Command Line Interface User Manual

EX Series Secure WAN Manager

Document No.: D-020-01-00-0023

Ver. 3.1 4/20/2011

Headquarters

A10 Networks, Inc.
2309 Bering Dr.
San Jose, CA 95131

Tel: 408 325 8668 (main)
Tel: 408 325 8676 (support)
Fax: 408 325 8666

www.a10networks.com

Information in this document is subject to change without notice.

Trademarks

A10 Networks, the A10 logo, ACOS, aFleX, aFlow, aGalaxy, aVCS, aXAPI, IDaccess, IDSENTRIE, IP to ID, SmartFlow, SoftAX, VirtualADC, Virtual Chassis, and VirtualN are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners.

Patents Protection

A10 Networks products including all AX Series products are protected by one or more of the following US patents and patents pending: 7716378, 7675854, 7647635, 7552126, 20090049537, 20080229418, 20080040789, 20070283429, 20070271598, 20070180101

Confidentiality

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc. This information may contain forward looking statements and therefore is subject to change.

A10 Networks Inc. Software License and End User Agreement

Software for all AX Series products contains trade secrets of A10 Networks and its subsidiaries and Customer agrees to treat Software as confidential information.

Anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not:

1) reverse engineer, reverse compile, reverse de-assemble or otherwise translate the Software by any means

2) sublicense, rent or lease the Software.

Disclaimer

The information presented in this document describes the specific products noted and does not imply nor grant a guarantee of any technical performance nor does it provide cause for any eventual claims resulting from the use or misuse of the products described herein or errors and/or omissions. A10 Networks, Inc. reserves the right to make technical and other changes to their products and documents at any time and without prior notification.

No warranty is expressed or implied; including and not limited to warranties of non-infringement, regarding programs, circuitry, descriptions and illustrations herein.

Environmental Considerations

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

Further Information

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location which can be found by visiting www.a10networks.com.

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING A10 NETWORKS OR A10 NETWORKS PRODUCTS, OR SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

A10 NETWORKS IS WILLING TO LICENSE THE PRODUCT (EX Series) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN A10 NETWORKS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

The following terms of this End User License Agreement ("Agreement") govern Customer's access and use of the Software, except to the extent there is a separate signed agreement between Customer and A10 Networks governing Customer's use of the Software

License. Conditioned upon compliance with the terms and conditions of this Agreement, A10 Networks Inc. or its subsidiary licensing the Software instead of A10 Networks Inc. ("A10 Networks"), grants to Customer a nonexclusive and nontransferable license to use for Customer's business purposes the Software and the Documentation for which Customer has paid all required fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the product or products and made available by A10 Networks in any manner (including on CD-Rom, or on-line).

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in or for execution on A10 Networks equipment owned or leased by Customer and used for Customer's business purposes.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and A10 Networks retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of A10 Networks, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

a. transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand A10 Networks equipment

b. make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same

c. reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction

d. disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of A10 Networks. Customer shall implement reasonable security measures to protect such trade secrets.

Software, Upgrades and Additional Products or Copies. For purposes of this Agreement, "Software" and “Products” shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware and hardware, as provided to Customer by A10 Networks or an authorized A10 Networks reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by A10 Networks or an authorized A10 Networks reseller.

OTHER PROVISIONS OF THIS AGREEMENT:

a. CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES

b. USE OF UPGRADES IS LIMITED TO A10 NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LEASEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED

c. THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation.

Trademarks. A10 Networks, the A10 logo, ACOS, aFleX, aFlow, aGalaxy, aVCS, aXAPI, IDaccess, IDsentrie, IP-to-ID, SoftAX, Virtual Chassis, and VirtualN are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners.

Patents Protection. A10 Networks products including all AX Series are protected by one or more of the following US patents and patents pending: 7716378, 7675854, 7647635, 7552126, 20090049537, 20080229418, 20080040789, 20070283429, 20070271598, 20070180101.

Limited Warranty

Disclaimer of Liabilities. REGARDLESS OF ANY REMEDY SET FORTH FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL A10 NETWORKS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE PRODUCT OR OTHERWISE AND EVEN IF A10 NETWORKS OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall A10 Networks’ or its suppliers' or licensors' liability to Customer, whether in contract, (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whetherCustomer has accepted the Software or any other product or service delivered by A10 Networks. Customer acknowledges and agrees that A10 Networks has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The Warranty and the End User License shall be governed by and construed in accordance with the laws of the State of California, without reference to or application of choice of law rules or principles. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. This Agreement constitutes the entire and sole agreement between the parties with respect to the license of the use of A10 Networks Products unless otherwise supersedes by a written signed agreement.

Preface

Document Description

This document describes the Command Line Interface of A10 Networks' EX Series Edge Accelerators. The document includes a list of all available commands, syntax, examples and other information useful in configuration and usage of the EX Series Secure WAN Manager.

FIGURE 1. EX Series Secure WAN Manager

How to use this Document

Conventions

This section describes how to interpret special formatting used within this document.

Examples are provided here for determining command input and system responses resulting from command input.

CLI Conventions

Prompt Convention (EX**)**

Within this software documentation, the term EX Series Secure WAN Manager is generally used interchangeably to refer to a variety of EX Series Secure WAN Manager products.

EX Conventions

Convention	Description
`^ or Ctrl.`	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl+D means hold down the Control key while you press the D key. Keys are indicated in capital letters and are not case sensitive.
string	A string is a non-quoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string.

Command Syntax

<table>
<tr><th>Convention</th><th>Description</th></tr>
<tr><td><b>boldface</b></td><td>Boldface text indicates commands and keywords that you enter literally as shown.</td></tr>
<tr><td><i>italics</i></td><td>Italic text indicates arguments for which you supply values.</td></tr>
<tr><td>[<i>x</i>]</td><td>Square brackets enclose an optional element (keyword or argument).</td></tr>
<tr><td>|</td><td>A vertical line indicates a choice within an optional or required set of keywords or arguments.</td></tr>
<tr><td>[<i>x</i> | <i>y</i>]</td><td>Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.</td></tr>
<tr><td>{<i>x</i> | <i>y</i>}</td><td>Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.</td></tr>
<tr><td></td><td>Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:
[x {y | z}],
braces and a vertical line within square brackets indicate a required choice within an optional elements.</td></tr>
</table>

Example Conventions

Convention	Description
`screen`	Examples of information displayed on the screen are set in New Courier font.
`boldface screen`	Examples of text that you must enter are set in New Courier bold font.
`< >`	Angle brackets enclose text that is not printed to the screen, such as passwords.
`!`	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the EX Series Secure WAN Manager software for certain processes.)
`[ ]`	Square brackets enclose default responses to system prompts.

Command Descriptions

Detailed Command Descriptions

The following section of this document provides detailed command descriptions. The command names are presented at the top left of each command description for convenience. Additional information is also provided. The following is an example of how the descriptions are formatted.

command example

Commands are shown in 16 pt. “Arial Narrow” bold font in the left column; for example, “command example” as shown above to the left.

Syntax Description

```
command attribute
```

`attribute` Command attribute description.

Default

Enabled, disabled, and so on.

Mode

EXEC

Usage

How to use the command.

Example

Application example for the command.

```
Prompt:command attribute

more commands attribute
```

Introduction

System Access

The command line interface (CLI) of the EX Series Secure WAN Manager can be accessed through a console connection, an SSH session, or a Telnet session. Regardless of which connection method is used, access to the EX Secure WAN Manager command line interface is generally referred to as an EXEC session.

EX Secure WAN Manager software and documentation utilizes the term EX to refer to the system base prompt.

Session Access Modes

As a security feature, the EX Secure WAN Manager operating system separates session access levels into the following three modes:

- User EXEC Mode allows the user to access only a *limited* set of basic monitoring commands.
- Privileged EXEC Mode allows the user to access all EX Secure WAN Manager configuration mode and management mode commands.
- Configuration Mode allows the user to configure the system's IP address, as well as configure switching and routing features.

User EXEC Mode: EX>

This is the first level entered when a CLI session begins. At this level, users can view basic system information but cannot configure system or port parameters.

When an EXEC session is started, the EX Secure WAN Manager will display the EX> prompt. The right arrow (>) in the prompt indicates that the system is at the "User EXEC Mode". This level is mainly used for monitoring and does *not* contain any commands that might control (e.g. reload or configure) the operation of the EX Series Secure WAN Manager.

You can list the commands available at the User EXEC mode by typing a question mark (**?**) and then pressing **enter** at the prompt, e.g. EX>**?**.

Privileged EXEC Mode: `EX#`

The Privileged EXEC Mode is also called the "enable" level because the **`enable`** command must be entered from the CLI to gain access. Privileged EXEC Mode can be password secured, if desired.

The "privileged" user can perform tasks such as modifying the system configuration, saving the system configuration to flash, and clearing data such as statistics or counters.

Critical commands (e.g. configuration and management) require that the user be at the "Privileged EXEC Mode". To access this level, you must first be logged in at the "User EXEC Mode". Then, type **`enable`** at the `EX>` prompt and press **`enter`**.

If configured, the EX Secure WAN Manager will prompt you to enter the password. When the correct password is entered, the prompt will change from `EX>` to `EX#` to indicate that you are now at the "Privileged EXEC Mode".

To switch back to the "User EXEC Mode", type **`disable`** at the `EX#` prompt. Typing a question mark (**?**) at the "Privileged EXEC Mode" will reveal many more command options than were available at the "User EXEC Mode".

Configuration Mode: `EX(config)#`

And yet a third mode exists – "Configuration Mode". From this mode, you can configure the system's IP address, as well as configure switching and routing features. To access this third level, you must first be logged into "Privileged EXEC Mode". Then, enter the following CONFIG command at the prompt, as shown below:

```
EX#config
```

You will notice that the prompt changes to include "`(config)`":

```
EX(config)#
```

CLI Quick Reference

Entering the **`help`** command (available at any command level) returns the CLI Quick Reference:

```
EX#help

CLI Quick Reference
===============

1. Online Help

Enter “?” at a command prompt to list the commands available at that CLI level.
Enter "?" at any point within a command to list the available options.

Two types of help are provided:
1) When you are ready to enter a command option, type "?" to display each
possible option and its description.  For example: show ?
2) If you enter part of an option followed by "?", each command or option that
matches the input is listed.  For example: show us?

2. Word Completion

The CLI supports command completion, so you do not need to enter the entire
name of a command or option. As long as you enter enough characters of the
command or option name to avoid ambiguity with other commands or options, the
CLI can complete the command or option.
After entering enough characters to avoid ambiguity, press "tab" to
auto-complete the command or option.
```

Context-Sensitive Help

Enter a question mark (**?**) at the system prompt to display a list of available commands for each command mode. The context-sensitive help feature provides a list of the arguments and keywords available for any command.

To view help that is specific to a command name, a command mode, a keyword, or an argument, enter any of the following commands:

Command	Purpose
`Help`	Displays the CLI Quick Reference
`abbreviated-command-help?`	Lists all commands beginning with abbreviation before the (**?**). If the abbreviation is not found, the EX Series Secure WAN Manager returns: % Ambiguous command

Command	Purpose
abbreviated-command-complete<Tab>	Completes a partial command name if unambiguous.
?	Lists all valid commands available at the current level
command ?	Lists the available syntax options (arguments and keywords) for the entered command.
command keyword ?	Lists the next available syntax option for the command.

A space (or lack of a space) before the question mark (**?**) is significant when using context-sensitive help. To determine which commands begin with a specific character sequence, type in those characters followed directly by the question mark; e.g. EX>**te?**. Do not include a space. This help form is called “word help”, because it completes the word for you.

To list arguments or keywords, enter a question mark (**?**) in place of the argument or the keyword. Include a space before the (**?**); e.g. EX> **terminal ?**. This form of help is called “command syntax help”, because it shows you which keywords or arguments are available based on the command, keywords, and arguments that you already entered.

Users can abbreviate commands and keywords to the minimum number of characters that constitute a unique abbreviation. For example, you can abbreviate the **config terminal** command to **conf t**. If the abbreviated form of the command is unique, then the EX Series Secure WAN Manager accepts the abbreviated form and executes the command.

Context Sensitive Help Examples

The following example illustrates how the context-sensitive help feature enables you to create an access list from configuration mode.

Enter the letters **co** at the system prompt followed by a question mark (**?**). Do not leave a space between the last letter and the question mark. The system provides the commands that begin with co.

```
EX#co?
config    Entering config mode
```

Enter the **config** command followed by a space and a question mark to list the keywords for the command and a brief explanation:

```
EX#config ?
terminal  Config from the terminal
<cr>
```

The **<cr>** symbol (cr stands for carriage return) appears in the list to indicate that one of your options is to press the **Return** or **Enter** key to execute the command, without adding any additional keywords.

In this example, the output indicates that your only option for the **config** command is **config terminal** (configure manually from the terminal connection).

The "no" and "default" Forms of Commands

Most configuration commands have a **no** form. Typically, you use the no form to disable a feature or function. Entering the command *without* the **no** keyword is used to re-enable a disabled feature or to enable a feature that is disabled by default; e.g. if terminal auto-size has been enabled previously.

To disable terminal auto-size, use the **no terminal auto-size** form of the **terminal auto-size** command. To re-enable it, use the **terminal auto-size** form. This document describes the function of the no form of the command whenever a no form is available.

Using Command History

The CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. To use the command history feature, perform any of the tasks described in the following sections:

- Setting the command history buffer size
- Recalling commands
- Disabling the command history feature

Setting the Command History Buffer Size

The EX Series Secure WAN Manager records command lines in its history buffer. To change the default number of command lines that the system will record during the current terminal session, use the following commands:

Convention	Description
EX# **terminal history** [**size** *number-of-lines*]	Enables the command history feature for the current terminal session
EX# **terminal no history size**	Resets the number of lines saved in the history buffer to the default of 100 lines.
EX(config-line)# **history** [**size** *number-of-lines*]	Enables the command history feature for all the configuration sessions.

Recalling Commands

To recall commands from the history buffer, use one of the following commands or key combinations:

Command or Key Combination	Description
Ctrl+**P** or **Up Arrow** key.[1]	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl+**N** or **Down Arrow** key. [1].	Returns to more recent commands in the history buffer after recalling commands with **Ctrl+P** or the **Up Arrow** key. Repeat the key sequence to recall successively more recent commands.
EX> **show history**	While in EXEC mode, lists the most recent commands entered.

[1] The arrow keys function only on ANSI-compatible terminals.

Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the EX Series Secure WAN Manager CLI. The following subsections describe these features:

- Moving the cursor on the command line
- Completing a partial command name
- Recalling deleted entries
- Editing command lines that wrap
- Deleting entries

- Continuing output at the --MORE-- prompt
- Re-displaying the current command line

Positioning the Cursor on the Command Line

The table below lists key combinations used to position the cursor on the command line for making corrections or changes. The Control key (**`ctrl`**) must be pressed simultaneously with the associated letter key. The Escape key (**`esc`**) must be pressed first, followed by its associated letter key. The letters are not case sensitive. Many letters used for CLI navigation and editing were chosen to simplify remembering their functions. In the following table, characters bolded in the Function Summary column indicate the relation between the letter used and the function.

Keystrokes	Function Summary	Function Details
`Left Arrow` `or` **`ctrl`+`B`**	**B**ack character	Moves the cursor left one character. When entering a command that extends beyond a single line, press the Left Arrow or Ctrl+B keys repeatedly to move back toward the system prompt to verify the beginning of the command entry, or you can also press Ctrl+A.
`Right Arrow` `or` **`ctrl`+`F`**	**F**orward character	Moves the cursor right one character.
`ctrl`+`A`	Beginning of line	Moves the cursor to the very beginning of the command line.
`ctrl`+`E`	**E**nd of line	Moves the cursor to the very end of the line.

Completing a Partial Command Name

If you do not remember a full command name, or just want to reduce the amount of typing you have to do, enter the first few letters of a command and then press **`tab`**. The CLI parser then completes the command if the string entered is unique to the command mode. If the keyboard has no **`tab`** key, you can also press **`ctrl+I`**.

The CLI will recognize a command once you have entered enough characters to make the command unique. For example, if you enter **`conf`** while in the privileged EXEC mode, the CLI will associate your entry with the config command, because only the config command begins with conf. The CLI recognizes the unique string **`conf`** for privileged EXEC mode of config after pressing the **`tab`** key:

```
 EX# conf<tab>
 EX# config
```

When using the command completion feature, the CLI displays the full command name. Commands are not executed until the **enter** key is pressed. This allows you to modify the command if the derived command is not what you expected from the abbreviation. Entering a string of characters that indicate more than one possible command, e.g. **te**, results in the following response from the CLI:

```
 EX>te
% Ambiguous command

 EX
```

If the CLI can not complete the command, enter a question mark (**?**) to obtain a list of commands that begin with the characters entered. Do not leave a space between the last letter you enter and the question mark (?).

In the example above, **te** is ambiguous. It is the beginning of both the telnet and terminal commands, as shown in the following example:

```
 EX>te?
   telnet    Open a tunnel connection
   terminal  Set terminal line parameters
 EX>te
```

The letters entered before the question mark (**te**) are reprinted to the screen to allow continuation of command entry from where you left off.

Deleting Command Entries

If you make a mistake or change your mind, you can use the following keys or key combinations to delete command entries:

Keystrokes	Purpose
backspace	The character immediately left of the cursor is deleted.
delete or **ctrl+D**	The character that the cursor is currently on is deleted.

Keystrokes	Purpose
ctrl+K	All characters from the cursor to the end of the command line are deleted.
ctrl+U or **ctrl+X**	All characters from the cursor to the beginning of the command line are deleted.
ctrl+W	The word to the left of the cursor is deleted.

Recalling Deleted Entries

The CLI stores deleted commands or keywords in a history buffer. In the buffer, only character strings that begin or end with a space are stored; individual characters that you delete (using **backspace** or **ctrl+D**) are not. The buffer stores the last ten items deleted using **ctrl+K**, **ctrl+U**, or **ctrl+X**.

Editing Command Lines that Wrap

The CLI provides a wrap-around feature for commands extending beyond a single line on the display.

When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, press **ctrl+B** or the left arrow key repeatedly until you scroll back to the command entry, or press **ctrl+A** to return directly to the beginning of the line.

The EX Series Secure WAN Manager software assumes you have a terminal screen that is 80 columns wide. If you have a different screen-width, use the **terminal width** EXEC command to set the appropriate width for your terminal.

You can use line wrapping in conjunction with the command history feature to recall and modify previous complex command entries. See the Recalling Commands section in this chapter for information about recalling previous command entries.

Continuing Output at the --MORE-- Prompt

When working with the CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many **?**, **show**, or **more** commands, the output is paused and a **--MORE--** prompt is displayed at the bottom of the screen.

To proceed, press the **enter key** to scroll down one line, or press the **spacebar** to display the next full screen of output.

Redisplay the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command line entry. To redisplay the current command line (refresh the screen), use either of the following key combinations:

Keystrokes	Purpose
ctrl+L or ctrl+R	Re-displays the current command line

Searching and Filtering CLI Output

The CLI permits searching through large amounts of command output by filtering the output to exclude information that you do not need. The **show** command supports the following output filtering options:

- **begin** *string* – Begins the output with the line containing the specified string.
- **include** *string* – Displays only the output lines that contain the specified string.
- **exclude** *string* – Displays only the output lines that ***do not*** contain the specified string.
- **section** *string* – Displays only the output lines for the specified section.

