
```

```
internal
```

Specify that IP addresses in this network object are on the internal (LAN) side of the appliance

```
external
```

Specify that IP addresses in this network object are on the external (WAN) side of the appliance.

```
inherit
```

Specify that the location is automatically generated from existing network objects. For example if all subnets fall within an existing network object that is has a location of internal, this network object will also be internal.

```
network-object <name> subnet-report
```

Specify that this network object should be included in subnet reports.

Example: Create a network object called 'localServer' that is an internal host on 192.168.1.1/255.255.255.255, and enable subnet reporting:

```
(config) # network-object localServer subnet 192.168.1.1 /32
(config) # network-object localServer location internal
(config) # network-object localServer subnet-report
```

Example: Create an network object called 'IPv6 Server' that is an external host on 2001:db8::1234:5678/128

```
(config)# network-object "IPv6 Server" subnet 2001:db8::1234:5678 /128
```

```
(config)# network-object "IPv6 Server" location external
```

NTP

To enable a NTP server, use the "ntp" command.

```
(config)# ntp {sever|enable|disable}
```

Configure an NTP server.

```
(config)# server <hostname or IPv4 address> [version <ntp version>]
```

Enable NTP time synchronization.

```
(config)# ntp enable
```

Disable NTP time synchronization.

```
(config)# ntp disable
```

PBR

Configure the appliance with Policy Based Routing (PBR) so an Exinda appliance can be inserted in the network out-of-path, but retain in-path optimization capabilities

Specify the IP address to send the traffic to after it arrives at the interface.

```
(config)# pbr interface <interface-name> ip next-hop <ip-address>
```

Set the PBR interface to provide QoS based on queue mode.

```
(config)# pbr interface <interface-name> mq mode [auto-license|multi|single]
```

`auto-license`—Single- or Multi-queue is automatically selected based on the license.

`multi`—QoS uses a multi-queue network interface configuration.

`single`—QoS uses a single-queue network interface configuration.

Specify the bandwidth at which the PBR interface auto-license mode switches from single-queue to multi-queue

```
(config)# pbr interface <interface-name> mq switch-bandwidth <bandwidth>
```

Display the parameters of the PBR interface configurations.

```
(config)# show pbr
```

PDF Reports

To create a new PDF report, use the "report pdf" command.

```
(config)# report pdf <name> {basic|custom|detailed|email|email-
report|frequency|netpercentile|password|vc-axis-unit}
```

```
(config)# no report pdf <name>
```

```
(config)# report pdf <name> basic {aps|network|tcp|health|sla|subnets|edge-
cache|voip|prioritization|flows}
```

`aps` — Include APS reports.

`network` — Include Network reports.

`tcp` — Include TCP efficiency reports.

`health` — Include TCP health reports.

`sla` — Include SLA reports.

`subnets` — Include Subnets reports.

`edge-cache` — Include Edge Cache reports.

`prioritization` — Include Prioritization Ratio reports.

`flows` — Include Flow reports.

```
(config)# detailed {appliance|interface|peer|pps|subnet|vcircuit}
```

Include and configure the Appliance statistics report.

```
(config)# appliance {aa_connection|connection|cpu_usage|cpu_temperature|memory_
usage|swap_usage|diskio}
```

Include and configure the Interface report.

```
(config)# interface {ALL|<interface>)
```

Include and configure the WAN Memory report.

```
(config)# peer {all|<peer name>}
```

Include and configure the PPS report.

```
(config)# pps {ALL|<interface>)
```

Include and configure the Subnet report.

```
(config)# subnet <subnet name> {application|host|conversation|url|user}
```

Include and configure the Virtual Circuit report.

```
(config)# vcircuit <vc name> {discard|optimizer}
```

Set the percentile line displayed in the report.

```
(config)# report pdf <report-name> netpercentile {none|70|75|80|85|90|95}
```

Set the virtual circuit axis unit that is applied to report documents.

```
(config)# report pdf <report-name> vc-axis-unit {Bytes|Percent}
```

Specify a start and end date/time for the custom, on-demand report. Time format is YYYY/MM/DD HH.

```
frequency {on-demand|scheduled}

on-demand {last_60_minutes|last_24_hours|last_7_days|last_30_days|last_12_
months|current_hour|today|this_week|this_month|this_year|last_hour|yesterday|last_
week|last_month|last_year|custom}

scheduled {hourly|daily|weekly|monthly|custom_daily|custom_weekly|custom_monthly}

custom {start <tim>|end <time>}
```

Email address for the scheduled CSV report. Optional for on-demand CSV reports.

```
(config)# report pdf <name> email <email address>
```

PDF reports that have an email address configured can generate and email the report on-demand. Reports scheduled to be generated hourly or reports for the last hour cannot be emailed on-demand.

```
(config)# report pdf <name> email-report
```

The PDF file will be password protected if this field is set.

```
(config)# report pdf <name> password <password>
```

Generate detailed interface statistic reports for WCCP or a policy-based routing interface (for example, `eth2`).

```
(config)# report pdf <report-name> detailed interface WCCP
(config)# report pdf <report-name> detailed interface eth2
```

Generate detailed PPS statistics reports for WCCP or a policy-based routing interface (for example, `eth2`).

```
(config)# report pdf <report-name> detailed pps WCCP
(config)# report pdf <report-name> detailed pps eth2
```

Example: Create a custom time-range PDF report.

