CLI Reference Guide

Exinda ExOS Version 6.3

Table of Contents

Part

1 Introduction

CLI Reference Guide

Exinda Firmware Version: 6.3

1.1 Using this Guide

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

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

1.2 Further Reading

In addition to this Reference Guide, the following additional user documentation is available:

- Exinda Quick Start Guides
- Exinda User Manual
- Exinda Topologies Guide
- Exinda "How To" Guides

Please visit http://www.exinda.com for more information.

Part II

2 Overview

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

1. Secure Shell (SSH) (recommended)
2. Web User Interface (Web UI) from Tools | Console
3. Telnet
4. Serial Console Interface

This Command Line Reference focuses purely on the commands that may be used for the above interfaces. The commands will perform every operation that can be achieved via the Web UI.

To enter configuration (conf) mode, type `enable`, then `configure terminal`.

```
> enable
# configure terminal
(config)#
```

Enter configuration information at the `(config)#` prompt. To save the running configuration, type `configuration write`.

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

```
cli session terminal width <number of characters>

cli session terminal length <number of lines>
```

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/down arrow keys. Command line editing is available, using the left/right keys to navigate. Use "ctrl-w" to delete from the cursor to start of line.

Auto logout is enabled by default. To change the auto logout time use the following command:

```
cli default auto-logout <minutes>
```

To enable or disable paging use the following command:

```
[no] cli default paging enable
```

Use the "show cli" command to see current CLI settings.

The following syntax convention is used in this guide:

{}: Options are enclosed in curly braces and are separated by '|'.
[]: Optional keywords are enclosed in square brackets.
<>: User input is required where variable are enclosed in greater-than and less-than symbols.

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

To set a configuration variable or perform an action:

```
(config) # command <arg1> <arg2> ...
```

To remove the configuration or undo the action

```
(config) # no command <arg1> <arg2> ...
```

To show the current configuration:

```
(config) # show command
```

Example: system IP configuration

To set an IP address on the eth1 interface:

```
(config) # interface eth1 ip address 192.168.0.229 /24
```

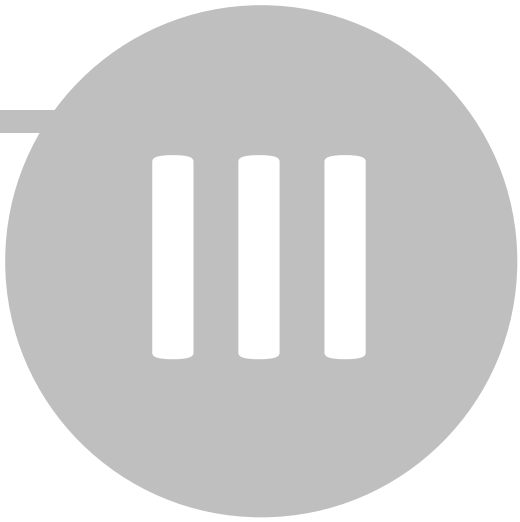
To show a summary of current interface configuration:

```
(config) # show interfaces summary
```

To remove the IP address on the eth1 interface:

```
(config) # no interface eth1 ip address
```

Part



3 CLI Commands

3.1 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

3.2 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")

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

Enable or disable the specified bridge.

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

Specify the ageing time for this bridge.

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

Specify the forwarding time for this bridge.

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

Specify the hello time for this bridge.

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

Specify the max age for this bridge.

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

Specify the priority for this bridge.

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

Enable or disable the Spanning Tree Protocol for this bridge.

To show current bridge configuration use the following command:

```
show bridges
```

3.3 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 mask 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.

3.4 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
```

3.5 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.

3.6 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>
```

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

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

```
cluster master interface <inf>
```

```
cluster master address vip <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) #
```

Use the following command to show a brief overview of the current cluster configuration

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

The following CLI commands can be used to control how data is synchronized between cluster members:

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

```
all
```

Acceleration, monitor and optimizer data are synchronized

```
acceleration
```

Synchronize monitor data only

```
monitor
```

Synchronize monitor data only

```
optimizer
```

Synchronize optimizer data only

See the Clustering and HA How-To Guide for more information.

3.7 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.

3.8 WCCP

Use the wccp command to configure WCCP on the appliance. WCCP allows for out-of-band 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.

3.9 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
```

3.10 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
```

3.11 Firmware Update

To install a new firmware use the image command.

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

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

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

```
install <image>
```

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.

```
delete <image>
```

Delete an inactive system image from the hard disk.

```
boot next
```

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

3.12 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.

3.13 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}
```

3.14 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.

3.15 Storage

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
```

3.16 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.

3.17 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.

3.18 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
```

3.19 NTP

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

```
ntp {sever|enable|disable}
```

```
server <IPv4 or IPv6 address> [version <ntp version>]
```

Configure an NTP server.

```
enable
```

Enable NTP.

```
disable
```

Disable NTP.

Example: Set an NTP server and enable the service.