Use “ **|** ” as a delimiter between the **show** command and the display filter.

You can use regular expressions in the filter string, as shown in this example:

```
EX(config)#show arp | include 192.168.1.3*
192.168.1.3         001d.4608.1e40       Dynamic      ethernet4
192.168.1.33        0019.d165.c2ab       Dynamic      ethernet4
```

The output filter in this example displays only the ARP entries that contain IP addresses that match "192.168.1.3" and any value following "3". The asterisk (*) matches on any pattern following the "3". (See "Regular Expressions" on page 31.)

The following example displays the startup-config lines for "logging":

```
EX(config)#show startup-config | section logging
logging console error
logging buffered debugging
logging monitor debugging
logging buffered 30000
logging facility local0
```

Regular Expressions

Regular expressions are patterns (e.g. a phrase, number, or more complex pattern) used by the CLI string search feature to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. A simple regular expression can be an entry like Serial, misses, or 138. Complex regular expressions can be an entry like 00210... , (is), or [Oo]utput.

A regular expression can be a single-character pattern or a multiple-character pattern. This means that a regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. The pattern in the command output is referred to as a *string*. This section describes creating single-character patterns.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A–Z, a–z) or digit (0–9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. The following table lists the keyboard characters that have special meaning.

Character	Meaning
.	Matches any single character, including white space
*	Matches 0 or more sequences of the pattern
+	Matches 1 or more sequences of the pattern
?	Matches 0 or 1 occurrences of the pattern
^	Matches the beginning of the string
$	Matches the end of the string
_ (underscore)	Matches a comma (,), left brace {, right brace }, left parenthesis (, right parenthesis), the beginning of the string, the end of the string, or a space.

Show This Command

Most configuration sublevels have a **show this** command. This command displays information about the object at the current CLI configuration level. For example, the following command adds a Link Load Balancing (LLB) link to the EX device and then displays configuration settings and statistics for the link using **show this**:

```
EX(config)#llb link llblink1 192.168.1.99 /24
EX(config-llb link:llblink1)#show this
Name:                llblink1
Status:              Up
Gateway:             192.168.1.99
Mask:                255.255.255.0
Source NAT           Enable
Bandwidth:           1000 (kbps)
Price:               unlimited        1000
Connection Limit:    0
Weight:              1
Health Monitor:
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (pkts)
Received:            0 (bytes) / 0 (pkts)
Upstream:            0 (kbps) / 0 (pps)
Downstream:          0 (kbps) / 0 (pps)
Current Connection:  0
Connetion/sec:       0
Total Connection:    0
```

Quick Start

This chapter describes how to prepare the EX Secure WAN Manager for management access, gives an overview of the product features, and provides basic configuration examples.

Major Features

The EX Secure WAN Manager is a WAN optimization and load-balancing device that enables management of precious WAN bandwidth with the following features:

- **Identity based bandwidth usage reporting and applications logging.**
- **Applications Visibility** – with traffic monitoring and logging by class, and display of statistics based on the following criteria:
  - **ID Based Applications Logging** – see “Application Logging (applog) Configuration” on page 57 and “Application Protocol Logging Commands” on page 165
  - **ID Based Bandwidth Reporting** – see “Application Logging (applog) Configuration” on page 57, “ip2id static” on page 277 and “ip2id IDsentrie” on page 276
- **Load Balancing** – balance traffic across multiple WAN links based on a variety of criteria, including:
  - **LLB**: see “Link Load Balancing (Inbound and Outbound LLB)” on page 40 and “Link Load Balancing (llb) Commands” on page 99
  - **FWLB**: see “Firewall Load Balancing (FWLB) Configuration” on page 63 and “Firewall Load Balancing Commands” on page 173
  - **CLB**: see “Cache Load Balancing (CLB) Configuration” on page 79 and “Transparent Cache Switching Commands” on page 212
  - **SLB**: see “Server Load Balancing (SLB) Configuration” on page 75 and “Server Load Balancing Commands” on page 197
- **Quality of Service ()** – features provide rate limiting, rate shaping, and priority marking. See “Quality of Service (QoS) Configuration” on page 47 and “QoS Commands” on page 112.
- **Intrusion Prevention System (IPS)** – use IPS to detect, log, and take action against many types of intrusions. See “Intrusion Prevention System (IPS) Configuration” on page 71 and “IPS Commands” on page 179.
- **Layer 2 and 3 Support** – EX Secure WAN Manager can operate as a Layer 2 or Layer 3 device, supports multiple VLANs, and RIP & OSPF

routing. See “vlan” on page 299, “RIP CLI Commands” on page 231 and “OSPF CLI Commands” on page 236.

- **System Management** – EX Secure WAN Manager provides extensive management features including logging options, SNMP support, and admin access-control options. See “System Management” on page 94.
- **High Availability (HA)** – EX Secure WAN Manager units can be configured in pairs, with one unit providing service while the other operates in standby mode, ready to take over if the primary EX Secure WAN Manager becomes unavailable. See “HA for Gateway Mode Configuration” on page 83, “HA for Transparent Mode Configuration” on page 89 and “High Availability (HA) Commands” on page 253.

This chapter also provides information about basic system management tasks. See “System Management” on page 94.

Definition of *Connections*

Most EX Secure WAN Manager features, including the load-balancing features, operate based on connections. On the EX Secure WAN Manager, a *connection* is a set of packets that have the same protocol and address information. For example, a TCP or UDP connection consists of packets that have the same values for all the following:

- IP protocol (ex: TCP or UDP)
- Source IP address
- Source protocol port
- Destination IP address
- Destination protocol port

In general, the EX Secure WAN Manager makes and load balancing decisions for the first packet in a new connection, and applies those same decisions to subsequent packets in the same connection.

Some features distinguish between inbound connections and outbound connections.

- *Inbound connection* – A connection is inbound if its first packet is received on an external EX Secure WAN Manager interface. An *external interface* is one connected to the Internet.
- *Outbound connection* – A connection is outbound if its first packet is received on an internal EX Secure WAN Manager interface. An *internal interface* is one connected to the private network.

A packet in a connection is a *forward packet* if it flows in the same direction as the first packet of the connection, while a *reverse packet* is a packet that flows in the reverse direction.

First Steps

To prepare an EX Secure WAN Manager for configuration and management, perform the following tasks:

1. Connect to the factory default IP address, or configure a new IP address. The factory default IP address is 192.168.1.10 /24 on Ethernet interface 4.
2. Change the password for the admin account.
3. Set the system date, time, and timezone.

An IP connection is required in order for a browser to be able to log onto the EX Secure WAN Manager Graphical User Interface (GUI). Other provisioning steps can be performed using the CLI or the GUI.

You can access the CLI on a console connection over the serial interface or a Secure Shell (SSH) or Telnet connection through an IP interface.

Connecting to the CLI

You can establish a console connection over the serial interface or a Secure Shell (SSH) or Telnet connection through an IP interface.

Connecting Through the Serial Interface

1. Using the supplied RS-232 cable, connect the EX Secure WAN Manager's RS-232 serial port to the PC's COM or USB port.
2. Power on the PC and EX Secure WAN Manager, if they are not already on.
3. On the PC, set the terminal emulation application to use the following modem settings:
   - for 9600 baud
   - 8-N-1 (8 bits - no parity - 1 stop bit)

   When the serial connection is established, the login prompt is displayed on the terminal.
4. Go to "Connecting Through SSH or Telnet" on page 36.

Connecting Through SSH or Telnet

1. Power on the PC and EX Secure WAN Manager, if they are not already on.
2. If you plan to log on through the default IP address, change the PC's IP address to one in the 192.168.1.x subnet.
3. On the PC, open an SSH or Telnet connection to the EX device's IP address.
4. Go to "Connecting Through SSH or Telnet" on page 36.

Log In to the EX Secure WAN Manager CLI

1. Log in to the EX Secure WAN Manager with the default user name (*admin*) and the default password (*a10*).

```
login as: admin
Using keyboard-interactive authentication.
Password:***
[type ? for help]
```

2. Enable the Privileged EXEC Mode by typing **enable** and pressing the enter key. The is no default password for a new system until you assign one. In this case, just press the **enter** key.

```
EX>enable
Password:***
EX#
```

3. Enable the configuration mode by typing **config** and pressing enter.

```
EX#config
EX(config)#
```

Configure an IP Interface

Using the CLI, you can configure an IP interface to be a management interface, a data interface, or both.

Note: If you are logging in on the default IP address, you do not need to configure an IP interface at this time.

Here are the CLI commands for configuring each the IP address.

1. In the factory default configuration, Ethernet port 4 has the IP address 192.168.1.10/24.
2. The admin can use either a console connection or use another PC with IP address 192.168.1.x/24, and connect the PC to Ethernet port 4.

3. Assuming the admin wants to configure the IP address for Ethernet port 1, IP address 192.168.2.228 and 255.255.255.0, as shown below, are only examples.
   - **Note:** Out of the box, Ethernet port 4 has the IP address 192.168.1.10/24. The admin can *not* assign IP address 192.168.1.x/24 to any port other than Ethernet port 4, unless the IP address on Ethernet port 4 is removed or changed to another subnet.

```
EX(config)#interface ethernet 1
EX(config-if:ethernet1)#ip address 192.168.2.228 /24
```

4. Verify the interface IP address change:

```
EX(config-if:ethernet1)#show interfaces ethernet 1
ethernet1 is up, line protocol is up
 Hardware is Ethernet, address is 0013.7217.3C1F
 Internet address is 192.168.2.228/24, broadcast is 192.168.2.255
...
EX(config-if:ethernet1)#
```

Set the Enable Password

Access to the Privileged EXEC and configuration levels of the CLI are secured by the enable password. By default, the password is blank. A10 Networks recommends that you set the enable password.

To set the enable password, enter a command such as the following:

```
EX(config)#enable-password moresecurenow1
```

To test the enable password:

1. Log out of the CLI:

```
EX(config)#exit
EX#exit
WARNING:System configuration has been modified
Are you sure to quit (N/Y)?:Y
```

2. Log back into the CLI.
3. Log onto Privileged mode:

```
EX>enable
Password:moresecurenow1
EX#
```

Change the Admin Password

The EX Secure WAN Manager configuration contains an admin account by default:

- username: *admin*
- Password: *a10*

To ensure that you always have access to the device, this account cannot be deleted. However, you can change and should the password. A10 Networks recommends that you change the admin password as soon as possible to secure access to the device.

Here is an example of how to change the admin password:

```
EX#configure
EX(config)#admin admin password newadminpwd
EX(config-admin:admin)#exit
EX(config)#
```

For information about other configurable admin settings, see “admin” on page 261.

Set the System Date, Time and Time Zone

Most of the statistics displayed have time stamps. To ensure that the time stamps are accurate, set the system time, date, and timezone.

To set and verify the time and date, an example is shown below:

```
EX#clock set 05:08:00 31 Oct 2006
EX#show clock
13:08:08.736 GMT Tue Oct 31 2006
```

To set and verify the timezone, follow this example:

```
EX(config)#clock timezone ?
  Pacific/Midway              (GMT-11:00)Midway Island, Samoa
  Pacific/Honolulu            (GMT-10:00)Hawaii
  America/Anchorage           (GMT-09:00)Alaska
  America/Los_Angeles         (GMT-08:00)Pacific Time(US & Canada)
...
  Atlantic/Cape_Verde         (GMT-01:00)Cape Verde Is.
--MORE--

EX(config)#clock timezone America/Los_Angeles
EX(config)#show clock
*05:08:58.736 PST Tue Oct 31 2006
```

The **clock timezone ?** command lists the available timezones. Press the space bar to page through the list. In the **show clock** output, the timezone abbreviation indicates the timezone (in this case, “PST”).

See “clock set” on page 270 and “clock timezone” on page 270.

Quick Start Examples

Examples of typical applications for the EX Series Secure WAN Manager are shown in this section.

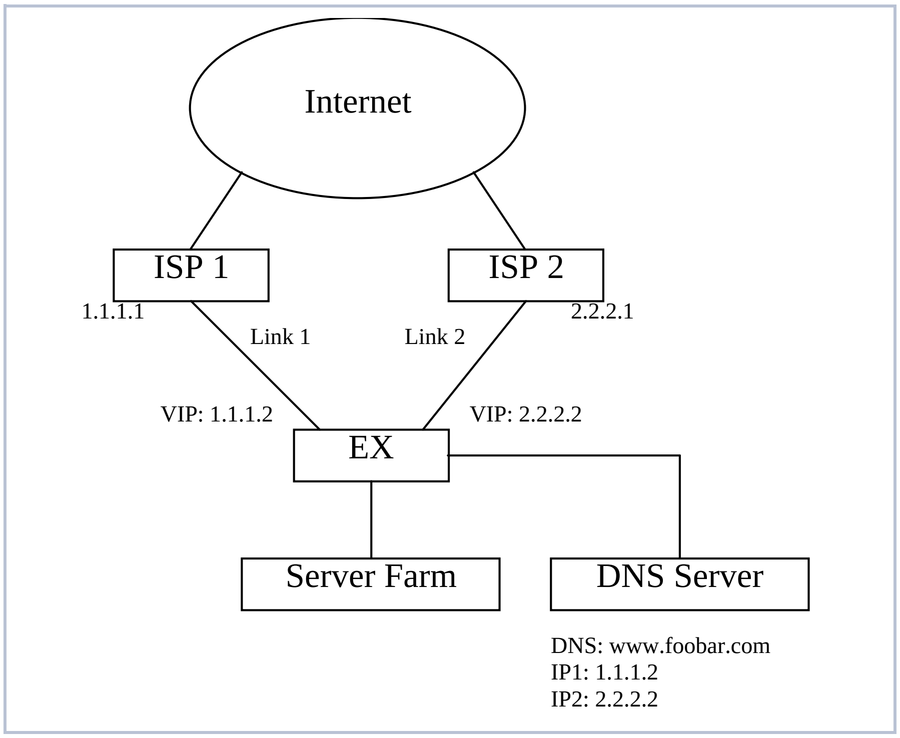
Link Load Balancing (Inbound and Outbound LLB)

Inbound LLB Configuration

Overview

In an inbound LLB configuration, connection requests from the Internet for services in the internal network are load balanced across available ISP links. Figure 2 shows a typical inbound link load balancing topology.

FIGURE 2. Typical Inbound Link load balancing topology



There are two virtual IP addresses: 1.1.1.2 and 2.2.2.2, configured on EX2100, each of which corresponds to a link. Both of the virtual IP addresses refer to the same server farm behind EX2100. Clients on the Internet access the service provided by the server farm by accessing the domain name "www.foobar.com", which resolves to the two virtual IPs.

Inbound link load balancing is implemented by watching the reverse part of inbound DNS connections (UDP port 53). If the domain name being resolved is bound to a link group, a link is selected from that group using the configured load-balancing method. Then EX2100 shuffles the IP addresses in the DNS reply to place the one that corresponds to the selected link on the top, so that later client requests will go through that link.

Note: The DNS LLB method requires the DNS traffic to and from the client to pass through the EX Secure WAN Manager. If the DNS server is in the same internal network as the servers the client is trying to access (as shown in Figure 2), you only need to bind the domain name to the LLB group.

If the DNS server is not in the internal network, you can configure the EX device to act as a proxy for the DNS server for the domain to be load balanced. In this case, a client DNS request for the domain is sent to the EX device, which sends the request to the DNS server. When the EX device receives the reply from the DNS server, the EX device sends the reply to the client. If required by LLB, the EX device re-orders the IP addresses in the reply before sending the reply to the client.

Summary of Steps

1. Optionally, configure Layer 3 health monitors to check the health of load-balanced paths.
2. If required, configure a DNS proxy for each domain to be load balanced. (See the note above.)
3. Configure the LLB links.
4. Configure the LLB domain.
5. Configure the LLB group.
6. Configure default routes to both gateways.

Command Syntax

The configuration example in this section uses the following commands. Only the commands used in this configuration example are shown here. For additional syntax information, see “Commands” on page 97.

1. To configure a Layer 3 health monitor for path health checking, use the following command at the global configuration level:

   ```
   health monitor monitor-name method icmp
     transparent ipaddr
   ```

   The **transparent** option is required and configures the health method to check the full path to the other end of the link. The *ipaddr* specifies the IP address of the device at the other end of the link.

2. To configure a DNS proxy, use the following command:

   ```
   dns proxy-server ip-address domain domain-name
   ```

   The *ip-address* is the IP address of the DNS server. The *domain-name* is the domain to be load balanced. Enter this command at the global configuration level.

3. To configure LLB links, use the following commands:

   ```
   llb link name
   [ip-address {subnet-mask | /mask-length}]
   ```

   Enter this command at the global configuration level to create the LLB link. The command changes the CLI to the configuration level for the link.

4. To configure LLB domains, use the following commands:

   ```
   llb domain domain
   ```

   Enter this command at the global configuration level to create an LLB domain. The command changes the CLI to the configuration level for the domain, where the following commands are available.

   ```
   host host [host [host ...]]
   ```

   This command configures hosts in the domain. Examples of commonly configured host names include “www” and “ftp”.

   ```
   policy {include | exclude}
   ```

   This command specifies when a fully qualified domain name (FQDN) matches:

   - **include** – only when the FQDN matches the domain ***and*** one of its hosts
   - **exclude** – only when the FQDN matches the domain ***but does not*** match any of its hosts

5. To configure LLB groups, use the following commands:

   ```
   llb group name
   ```

   Enter this command at the global configuration level to create an LLB group or to edit an existing group. The command changes the CLI to the configuration level for the group, where the following commands are available.

```
bind link name [name ...]

bind domain name [name ...]

bind  class class [class ...]

bind default  class
```

The **bind link** command adds a link to the group. The **bind domain** command specifies the fully-qualified domain name (FQDN) that clients request. On DNS servers, the domain name is mapped to the IP addresses of the inbound LLB links.

The **bind class** command binds individual traffic classes to the group. To use the LLB group for all traffic classes that are not explicitly bound to the link by **bind class** commands, use the **bind default class** command. (In this example, only the default class is used, to bind all traffic classes to the LLB group.)

6. To configure a default route, use the following command:

```
[no] ip route 0.0.0.0 {0.0.0.0 | /0} next-hop-ipaddr
[ethernet port-num] [ve vlan-id] [distance]
```

For the *next-hop-ipaddr*, specify the IP address of the gateway. Configure a separate default route through each gateway.

Configuration Example

The following commands log in and to access the configuration level of the CLI.

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
EX(config)#
```

The following commands configure a Layer 3 health monitor for the load-balanced paths:

```
EX(config)#health monitor llbpathcheck method icmp transparent 192.168.1.100
```

The following command adds a DNS proxy for DNS server 10.10.10.66 and domain name “foobar.com”:

```
EX(config)#dns proxy-server 10.10.10.66 domain foobar.com
```

The following commands configure the LLB links. In this example, NAT is configured for traffic class “default”. The default traffic class includes all classes that are not explicitly configured on the link. In this example, no traffic classes are explicitly configured on the link. The default class therefore applies to all traffic classes on the link.

```
EX(config)#llb link SBC 1.1.1.1 255.255.255.0
EX(config-llb link:SBC)#exit
EX(config)#llb link Comcast 2.2.2.1 255.255.255.0
EX(config-llb link:Comcast)#exit
```

The following commands configure the LLB domain.