```
(config)# report pdf Custom
(config)# report pdf Custom basic aps
(config)# report pdf Custom basic network
(config)# report pdf Custom basic sla
(config)# report pdf Custom basic subnets
(config)# report pdf Custom detailed appliance connection
(config)# report pdf Custom detailed appliance cpu_temperature
(config)# report pdf Custom detailed appliance cpu_usage
(config)# report pdf Custom detailed appliance memory_usage
(config)# report pdf Custom detailed appliance swap_usage
(config)# report pdf Custom detailed interface ALL
(config)# report pdf Custom detailed interface eth11
(config)# report pdf Custom detailed pps ALL
(config)# report pdf Custom detailed pps br10
(config)# report pdf Custom detailed subnet ALL application
(config)# report pdf Custom detailed subnet ALL conversation
(config)# report pdf Custom detailed subnet ALL host
(config)# report pdf Custom detailed subnet ALL url
(config)# report pdf Custom detailed subnet ALL user
(config)# report pdf Custom detailed vcircuit ALL discard
(config)# report pdf Custom detailed vcircuit ALL optimizer
(config)# report pdf Custom frequency on-demand custom
(config)# report pdf Custom custom end "2009/08/28 19"
(config)# report pdf Custom custom start "2009/01/08 01"
```

Processes

To view information on a running process or service, use the "show pm process" command.

Example: Show the status of the collectord service.

```
(config) # show pm process collectord
Process collectord
```

```
Configuration:
Launchable:  yes
Auto-launch:  yes
Auto-relaunch:  yes
Launch path:  /opt/tms/bin/collectord
Re-exec path:  (none)
Argv:  /opt/tms/bin/collectord
      Max snapshots:   10
      Launch order:    0
Launch timeout:  0
Shutdown order:  0
CPU Affinity:  (not set)
Test liveness:  no
Hung count:  4

State:
Current status:  running
PID:  3489
Num. failures:  0
Last launched:  2011/04/04 10:40:20.949 (1 day 0 hr 26 min 28.079 sec ago)
Last terminated:
Next launch:
```

To view CPU and memory use of all processes, use the "show processes" command.

```
show processes [{limit|sort|threads}]
limit <lines>
```

Show processes, limit the number of lines displayed. Use this to generate a "top N" style display. The default sort order is CPU usage.

```
sort {cpu|memory|time}
```

Sort processes by CPU usage, memory (RSS as a percentage of total) or process time.

```
threads
```

Show process threads

Example: Show the top 5 processes by CPU usage.

```
(config) # show processes sort cpu limit 5
User        Memory Usage (kB)    %CPU %Memory S  Time     Process
         Virtual Resident Shared
-------- ------- -------- ------ ---- ------- - --------- --------------
```

```
admin    616m     341m   110m  4.0     8.8 S   7:25.02 collectord
admin       0        0      0  2.0     0.0 S   6:33.50 kipmi0
admin   73996      10m   8564  2.0     0.3 S   7:28.65 communityd
admin   61192     9496   6884  2.0     0.2 S   0:19.68 slad
admin       0        0      0  2.0     0.0 S   0:14.80 kworker/u:1
```

Protocols

To create a new protocol, use the "protocol" command.

```
protocol <protocol name> number <protocol number>
```

no protocol <protocol name>

Example: Create a protocol for ICMP with protocol number 1.

```
(config) # protocol icmp number 1
```

Radius

Radius authentication allows you to configure the Exinda appliance to authenticate user login attempts with a remote Radius server.

```
(config) # radius-server {host|key|retransmit|timeout}
```

Specify the hostname or IP address of the Radius server. IPv4 addresses can be used.

```
(config) # radius-server host <hostname or IP address>
```

Specify the key for accessing the Radius server.

```
(config) # radius-server key <key string>
```

Specify how often authentication requests should be retransmitted to the Radius server.

```
(config) # radius-server retransmit <retries>
```

Specify how many seconds before the connection to the Radius server times out.

```
(config) # radius-server timeout <seconds>
```

Real Time

To display a real-time breakdown of Application Performance Metrics (APM):

```
show realtime apm applications : Shows the application response metrics.
```

This includes RTT, network delay, server delay, and transaction delay.

```
show realtime apm hosts : Shows the TCP connection health details.
 This includes retransmitted bytes, aborted connections, refused connections,
 and ignored connections.
```

To display a real-time breakdown of application traffic:

```
show realtime appplications direction [inbound|outbound|both] limit <number-of-flows>
```

To display a breakdown of the real-time inbound and outbound conversations:

```
show realtime conversations
```

Options for show realtime conversations include:

```
>aatype : Indicates if the connection was processed by TCP Acceleration, Edge Cache or
was not accelerated.
>direction [inbound|outbound|both] : Filter which direction is show
>group : Group conversations that are the same application between the same hosts
>limit <number> : Limit output to the top <number> flows
>show-policies : Include details on which policy each flow is falling into
>users : Include details on the user assigned to each IP address
```

To display a breakdown of realtime connections, summarized by IP address.

```
show realtime hosts direction [inbound|outbound|both] limit <number-of-flows>
```

To display a list of all asymmetrical connections:

```
show monitor asymmetric-route
```

Reboot and Shutdown

To reboot the appliance use the reload command.

```
reload {force|halt|mode|noconfirm}
force
```

Force an immediate reboot of the system even if it's busy.

```
halt
```

Shut down (power off) the system.