```
(config)# ntp server 193.190.230.65
(config)# ntp enable
```

3.20 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
```

3.21 Web UI / Web Proxy

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

```
[no] web enable
```

Enable or disable the Web UI.

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

```
auto-logout <time>
```

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

```
http {enable|port|redirect}
```

Enable HTTP access, set the HTTP port and enable redirect to HTTPS

```
https {enable|certificate|customssl|port}
```

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

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

Configure renewal and timeout session settings.

```
[no] httpd compression
```

Enable or disable deflate compression encoding

```
[no] httpd listen
```

Enable or disable Web interface restrictions

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

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

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

```
proxy host <address> [port <port>]
```

Configure the web proxy host address and port.

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

Configure the type of proxy authentication.

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

Configure the username and password for basic authentication.

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

```
show web
```

3.22 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
```

3.23 Logging

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

```
show log
```

View the complete log file.

```
show log continuous
```

View the log file as it gets updated.

```
show log continuous {matching|not matching} <regex>
```

View new log messages that match a given regular expression.

```
show log {matching|not matching} <regex>
```

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

```
show log files <file>
```

View the contents of a saved log file.

```
show log files <file> {matching| not matching} <regex>
```

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

```
logging files rotation criteria frequency {daily|weekly|monthly}
```

Rotate log files on a fixed time-based schedule.

```
logging files rotation criteria size <megabytes>
```

Rotate log files when they pass a size threshold.

```
logging files rotation criteria size-pct <percentage>
```

Rotate logs when they surpass a specified percentage of disk.

```
logging files rotation max-num <number>
```

Specify the maximum number of old log files to keep.

```
logging files delete {current|oldest}
```

Delete log files.

```
logging local override class <class> priority
```

Specify minimum severity level for this class.

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

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

3.24 E-Mail

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

```
email {autosupport|dead-letter|diag-max-size|domain|mailhub-port|notify|return-
addr|return-host|send-test}
```

```
autosupport enable
```

Set handling of automatic support email.

```
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.

3.25 SNMP

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

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

```
community <community>
```

Set the read-only community string.

```
contact <contact>
```

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

```
enable
```

Enable SNMP-related functionality.

```
enable communities
```

Enable community-based authentication

```
enable traps
```

Enable sending of SNMP traps from this system

```
host <host or IP address>
```

Configure hosts to which to send SNMP traps.

```
listen {enable|interface <interface>}
```

Configure SNMP server interface access restrictions.

```
location <location>
```

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

```
port <port>
```

Specify the UDP port for the SNMP agent.

```
traps community <community>
```

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

```
traps event <event>
```

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

```
traps send-test
```

Send a test trap.

`user`

Configure SNMP access on a per-user basis.

3.26 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
```

3.27 Alarms

To configure alarms, use the 'stats' command.

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

`alarm`

Configure alarms based on sampled or computed statistics.

`chd`

Configure computed historical data points.

`clear-all`

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

`export`

Export statistics to a file.

`sample`

Configure sampled statistics.

Example: Enable the interface errors alarm.

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

3.28 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
```

3.29 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>
```

3.30 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
```

3.31 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
```

3.32 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
```

3.33 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
```

3.34 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
```

3.35 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
```

3.36 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
```

3.37 Adaptive Response

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

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

```
clear
```

Reset Adaptive Response network objects - clear all IP's 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.

Note: For more information, refer to the Adaptive Response How to Guide.

3.38 Active Directory

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

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

`port`

Set the listen port for the Active Directory daemon.

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

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`

Start the service

`stop`

Stop the service

`restart`

Restart the service

`enable`

Enable the service

`disable`

Disable the service

Use the "show service add" command to see the running state.

3.39 Monitoring and ASAM

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

```
monitor {display|ignore-internal|skype|bit-torrent|edonkey|layer7|clear|host-
resolution|sensitivity}
```

```
display {chart-size|graphing|real-time update|table-size}
```

Adjust various monitoring display settings.

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

`graphing`: Flash or non-flash.

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

`table-size`: Number of table items. Acceptable values are 1-1000.

```
ignore-internal
```

Enable ignore internal to internal traffic.

```
skype {high|med}
```

Set Skype monitoring sensitivity.

```
bit-torrent {high|med|low}
```

Set bit-torrent monitoring sensitivity.

```
edonkey {high|med|low}
```

Set eDonkey monitoring sensitivity.

```
layer7
```

Enable layer7 monitoring.

```
clear {all|aps|monitor|optimizer|sla|appliance|interface|network|reduction}
```

Clear monitoring data.

```
host-resolution {DNS|IP|Netbios|Network_Object}
```

Set host resolution method. Rank from 1-4.

```
sensitivity <sensitivity>
```

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

To configure ASAM settings, use the 'asam' command.

```
[no] asam {anonymousproxy|citrix|dcerpc|http|ssl} enable
```

This command enables/disables drill-down monitoring capabilities for the specified application.