```
EX(config)#llb domain foobar.com
EX(config-llb domain:foobar.com)#host www
EX(config-llb domain:foobar.com)#policy include
EX(config-llb domain:foobar.com)#exit
```

Note: The **policy include** command is shown for illustration purposes but is not required since **include** is the default.

The following commands configure the LLB group.

```
EX(config)#llb group mygroup
EX(config-llb group:mygroup)#bind link SBC
EX(config-llb group:mygroup)#bind link Comcast
EX(config-llb group:mygroup)#bind domain foobar.com
EX(config-llb group:mygroup)#bind default  class
```

The following commands configure default routes through the gateways:

```
EX(config)#ip route 0.0.0.0 /0 1.1.1.1
EX(config)#ip route 0.0.0.0 /0 2.2.2.1
```

Verify Inbound LLB Operation

To verify that the links are being load balanced, use the **nslookup** command on the clients, as shown in this example. Since the default load-balancing method (round-robin) is used, and persistence is not enabled, the IP addresses for the LLB domain should cycle among the link addresses.

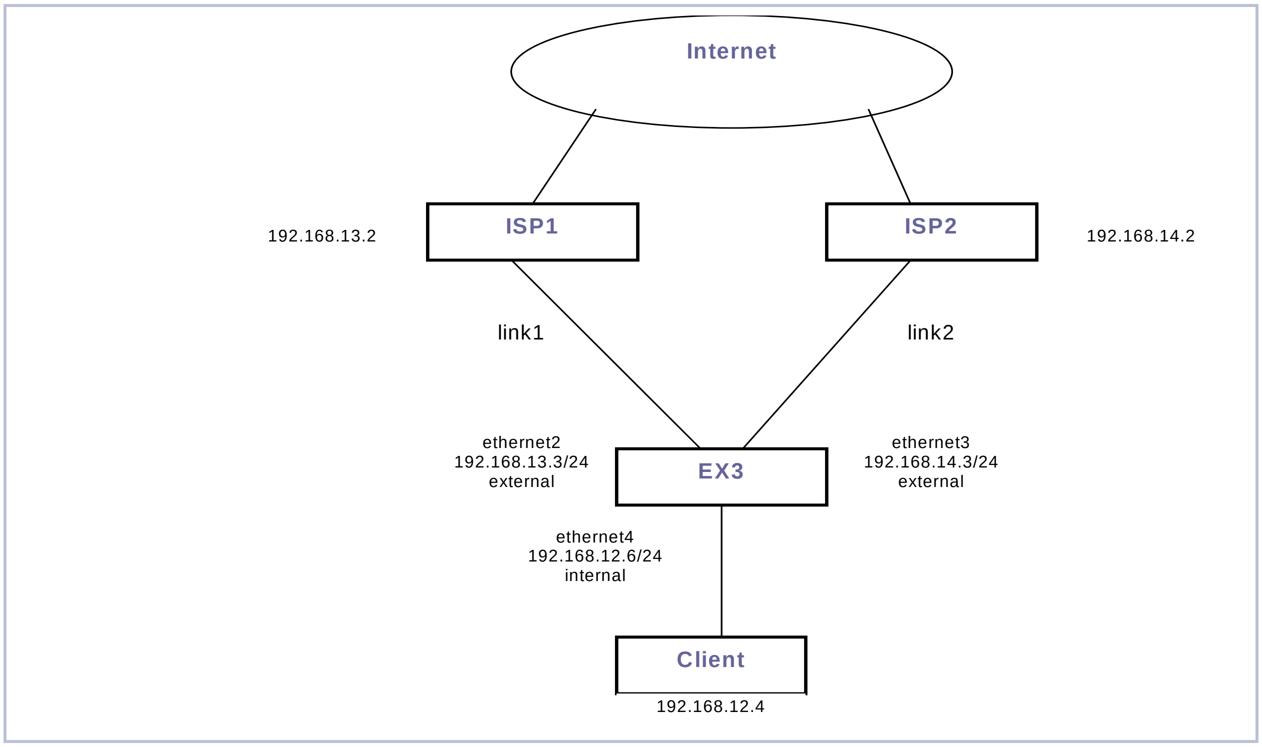
```
[root@Client]# nslookup -sil
> www.foobar.com
Name:   www.foobar.com
Address: 1.1.1.2
Name:   www.foobar.com
Address: 2.2.2.2

> www.foobar.com
Name:   www.foobar.com
Address: 2.2.2.2
Name:   www.foobar.com
Address: 1.1.1.2
```

Outbound LLB Configuration

Overview

In an outbound link load balancing configuration, connection requests from the internal network to the Internet are load balanced across the available ISP links. Figure 3 shows a typical inbound link load balancing topology.

FIGURE 3. Typical Outbound Link load balancing topology



Summary of Steps

1. Configure IP address pools, for use by NAT.
2. Configure the LLB links.
3. Configure the LLB group.
4. Verify LLB operation.

Command Syntax

The configuration commands used in this example are the same as those used in “Inbound LLB Configuration” on page 40. This example does introduce the following **show** command:

```
show llb link [name [name ...]] [detail]
```

Configuration Example

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX(config)#ippool pool3
EX(config-IP pool)#ip 192.168.13.254 to 192.168.14.254
EX(config-IP pool)#exit
EX(config)#llb link SBC 192.168.13.2 255.255.255.0
EX(config-llb link:SBC)#nat  class default ippool pool3
EX(config)#llb link Comcast 192.168.14.2 255.255.255.0
EX(config-llb link:Comcast)#nat  class default ippool pool3
EX(config)#llb group mygroup
EX(config-llb group:mygroup)#bind link SBC
EX(config-llb group:mygroup)#bind link Comcast
EX(config-llb group:mygroup)#bind default  class

EX#show llb link
Name     Gateway        Status   Curr Conn  Total Conn
SBC      192.168.13.2   Up       0          1
Comcast  192.168.14.2   Up       0          1

EX#show llb link detail
Name:                SBC
Status:              Up
Gateway:             192.168.13.2
Mask:                255.255.255.0

NAT IPs:             192.168.13.254
Bandwidth:           1000 (kbps)
Connection Limit:    0
Weight:              1
Health Monitor:
Enable/Disable:      Enabled
Sent:                9018 (bytes) / 148 (pkts)
Received:            210337 (bytes) / 157 (pkts)
Upstream:            0 (kbps) / 0 (pps)
Downstream:          0 (kbps) / 0 (pps)
Current Connection:  0
Connetion/sec:       0
Total Connection:    1

Name:                Comcast
Status:              Up
Gateway:             192.168.14.2
Mask:                255.255.255.0
```

```
NAT IPs:             192.168.14.254
Bandwidth:           1000 (kbps)
Connection Limit:    0
Weight:              1
Health Monitor:
Enable/Disable:      Enabled
Sent:                75 (bytes) / 1 (pkts)
Received:            113 (bytes) / 1 (pkts)
Upstream:            0 (kbps) / 0 (pps)
Downstream:          0 (kbps) / 0 (pps)
Current Connection:  0
Connetion/sec:       0
Total Connection:    1
```

Quality of Service (QoS) Configuration

Overview

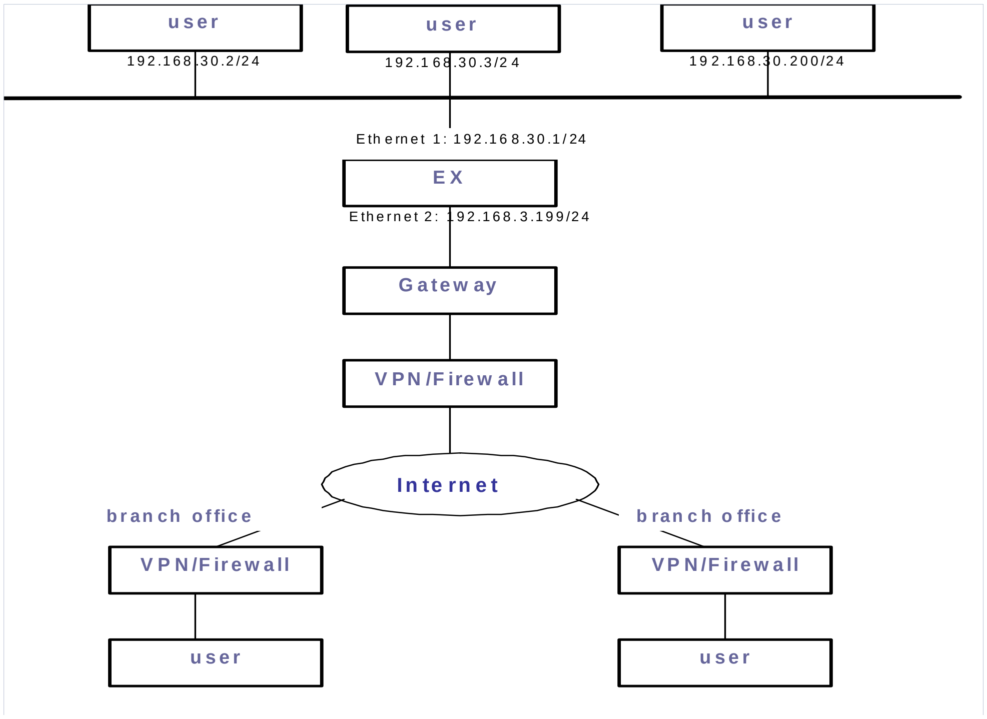
A user has a WAN link with 10M bits/sec bandwidth. The company's headquarters use a VoIP application to communicate with its branch offices all over the world. It is important to optimize WAN bandwidth with the most mission critical application, in this case VoIP.

Also, many of the branch offices need to access the company's internal Web portal on a timely basis, so it is the second most important application that needs to utilize the WAN link.

The network administrator decides to let the VoIP application have top priority to use its WAN Link, which can use up to 10M bits/sec of its bandwidth. Web traffic takes the second priority, but is only allowed to use up to 5M bits/sec. In this case, if VoIP is using 10M bits/sec bandwidth, then Web traffic has zero bandwidth.

The VoIP application uses the Session Initiation Protocol (SIP) to initialize the session, then uses the Real-Time Protocol (RTP) to transmit the voice data. Figure 4 shows the topology of this application.

FIGURE 4. Application Topology



Summary of Steps

1. Create Layer 7 traffic classes.
2. Create a traffic policy, add the traffic classes to the policy, and specify the action to take for class traffic.
3. Create interfaces, bind them to physical Ethernet interfaces, and apply the policy to the interfaces.
4. Verify operation and display the top (most active) classes.
5. Configure Simple Mail Transfer (SMTP) settings, to enable the EX device to email reports.
6. Display traffic reports.

Command Syntax

1. To configure classes, use the following commands:

   ```
   class name category category-name
   ```

   This command adds the specified class to the specified category, and changes the CLI to the configuration level for the class. The **category** is a high-level grouping of classes. In this example, the classes are added to the “VOIP” category.

```
match application name
```

This command, available at the configuration level for a class, assigns specific applications (for example, SIP and RTP) to the traffic class. (This command has many more options, which are not used in this example. See “qos class” on page 115.)

2. To configure policies, use the following commands:

```
 policy policy-name
```

This command creates or edits a policy for traffic management, and changes the CLI to the configuration level for the policy.

```
class class-name [precedence prec-value]
```

This command adds a traffic class to the policy. The **precedence** option is used for traffic that matches more than one class in the policy. If traffic matches two classes in the policy, the class with the lower precedence value will be used.

```
bandwidth {max max-rate [percent num]
  min min-rate [percent num]
  priority priority-value qlen queue-length}
```

This command limits the bandwidth for egress traffic leaving the interface.

3. To configure virtual interfaces, use the following command at the global configuration level:

```
 interface [name [name ...]]
```

This command adds or edits the specified interface, and changes the CLI to the configuration level for the interface.

```
port ethernet if-number [to if-number]

shape rate

 policy {ingress | egress} policy-name
```

The **port ethernet** command binds physical Ethernet interfaces to the interface. The **shape** command specifies the rate at which traffic is allowed to pass through the interface. The **policy** command applies a policy to ingress or egress traffic on the interface.

4. To display information, use the following commands:

```
show  interface
  [name [name ...] [statistics [options]]]

show  top [num] class
```

The **show interface** command shows the configuration of the specified interface. If you use the **statistics** option, statistics are displayed for the interface. The **show top class** command shows statistics for the most active traffic classes. The *num* option specifies how many classes for which to display information. The 10 most active classes are displayed by default.

5. To configure Simple Mail Transfer (SMTP) settings, to enable the EX device to email reports, use the following commands:

```
ip smtp {hostname | ip-address} [port port-num]

ip smtp mailfrom source-address

ip smtp needauthentication

ip smtp username user-name password password
```

The **mailfrom** option specifies the "from" email address of emails sent by the EX device. The **needauthentication** option specifies that a username and password are required to access the SMTP server. (For more information about the command, see "ip smtp" on page 224.)

6. To display traffic reports, use the following commands:

```
show traffic abuser top base-on [options]

show traffic class class-name [options]

show traffic connection [options]

show traffic external-talker ipaddr [options]

show traffic internal-talker ipaddr [options]

show   traffic   others-class   {dst   |   src}   ip
[options]

show traffic others-class {dst | src} [options]

show traffic packet-distribution [options]

show traffic rate [options]

show traffic tcp [options]

show traffic url [options]
```

The options are described in "Commands" on page 97.

Configuration Example

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
```

The following commands configure the “voip” traffic class.

```
EX(config)# class myvoip category voip
EX(config-class)#match application sip
EX(config-class)#match application rtp
EX(config-class)#exit
```

The following commands configure a policy to specify the handling of traffic in the voip class.

```
EX(config)# policy mypolicy
EX(config-policy)#class myvoip precedence 5
EX(config-policy-class)#bandwidth min 10000 max 10000 priority 0
EX(config-policy-class)#exit
EX(config-policy)#class http
EX(config-policy-class)#bandwidth min 0 max 5000 priority 1
EX(config-policy-class)#exit
EX(config-policy)#exit
```

The following commands configure Ethernet interfaces, prior to binding the interfaces to virtual interfaces.

```
EX(config)#interface ethernet 1
EX(config-if:ethernet1)#ip address 192.168.30.1 /24
EX(config-if:ethernet1)#interface ethernet 2
EX(config-if:ethernet2)#ip address 192.168.3.199 /24
EX(config-if:ethernet2)#external
EX(config-if:ethernet2)#exit
```

The following commands configure the virtual interfaces.

```
EX(config)# interface inside
EX(config--intf)#port ethernet 1
EX(config--intf)#shape 10000
EX(config--intf)# policy egress mypolicy
EX(config--intf)#exit
EX(config)# interface outside
EX(config--intf)#port ethernet 2
EX(config--intf)#shape 10000
EX(config--intf)# policy egress mypolicy
EX(config--intf)#exit
```

The following command displays configuration information for the interfaces.

```
EX#show  interface

 interface inside
  port ethernet 1
  shape 10000
   policy egress mypolicy

 interface outside
  port ethernet 2
  shape 10000
   policy egress mypolicy
```

The following command displays statistics for the interfaces.

```
EX#show  interface inside outside statistics

  shape interface inside 10000
     Average Rate: 83 Kbps
     Queue length: 0
     Dropped packets: 0
  inside egress Policy mypolicy:
     Class: myvoip prec 5
       Current rate:  83 Kbps
       Average rate : 83 Kbps
       Peak rate:  88 Kbps
       Active sessions : 1
       Dropped packets:  0
       Queue length:  0
     Class: http prec 10
       Current rate:  0 Kbps
       Average rate : 0 Kbps
       Peak rate:  0 Kbps
       Active sessions : 0
       Dropped packets:  0
       Queue length:  0
     Class: default-class prec 10
       Current rate:  0 Kbps
       Average rate : 0 Kbps
       Peak rate:  280 Kbps
       Active sessions : 2

shape interface outside 10000
     Average Rate: 90 Kbps
     Queue length: 0
     Dropped packets: 0
  outside egress Policy mypolicy:
     Class: myvoip prec 5
       Current rate:  91 Kbps
       Average rate : 90 Kbps
       Peak rate:  101 Kbps
       Active sessions : 1
       Dropped packets:  0
       Queue length:  0
     Class: http prec 10
       Current rate:  0 Kbps
       Average rate : 0 Kbps
       Peak rate:  3 Kbps
       Active sessions : 0
       Dropped packets:  0
       Queue length:  0
     Class: default-class prec 10
       Current rate:  0 Kbps
       Average rate : 0 Kbps
       Peak rate:  1530 Kbps
       Active sessions : 2
```

The following command displays statistics for the busiest traffic classes. In this example, “myvoip” is the busiest class.

```
EX(config)#show  top class
 top 10 classes

 class myvoip :
   Inbound:  Curren rate: 81   Kbps, average rate: 83   Kbps, peak rate :90   Kbps
   Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :42   Kbps

 class rtp :
   Inbound:  Curren rate: 81   Kbps, average rate: 83   Kbps, peak rate :90   Kbps
   Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :31   Kbps

 class others :
   Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :306  Kbps
   Outbound: Curren rate: 1    Kbps, average rate: 1    Kbps, peak rate :1951 Kbps

 class rtcp :
   Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :1    Kbps
   Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :2    Kbps
```

```
class t120 :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps

class skype :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps

class skinny :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps

class sip :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :6    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :18   Kbps

class mgcp :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps

class megaco :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps

class h323q931 :
  Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
  Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :0    Kbps
```

The following commands configure the EX device to be able to send email to a Simple Mail Transfer Protocol (SMTP) server.