```
mode {kexec|bios|biosnext}
>kexec: Fast rebooting with kexec (skips the BIOS).
>bios: Slow rebooting via the BIOS (traditional reboot).
>biosnext: Slow rebooting via the BIOS (for the next boot only).
noconfirm
```

Reboot the system without asking about unsaved changes.

Schedules

Schedule objects define a time range - they can be used to enable Optimizer policies at different times e.g. Work Hours / After Hours. To create a new schedule, use the 'schedule' command.

```
schedule <name> days <start day> <end day> times <start time> <end time>
no schedule <name>
```

```
days
```

The schedule period (days) - specify a range of days.

```
times
```

The schedule period (time) - specify a range of hours.

Example: Create an 'After Hours' schedule that includes 6pm to 8am, Monday to Friday and all day Saturday and Sunday.

```
(config) # schedule "After Hours" days Monday Friday times 1800 2400
(config) # schedule "After Hours" days Monday Friday times 0000 0800
(config) # schedule "After Hours" days Saturday Saturday times 0000 2400
```

SDP

To enable and configure the SDP service, use the 'sdp' command.

```
sdp {address|enable|verify}
```

```
address <sdp ip or fqdn>
```

Set the SDP server address.

```
enable
```

Enable the SDP service.

```
verify
```

Enable SDP verify certificate.

To restart the SDP service:

```
service sdp restart
```

To show the SDP service running status

```
show service sdp
```

Serial Console Speed

The following table details the effect of the serial speed on the parts of the system that use the serial console. The speed in the table is the configured speed, or the default speed if it has never been configured. The 6062, 8062, and 10062 appliances have a default serial console speed of 115200. All order hardware has a default serial speed of 9600.

Item	Speed	Notes
BIOS	n/a	If a serial console is connected at boot time the BIOS output will adjust to match the serial speed. If no serial port is connected at boot time it will use the default speed for the model.
Boot menu	9600 or 115200	The boot menu will operate at the configured baud rate.

Item	Speed	Notes
Kernel log messages	9600 or 115200	The kernel log messages will operate at the configured baud rate.
Login	9600	The serial port will operate at 9600 baud.
Login	115200	The serial port will operate at 115200 baud. However if a serial console at 9600 baud is connected while at the login prompt, and any key pressed, the serial login prompt will switch to 9600 baud. It will remain at 9600 baud until the user logs out and the login prompt is presented once again.

Caution It is recommended that the serial console speed be set to 9600 baud before downgrading to a version of firmware prior to version 6.3.8 as those versions do not fully support the serial console speed of 115200.

To view the currently configured serial console speed, and the default speed for that model of Exinda appliance:

```
(config) # show serial
```

To change the serial console speed

```
(config) # serial speed [9600|115200]
```

After changing the serial console speed, you must reboot the appliance to ensure that all areas of the system recognize the new speed.

SLA

To create, modify or remove an SLA object, use the "sla" command.

```
sla <sla object name> {destinationip|duration|enable|pingsize}
```

```
no sla <sla object name>
```

```
destinationip <address>
```

Specify the IP address to ping.

```
threshold <duration>
```

Threshold limit (msec).

```
duration <duration>
```

Set the duration (seconds) before an alert is raised. Available settings are 0, 30, 60, 300,1800 and 3600.

```
enable
```

Enable monitoring of the SLA object.

```
pingsize <size>
```

Specify the ping packet size (in bytes). Default is 64.

SNMP

To enable and configure SNMP, use the 'snmp-server' command.

```
(config)# snmp-server {community|contact|enable|host|listen|location|port|traps|user}
```

Set the read-only community string.

```
(config)# snmp-server community <community>
```

Set a value for the syscontact variable in MIB-II.

```
(config)# snmp-server contact <contact>
```

Enable SNMP-related functionality.

```
(config)# snmp-server enable
```

Enable community-based authentication

```
(config)# snmp-server enable communities
```

Enable sending of SNMP traps from this system

```
(config)# snmp-server enable traps
```

Specify the hostname or IP address to send SNMP traps to. IPv4 and IPv6 addresses can be used.

```
(config)# snmp-server host <hostname or IP address>
```

Specify the port for sending the SNMP trap.

```
(config)# snmp-server traps port <port>
```

Configure SNMP server interface access restrictions.

```
(config)# snmp-server listen {enable|interface <interface>}
```

Set a value for the syslocation variable in MIB-II.

```
(config)# snmp-server location <location>
```

Specify the UDP port for the SNMP agent.

```
(config)# snmp-server port <port>
```

Set the default community for traps sent to hosts which do not have a custom community string set

```
(config)# snmp-server traps community <community>
```

Specify which an event to be sent as an SNMP trap.

```
(config)# snmp-server traps event <event>
```

Send a test trap.

```
(config)# snmp-server traps send-test
```

Configure SNMP access on a per-user basis.

```
(config)# snmp-server user
```

Restrict a network object from accessing the SNMP server

```
(config)# snmp-server restrict <network-object>
```

SSH

SSH Servers:

Display the parameters of the SSH client.

```
(config)# show ssh client <client-name>
```

Display the parameters of the SSH server.

```
(config)# show ssh server <server-name>
```

Display the settings of the SSH server with full host keys.

```
(config)# show ssh server host-keys <server-name>
```

Restrict a network object from accessing the SSH server

```
(config)# ssh server restrict <network-object>
```

Enable SSH access to the system.