3.40 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}
```

3.41 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|server-delay|network-loss |network-jitter|round-trip-time} thr
```

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

Set the network delay threshold (ms)

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

Set the server-delay threshold (ms)

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

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

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

Set the network-jitter threshold (ms)

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

Set the round trip time threshold (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].

aps <name> alert enable

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

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

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)

To show all aps objects

```
show aps
```

To show details of a specific aps object

```
show aps <name>
```

For further information see the Application Performance Score HowTo.

3.42 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>

name
```

The APM object name.

```
application
```

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

```
metric
```

The Application Performance Metric that this object will monitor. 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)

Note: for more information on Application Performance Metrics, refer to the Application Performance Score HowTo Guide.

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

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

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

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

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

Specify the threshold that will trigger an alert.

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

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

3.43 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.

3.44 PDF Reports

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

```
report pdf <name> {basic|detailed|frequency|custom|email|email-report|password}
no report pdf <name>
```

```
basic {aps|network|sla|subnets|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.

`detailed {appliance|interface|peer|pps|subnet|vcircuit}`

`appliance {aa_connection|connection|cpu_usage|cpu_temperature|memory_usage|swap_usage|diskio}`:

Include and configure the Appliance statistics report.

`interface {ALL|<interface>)`:

Include and configure the Interface report.

`peer {all|<peer name>}`:

Include and configure the WAN Memory report.

`pps {ALL|<interface>)`:

Include and configure the PPS report.

`subnet <subnet name> {application|host|conversation|url|user}`:

Include and configure the Subnet report.

`vcircuit <vc name> {discard|optimizer}`:

Include and configure the Virtual Circuit report.

`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 {daily|weekly|monthly|custom_daily|custom_weekly|custom_monthly}`

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

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

`email <email address>`

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

`email-report`

PDF reports that have an email address configured can generate and email the report on-demand.

```
password <password>
```

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

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"
```

3.45 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 {daily|weekly|monthly}

email <email address>
```

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

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
```

3.46 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 wh

```
default accelerateqos singlevc
```

Install default Acceleration and QoS with a single virtual circuit (WAN). Use this configuration when Interne

```
enable
```

Enable the Optimizer.

```
global-qos
```

Enable Global QoS mode.

```
restart
```

Restart the Optimizer.

3.46.1 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
```

3.46.2 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.

```
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.

`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
```

3.46.3 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
```

3.47 Acceleration

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

```
service <service> {start|stop|restart|enable|disable}
```

`start`

Start the service

`stop`

Stop the service

`restart`

Restart the service

`enable`

Enable the service

`disable`

Disable the service

Note: some modules do not support enable / disable.

To see the status of a service, use the "show service <service>" command

3.47.1 TCP Acceleration

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

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

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.

```
enable
```

Enable TCP Acceleration.

```
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.

3.47.2 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.

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

Enable/disable LZ-compression or small matching.

3.47.3 SMB Acceleration

To configure SMB acceleration settings, use the "acceleration smb" command.

```
acceleration smb {application|enable|read-ahead|write-ahead|disk-cache|prefetch|
transaction|force-smb}
```

To show SMB acceleration settings:

```
show acceleration smb {applications|v1|v2} {config|connections|connections list}
```

To enable/disable SMB acceleration:

```
[no] acceleration smb enable
```

To add applications supported by the SMB/SMB2 module:

```
[no] acceleration smb application <application>
```

To clear the SMB disk cache:

```
acceleration smb cache clear
```

To enable SMB acceleration:

```
acceleration smb v1 enable
```

To enable SMB meta-caching:

```
acceleration smb v1 meta-cache
```

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

```
acceleration smb v1 prefetch <prefetch-kbytes>
```

To enable/disable SMB read-ahead :

```
[no] acceleration smb v1 read-ahead
```

To enable/disable SMB write-behind :

```
[no] acceleration smb v1 write-behind
```

To enable SMB2 acceleration:

```
acceleration smb v2 enable
```

To enable SMB meta-caching:

```
acceleration smb v2 meta-cache
```

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

```
acceleration smb v2 prefetch <prefetch-kbytes>
```

To enable/disable SMB read-ahead :

```
[no] acceleration smb v2 read-ahead
```

To enable/disable SMB write-behind :

```
[no] acceleration smb v2 write-behind
```

3.47.4 SSL Acceleration

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

```
acceleration ssl {enable|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 show currently configured SSL acceleration servers:

```
show acceleration ssl servers
```

3.47.5 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
```

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.

3.47.6 NCP Acceleration

To enable or disable Novell NCP acceleration, use the "acceleration ncp" command.

```
[no] acceleration ncp enable
```

3.47.7 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
```

3.47.8 SMB Prepopulation

To configure SMB prepopulation, use the "acceleration prepopulate SMB" command.

```
acceleration prepopulate smb <prepopulate-name> {location|password|recursive|start|stop|usernar
```

```
<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

3.48 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>
```