```
EX(config)#ip smtp mail.example.com
EX(config)#ip smtp mailfrom EXdevice1@example.com
EX(config)#ip smtp needauthentication
EX(config)#ip smtp username admin1 password mypwd123
```

The following command shows a traffic report for the top 10 internal talkers:

```
EX(config)#show traffic rate top-internal-talker top-num 10

Traffic Rate Statistics Summary
=========================================
Start Time          : 2010-01-30 15:32:00
End Time            : 2010-01-30 16:02:00
Connection Direction: All

------------------------------------------------------------------------------
---------------------------------------------------
Talker           Username                         bps (Inb/Outb)    Bytes
(Inb/Outb)  pps (Inb/Outb)    Pkts (Inb/Outb)   Percent
------------------------------------------------------------------------------
---------------------------------------------------
```

```
10.100.215.11   N/A                         6.8M (0/6.8M)    1.5G (0/1.5G)
8.9K (0/8.9K)     15M (0/15M)       28.91%
10.100.213.50   N/A                              3.7M (2.3M/1.3M)  838M
(539M/299M)  2.8K (1.4K/1.4K)  5.0M (2.5M/2.4M)  15.65%
10.100.211.26   N/A                         2.9M (216K/2.7M) 660M (47M/613M)
1.9K (417/1.5K)   3.3M (732K/2.6M)  12.33%
10.100.211.29   N/A                         2.9M (212K/2.7M) 659M (46M/612M)
1.9K (409/1.5K)   3.4M (718K/2.7M)  12.30%
10.100.213.163  N/A                              1.5M (638K/947K)  348M
(140M/208M)  317 (147/170)     557K (257K/299K)  6.50%
10.100.215.25   N/A                         1.2M (989K/263K) 275M (217M/57M)
371 (209/162)     651K (366K/284K)  5.13%
10.100.213.170  N/A                         644K (467K/177K) 141M (102M/38M)
122 (70.10/52.39)  215K (123K/92K)   2.64%
10.100.1.76     N/A                         445K (429K/16K)  97M (94M/3.5M)
64.94 (38.50/26.44)  114K (67K/46K)    1.82%
10.100.215.126  N/A                         381K (23K/358K)  83M (5.0M/78M)
123 (41.23/82.12)  216K (72K/144K)   1.56%
10.100.213.139  N/A                         371K (135K/236K) 81M (29M/51M)
74.75 (36.32/38.43)  131K (63K/67K)    1.52%
```

The following command shows a traffic report for the top 10 external talkers:

```
EX(config)#show traffic rate top-external-talker top-num 10

Traffic Rate Statistics Summary
=========================================
Start Time          : 2010-01-30 15:32:30
End Time            : 2010-01-30 16:02:30
Connection Direction: All

------------------------------------------------------------------------------
---------------------------------------------------
Talker           Domain                           bps (Inb/Outb)    Bytes
(Inb/Outb)  pps (Inb/Outb)    Pkts (Inb/Outb)   Percent
------------------------------------------------------------------------------
---------------------------------------------------
10.10.10.23                                 6.8M (0/6.8M)    1.5G (0/1.5G)
8.9K (0/8.9K)     15M (0/15M)       29.20%
10.100.20.18                                6.0M (445K/5.5M) 1.3G (97M/1.2G)
3.9K (859/3.1K)   7.0M (1.4M/5.5M)  25.57%
10.100.1.207                                     2.3M (1.8M/539K)  538M
(420M/118M)  764 (395/369)     1.3M (693K/648K)  10.15%
10.100.1.141                                     1.3M (541K/818K)  298M
(118M/179M)  2.1K (1.0K/1.0K)  3.7M (1.8M/1.8M)  5.62%
10.100.20.185                               1.2M (989K/263K) 275M (217M/57M)
371 (209/162)     651K (366K/284K)  5.18%
10.100.20.176                               968K (753K/216K) 212M (165M/47M)
199 (105/93.20)   349K (185K/163K)  4.01%
```

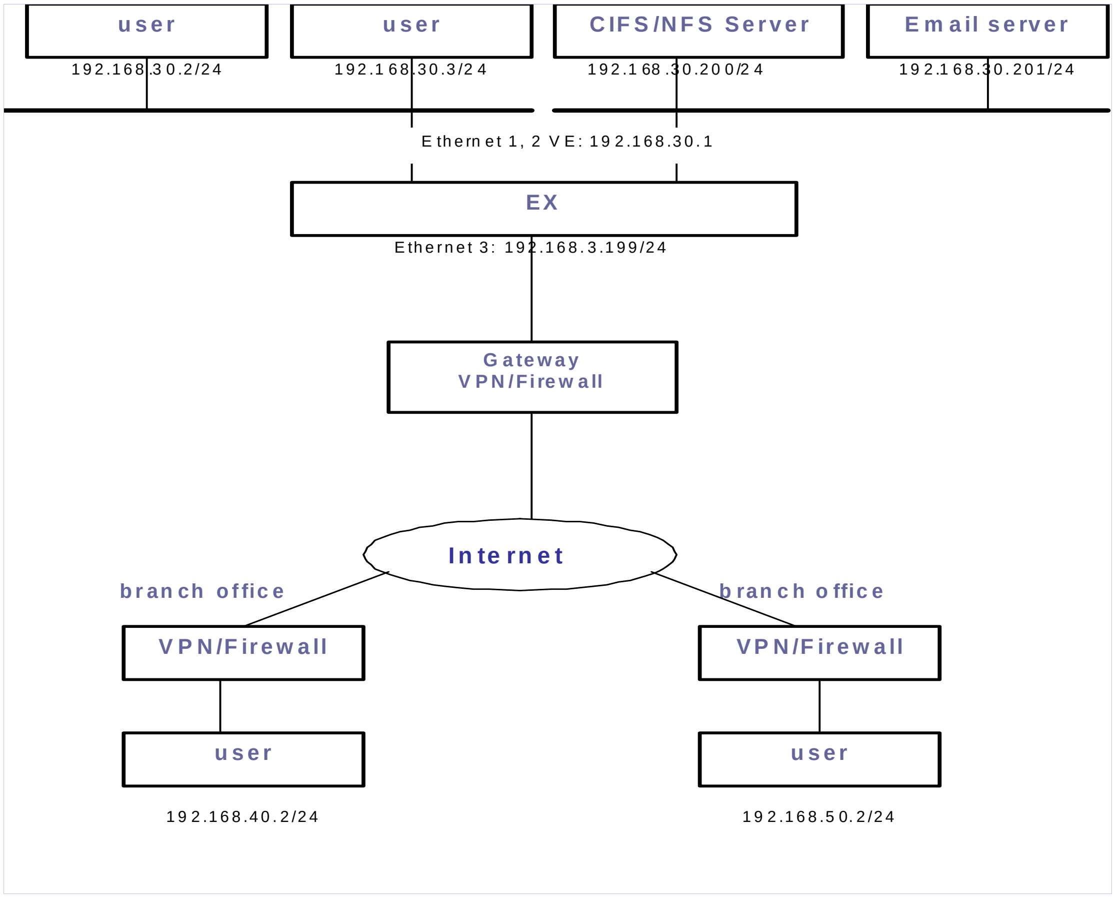
```
10.100.20.146                                      852K (425K/427K)  187M (93M/93M)
122 (60.80/61.27)  214K (106K/107K)  3.53%
10.100.20.124                                      604K (166K/438K)  132M (36M/96M)
114 (48.48/65.26)  199K (85K/114K)   2.50%
10.100.20.26                                       387K (23K/364K)   85M (5.1M/79M)
135 (47.71/87.50)  237K (83K/153K)   1.60%
10.100.32.184                                      385K (24K/361K)   84M (5.2M/79M)
128 (42.89/85.53)  225K (75K/150K)   1.59%
```

Application Logging (applog) Configuration

Overview

The EX Secure WAN Manager supports logging of application operations for instant messaging, file access, and email. Administrators can selectively enable logging for application operations of interest.

FIGURE 5. Application Logging Topology



Ethernet 1 and Ethernet 2 are configured to form a VLAN, so all traffic that accesses the CIFS/NFS/Email servers goes through the EX Secure WAN Manager.

Summary of Steps

1. Configure a VLAN and configure a Virtual Ethernet (VE) interface on the VLAN.
2. Configure an application log (applog) filter.
3. (Optional) Configure an applog alias.
4. Enable application logging.
5. (Optional) Change the set of actions to log for each logged application. By default, logging is enabled for all actions that can be logged.
6. (Optional) Enable dynamic IP-to-ID mapping using an IDsentrie device, or configure static IP-to-ID mappings. IP-to-ID mappings enable the EX device to show usernames as well as IP addresses in applog entries (logged application actions).
7. Display applog entries.

Command Syntax

1. To configure VLANs and VEs, use the following commands:

   ```
   vlan vlan-id
   ```

   This command creates a VLAN and enters the configuration level for the VLAN.

   ```
   tagged ethernet port-num
     [ethernet port-num ... | to port-num]

   untagged ethernet port-num
     [ethernet port-num ... | to port-num]

   interface ve ve-num

   ip address ip-address {subnet-mask | /mask-length}
   ```

   The **tagged** and **untagged** commands add physical Ethernet interfaces to the VLAN. Use the **tagged** command to add interfaces that also will be members of at least one other VLAN. Use the **untagged** command to add interfaces that will be members of this VLAN only.

   The **interface ve** command changes the CLI to the configuration level for the VLAN's Virtual Ethernet (VE) interface. The VE is created automatically when you configure the VLAN. For *ve-num*, use the same number as the VLAN ID.

   The **ip address** command configures an IP address on the VE, and thus on the VLAN.

2. To configure an application log (applog) filter, use the following commands:

   ```
   applog filter filter-name
   ```

   This command creates an applog filter and changes the CLI to the configuration level for the filter.

   ```
   include ip-address {subnet-mask | /mask-length}

   exclude ip-address {subnet-mask | /mask-length}
   ```

   The **include** command specifies an IP host or subnet to log. Conversely, the **exclude** command specifies a host or subnet to exclude from logging.

3. To configure an applog alias, use the following command:

   ```
   applog alias alias-name {aim | msnim | yim | ftp |
   nfs | cifs | smtp | pop3 | qq}
   ```

   Configuring an alias simplifies the task of binding applications to applog filters. You can bind an applog filter to multiple applications by binding the filter to the alias for those applications.

4. To enable application logging, use the following command to bind the applog filter to individual applications or to an applog alias:

   ```
   applog bind filter-name [alias alias-name] |
   [aim] [msnim] [yim] [ftp] [nfs] [cifs] [smtp] [pop3]
   [qq]
   ```

5. To change the set of actions to log for each logged application, use the following command:

   ```
   [no] applog enable application [action] [action ...]
   ```

   Logging is enabled for all actions by default. To disable logging for an action, use the **no** option in front of the command. For example, to disable logging of the CIFS logoff action, enter the following command:

   ```
   no applog enable cifs logoff
   ```

6. To configure IP-to-ID mappings, use either of the following commands:

   ```
   ip2id static ip-address user-name

   ip2id IDsentrie host {hostname | ip-address}
   port port username user-name password password
   [interval minutes]
   ```

   The **ip2id static** command configures IP-to-ID mappings. The **ip2id IDsentrie** command configures the EX device to dynamically retrieve IP-to-ID mappings from an IDsentrie device.

7. To display applog entries, use the following command:

   show applog

   (This command has many options for filtering the output. See "show applog" on page 307.)

Configuration Example

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
```

The following commands configure VLAN 2 and configure an IP address on the VLAN's VE.

```
EX(config)#vlan 2
EX(config-vlan:2)#untagged ethernet 1
EX(config-vlan:2)#untagged ethernet 2
EX(config-vlan:2)#exit
EX(config)#interface ve 2
EX(config-if:ve2)#ip address 192.168.30.1 /24
EX(config-if:ve2)#exit
```

The following commands configure the application filter. In this example, three subnets are included.

```
EX(config)#applog filter myfilter
EX(config-filter)#include 192.168.30.0 /24
EX(config-filter)#include 192.168.40.0 /24
EX(config-filter)#include 192.168.50.0 /24
EX(config-filter)#exit
```

The following command configures an alias for the applications to be logged in this example.

```
EX(config)#applog alias myapp smtp pop3 nfs cifs yim
```

The following command binds the applog filter to the applog alias. The applications referred to by the alias will be logged, when used by the IP addresses included in the applog filter.

```
EX(config)#applog bind myfilter alias myapp
```

The following command configures the EX device to dynamically obtain IP-to-ID mappings from an IDsentrie.

```
EX(config)#ip2id IDsentrie host 192.168.3.225 port 2391 username admin password
a10
```

The following command displays applog entries.

```
EX(config)#show applog
Type         Time             User Name            Application User Name
==============================================================================
aim          Dec  9 17:44:09  user4@ldap           user4_raksha
  Source IP           : 192.168.3.88
  Source Hostname     : user2
  Destination IP      : 64.12.161.153
  Action              : logon
  Action Detail       :
==============================================================================
msnim        Dec  9 17:19:58  user5@aexample.com   user5@webmailapp.com
  Source IP           : 192.168.3.55
  Source Hostname     : dell-1100
  Destination IP      : 207.46.109.39
  Action              : logoff
  Action Detail       :
==============================================================================
yim          Dec  9 17:44:09 user4@ldap            user4_raksha
  Source IP           : 192.168.3.79
  Source Hostname     : B893D7C217924A2
  Destination IP      : 76.13.15.55
  Action              : logon
  Action Detail       :
==============================================================================
ftp          Dec  9 17:23:37  N/A                  upgrade
  Source IP           : 192.168.3.2
  Source Hostname     : ex
  Destination IP      : 192.168.3.29
  Action              : retrieve
  Action Detail       : file /tftp-
boot/rima_image/upgrade/BLD_RIMA_MAIN_2_4_0_186_20081205_103224_GMT.upg
==============================================================================
ftp          Dec  9 17:23:31  N/A                  upgrade
  Source IP           : 192.168.3.2
  Source Hostname     : ex
  Destination IP      : 192.168.3.29
  Action              : logon
  Action Detail       :
==============================================================================
nfs          Dec  9 17:18:53  N/A                  0.0@GSLB
  Source IP           : 192.168.3.2
  Destination IP      : 192.168.3.85
  Action              : read
  Action Detail       : file
```

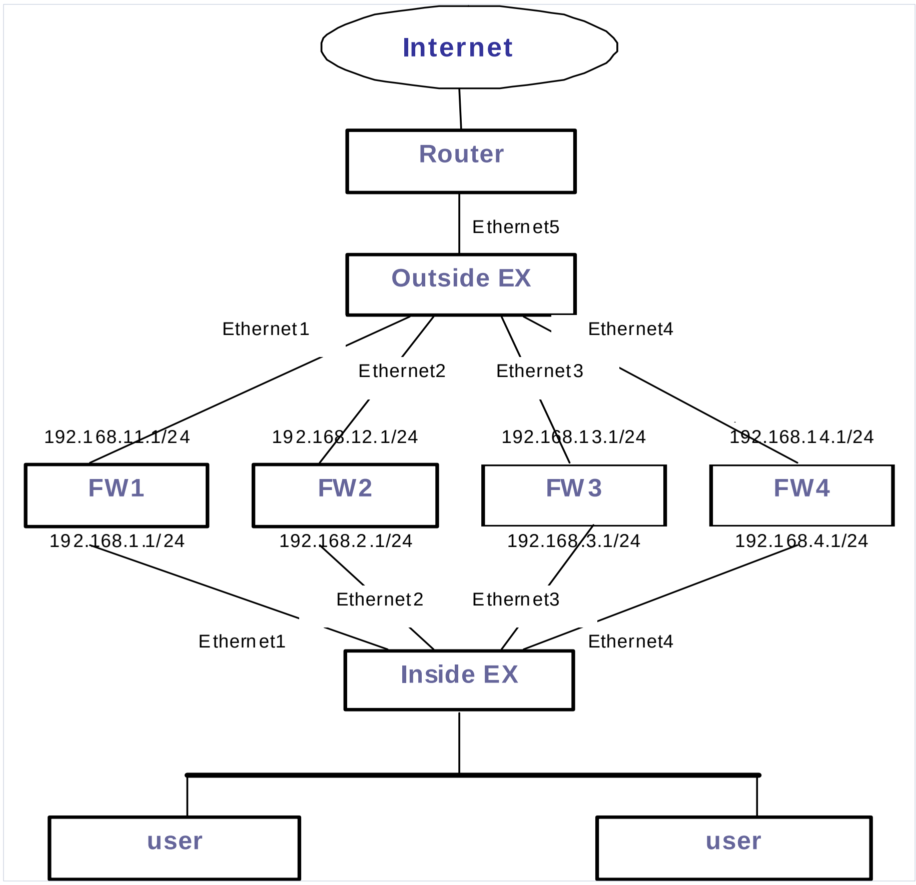
```
==============================================================================
cifs         Dec  9 17:49:49  user7@ldap           user7@DOCSERVER-BJ
  Source IP           : 192.168.3.18
  Source Hostname     : computer
  Destination IP      : 192.168.3.91
  Action              : open
  Action Detail      : file \\192.168.3.91\ \Release 2.4\Test  Point\R2.4.0 and
Lancope_QA_testpoint_Disable_SSHV1_Mainline_awang(working).xls
==============================================================================
smtp         Dec  9 17:49:07  N/A                  user9@example.com
  Source IP           : 192.168.3.8
  Source Hostname     : email-server
  Destination IP      : 75.48.114.228
  Action              : mail
  Action Detail       : subject [Bug 99999] forgot to tell the tech writer
                          something again
                        to all@example.com
                        attachment EMPTY.
==============================================================================
pop3         Dec  9 17:51:14 user88@example.com.cn user88@example.com.cn
  Source IP           : 192.168.3.93
  Source Hostname     : example-user88pc
  Destination IP      : 218.241.65.21
  Action              : mail
  Action Detail       : subject user88 commits BugID: 99999 on linux-kernel of
br_ax_1_2_4_release MODIFIED: patches, config_sto.patch...
                        from user77@example.com
                        attachment EMPTY.
==============================================================================
qq           Dec  9 17:45:06  it1@example.com.cn 26960568
  Source IP           : 192.168.3.117
  Source Hostname     : IT-PC
  Destination IP      : 58.251.63.57
  Action              : logon
  Action Detail       :
==============================================================================
http         Dec  9 17:51:48  N/A
  Source IP           : 192.168.3.38
  Source Hostname     : user66
  Destination IP      : 72.14.235.100
  Action              : post
  Action Detail       :
URL:http://docs.google.com/RawDocContents?action=store&justBody=true&docID=d68
sh6n_123czzf4zcg&tok=ucmpionconv51228789419109&ct=57&tzo=480&strip=false
                        DATA:revisio-
nID=d68sh6n_123czzf4zcg%3A132&POST_TOKEN=P9KRPR4BAAA.1FckinCyTDyxW05VRfzB2FDJ6
3dvuw7DPVDqreO
==============================================================================
```

Firewall Load Balancing (FWLB) Configuration

Overview

EX Secure WAN Manager's FWLB can distribute traffic across two or more firewalls to provide increased firewall service scalability and redundancy.

FIGURE 6.   FWLB Topology



In this example, a pair of EX devices is configured to provide FWLB for four firewalls. One EX device is deployed between the inside hosts and the firewalls. This is the inside EX device. The other EX device is deployed between the firewalls and the Internet. This is the outside EX device. An FWLB configuration must have inside and outside EX devices.

Summary of Steps

1. Specify the traffic classes to load balance. You can specify individual classes. To load balance all traffic classes, specify the “default” class.
2. Create the firewall nodes and firewall group.
3. Specify the EX device’s location in the network, inside or outside, relative to the firewalls.
4. Specify the IP address of the peer EX device (the device on the other side of the firewalls).
5. Specify the locations of the physical Ethernet interfaces, internal or external. Internal interfaces are connected to the internal hosts on the protected side of the network. External interfaces are connected to the Internet. Each EX device will have both internal and external FWLB interfaces.
6. Verify FWLB operation.

Command Syntax

1. To specify the traffic classes to load balance, use the following commands:

   ```
   class name category category-name
   ```

   This command creates the class if not already created, and changes the CLI to the configuration level for the class. To provide FWLB for all traffic classes, use **default** as the class name.

   ```
   match
     [dport protocol-port]
     [sport protocol-port]
   ```

   This command specifies the Layer 4 source and destination application ports that belong to the traffic class.

Note: The **match** command has many more options, which are not used in this example. See “qos class” on page 115. All match options except **application** *name* are supported for FWLB.

2. To create the firewall nodes and firewall group, use the following commands:

   ```
   fwlb node name
   [ip-address {subnet-mask | /mask-length}]
   ```

   This command creates a firewall node and changes the CLI to the configuration level for the node.

The following command creates a firewall group and changes the CLI to the configuration level for the group.

```
fwlb group name
```

At the configuration level for the firewall group, you can use the following commands to bind firewall nodes and traffic classes to the group:

```
bind node name [name ...]

bind  class [class [class ...]]

bind default  class
```

The **bind node** command binds a firewall node to the group. The **bind class** command binds individual traffic classes to the group. The **bind default class** command binds all traffic classes to the group, except any classes that are not explicitly bound to the group, or that are explicitly unbound from the group.