```
(config)# ssh server enable <server-name>
```

Generate a new RSA or DSA host key.

```
(config)# ssh server host-key generate
```

Enable SSH interface restrictions on access to the system.

```
(config)# ssh server listen enable
```

Add an interface to the SSH server access restriction list

```
(config)# ssh server listen interface <interface-name>
```

Specify the minimum version of the SSH protocol that is supported.

```
(config)# ssh server min-version <version-number>
```

Set the ports the SSH server listens on.

```
(config)# ssh server ports <port-number>
```

Enable x11 forwarding on the SSH server

```
(config)# ssh server x11-forwarding enable
```

SSH Clients:

Display the parameters of the SSH client.

```
(config)# show ssh client <client-name>
```

Configure whether the SSH client checks for a host key from the list of known host keys.

```
(config)# ssh client global host-key-check [yes|no|ask]
```

Add a global SSH client known host entry.

```
(config)# ssh client global known-host <known host entry>
```

Configure the authorized key for the specified SSH user.

```
(config)# ssh client user <user name> authorized-key sshv2
```

Identify the type of key used by the SSH user.

```
(config)# ssh client user <user name> identity <key type>
```

Set the known host for the SSH user.

```
(config)# ssh client user <user name> known-host <known host>
```

Static Users

The Active Directory feature provides a dynamic mapping from an IP address to a user name. In addition static network users can be created with the "network-user static-user" command.

```
[no] network-user static-user <user name> address <IPv4 or IPv6 address> [group]
```

```
name
```

The name of the user.

```
address
```

The corresponding static IPv4 or IPv6 address of the user. Multiple addresses may be specified.

```
group
```

The group that the user belongs to (optional)

To create a dynamic Network Object based on a user or group, use the "network-user network-object" command:

```
[no] network-user network-object <network object> {group | user} <user or group>
```

Example: Create a dynamic Network Object called 'Students Network Object' from the Active Directory 'Students' group

```
(config)# network-user network-object "Students Network Object" group Students
```

Storage

Note For examples of storage configuration, see Configure Storage with CLI.

Caution Put the Exinda appliance into bypass before changing the partition size of wan-memory. See "Bypass" on page 15 or NIC Settings.

Use the "storage" command to manage the disk storage used by system services.

```
storage service {edge-cache|cifs|monitor|users|wan-memory|virt} {format|size}
```

```
format
```

Format the volume for the specified service.

```
size
```

Resize the volume for the specified service

```
storage tasks clear
```

Clear the current storage tasks list.

Use the "show storage" command to show the current storage configuration.

```
show storage [{raid|service|tasks}]
```

```
service <service>
```

Show the current storage running state for the specified service.

```
tasks
```

Show currently running storage tasks (e.g. size or format operations)

```
raid adapter {<A>}
```

Show information about RAID adapters.

```
raid adapter <A> logical <L>
```

Show information about logical drives on a specified adapter.

```
raid adapter <A> drive
```

Show information about physical drives on a specified adapter.

```
raid adapter <A> eventlog {last <N>|all}
```

Show the eventlog for a specified adapter. Use "last <N>" to show the last N events.

To show smartctl output:

```
show storage smart device sda attributes
```

TACACS+

TACACS+ authentication allows you to configure the Exinda appliance to authenticate user login attempts with a remote TACACS+ server.

```
(config) # tacacs-server {host|key|retransmit|timeout}
```

Specify the hostname or IP address of the TACACS+ server. IPv4 addresses can be used.

```
(config) # tacacs-server host <hostname or IP address>
```

Specify the key for accessing the TACACS+ server.

```
(config) # tacacs-server key <key string>
```

Specify how often authentication requests should be retransmitted to the TACACS+ server.

```
(config) # tacacs-server retransmit <retries>
```

Specify how many seconds before the connection to the TACACS+ server times out.

```
(config) # tacacs-server timeout <seconds>
```

Telnet

Enable the Telnet server.

```
(config)# telnet-server enable
```

Restrict a network object from accessing the Telnet server.

```
(config)# telnet-server restrict <network-object>
```

Time

To configure your time zone, use the "clock" command.

```
clock {timezone|set}
```

```
timezone <region> <city>
```

Set the system's time zone.

```
set <hh>:<mm>:<ss>
```

Set the time. Value must be a time in the format of '23:59:59'. Time adjustment is not allowed if NTP is enabled.

Example: Set the time zone and adjust the system clock.

```
(config)# clock timezone Australia Melbourne
(config)# clock set 23:00:00
```

Virtualization

To create or edit Virtual Machines, use the 'virt' command.

```
[no] virt {enable|vm|vnet|volume}
```

```
enable
```

Enable/disable virtualization feature.

```
vm <name> ...

arch {i386|x86_64}: Set CPU architecture.

boot {auto-power|device order {cdrom|hd}}: Configure boot options.

comment <comment>: Set a comment describing this virtual machine.

console {connect|graphics|text}: Configure or connect to the text or graphical
console.

copy <new_name>: Make a duplicate copy of this virtual machine.

feature {pae|acpi|apic} enable: Enable/disable certain virtualization features.

install: Install an operating system onto this virtual machine (temporarily attach a
CD and boot from it).

interface <name> {bridge|macaddr|model|name|order|type|vnet}: Configure virtual
interfaces.

manufacture: Manufacture this virtual machine with an appliance image.

memory <MB>: Set memory allowance.

power {cycle|off|on}: Turn this virtual machine on or off, plus other related options.

rename <new_name>: Rename this virtual machine.

storage {create|device}: Configure storage for this virtual machine.

vcpus count <num>: Specify number of virtual CPUs.

vnet <name> ...

>dhcp range <low_ip> <high_ip>: Configure a DHCP range to assign to this vnet.
```

```
>forward {none|nat|route} interface <name>: Configure the type of forwarding.

>ip address <ip> <netmask>: Configure the IP address of this vnet.

>vbridge name <name>: Create a virtual bridge.

volume ...

create disk file <name> size-max <MB>: Create an empty virtual disk image.

fetch <url>: Fetch a virtual disk image (*.img) or a CD ROM image (*.iso) from the
URL.

file {create|copy|move|upload}: Perform basic file operations.
```

VLANs

VLAN interfaces are typically used in a trunk Topology to associate a VLAN ID to the interface used to manage the appliance. To create a VLAN interface use the "vlan vlan-id" command.

```
vlan vlan-id <id> interface <inf>
```

The VLAN interface can now be configured using the "interface" command.

VLAN objects are used in the Optimizer to filter traffic by VLAN identifier. To create new VLAN object use the "vlan object" command.

```
vlan object <name> {id | priority}
no vlan <name>

id <low (0-4094)> <high (0-4094)>
```

Create a VLAN object by specifying an ID range. To match a single ID use the same number for low and high.

```
priority <low (0-7)> <high (0-7)>
```

Create a VLAN by specifying a priority range. To match a single priority, specify the same number for both low and high.

Example: Create a VLAN Object that defines all tagged VLANs with a VLAN ID between 2 and 7 (inclusive).

```
(config) # vlan object VLAN1 id 2 7
```

Example: Create a VLAN Object that defines all tagged VLANs with a VLAN priority of 2.

```
(config) # vlan object VLAN2 priority 2 2
```

Use the "show vlan object" command to show VLAN objects:

```
(config) # show vlan object VLAN1

Object: VLAN1

   ID, Lower limit:           2

   ID, Higher limit:          7

   Priority, Lower Limit:     0

   Priority, Higher Limit:    7
```

```
    Type:                       802.1Q
```

WCCP

Use the wccp command to configure WCCP on the appliance. WCCP allows for out-of-path application acceleration.

```
 [no] wccp interface <inf>
```

Assign an interface to use for WCCPv2 traffic.

```
wccp service <service group (1-99)> group-address | password | router
```

Configure WCCP services:

```
router <address>
```

Add a router to contact for the specified service

```
group-address <multicast address>
```

Configure the multicast address for sending WCCPv2 messages to

```
password <password (1-8 characters)>
```

Configure the password for the specified service

See the WCCP HowTo Guide for more information.

Web UI and Web Proxy

The following commands can be used to configure the web user interface (Web UI)

Enable or disable the Web UI.

```
>[no] web enable
```

Configure the length of user inactivity before auto-logout (in seconds).

```
web {auto-logout|http|httpd|session|https|proxy}
auto-logout <time>
```

Configure HTTPS access to the Web UI, including the listen port and custom SSL certificates.

```
http {enable|port|redirect}
  Enable HTTP access, set the HTTP port and enable redirect to HTTPS
https {enable|certificate|customssl|port}
```

Configure renewal and timeout session settings.

```
web session {renewal|timeout>
```

Enable or disable deflate compression encoding

```
 [no] httpd compression
```

Enable or disable Web interface restrictions

```
 [no] httpd listen
```

Restrict the listen interface for the Web UI. The configured interface should be statically configured (DHCP disabled)

```
web httpd listen interface <inf>
```

Use the following commands to configure access to a Web proxy:

Configure the web proxy host address and port. IPv4 and IPv6 addresses can be used.

```
proxy host <hostname or IP address> [port <port>]
```

Configure the type of proxy authentication.

```
proxy auth authtype {none|basic}
```

Configure the username and password for basic authentication.

```
proxy auth basic {password|username}
```

Use the following command to show Web UI configuration and running state

```
show web
```

Restrict a network object from accessing management services

```
web https restrict <network-object>
```

Other Commands

Iperf: TCP/UDP Bandwidth Measurement Tool.

This command requires 2 Exinda appliances. One needs to be run as an iperf server.

```
iperf -s
```

The other needs to be run as an iperf client, which connects to the iperf server.

```
iperf -c <ip address of server>
```

Ping: Send ICMP echo requests to a specified host.

```
ping <hostname or ip address of remote host>
```

Traceroute: Trace the route packets take to a destination.

```
traceroute <hostname or ip address of remote host>
```

Optimizer

To configure the optimizer, use the 'optimizer' command.

```
optimizer {default|enable|global-qos|restart}
To  configure QoS and/or Acceleration using one of the default circuit/vcircuit/policy
 configurations:
default accelerate
Install default Acceleration, no QoS
default accelerateqos dualvc
```

```
Install default Acceleration and QoS  with two virtual circuits
(WAN and Internet). Use this configuration when both WAN and Internet are accessed fro
m the appliance.
```

```
default accelerateqos singlevc
```

```
Install default Acceleration and QoS with a single virtual circuit
(WAN). Use this configuration when Internet traffic is accessed from the WAN
(routed from another site).
```

```
enable
```

```
Enable the Optimizer.
```

```
global-qos
```

```
Enable Global QoS mode.
```

```
restart
```

```
Restart the Optimizer.
```

Circuits

To create a new optimizer circuit, use the 'circuit' command.