3. To specify the EX device's location in the network, inside or outside, relative to the firewalls, use the following command:

   ```
   fwlb enable {inside | outside}
   ```

4. To specify the IP address of the peer EX device (the device on the other side of the firewalls), use the following command:

   ```
   fwlb peer ip-address {subnet-mask | /mask-length}
   ```

   Enter the command separately for each subnet. In this example, the command needs to be entered four times.

5. To specify the physical Ethernet interfaces connected to the firewalls, use the following commands:

   ```
   interface ethernet num

   {internal | external}
   ```

   The **interface ethernet** command changes the CLI to the configuration level for an interface. Use the *num* option to specify the interface number.

   The **internal** | **external** command specifies the side of the configuration that is reached through the interfaces.

   - If the interface connects the EX device to the internal hosts, specify **internal**.
   - If the interface connects the EX device to the Internet, specify **external**.

6. To verify FWLB configuration and operation, use the following commands:

   show fwlb node [*name* [*name* ...]] [**detail**]

   show fwlb group [*name* [*name*...]] [**detail**]

Configuration Example for Inside EX Device

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
```

The following commands configure a traffic class and specify the source and destination application ports that belong to the class.

```
EX(config)# class myhttp category Misc
EX(config-class)# match dport 80
EX(config-class)# match sport 80
EX(config-class)# match sport 443
EX(config-class)# match dport 443
EX(config-class)#exit
```

The following commands configure the FWLB nodes and FWLB group.

```
EX(config)#fwlb node fw1 192.168.1.1 /24
EX(config-fwlb node:fw1)#exit
EX(config)#fwlb node fw2 192.168.2.1 /24
EX(config-fwlb node:fw2)#exit
EX(config)#fwlb node fw3 192.168.3.1 /24
EX(config-fwlb node:fw3)#exit
EX(config)#fwlb node fw4 192.168.4.1 /24
EX(config-fwlb node:fw4)#exit
EX(config)#fwlb group fwgroup1
EX(config-fwlb group:fwgroup)#bind node fw1
EX(config-fwlb group:fwgroup)#bind node fw2
EX(config-fwlb group:fwgroup)#bind  class myhttp
EX(config-fwlb group:fwgroup)#exit
EX(config)#fwlb group fwgroup2
EX(config-fwlb group:fwgroup)#bind node fw3
EX(config-fwlb group:fwgroup)#bind node fw4
EX(config-fwlb group:fwgroup)#bind default  class
EX(config-fwlb group:fwgroup)#exit
```

The following command specifies the EX device’s location in the topology:

```
EX(config)#fwlb enable inside
```

The following commands specify the IP addresses of the peer EX device on the other side of the firewalls.

```
EX(config)#fwlb peer 192.168.11.1 /24
EX(config)#fwlb peer 192.168.12.1 /24
EX(config)#fwlb peer 192.168.13.1 /24
EX(config)#fwlb peer 192.168.14.1 /24
```

The following commands specify the physical Ethernet interfaces that connect the EX device to the Internet and to the internal hosts.

```
EX(config)#interface ethernet 1
EX(config-if:ethernet1)#external
EX(config-if:ethernet1)#exit
EX(config)#interface ethernet 2
EX(config-if:ethernet2)#external
EX(config-if:ethernet2)#exit
EX(config)#interface ethernet 3
EX(config-if:ethernet3)#external
EX(config-if:ethernet3)#exit
EX(config)#interface ethernet 4
EX(config-if:ethernet4)#external
EX(config-if:ethernet4)#exit
EX(config)#interface ethernet 5
EX(config-if:ethernet5)#internal
EX(config-if:ethernet5)#exit
```

Configuration Example for Outside EX Device

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
EX(config)# class myhttp category Misc
EX(config-class)# match dport 80
EX(config-class)# match sport 80
EX(config-class)# match dport 443
EX(config-class)# match sport 443
EX(config-class)#exit
EX(config)#fwlb node fw1 192.168.11.1 /24
EX(config-fwlb node:fw1)#exit
EX(config)#fwlb node fw2 192.168.12.1 /24
EX(config-fwlb node:fw2)#exit
EX(config)#fwlb node fw3 192.168.13.1 /24
EX(config-fwlb node:fw3)#exit
EX(config)#fwlb node fw4 192.168.14.1 /24
EX(config-fwlb node:fw4)#exit
EX(config)#fwlb group fwgroup1
EX(config-fwlb group:fwgroup)#bind node fw1
EX(config-fwlb group:fwgroup)#bind node fw2
EX(config-fwlb group:fwgroup)# bind  class myhttp
EX(config-fwlb group:fwgroup)#exit
EX(config)#fwlb group fwgroup2
EX(config-fwlb group:fwgroup)#bind node fw3
EX(config-fwlb group:fwgroup)#bind node fw4
EX(config-fwlb group:fwgroup)# bind default  class
EX(config-fwlb group:fwgroup)#exit
EX(config)#fwlb enable outside
EX(config)#fwlb peer 192.168.1.1 /24
EX(config)#fwlb peer 192.168.2.1 /24
EX(config)#fwlb peer 192.168.3.1 /24
EX(config)#fwlb peer 192.168.4.1 /24
EX(config)#interface ethernet 1
EX(config-if:ethernet1)#internal
EX(config-if:ethernet1)#exit
EX(config)#interface ethernet 2
EX(config-if:ethernet2)#internal
EX(config-if:ethernet2)#exit
EX(config)#interface ethernet 3
EX(config-if:ethernet3)#internal
EX(config-if:ethernet3)#exit
EX(config)#interface ethernet 4
EX(config-if:ethernet4)#internal
EX(config-if:ethernet4)#exit
EX(config)#interface ethernet 5
EX(config-if:ethernet5)#external
EX(config-if:ethernet5)#exit
```

FWLB Information Displayed on Inside EX Device

Here is an example of FWLB configuration information and statistics. The commands in this example are entered on the inside EX device.

```
EX#show fwlb node detail
Name:                fw1
Type:                Firewall
Status:              Running
IP Addr:             192.168.1.1
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                464712931 (bytes) / 1254721 (packets)
Received:            964900745 (bytes) / 1222175 (packets)
```

```
Current Connection:  737
Total Connection:    104388

Name:                fw2
Type:                Firewall
Status:              Running
IP Addr:             192.168.2.1
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                442186432 (bytes) / 1360295 (packets)
Received:            1288372883 (bytes) / 1443133 (packets)
Current Connection:  706
Total Connection:    103569

Name:                fw3
Type:                Firewall
Status:              Running
IP Addr:             192.168.3.1
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                464713763 (bytes) / 1254323 (packets)
Received:            964900547 (bytes) / 1222452 (packets)
Current Connection:  737
Total Connection:    104388

Name:                fw4
Type:                Firewall
Status:              Running
IP Addr:             192.168.4.1
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                442186432 (bytes) / 1360295 (packets)
Received:            1288372883 (bytes) / 1443133 (packets)
Current Connection:  706
Total Connection:    103569

EX #show fwlb group detail
Name:                fwgroup2
Method:              Round Robin
Persistent:          Disabled
Sent:                906966253 (bytes) / 2615079 (packets)
Received:            2252224646 (bytes) / 2663715 (packets)
```

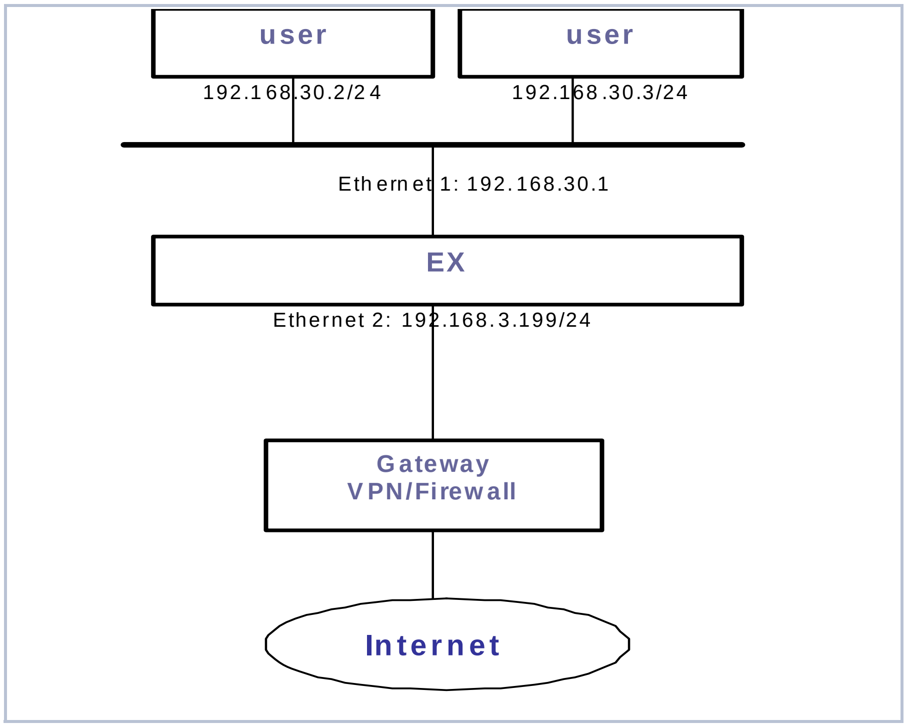
```
Current Connection:  1449
Total Connection:    207782
Members:             fw1
                     fw2
 Classes:         myhttp

Name:                fwgroup1
Method:              Round Robin
Persistent:          Disabled
Sent:                83222323 (bytes) / 24232322 (packets)
Received:            232325667565 (bytes) / 245656564 (packets)
Current Connection:  1643
Total Connection:    2334478
Members:             fw3
                     fw4
 Classes:         <default>
```

Intrusion Prevention System (IPS) Configuration

Overview

EX Secure WAN Manager supports attack detection and defense using the Intrusion Prevention System (IPS). You can configure IPS to detect and take action against specific types of malicious traffic.

FIGURE 7. IPS Application Topology



Summary of Steps

1. Configure an IPS group (unless you plan to use the default IPS group).
2. Bind the IPS group to physical interfaces.
3. Display IPS log entries and statistics.

Command Syntax

1. To display the default IPS group, use the following command:

```
show default | sec ips
```

To configure an IPS group, use the following commands:

```
ips group group-name
```

This command creates the IPS group and changes the CLI to the configuration level for the group.

The following commands configure the IPS filters used in this example.

```
tcp checkflag {drop | clearsession | reset |
  resetclient | resetserver} [log]

tcp synflood
[threshold synnumbers [interval milliseconds [log]]]

udp flood
[threshold threshold [interval millisecond
[hold seconds [log]]]]

icmp flood
[threshold threshold [interval millisecond
[hold seconds [log]]]]

exceed rate destination
[threshold threshold [interval milliseconds
[hold seconds [log]]]]

exceed rate source
[threshold threshold [interval milliseconds
[hold seconds [log]]]]
```

Many more IPS filters are available. See "IPS Commands" on page 179 for more information.

2. To bind an IPS group to physical interfaces, use the following commands:

   ```
   interface ethernet num
   ```

   The **interface ethernet** command changes the CLI to the configuration level for an interface. Use the *num* option to specify the interface number.

   ```
   ips group-name
   ```

   The **ips** command binds the specified IPS group to the interface.

3. To display IPS log entries and statistics, use the following commands:

   ```
   show log | sec IPS

   show ips counters
   [ethernet portnum [ethernet portnum ...]]
   ```

The **show log** command displays log messages contained in the log buffer. The **| sec IPS** option is an output filter that displays only messages that contain the string “sec IPS”.

Note: For log messages to be generated when traffic matches an IPS filter, you must use the **log** option with the filter.

The **show ips counters** command displays statistics counters for the types of attacks detected by the IPS filters.

Configuration Example

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
```

The following command displays the default IPS group.

```
EX#show default | sec ips
ips group default
 exceed rate source threshold 2000 interval 1000 hold 120 log
 icmp ping maxlength
 ip land log drop
 tcp checkflag log drop
 tcp flood threshold 2000 interval 100 hold 120 log
 tcp synflood threshold 30000 interval 1000 log
 tcp synfragment log drop
 udp flood threshold 2000 interval 100 hold 120 log
```

The following commands configure a new IPS group.

```
EX(config)#ips group myipsgroup
EX(config-ips-group)#tcp checkflags log drop
EX(config-ips-group)#tcp synflood
EX(config-ips-group)#udp flood
EX(config-ips-group)#icmp flood
EX(config-ips-group)#exceed rate destination
EX(config-ips-group)#exceed rate source
```

The following commands bind the IPS group to a physical Ethernet interface.

```
EX(config)#interface ethernet 2
EX(config-if:ethernet2)#ips myipsgroup
```

The following command shows IPS statistics counters.

```
EX#show ips counters
IPS Statistics of the system is:
    hold source ip :                            0
    ping of death :                             0
    unknown protocol :                          0
    ip land :                                   0
    syn fragment :                              0
    tcp check flag :                            1
    icmp broadcast echo request :               0
    udp broadcast echo request :                0
    icmp broadcast :                            0
    ip record route option :                    0
    ip strict source route option :             0
    ip security option :                        0
    ip loose source route :                     0
    ip malformed option :                       0
    ip with option :                            0
    ip time stamp option :                      0
    ip stream option :                          0
    ip fragment packet :                        0
    syn flood :                                 0
    icmp type :                                 0
    icmp flood :                                0
    tcp flood :                                 0
    udp flood :                                 0
    icmp address sweep :                        0
    udp address sweep :                         0
    port scan :                                 0
    exceed rate destination :                   0
    exceed rate source :                        0
```

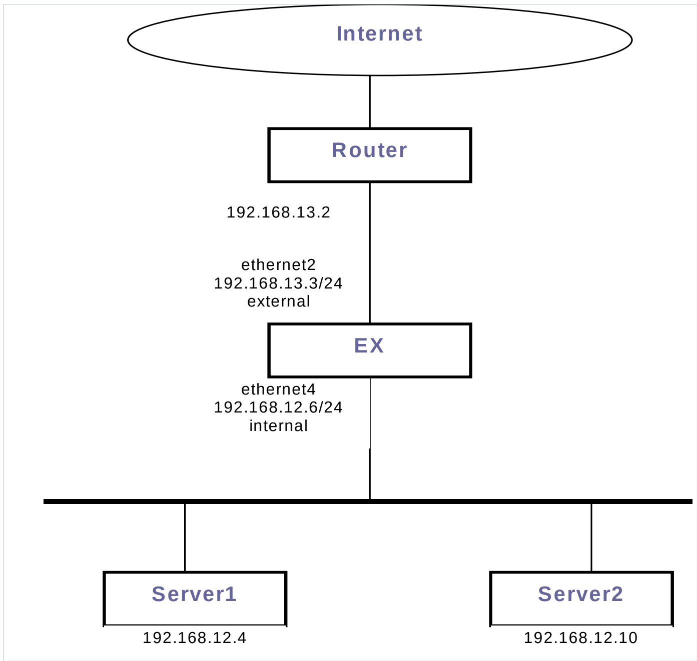
Server Load Balancing (SLB) Configuration

Overview

In a server load balancing configuration, client requests are distributed to the servers in the server farm based on the server farm virtual IP and service port.

In this example, the company is hosting a Web site which can be accessed from the Internet. For simplicity, this example uses only two servers. In reality, there can be many more servers in the server group.

FIGURE 8. Server Load Balancing Topology



Note: This example assumes the company's Web page is hosted on port 8080.

SLB can be used to load balance connections from external clients (clients on the Internet) and from internal clients (clients in the same network as the servers.)

Summary of Steps

1. Configure an HTTP health monitor.
2. Configure the SLB nodes.
3. Configure the SLB group.
4. Configure the SLB virtual server.
5. Verify the SLB configuration and operation.

Command Syntax

1. To configure an HTTP health monitor, use the following command:

```
health monitor monitor-name method http
[port port-num] [url string]
[expect {string | response-code code-list}]
[username name]
```

2. To configure the SLB nodes, use the following commands:

```
slb node name ip-address
{subnet-mask | /mask-length}]

bind health monitor name

port tcp port
```

The **slb node** command creates the SLB node (real server) and changes the CLI to the configuration level for the server. The **bind health monitor** command binds a configured health monitor to the server. The **port** command adds a protocol port to the server, and changes the CLI to the configuration level for the port. (In this example, no configuration occurs at the port level.)

3. To configure the SLB group, use the following commands:

```
slb group tcp group

bind port node-name port-num
```

The **slb group tcp** command creates the a service group for TCP services and changes the CLI to the configuration level for the group. The **bind port** command binds the real servers and their protocol ports to the service group.

4. To configure the SLB virtual server, use the following commands:

```
slb virtual server name ip-address
{subnet-mask | /mask-length}

port tcp port-num group-name l4
```

The **slb virtual server** command creates the virtual server and changes the CLI to the configuration level for it.

The **port** command binds protocol ports on the real servers to the virtual server, by binding to the group that contains the real servers. The *port-num* can be a protocol port number or well-known name, if recognized by the EX device. To display a list of the well-known names recognized by the EX device, enter **port ?**. Port number 0 is a wildcard that matches on all TCP ports (Likewise, if you specify **udp** as the protocol, 0 matches on all UDP ports.)

To display a list The **l4** option indicates that the group is port-based (is a TCP or UDP group).

5. To verify the SLB configuration and operation, use the following command:

```
show slb node [name [name ...]] [detail]
```

Configuration Example

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX>en
Password:*****
EX#conf
```

The following commands configure the HTTP health monitor.

```
EX(config)#health monitor http8080 method http port 8080
```

The following commands configure the SLB nodes.

```
EX(config)#slb node server1 192.168.12.4 255.255.255.0
EX(config-slb node:server1)#bind health monitor http8080
EX(config-slb node:server1)#port tcp 8080
EX(config-slb node:server1-port:TCP 8080)#exit
EX(config-slb node:server1)#exit
EX(config)#slb node server2 192.168.12.10 255.255.255.0
EX(config-slb node:server2)#bind health monitor http8080
EX(config-slb node:server2)#port tcp 8080
EX(config-slb node:server2-port:TCP 8080)#exit
EX(config-slb node:server2)#exit
```

The following commands configure the SLB service group.

```
EX(config)#slb group tcp mygroup
EX(config-slb group tcp:mygroup)#bind port server1 8080
EX(config-slb group tcp:mygroup)#bind port server2 8080
EX(config-slb group tcp:mygroup)#exit
```

The following commands configure the virtual server.

```
EX(config)#slb virtual server myserver 192.168.12.250 255.255.255.0
EX(config-slb virtual server:myserver)#port tcp 8080 mygroup l4
EX(config-slb virtual server:myserver)#exit
```

The following commands verify the configuration and its operational status.