```
circuit <circuit name> {bandwidth|bridge|order}
no circuit <circuit name>
```

```
bandwidth {inbound|outbound} <bandwidth_kbps>
```

Set inbound and outbound bandwidth in kbps.

```
bridge {ALL|<name>}
```

Configure bridge to attach this circuit to.

```
order <order_number>
```

Configure Circuit ordering number.

Example: Create a new circuit with 200kbps bandwidth in both directions.

```
(config) # circuit circuit_1 order 1
(config) # circuit circuit_1 bandwidth inbound 200
(config) # circuit circuit_1 bandwidth outbound 200
(config) # circuit circuit_1 bridge ALL
```

Virtual Circuits

To create new virtual circuit within an existing circuit use the circuit command.

```
circuit <circuit_name> vcircuit <vcircuit_name> {app-group|app-
name|bandwidth|connection-limit|direction|dynamic|network-object|order|schedule|vlan}
no circuit <circuit_name> vcircuit <vcircuit_name>
```

```
app-group <name>
```

Set the Application Group to match.

```
app-name <name>
```

Set the Application to match.

```
bandwidth <num> {kbps|%}
```

Set the virtual circuit bandwidth. If `kbps` or `%` are not specified, `kbps` is used.

```
connection-limit <num>
```

Limit the number of connections to the VC. "0" means no connection limit.

```
direction {inbound|outbound|both}
```

Specify the direction - values can be inbound, outbound or both (bi-directional).

```
dynamic ...
```

```
bandwidth {burst {auto|<num> {kbps|%}}|guaranteed <num> {kbps|%}): Specify the Dynamic
Virtual Circuit bandwidth values. If kbps or % are not specified, kbps is used.
```

```
enable: Enable/disable Dynamic Virtual Circuit.
```

```
external: Specify that hosts are on the external side of the appliance.
```

```
host-limit <num>: Configure number fo unique hosts to allow into this Dynamic Virtual
Circuit.
```

```
internal: Specify that hosts are on the internal side of the appliance.
```

```
network-object <name>
```

Set the Network Object to match.

```
order <num>
```

Set the virtual circuit ordering number.

```
schedule
```

Set the Schedule to match.

```
vlan <name>
```

Set the VLAN to match.

Example: Create a virtual circuit that captures all traffic in both directions and assign it 200kbps.

```
(config)# circuit circuit_1 vcircuit VC1 order 1
(config)# circuit circuit_1 vcircuit VC1 bandwidth 200 kbps
(config)# circuit circuit_1 vcircuit VC1 direction both
(config)# circuit circuit_1 vcircuit VC1 network-object ALL
```

Policies

To create a new Optimizer Policy, use the "policy" command. Policies can then be used in Optimizer Virtual Circuits.

```
policy <policy_name> {action|enabled|filter|schedule}
```

```
action ...
```

```
>optimize ...
```

```
aa ...
```

```
enable: Enable/disable Application Acceleration for this policy.
```

```
reduction-type {disk|lz|none}: Configure the type of reduction to apply to this
policy.
```

```
type {acceleration|compression|edge-cache}: Configure the type of acceleration to
apply to this policy (note: compression is legacy).
```

```
mark ...
```

```
dscp <num>: Configure a DSCP number to mark.
```

```
tos {normal|min-cost|max-reliability|max-throughput|min-delay}: Configure a ToS name
to mark.
```

```
vlan {id|priority} <num>: Configure VLAN ID and/or priority to mark.
```

```
qos ...
```

```
bandwidth {burst <num> {kbps|%}|guaranteed <num> {kbps|%}: Configure the bandwidths
for this policy.
```

```
enable: Enable/disable QoS for this policy.
```

```
priority <num>: Configure the priority of this policy.
```

```
>ignore: Ignore the matching traffic, just pass it through.
```

```
>discard: Discard the matching traffic.
```

```
schedule <schedule_name>
```

Select the policy schedule (when the policy should be active). The default is 'ALWAYS'.

```
filter <num> ...
```

```
>app-group <name>: Specify an application group to match.
```

```
>app-name <name>: Specify a Single application to match.
```

```
>network-object {destination|source} <name>: Specify the source/destination Network
Object to match.
```

```
>direction {inbound|outbound|both}: Specify the traffic direction, both, inbound or
outbound.
```

```
>vlan <name>: Specify a VLAN Object to match.
```

```
>dscp <num>: Specify a DSCP value to match.
```

```
>tos {normal|min-cost|max-reliability|max-throughput|min-delay}: Specify a ToS name to
match.
```

```
enable
```

Enable/disable this Policy.

Example: Create an Optimizer Policy that matches all traffic belonging to the 'Web' Application Group and guarantees 20% of the bandwidth to that traffic, allowing it to burst to 100%.