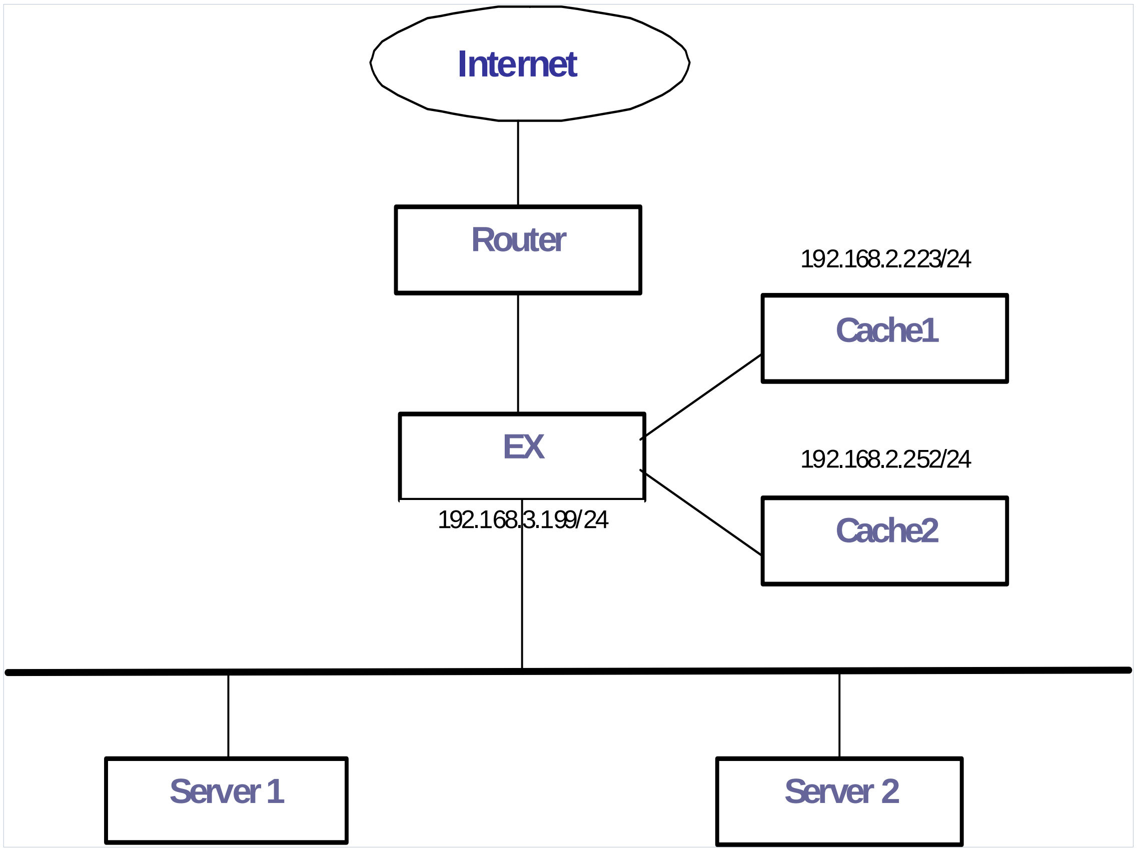
```
EX(config)#show slb node
Name     Type     IP           Status Curr Conn Total Conn
server1 Server 192.168.12.4  Running       0          1
server2 Server 192.168.12.10 Running     0      1

EX(config)#show slb node detail
Name:                server1
Type:                Server
Status:              Running
IP Addr:             192.168.12.4
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      http8080
Enable/Disable:      Enabled
Sent:                1924 (bytes) / 27 (packets)
Received:            33114 (bytes) / 27 (packets)
Current Connection:  0
Total Connection:    1
Ports:
Node     Protocol Port Status Curr Conn  Total Conn
server1  TCP       8080 Running    0          1

Name:                server2
Type:                Server
Status:              Running
IP Addr:             192.168.12.10
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      http8080
Enable/Disable:      Enabled
Sent:                538 (bytes) / 6 (packets)
Received:            876 (bytes) / 4 (packets)
Current Connection:  0
Total Connection:    1
Ports:
Node    Protocol Port Status  Curr Conn  Total Conn
server2 TCP     8080 Running    0          1
```

Cache Load Balancing (CLB) Configuration

Overview

Cache load balancing (CLB) enables you to improve application response times by redirecting incoming requests to cached content on the edge of the network. For incoming requests, the EX device forwards traffic to a cache server, then sends the cached content to the client that requested it.

FIGURE 9. Cache Load Balancing Application Topology



Summary of Steps

1. Create a traffic class for CLB traffic.
2. Create the cache nodes.
3. Create the cache group.
4. Verify CLB operation.

Command Syntax

1. To create a traffic class for CLB traffic, use the following commands:

   ```
    class name category category-name
   ```

   This command creates the class if not already created, and changes the CLI to the configuration level for the class.

   ```
   match dport protocol-port
   ```

   This command specifies the Layer 4 destination application port that belongs to the traffic class. (This command has many more options, which are not used in this example. See “qos class” on page 115.)

2. To create the cache nodes, use the following command:

   ```
   clb node name ip-address
   {subnet-mask | /mask-length}
   ```

   This command creates the cache server and changes the CLI to the configuration level for the server. (In this example, no additional configuration occurs at the CLB node level.)

3. To create the cache group, use the following commands:

   ```
   clb group name

   bind node node-name

   bind  class class
   ```

   The **clb group** command creates the cache service group and changes the CLI to the configuration level for it. The **bind node** command adds cache servers to the group. The **bind class** command assigns traffic classes to the group. CLB service is provided to the specified traffic classes.

4. To verify CLB operation, use the following commands:

   ```
   show clb node [name [name ...]] [detail]

   show clb group [name [name ...]] [detail]
   ```

Configuration Example

```
login as: admin
Welcome to EX
Using keyboard-interactive authentication.
Password:*******
[type ? for help]
EX>en
Password:*****
EX#conf
```

The following commands create the Layer 4 traffic class.

```
EX(config)# class myhttp category misc
EX(config-class)# match dport 80
EX(config-class)#exit
```

The following commands create the CLB nodes.

```
EX(config)#clb node cache1 192.168.2.223 /24
EX(config-clb node:cache1)#exit
EX(config)#clb node cache2 192.168.2.252 /24
EX(config-clb node:cache2)#exit
```

The following commands create the CLB group.

```
EX(config)#clb group clbgroup
EX(config-clb group:clbgroup)#bind node cache1
EX(config-clb group:clbgroup)#bind node cache2
EX(config-clb group:clbgroup)#bind  class myhttp
EX(config-clb group:clbgroup)#exit
```

The following commands verify the CLB configuration and operational status.

```
EX#show clb group detail
Name:                    clbgroup
Method:                  Round Robin
Persistent:              Disabled
Sent:                    192660 (bytes) / 1120 (packets)
Received:                1240759 (bytes) / 1486 (packets)
Current Connection:      0
Total Connection:        87
Members:                 cache1
                         cache2
EX #show clb node detail
Name:                    cache1
Type:                    Cache
Status:                  Running
IP Addr:                 192.168.2.223
Mask:                    255.255.255.0
Connection Limit:        0
Weight:                  1
```

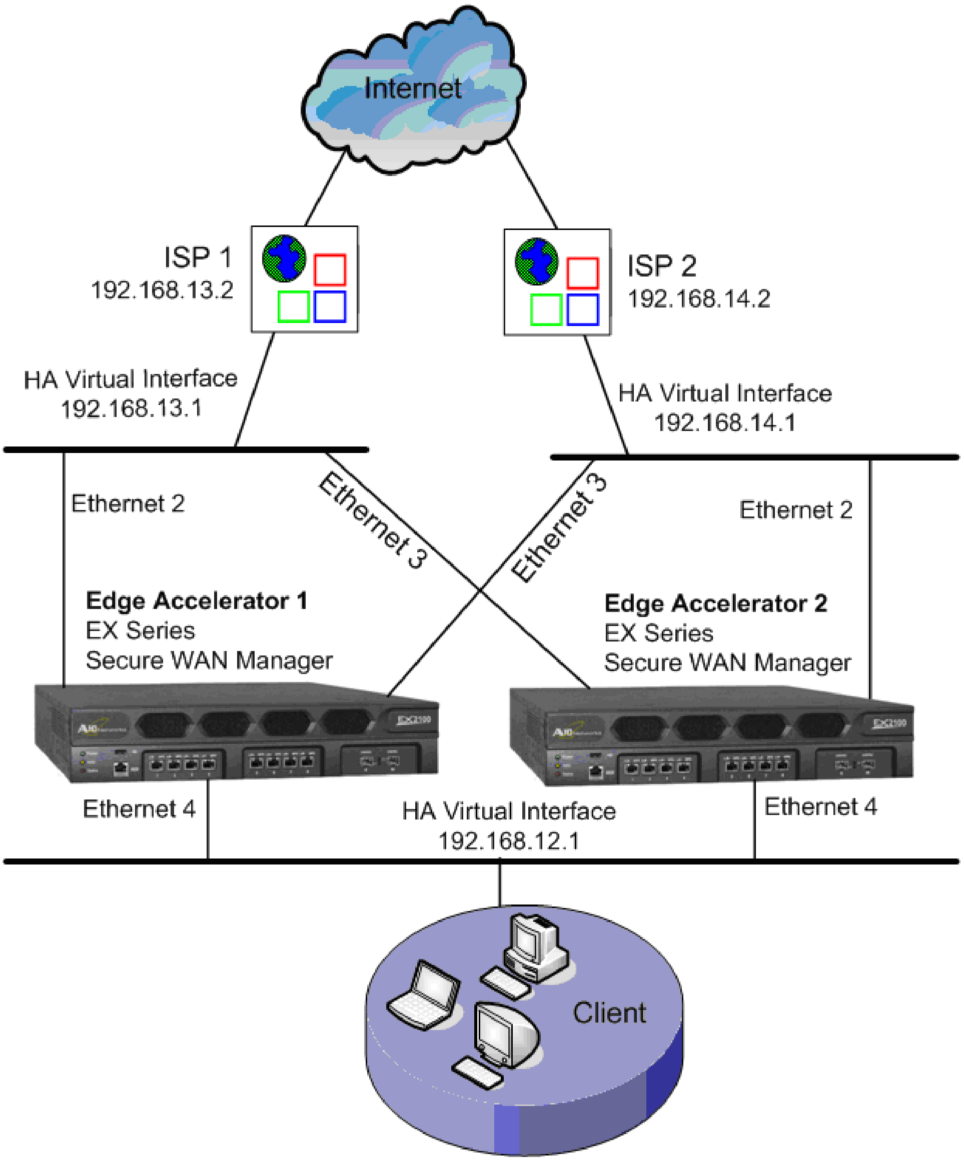
```
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                192660 (bytes) / 1120 (packets)
Received:            1240759 (bytes) / 1486 (packets)
Current Connection:  0
Total Connection:    87

Name:                cache2
Type:                Cache
Status:              Running
IP Addr:             192.168.2.252
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                192670 (bytes) / 1123 (packets)
Received:            1240760 (bytes) / 1490 (packets)
Current Connection:  0
Total Connection:    87
```

HA for Gateway Mode Configuration

Overview

EX devices support HA in gateway mode. In gateway mode, both EX devices need to be configured with a virtual IP address, which is associated with a virtual group. Multiple virtual IP addresses on different physical ports can be grouped together using a virtual group tag.

FIGURE 10. HA for Gateway Mode Topology



Summary of Steps

1. Configure virtual groups on each EX device.
2. Verify HA status.
3. Test failover.

Command Syntax

1. To configure the virtual groups used in this example, use the following commands:

   ```
   vgroup group-id
   ip ip-address
   tag number
   activate
   ```

   The **vgroup** command creates a virtual group and changes the CLI to the configuration level for the group, where the following commands are available.

   The **ip** command configures a virtual IP address for the virtual group. The IP address must be a valid host IP address and can not be the same as a real IP address configured on the interface.

   The **tag** command assigns a tag to the virtual group and allows multiple virtual groups to be used as a single group. In this example, three virtual groups are configured on each EX device. Each virtual group has a virtual IP address in a different subnet. However, all three groups are configured to work as a single group, by assigning the same tag value to all three groups. Use the same tag value on both EX devices.

   If your topology contains multiple HA pairs of EX devices, use the **tag** command to set a unique tag value for each HA pair. The tag value enables an EX device to recognize traffic for its own HA group and ignore traffic for other HA groups.

   The **activate** command activates HA on the virtual group.

2. To verify the HA configuration and operational status, use the following commands:

   ```
   show vrrp [vgroup-num] [detail]
   show ip interface [ethernet port-num [port-num ...]
   ```

3. To test failover, use the following command at the configuration level for an interface to shut down the interface:

   ```
   shutdown
   ```

Wait a few seconds, then use the **show vrrp** command to verify that failover has occurred.

When finished, re-enable the interface by entering the following command at the configuration level for an interface:

```
no shutdown
```

Configuration Example for EX1

```
login as: admin
Welcome to EX1
Using keyboard-interactive authentication.
Password:*******
[type ? for help]

EX1>en
Password:*****
EX1#conf
```

The following commands configure the virtual groups.

```
EX1(config)#interface ethernet 2
EX1(config-if:ethernet2)#vgroup 2
   Add virtual group ok.
EX1(config-if:ethernet2-virtual group:2)#ip 192.168.13.1 /24
   Virtual IP address add ok.
EX1(config-if:ethernet2-virtual group:2)#tag 1
   Tag setting ok.
EX1(config-if:ethernet2-virtual group:2)#activate
   Turn on virtual group ok.

EX1(config)#interface ethernet 3
EX1(config-if:ethernet3)#vgroup 3
   Add virtual group ok.
EX1(config-if:ethernet3-virtual group:3)#ip 192.168.14.1 /24
   Virtual IP address add ok.
EX1(config-if:ethernet3-virtual group:3)#tag 1
   Tag setting ok.
EX1(config-if:ethernet3-virtual group:3)#activate
   Turn on virtual group ok.

EX1(config)#interface ethernet 4
EX1(config-if:ethernet4)#vgroup 1
   Add virtual group ok.
EX1(config-if:ethernet4-virtual group:1)#ip 192.168.12.1 /24
   Virtual IP address add ok.
EX1(config-if:ethernet4-virtual group:1)#tag 1
   Tag setting ok.
EX1(config-if:ethernet4-virtual group:1)#activate
   Turn on virtual group ok.
```

Configuration Example for EX2

The following commands configure the virtual groups. The virtual group configuration is the same as on EX1.

```
EX2(config)#interface ethernet 2
EX2(config-if:ethernet2)#vgroup 2
   Add virtual group ok.
EX2(config-if:ethernet2-virtual group:2)#ip 192.168.13.1 /24
   Virtual IP address add ok.
EX2(config-if:ethernet2-virtual group:2)#tag 1
   Tag setting ok.
EX2(config-if:ethernet2-virtual group:2)#activate
   Turn on virtual group ok.

EX2(config)#interface ethernet 3
EX2(config-if:ethernet3)#vgroup 3
   Add virtual group ok.
EX2(config-if:ethernet3-virtual group:3)#ip 192.168.14.1 /24
   Virtual IP address add ok.
EX2(config-if:ethernet3-virtual group:3)#tag 1
   Tag setting ok.
EX2(config-if:ethernet3-virtual group:3)#activate
   Turn on virtual group ok.

EX2(config)#interface ethernet 4
EX2(config-if:ethernet4)#vgroup 1
   Add virtual group ok.
EX2(config-if:ethernet4-virtual group:1)#ip 192.168.12.1 /24
   Virtual IP address add ok.
EX2(config-if:ethernet4-virtual group:1)#tag 1
   Tag setting ok.
EX2(config-if:ethernet4-virtual group:1)#activate
   Turn on virtual group ok.
```

Command Example for Verifying HA Configuration and Status on EX2

In this configuration, EX2 is the HA Master, and the virtual IP address is bound to the Master. Since the virtual IP address is the default gateway in the topology, the traffic will go through the Master.

```
EX2(config)#show vrrp

   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ethernet4  1     100   P  Master     0b08.8656          192.168.12.1
   ethernet4  1     100   P  Backup     0b08.eeae          192.168.12.1

   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ethernet2  2     100   P  Master     0b08.86566         192.168.13.1
   ethernet2  2     100   P  Backup     0b08.eeae          192.168.13.1

   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ethernet3  3     100   P  Master     0b08.8656          192.168.14.1
   ethernet3  3     100   P  Backup     0b08.eeae          192.168.14.1
```

Command Example for Verifying HA Configuration and Status on EX1

In this example, EX1 is the HA Backup.

```
EX1(config)#show vrrp

   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ethernet4  1     100   P  Backup     0b08.eeae       192.168.12.1
   ethernet4  1     100   P  Master     0b08.8656       192.168.12.1

   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ethernet2  2     100   P  Backup     0b08.eeae       192.168.13.1
   ethernet2  2     100   P  Master     0b08.8656       192.168.13.1

   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ethernet3  3     100   P  Backup     0b08.eeae       192.168.14.1
   ethernet3  3     100   P  Master     0b08.8656       192.168.14.1
```

Command Example for Testing Failover

Enter the following commands on EX2 to disable one of the interfaces:

```
EX2(config)#interface ethernet 2
EX2(config-if:ethernet2)#shutdown
```

After a few seconds, enter the following command to verify that failover has occurred.

```
EX2(config)#show vrrp

   Interface  vrId  Prio  P  State     Primary addr     Virtual addr
   ethernet4  1     100   P  Backup    0b08.8656        192.168.12.1
   ethernet4  1     100   P  Master    0b08.eeae        192.168.12.1

   Interface  vrId  Prio  P  State     Primary addr     Virtual addr
   ethernet2  2     100   P  Backup    0b08.86566       192.168.13.1
   ethernet2  2     100   P  Master    0b08.eeae        192.168.13.1

   Interface  vrId  Prio  P  State     Primary addr     Virtual addr
   ethernet3  3     100   P  Backup    0b08.8656        192.168.14.1
   ethernet3  3     100   P  Master    0b08.eeae        192.168.14.1
```

EX1 becomes the Master, and the virtual IP address binds to the Master. To verify this, enter the following commands on EX1:

```
EX1(config)#show vrrp

   Interface  vrId  Prio  P  State     Primary addr     Virtual addr
   ethernet4  1     100   P  Master    0b08.eeae        192.168.12.1
   ethernet4  1     100   P  Backup    0b08.8656        192.168.12.1

   Interface  vrId  Prio  P  State     Primary addr     Virtual addr
   ethernet2  2     100   P  Master    0b08.eeae        192.168.13.1
   ethernet2  2     100   P  Backup    0b08.8656        192.168.13.1

   Interface  vrId  Prio  P  State     Primary addr     Virtual addr
   ethernet3  3     100   P  Master    0b08.eeae        192.168.14.1
   ethernet3  3     100   P  Backup    0b08.8656        192.168.14.1
```

On EX2, re-enable the shutdown interface. Unless you have disabled HA pre-emption, EX2 should become the HA Master again.