```
(config)# policy Policy_1
(config)# policy Policy_1 schedule ALWAYS
(config)# policy Policy_1 action optimize
(config)# policy Policy_1 action optimize qos bandwidth burst 100 %
(config)# policy Policy_1 action optimize qos bandwidth guaranteed 20 %
(config)# policy Policy_1 action optimize qos priority 2
(config)# policy Policy_1 action optimize qos enable
(config)# policy Policy_1 filter 1
(config)# policy Policy_1 filter 1 app-group Web
(config)# policy Policy_1 filter 1 network-object destination ALL
(config)# policy Policy_1 filter 1 direction both
(config)# policy Policy_1 filter 1 network-object source ALL
(config)# policy Policy_1 filter 1 vlan ALL
(config)# policy Policy_1 enabled
```

Service

To manage Application Acceleration modules, use the "service" command:

```
(config)# service <service> {start|stop|restart|enable|disable}
```

See the status of a service:

```
(config)# show service <service>
```

Start the service:

```
(config)# service <service> start
```

Stop the service:

```
(config)# service <service> stop
```

Restart the service:

```
(config)# service <service> restart
```

Enable the service:

```
(config)# service <service> enable
```

Disable the service:

```
(config)# service <service> disable
```

Note Not all modules support `enable` and `disable`.

TCP Acceleration

To configure TCP acceleration settings, use the "acceleration tcp" command.

```
acceleration tcp {cc|discovery|dual-bridge-bypass|keep-alive|transport|window-scale}
no acceleration tcp {discovery|dual-bridge-bypass|keep-alive}
```

```
cc {cubic|hybla|highspeed|veno|reno|bic|vegas|htcp|yeah|illinois|scalable|lp|westwood}
```

Select WAN side congestion control algorithm.

```
discovery
```

Enable appliance auto-discovery.

```
dual-bridge-bypass
```

Enable checking of the incoming bridge. Enabled by default.

```
keep-alive {enable|timeout}
```

```
>enable - Enables the sending of keep-alive packets on the WAN. The timeout specifies
when to activate the keep-alives if enabled.
```

```
>timeout - Specifies the amount of time, in seconds, that a connection may be idle
before sending keep-alive packets is enabled. Keep-alive packets are sent once per
minute until either a response is received, or 5 minutes passes. If five minutes
passes without a response the connection is terminated.
```

```
>transport {transparent|tunnelled}
```

Set the transport mode, transparent or tunnel (protocol 139).

```
window-scale <factor>
```

Window Scaling Factor determines how large the TCP window is allow to grow per connection. The default Window Scaling Factor is 5, which equates to a TCP window of 2MB. Both the Window Scaling Factor and the TCP Window size are displayed; for example:

```
# acceleration tcp window-scale ?
<factor>
  0  (64k)
  1  (128k)
  2  (256k)
  3  (512k)
  4  (1M))
  5  (2M)
...
```

WAN Memory

To configure WAN Memory acceleration settings, use the 'acceleration wm' command.

```
acceleration wm {cache|enable|persistence|reduction}
no acceleration wm {enable|persistence enable|reduction}
```

`cache clear`—Clear the contents of the cache by expiring 100% of it's contents.

`enable`—Enable/disable WAN Memory byte-level caching.

`persistence`—Clear or enable/disable disk cache persistence on next restart.

Enable/disable LZ-compression or small matching.

```
reduction {lz-compression|small-matcher} enable
```

Enable WAN Memory cache synchronization across all appliances in the cluster:

```
(config)# acceleration wm cache sync
```

SMB Acceleration

Display SMB acceleration settings:

```
(config)# show acceleration smb {applications|signed-servers|v1|v2}
```

List the applications that support SMB.

```
(config)# show acceleration smb applications
```

List the SMB signed servers.

```
(config)# show acceleration smb signed-servers
```

Configure SMB acceleration settings with the `acceleration smb` commands.

```
(config)# acceleration smb {application|cache|enable|v1|v2}
```

Enable/disable SMB acceleration.

```
(config)# [no] acceleration smb enable
```

Add applications supported by the SMB module.

```
(config)# [no] acceleration smb application <application>
```

Clear the SMB disk cache.

```
(config)# acceleration smb cache clear
```

SMB1 commands

Display the configuration for SMB1.

```
(config)# show acceleration smb v1 config
```

Display the SMB1 connections.

```
(config)# show acceleration smb v1 connections
```

Display the SMB1 connections, along with the sources and destinations of the connection.

```
(config)# show acceleration smb v1 connections list
```

Display the SMB1 connections, the sources and destinations of the connection, and the client/server operating systems and shared file directories.

```
(config)# show acceleration smb v1 connections list detailed
```

Configure SMB1 acceleration settings with the `acceleration smb v1` commands.

```
(config)# acceleration smb v1 {enable|meta-cache|prefetch|read-ahead|write-behind}
```

Enable/disable SMB1 acceleration:

```
(config)# [no] acceleration smb v1 enable
```

Enable/disable SMB1 meta-caching:

```
(config)# [no] acceleration smb v1 meta-cache
```

Set the amount to pre-fetch (in kbytes). Value must be between 0 and 8192.

```
(config)# acceleration smb v1 prefetch <prefetch-kbytes>
```

Enable/disable SMB1 read-ahead :

```
(config)# [no] acceleration smb v1 read-ahead
```

Enable/disable SMB1 write-behind :

```
(config)# [no] acceleration smb v1 write-behin
```

Enable/disable SMB1 signing :

```
(config)# [no] acceleration smb v1 signing enable
```

SMB2 commands

Display the configuration for SMB2.

```
(config)# show acceleration smb v2 config
```

Display the SMB2 connections.

```
(config)# show acceleration smb v2 connections
```

Display the SMB2 connections, along with the sources and destinations of the connection.