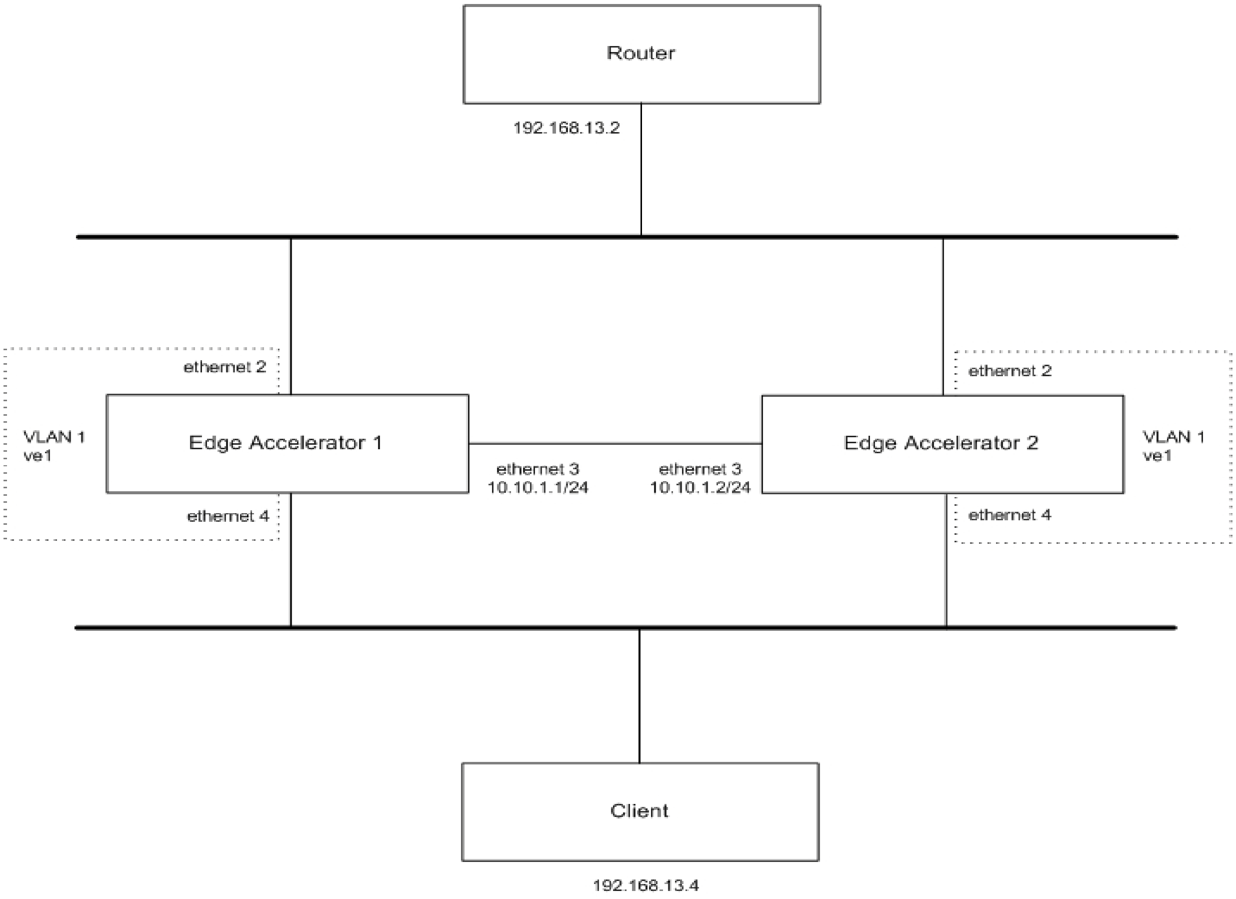
```
EX2(config)#interface ethernet 2
EX2(config-if:ethernet2)#no shutdown
```

HA for Transparent Mode Configuration

Overview

EX devices also support HA in transparent mode. In this mode, both EX devices require heartbeat messages on the HA virtual group. HA in transparent mode uses a Virtual Ethernet (VE) interface instead of a virtual IP address. The virtual group's VE interface is up on the Master and down on the Backup. The traffic will go through the Master.

FIGURE 11. HA Transparent Mode Application Topology



Summary of Steps

1. Configure virtual groups on each EX device.
2. Verify HA status.
3. Test failover.

Command Syntax

1. To configure the virtual groups used in this example, use the following commands:

   ```
   vlan vlan-id
   ```

   This command creates a VLAN and enters the configuration level for the VLAN.

   ```
   untagged ethernet port-num
     [ethernet port-num ... | to port-num]
   ```

   The **untagged** command adds physical Ethernet interfaces to the VLAN. (Use the **tagged** command to add interfaces that also will be members of at least one other VLAN. Use the **untagged** command to add interfaces that will be members of this VLAN only.)

   ```
   interface ethernet num
   ```

   ```
   ip address ip-address {subnet-mask | /mask-length}
   ```

   The **interface ethernet** command changes the CLI to the configuration level for an interface. Use the *num* option to specify the interface number. The **ip address** command configures an IP address on the interface.

Note: When you configure an IP address on the interface, the interface is removed from transparent mode and no longer is associated with the device’s global IP address.

```
interface ve ve-num
```

```
vgroup group-id
```

```
heartbeat ethernet port-num
```

```
tag number
```

```
activate
```

The **vgroup** command creates a virtual group and changes the CLI to the configuration level for the group, where the following commands are available.

The **ip** command configures a virtual IP address for the virtual group. The IP address must be a valid host IP address and can not be the same as a real IP address configured on the interface.

The **interface ve** command changes the CLI to the configuration level for the Virtual Ethernet (VE) interface belonging to a VLAN. The **vgroup** command creates a virtual group and changes the CLI to the configuration level for the group, where the following commands are available.

The **heartbeat ethernet** command enables an interface in the virtual group to send heartbeat messages. The Backup EX device listens for heartbeat messages from the Master EX device. If the messages stop arriving, the Backup EX device fails over to become the Master.

If your topology contains multiple HA pairs of EX devices, use the **tag** command to set a unique tag value for each HA pair. The tag value enables an EX device to recognize traffic for its own HA group and ignore traffic for other HA groups. The example in Figure 11 on page 89 does not require a tag.

The **activate** command activates HA on the virtual group.

2. To verify the HA configuration and operational status, use the following commands:

```
show vrrp [vgroup-num] [detail]

show interfaces ve [vlan-id ...]
```

3. To test failover, use the following command at the configuration level for an interface to shut down the interface:

```
shutdown
```

Wait a few seconds, then use the **show vrrp** command to verify that failover has occurred.

When finished, re-enable the interface by entering the following command at the configuration level for an interface:

```
no shutdown
```

Configuration Example for EX1

```
login as: admin
Welcome to EX1
Using keyboard-interactive authentication.
Password:*******
[type ? for help]
EX1>en
Password:*****
EX1#conf
```

The following commands configure the virtual groups.

```
EX1(config)#vlan 2
EX1(config-vlan:1)#untagged ethernet 2 ethernet 4
EX1(config)#interface ethernet 3
EX1(config)#interface ve 2
EX1(config-if:ve2)#ip address 192.168.13.1 /24
EX1(config-if:ve2)# vgroup 1
   Add virtual group ok.
EX1(config-if:ve1-virtual group:1)#heartbeat ethernet 3
   heartbeat setting ok.
EX1(config-if:ve1-virtual group:1)#activate
   Turn on virtual group ok.
```

Configuration Example for EX2

```
EX2(config)#vlan 1
EX2(config-vlan:1)#untagged ethernet 2 ethernet 4
EX2(config)#interface ethernet 3
EX2(config)#interface ve 1
EX1(config-if:ve1)#ip address 192.168.13.1 /24
EX2(config-if:ve1)# vgroup 1
   Add virtual group ok.
EX2(config-if:ve1-virtual group:1)#heartbeat ethernet 3
   heartbeat setting ok.
EX2(config-if:ve1-virtual group:1)#activate
   Turn on virtual group ok.
```

Command Example for Verifying HA Configuration and Status on EX1

In this example, EX1 is the Backup, so the VE interface is down.

```
EX1(config)#show vrrp
   Interface  vrId  Prio  P  State      Primary addr       Virtual addr
   ve2        1     100   P  Backup     0b08.8656          None
   ve1        1     100   P  Master     0b08.eeae          None
```

Command Example for Verifying HA Configuration and Status on EX2

In this example, EX2 is the Master, the VE interface is up. Traffic will go through the Master.

```
EX3(config)#show vrrp
Interface     vrId  Prio  P  State      Primary addr      Virtual addr
   ve1        1     100   P  Master     0b08.eeae         None
   ve2        1     100   P  Backup     0b08.8656         None
```

Command Example for Testing Failover

Enter the following commands on EX2 to disable the VE interface:

```
EX2(config)#interface ve 1
EX2(config-if:ve1)#shutdown
```

EX1 becomes the Master, and the VE interface binds to the Master. To verify this, enter the following commands on EX1:

```
EX1(config)#show vrrp
   Interface  vrId  Prio  P  State      Primary addr      Virtual addr
   ve2        1     100   P  Master     0b08.8656         None
   ve1        1     100   P  Backup     0b08.eeae         None
```

System Management

The following sections show how to perform essential system management tasks.

Reset Configuration to Factory Defaults

CAUTION! You may want to save a copy of the configuration first, just in case you need to re-create portions of it later. To save a copy of the configuration on a remote server, see “backup” on page 267.

If you ever need to clear the configuration and restore it to the factory defaults, use the following command at the global configuration level:

```
reset [all]
```

You can select whether to clear all configuration information, or to clear all except network connectivity information:

- If you enter the command without the **all** option, network connectivity information is retained. Interfaces, VLANs, and routes are not removed from the configuration.
- If you use the **all** option, interfaces, VLANs, and routes are also removed.

Reset Admin Username and Password

If you forget the password for the “admin” account, you can reset it to its default value. This procedure also allows you to reset the enable password to its default.

Defaults:

- Admin – Username “admin”, password “a10”
- Enable – Password is blank

Note: This procedure requires a console connection to the CLI.

1. Attach a terminal to the serial console port.
2. At the login prompt, type **reset**.
3. At the password prompt, type the EX device's serial number.

Note: If no serial number is present, use "a10".

4. Answer the questions to reset the admin and enable passwords.

Here is an example:

```
Welcome to EX
EX login: reset
Password:EX2K000105238777

Do you want to reset admin password to default?[y/n]:y

Do you want to reset enable password to default?[y/n]:y
```

System Software Recovery

System software recovery is used to restore the system software to the version stored in the compact flash. Typically, this procedure is used for downgrading an EX device to a prior version.

1. Attach a terminal to the serial console port.
2. Power on the EX device (or cycle power to reboot).
3. Press F2 when you see the first screen displayed on the terminal, to select the boot device.
4. Select Compact Flash and press Enter.
5. Log in as the admin.
6. Enter enable mode, by typing **enable**.
7. Enter configuration mode, by typing **config**.

Here is an example for models EX 2100 and EX 2200:

```
EX>enable
Password:********
EX#config
EX(config)#raid
EX(config-raid)#install
The install action will recovery the disk, continue? [yes/no]:yes
```

Here is an example for model EX 1000:

```
EX>enable
Password:********
EX#config
EX(config)#update disk
```

System Upgrade

To upgrade the system software:

1. To save the configuration and commit any unsaved changes in the running-config to the startup-config, enter the following command:

   ```
   write memory
   ```

2. To save a system backup to a remote server, enter the following command:

   ```
   backup url
   ```

   The URL can be one of the following:

   ```
   tftp://host/file-name
   ftp://[user@]host[:port]/file-name
   scp://[user@]host/file-name
   rcp://[user@]host/file-name
   ```

   You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password.

   You can enter a path name with the file name.

3. To install the new software image, enter the following command:

   ```
   upgrade url
   ```

4. When the prompt appears, enter **yes** to reboot the EX device or **no** to prevent the reboot after the new image is installed.

The following commands upgrade an EX device to v2.1:

```
EX(config)#write memory
Building configuration...
[OK]
EX(config)#backup scp://exadmin@192.168.1.12/home/exadmin/
Password []?********
Destination file name [/home/exadmin/]?delme.bk
Export config...
backup_config.2008-07-01-18-30-13.2667
Transferring file...
Transfer succeed!
EX(config)#
```

Here is another example. In this example, the destination file name is included on the command line. In the previous example, the destination file name is specified separately at the prompt.

```
EX(config)#write memory
Building configuration...
[OK]
EX(config)#backup scp://exadmin@192.168.1.12/home/exadmin/delme.bk
Password []?********
Export config...
backup_config.2008-07-01-18-30-48.2667
Transferring file...
Transfer succeed!
EX(config)#
```

Commit Configuration Changes

When you make configuration changes, they appear in the running-config but are not committed to the startup-config. The running-config contains the active configuration whereas the startup-config contains the configuration that will be reloaded following a system reboot.

To commit configuration changes to the startup-config, use the following command at any configuration level of the CLI:

write memory

Here is an example:

```
EX(config)#write memory
Building configuration...
[OK]
```

Add, Modify, and Remove Admin Users

You can add additional admin accounts, as well as modify or delete them.

Note: To manage admin accounts, you must be logged in with an admin account that has read-write privileges.

Note: The “admin” admin account cannot be deleted.

Show Admin Accounts

To show the admin accounts that are currently configured on the EX device, use the **show admin** command. Here is an example:

```
EX(config-admin:test)#show admin
UserName                        Status    Privilege
-------------------------------------------------------
admin                           Enabled   Root
dangadmin                       Enabled   Read only
test                            Enabled   Read only
```

Add or Modify an Admin User

To add or modify an admin account, enter the following command at the global configuration level of the CLI:

```
admin admin-username [password password]
```

This command changes the CLI to the configuration level for the account. If the account is new, the command also creates the account.

If you do not specify a password, the default password “a10” is assigned. The default privilege level is read-only.

To modify the password, privilege level, and other settings, see “Admin Configuration Commands” on page 261.

Remove an Admin User

To remove an admin user, enter the following command at the global configuration level:

```
no admin admin-username
```

Example

The following commands remove the admin account called “test” and verify that the account has been removed:

```
EX(config)#no admin test
Remove admin user <test> successful !
EX(config-admin:test)#show admin
UserName                        Status    Privilege
-------------------------------------------------------
admin                           Enabled   Root
dangadmin                       Enabled   Read only
```

List and Delete Active CLI or GUI Sessions

To list the current management sessions on the EX device, enter the show session admin command. Here is an example.

```
EX(config)#show session admin
 ID   User Name   Start Time                   Source IP        Type   Cfg Mode
*1     admin       16:12:18 PDT Fri Jun 20 2008   192.168.1.130    CLI    Yes
2      admin2      17:03:10 PDT Thu Jun 19 2008   192.168.1.55     CLI    No
3      admin2      17:03:10 PDT Thu Jun 19 2008   192.168.1.55     GUI    No
```

The asterisk indicates your session.

To delete a session, use the following command from the Privileged EXEC Mode of the CLI. Here is an example:

clear session admin {**all** | *sessionID*}

For *sessionID*, enter the number in the ID column of the **show session admin** output.

Here is an example:

```
EX(config)#exit
EX#clear session admin 3
EX#show session admin
 ID   User Name   Start Time                   Source IP        Type   Cfg Mode
*1     admin       16:12:18 PDT Fri Jun 20 2008   192.168.1.130    CLI    No
2      admin2      17:03:10 PDT Thu Jun 19 2008   192.168.1.55     CLI    No
```

Note: The configuration mode (Cfg Mode) for your session is shown as No instead of Yes because you have exited the configuration mode in order to enter the **clear** command.

Commands

Conventions

Command Syntax Conventions

boldface Boldface text indicates commands and keywords that you enter literally as shown.

italics Italic text indicates arguments for which you supply values.

[x] Square brackets enclose optional elements (keywords or arguments).

| A vertical line indicates a choice within an optional or required set of keywords or arguments.

[x | y] Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.

{x | y} Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example: [x {y | z}], braces and a vertical line within square brackets indicate a required choice within an optional element.

Example Conventions

`screen` Examples of information displayed on the screen are set in New Courier font.

`boldface` Examples of text that you must enter are set in New Courier bold font.

< > Angle brackets enclose text that is not printed to the screen, such as passwords.

! An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the EX Series Secure WAN Manager software for certain processes.)

[ ] Square brackets enclose default responses to system prompts.

The “no” Form of Commands

Most configuration commands have a **no** form. Typically, you use the **no** form to disable a feature or function. The command *without* the **no** keyword is used to re-enable a disabled feature or to enable a feature that is disabled by default; for example, if the terminal auto-size has been enabled previously. To disable terminal auto-size, use the **no terminal auto-size** form of the **terminal auto-size** command. To re-enable it, use the **terminal auto-size** form. This document indicates whether a command supports a **no** version by showing “`[`**`no`**`]`” at the beginning of the command name.

In some cases, the **no** form of a command has slightly different syntax than the normal form of the command. For syntax information, enter the following: **no** *`command-name`* **?**

Link Load Balancing (llb) Commands

llb default group

Set a default LLB group.

Syntax Description

```
llb default group name
no llb default group
```

Parameter	Description
name	LLB group name.

Default

None

Mode

Configuration mode

Usage

The normal form of this command sets a default LLB group. The **no** form of this command unsets the default group.

There is no **default** form of this command.

The EX device can have only one default LLB group. All LLB links created after you set the default LLB group will automatically be bound to the default group.

Example

The following command sets LLB group "*llb-group-1*" as the default:

```
EX(config)#llb default group llb-group-1
```

llb dns

Optimize the list of IP addresses in DNS answers.

Syntax Description

```
[no] llb dns {best-reply | only-return-active-ip}
```

Parameter	Description
best-reply	Removes all but the best IP from the DNS answer. DNS reply contains at most 1 IP or answer. The best IP is never associated with an inactive link.
only-return-active-ip	Removes all answers associated with down links from the DNS reply. If all links are down, the reply will consist of 0 answers.

Default

The EX device modifies DNS answers based on link state and preference. By default, the DNS answers are ordered by preference.

Mode

Configuration mode

Usage

When links are down, DNS answers may contain IPs for inactive links. To avoid this, use the DNS **only-return-active-ip** option.

For cases where only the best IP should be returned, use the DNS best-reply option. The DNS reply will contain at most only 1 IP or answer. The answer may have 0 IPs in the reply. The best IP is never associated with an inactive link; thus, **only-return-active-ip** is implicit.

These options are mutually exclusive. Only one option can be set globally.

llb domain

Create, edit, or delete an LLB domain.

Syntax Description

```
[no] llb domain domain-name
```

Parameter	Description
domain-name	Domain name fragment, 1-127 characters.

This command changes the CLI to the configuration level for the specified LLB domain, where the following LLB-domain related commands are available:

Command	Description
`[no] host host [host ...]`	Adds host names to the LLB domain. Each host name can be 1-63 characters long. You can configure up to 4096 hosts on the EX device. Up to 4096 hosts can be in a given domain. A fully-qualified domain name (FQDN) matches a host if the concatenation of: the host, a dot (“.”), and the host's parent domain, is equal to the FQDN in a case-insensitive way.

`[no] policy {include | exclude}`	Changes the include/exclude policy. **include** – An FQDN matches only when it matches the domain and one of its hosts. **exclude** – An FQDN matches only when it matches the domain but does not match any of its hosts.

Default

The EX device does not have any LLB domains by default. When you create an LLB domain, it has the following default settings:

- **host** – none
- **policy** – include

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing domain uniquely identified by *domain*, and enters the configuration level for the domain.

The **no** form of this command removes the specified domain(s). If you do not specify a domain name, all LLB domains are removed after user confirmation.

You can configure up to 256 domains.

The LLB domain and host are used in DNS spoofing for inbound LLB.

A fully-qualified domain name (FQDN) matches a domain when the domain is a postfix of that FQDN.