```
(config)# show acceleration smb v2 connections list
```

Configure SMB2 acceleration settings with the `acceleration smb v2` commands.

```
(config)# acceleration smb v2 {enable}
```

Enable/disable SMB2 acceleration:

```
(config)# [no] acceleration smb v2 enable
```

Enable/disable SMB2 signing :

```
(config)# [no] acceleration smb v2 signing enable
```

SSL Acceleration

To configure SSL acceleration settings, use the 'acceleration ssl' command.

```
acceleration ssl {enable|flush|reset|server}
```

To enable (or disable) SSL acceleration

```
[no] acceleration ssl enable
```

To configure the SSL server to accelerate to:

```
acceleration ssl server <server-name> {address|certificate|port|validation}
address <address>
Configure the IPv4  address of the server to accelerate to.
port <number>
Configure the port number of the application running on the server to accelerate to.
certificate <certificate-name>
Select the certificate to use when accelerating to this server.
validation certificate <certificate-name>
```

Accept specific certificate for validation of the SSL server

```
validation none
```

Accept any certificate

```
validation reject
```

Reject any certificate

To reset a disabled SSL acceleration server:

```
acceleration ssl reset <server-name>
```

To flush OCSP response cache of the SSL acceleration server"

```
acceleration ssl flush <server-name>
```

To show currently configured SSL acceleration servers:

```
show acceleration ssl server <server-name>
```

To create an SSL server:

```
acceleration ssl server <server-name>
```

Use the following sub-commands to specify the parameters for the new SSL server:

```
acceleration ssl server <server-name> address <IP address> -
 Specify the IP address of the SSL server.
```

```
acceleration ssl server <server-name> certificate <certificate-name> -
 Specify the certificate for the SSL server. client-auth-
cert ? will display a list of available certificates.
```

```
acceleration ssl server <server-name> client-auth-cert <certificate-name> -
 Specify the certificate for client authentication on the SSL server. client-auth-
cert ? will display a list of available certificates.
```

```
acceleration ssl server <server-name> port <port_number> -
 Specify the port of the SSL server.
```

```
acceleration ssl server <server-name> revocation [none|ocsp-aia|ocsp-server] -
 Specify the revocation status check of the SSL server.
```

```
acceleration ssl server <server-name> validation [certificate|none|reject] -
 Specify the validation on the SSL server.
```

Edge Cache Acceleration

To configure Edge Cache acceleration, use the "acceleration edge-cache" command.

```
>acceleration edge-cache {application|cache|connect-timeout|never-cache|object-
size|peer|range-offset}
```

```
>no acceleration edge-cache {application|never-cache|peer}
```

```
>application <application>
```

Edge Cache will accelerate traffic matching the HTTP application by default. Add or remove additional applications using this command.

Note: Only applications that use the HTTP protocol are supported.

```
cache clear
```

Clear the object cache.

```
connect-timeout <seconds>
```

Specify the timeout in seconds that Edge Cache should wait for a response when fetching objects from the WAN.

```
never-store <URL or domain>
```

Add or remove a URL or domain that should never be cached.

```
object-size {maximum|minimum> <size>
```

Specify the maximum and minimum size of objects to store. The size parameter should use SI units e.g. 100M or 512k.

```
range-offset <limit>
```

Specify the range offset limit. Use this configuration option to prevent delays when skipping ahead during video downloads.

```
peer <hostname> [{http-port|icp-port|option {default|proxy-only|no-
query|weight=n|closest-only|originserver|round-robin}}]
```

Add or remove an Edge Cache peer. Peering creates a community of Edge Cache appliances that will share object data.

```
http-port <port>
```

Specify the peer HTTP port

```
icp-port <port>
```

Specify the peer ICP port

```
option default
```

Use the default peer options

```
option proxy-only
```

Do not cache objects from this peer.

```
option no-query
```

This peer does not support ICP

```
option weight=n
```

Specify the peer priority. Peers with higher priority will be consulted first.

```
option round-robin
```

Specify that peers should be consulted in round-robin order.

```
option closest-only
```

Only forward closest parent ICP misses.

```
option originserver
```

Specify that this peer is an origin server

Use the "show acceleration edge-cache" command to see the current Edge Cache configuration settings.

Note: for more information, refer to the Edge Cache HowTo Guide.

NCP Acceleration

To enable or disable Novell NCP acceleration, use the "acceleration ncp" command.

```
[no] acceleration ncp enable
```

Prepopulation

To configure acceleration prepopulation, use the "acceleration prepopulate" command.

```
acceleration prepopulate <prepopulate-name>
{location|password|recursive|start|stop|username}
```

```
<prepopulate-name>
```

Specify a name for a new prepopulation

```
location
```

Configure the server and path

```
password
```

Configure a password

```
recursive
```

To download recursively via the path

```
start
```

Start prepopulating

```
stop
```

Stop prepopulating

```
username
```

Configure a username

To clear prepopulated data:

```
acceleration prepopulate cache clear
```

SMB Prepopulation

To configure SMB prepopulation, use the "acceleration prepopulate SMB" command.

```
acceleration prepopulate smb <prepopulate-name>
{location|password|recursive|start|stop|username}
```

`<prepopulate-name>`—Specify a name for a new prepopulation

`location`—Configure the server and path

`password`—Configure a password

`recursive`—Download recursively via the path

`start`—Start prepopulating

`stop`—Stop prepopulating

`username`—Configure a username