Example

The following command creates a new domain called “a10networks.com”:

```
EX(config)#llb domain a10networks.com
EX(config-llb domain:a10networks.com)#
```

Example

The following command binds the LLB domain "*a10networks.com*" to LLB group "*llb-group-1*":

```
EX(config-llb group:llb-group-1)#bind domain a10networks.com
```

Example

The following command adds hosts *www* and *ftp* to the current domain.

```
EX(config-llb domain:a10networks.com)#host www ftp
```

llb group

Create, edit, or delete and LLB group.

Syntax Description

```
llb group name

no llb group [name [name ...]]
```

Parameter	Description
name	LLB group name, 1-31 characters

This command changes the CLI to the configuration level for the specified LLB group, where the following LLB-group related commands are available:

Command	Description
`[no] bind link name [name ...]`	Adds LLB links to the LLB group. LLB links must be configured (using the **llb link** command) before you can add them to a group.
`[no] bind qos class class [priority num]`	Binds a QoS class to the LLB group. The **priority** can be 1-512. Traffic that matches a QoS class bound to the group will be load balanced among the links in the group. You can bind multiple classes to a group. A given QoS class can be bound to only one LLB group. If you bind a class that is already bound to another group, the class is unbound from the other group. The traffic class must be configured (using the **qos class** command) before you can bind it to a group.
`[no] bind default qos class`	Binds the virtual “match-all” QoS class to the LLB group. The “match-all” class can be bound to only one LLB group.
`[no] bind domain name [name ...]`	Binds LLB domains to the LLB group.

There is no limit to the number of domains that can be bound to an LLB group.

An LLB domain must be configured (using the **llb domain** command) before you can bind it to a group.

method {round-robin | weighted-round-robin | least | weighted-least | bandwidth | round-trip-time | bandwidth-price}

Changes the load balancing method used to select LLB links in the LLB group.

Note: RTT collection is enabled only if the method is **round-trip-time**.

[**no**] **persistent** [**age** *seconds* | **by destination**]

Enables persistence of LLB sessions. When you enable persistence, the EX device always sends traffic for a given connection to the same link. After the link is selected for the first packet in a connection, traffic for the same or similar connections (in terms of IP address) is sent to the same link.

age *seconds* – Specifies the number of seconds sessions remain persistent. You can specify 60-86400 seconds. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.

by destination – Changes persistence from source-IP-based persistence to destination-IP-based persistence.

[**no**] **prefer link** *name* **for** {**qos class** *class* | **default qos class**}

Sets the preferred links for QoS classes in the current LLB group.

This command can be used to override the load balancing method configured in the LLB group. If a link is set as the preferred link for a QoS class, the link will always be selected for traffic matching that class.

The link must be a member of the group. If a link is a member of multiple groups, the link can have different preference settings in each group.

A link can be the preferred link for more than one traffic class within the same group. However, a traffic class can have only one preferred link.

Default The EX device does not have any default LLB groups. When you create an LLB group, it has the following default settings:

- **bind link** – none
- **bind qos class** – None. When you bind a class, the default priority is 256.
- **bind default qos class** – By default, an LLB group is ***not*** bound to the virtual "match-all" QoS class.
- **bind domain** – none
- **method** – round-robin
- **persistent** – disabled

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing LLB group uniquely identified by *name*, and enters the configuration level for the group.

The **no** form of this command deletes an existing LLB group, or if no *name* is specified, removes all LLB groups after user confirmation.

Example The following command creates LLB group "*llb-group-1*":

```
EX(config)#llb group llb-group-1
EX(config-llb group:llb-group-1)#
```

Example The following command adds LLB links "*ISP1*" and "*ISP2*" to LLB group "*llb-group-1*":

```
EX(config-llb group:llb-group-1)#bind link ISP1 ISP2
```

Example The following command binds LLB group “llb-group-1” to QoS class “http”:

```
EX(config-llb group:llb-group-1)#bind qos class http
```

Example The following commands set member link ISP1 as the preferred link for QoS class “http”, and set lSP2 as the preferred link for QoS class “smtp”:

```
EX(config-llb group:llb-group-1)#prefer link lSP1 for qos class http
EX(config-llb group:llb-group-1)#prefer link lSP2 for qos class smtp
```

llb link

Create, edit, or delete a Link Load Balancing (LLB) link.

Syntax Description

```
llb link name
[ip-address {subnet-mask | /mask-length}]

no llb link [name [name ...]]
```

Parameter	Description
name	Link name, 1-31 characters.
ip-address	IP address.
subnet-mask **|** */mask-length*	Network mask or mask length.

This command changes the CLI to the configuration level for the specified LLB link, where the following LLB-link related commands are available:

Command	Description
[**no**] **alternate-subnet** *ip-address* {*subnet-mask* | */mask-length*}	Load balances inbound client traffic based on a destination subnet that is different from the subnet the link is in. the EX device will use the link for inbound client traffic sent to the alternate subnet. Without this option, the EX device load balances client traffic addressed to the subnets the LLB links are in. You can configure a maximum of 8 alternate subnets on each LLB link.
[**no**] **bandwidth** *bw*	Changes the maximum bandwidth of the LLB link. Specify the bandwidth in kbps, from 1 up to the maximum bandwidth of the physical link (8000000, model specific). The bandwidth setting does not put a hard limit on bandwidth usage. The bandwidth is used by the distribution algorithm in LLB. The bandwidth-price load-balancing method (set by the **method** command at the configuration level for an LLB group) can help achieve the most cost-effective link usage.

Price in this context indicates only which tier is cheaper and which is more expensive. The price is not necessarily equal to an ISP's price in dollars or any other currency unit.

Bandwidth tier price settings must be consistent; that is, no bandwidth tier can be both higher ***and*** cheaper than another tier.

`[no] bind health monitor` *`monitor-name`*

Binds a health monitor to the LLB link.

The monitor must first be defined (using the **health monitor** command) before it can be bound to a link.

Since most ISP routers deny ping requests, ping is not performed by default, and the EX device and assumes that an LLB link is "UP" if it is routable. However, if a monitor is explicitly specified, it will be used to check the LLB link's health status. In this case, the link will be marked as "Up" or "Down" according to the health check result. A "Down" LLB link is not available for load balancing.

`[no] bind` *`interface`*

Binds an interface to the LLB link. The *interface* can be one of the following:

ethernet *port-num* – Binds an Ethernet interface to the LLB link.

management – Binds the management interface to the LLB link.

ve *ve-num* – Binds a Virtual Ethernet (VE) interface to the LLB link.

You can bind one interface to an LLB link.

`[no] connection limit` *`limit`*

Sets the current LLB link's connection limit, 0-1000000; 0 means no limit.

The LLB link connection limit puts a hard limit on the number of concurrent connections (both inbound and outbound) that an LLB link can support. If the number of current connection of a link is equal to or greater than the limit, this link will not be selected again in load balancing, until

	the number of current connections drops below the limit. An LLB link’s current connection number can be greater than the limit in the following cases: – The LLB link’s connection limit is changed to a number less than its current number of connections. – New connections are coming from the LLB link; that is, the EX Series Secure WAN Manager is passively counting, rather than actively putting new connections onto the LLB link.
[no] **disable**	Disables the LLB link.
[no] **nat link**	Enables IP destination Network Address Translation (NAT) on the LLB link.
[no] **nat qos class** {**default** | *class-name*} [**ippool** *ippool-name*]	Enables IP source Network Address Translation (NAT) for QoS traffic classes on the current LLB link. **default** – The default traffic class. All classes other than the ones you explicitly specify with the class-name option are included in the default class. **class-name** – Name of a traffic class. **ippool-name** – Name of an IP pool. Addresses from the pool are used for source NAT. If you do not specify a pool name, the pool used by the default class is used. If the default class does not have a pool either, source NAT will not be performed. To prevent source NAT from being performed for traffic that matches a class even if NAT is set for the default class, use the following command: **no nat qos class** *class-name*

`[no]` **`price bandwidth {unlimited |`** *`bandwidth-tier`*`}` **`{pre-paid |`** *`price`*`}`

Changes the LLB link’s bandwidth price setting.

This command can be used to reflect an ISP’s service prices. For example, if an ISP charges on bandwidth usage, the typical billing policy consists of the following:

– Basic bandwidth tier for a basic fee. As long as the basic bandwidth is not exceeded, only the basic fee needs to be paid.

– Higher bandwidth tier with an additional fee; and so on.

Configuring an LLB link’s bandwidth tier prices and using the bandwidth-price method for the LLB group can help achieve the most cost-effective link usage.

“Price” here only differentiates between cheaper and more expensive links. It is not necessarily equal to an ISP’s price in dollars or any other currency unit.

Bandwidth tier price settings must be consistent; that is, no bandwidth tier can be both higher than ***and*** cheaper than another tier.

`[no]` **`weight`** *`weight`*

Changes the LLB link’s weight, 1-255. Weight is used by weighted link load balancing methods such as weighted-round-robin or weighted-least-connection, in combination with other information.

Default

The EX device does not have any default LLB links. When you create an LLB link, it has the following default settings:

- **alternate-subnet** – None
- **bandwidth** – 1000 kbps
- **bind health monitor** – None
- **bind port** – None
- **connection limit** – 0 (no limit)
- **disable** – LLB links are enabled by default.
- **nat link** – Disabled

- **nat qos class** – None
- **price bandwidth** – unlimited 1000
- **weight** – 1

Mode Configuration mode

Usage The normal form of this command creates a new or edits an existing LLB link uniquely identified by *name* and enters the configuration level for the link. When creating a new LLB link, the gateway IP address and mask are required. Otherwise, the link will be left in an incomplete state. You do not need to specify them again when editing an existing link.

Note: Do not use "detail" or "counters" as a link name. These words are reserved. This rule also applies anywhere else you can specify a name for something during configuration, unless explicitly stated otherwise.

The **no** form of this command deletes existing LLB link(s). If you enter the **no** form without a link name, all LLB links are deleted, after user confirmation.

There is no **default** form of this command.

An LLB link's gateway should be in the same network segment as the EX Series Secure WAN Manager; that is, reachable without intermediate routers. If this requirement is not met, the link will always be marked as "Down". A gateway can not be used by more than one LLB link.

An LLB link's gateway IP address and mask define the neighbourhood of the gateway. LLB is not applied to traffic destined for this neighbourhood.

Example The following command creates a new LLB link called *ISP1* with gateway IP address and mask 10.0.0.1/24.

```
EX(config)#llb link ISP1 10.0.0.1 /24
EX(config-llb link:ISP1)#
```

Example The following command enters configuration mode for a previously configured LLB link:

```
EX(config)#llb link ISP1
EX(config-llb link:ISP1)#
```

Example The following command deletes an LLB link:

```
EX(config)#no llb link ISP1 ISP2
```

Example The following command sets LLB link ISP1's bandwidth to 10000 kbps:

```
EX(config-llb link:ISP1)#bandwidth 10000
```

Example

The following commands configure a pre-paid bandwidth tier of 2000 kbps, and change the unlimited tier price to 3000.

```
EX(config-llb link:ISP1)#price bandwidth 2000 pre-paid
EX(config-llb link:ISP1)#price bandwidth unlimited 3000
```

Example

The following command binds the current LLB link with monitor *http*:

```
EX(config-llb link:ISP1)#bind health monitor http
```

Example

The following commands bind Ethernet interface 7 and 9 to the current LLB link:

```
EX(config-llb link:ISP1)#bind port ethernet 7
```

Example

The following command sets an LLB link's connection limit to 10000:

```
EX(config-llb link:ISP1)#connection limit 10000
EX(config-llb link:ISP1)#weight 10
```

Example

The following commands configure IP source NAT on the current LLB link. Traffic classes "cl1" and "cl2" will receive NAT addresses from IP pool "pl2", class "cl3" will not receive NAT service, and all other classes will receive NAT addresses from IP pool "pl3".

```
EX(config-llb link:ISP1)#nat qos class default ippool pl3
EX(config-llb link:ISP1)#nat qos class cl1 ippool pl2
EX(config-llb link:ISP1)#nat qos class cl2 ippool pl2
EX(config-llb link:ISP1)#no nat qos class cl3
```

Example

The following commands configure a pre-paid bandwidth tier of 2000 kbps, then change the unlimited tier price to 3000.

```
EX(config-llb link:ISP1)#price bandwidth 2000 pre-paid
EX(config-llb link:ISP1)#price bandwidth unlimited 3000
```

llb proximity mask

Change the proximity mask used for round-trip-time (RTT) collection.

Syntax Description

```
llb proximity mask {subnet-mask | /mask-length}
no llb proximity prefix mask
```

Parameter	Description
subnet-mask	Network mask in dot-decimal form
/mask-length	Network mask in decimal form

Default

The default proximity prefix mask is 20 bits: /20 or 255.255.240.0.

Mode

Configuration mode

Usage

This command is available under config mode.

The normal form of this command changes the current link load balancing proximity prefix mask. The **no** form of this command resets the current link load balancing proximity prefix mask to its default.

The proximity prefix mask is used in RTT collection. When the link load balancing method is **round-trip-time**, RTT collection is enabled. The RTT of an IP address is updated into the RTT of the network segment determined by logically AND-ing the IP address and the proximity prefix mask.

Example

The following examples sets the LLB proximity mask to 255.255.255.0:

```
EX(config)#llb proximity mask /24
```

Related Commands

llb group, **llb group** > **method**

llb rtt agetime

Change the age time for collected RTT information.

Syntax Description

```
llb rtt agetime seconds
no llb rtt agetime
```

Parameter	Description
seconds	Age time, 60-1800 seconds. RTT entries that remain unused for the number of seconds you specify are removed from the RTT cache.

Default

300 seconds

Mode

Configuration mode

Usage

The normal form of this command changes the RTT age time. The **no** form of this command resets the RTT age time to its default.

Example

The following command changes the RTT age time to 600 seconds:

```
EX(config)#llb rtt agetime 600
```

Related Commands

llb group, llb group > **method**

QoS Commands

qos abuser

Configure a set of criteria that indicates abuse of network resources. Abuser criteria can be used to define source or destination IP addresses in QoS match rules.

Syntax Description

```
[no] qos abuser {alert | criteria name}
```

Parameter	Description
`alert`	Enables the EX device to send alerts when traffic matches the entry (fall in) thresholds of a set of abuse criteria.
`criteria` *`name`*	Configures a set of criteria that indicates abusive traffic. This command changes the CLI to the configuration level for the criteria, where the following criteria-related commands are available: [**no**] **abuser** *ipaddr* [*ipaddr* ...] – Manually adds IP addresses to or removes them from an abuser list. [**no**] **behavior fall-in** *option* – Specifies the entry (fall in) thresholds for traffic to be considered abusive. The following options are supported: **long-live-conn max-cnt** *num* [**life-time** *minutes*] – Specifies the threshold for long-lived connections. The *num* option specifies the maximum number of long-lived sessions allowed to a user, and can be 1-200. The **life-time** *minutes* option specifies the maximum number of minutes a session can be active before it is considered to be long-lived, and can be 5-1440 minutes. **new-conn max-cnt** *num* **duration** *minutes* – Specifies the maximum number of new connections a user can have, 1-10000. The *duration* can be 1-1440 minutes. **new-conn-rate max-rate** *num* **duration** *minutes* – Specifies the maximum number of new connections a user can have per second, 1-200. The *duration* can be 1-60 minutes. **traffic-rate** [**inbound** | **outbound**] **max-rate** *kbps* **duration** *minutes* [**large-pkt-per-**

	cent *num* [**large-pkt-size** {**256** | **512** | **1024**}]] – Specifies the maximum traffic rate. – The **inbound** | **outbound** option specifies the traffic direction. By default, the command applies to both directions. – The **max-rate** can be 1-8000000 kbps. – The **duration** can be 1-1440 minutes. – The **large-pkt-percent** *num* [**large-pkt-size** {**256** | **512** | **1024**}] option specifies the maximum allowed percentage (1-100) of large packets. A packet is considered to be long if it is equal to or greater than the length you specify (256, 512, or 1024 bytes). [**no**] **behavior fall-out** *option*s – Specifies the exit (fall out) thresholds for traffic. A user's traffic must be at or below these thresholds in order for the user to be removed from the abuser list. The options are the same as the fall-in options. Specifying fall-out thresholds is optional. If you do not specify any fall-out thresholds, the fall-in thresholds are used.
qos	Enables you to configure more QoS settings without returning to the global configuration level of the CLI first.

Default

There are no default abuser criteria. When you configure one, some of the values have defaults, as described above.

Mode

Configuration mode

Usage

The action taken by the EX device on users in the abuser list is specified in the QoS policy for the traffic class.

qos autodetect

Autodetect QoS classes.

Syntax Description

```
[no] qos autodetect {interface | internal-subnet |
ip-protocol | vlan}
```

Parameter	Description
interface	Interface for which to autodetect classes.
internal-subnet	Internal-subnet for which to autodetect classes.
ip-protocol	IP-protocol for which to autodetect classes.
vlan	Vlan for which to autodetect classes.

Default

Autodetect is enabled for all parameters except internal-subnet.

Mode

Configuration mode

Usage

Classifying traffic to create classes using the auto-detection feature could often result in an excessive number of flows being classified as “Others”. To provide more helpful information (and reduce the amount of traffic classified as “Others”), a new category called "IP Protocols" has been introduced to the auto-detection feature. This new category will create a positive match for the following types of non-TCP and non-UDP traffic:
ICMP, IPSec, GRE, OSPF and other IP protocols.

Example

Classification of IP Protocols (non-TCP, non-UDP) is enabled by default. To disable the auto-detection of IP Protocols via the EX CLI (which will result in more flows being classified as “Others”, you can use the following command:

```
EX(config)#no qos autodetect ip-protocol
```

qos category

Create a QoS category.

Syntax Description

```
[no] qos category name description string
```

Parameter	Description
name	Category name, 1-31 characters.

string	Description of the category, 1-63 characters. The string can contain blanks.

Default

The EX device has the following QoS categories by default:

- Application
- Database
- DirectoryService
- Email
- File
- Messaging
- Misc
- Multimedia
- P2P
- Session
- Security
- VOIP

Mode

Configuration mode

Usage

To simplify report configuration, you can configure “views”. A view is a named set of QoS categories. Views simplify report configuration by enabling you to include multiple classes in a report. When you select a view for a report, all the classes in all the categories included in the view are included in the report. To configure views, see “qos view” on page 133.

Example

The following command creates a category named “Special”:

```
EX(config)#qos category Special description Class for Special Apps
```

qos class

Create, edit, or delete a QoS traffic class.

Syntax Description

```
[no] qos class name category category-name
```

Parameter	Description
name	Class name, 1-31 characters.
category-name	Category to which the class belongs.

This command changes the CLI to the configuration level for the specified QoS traffic class, where the following class-related commands are available:

Command **Description**

`[no] match` *options*

Defines the rules to use to identify the class to which traffic belongs. Only TCP or UDP traffic has a port number. If you configure a rule for other IP protocols with a source port or destination port, the rule will never match any packets.

Each rule can use one or more of the following options:

`aflex` *`name`* – Name of an aFleX script.

`application` *`name`* – Layer 7 application name. Enter **match application ?** for a list of supported applications. (For a full list of supported application, please see “Appendix” on page 407)

- **`except`** *`option`* – Excludes individual items from the match filter. The *option* can be any of the Layer 7 protocols listed in the Appendix.

`dip` – Destination IP address(es). The address(es) can be specified by one of the following:

- **`criteria`** *`criteria-name`* – Name of a configured set of abuser criteria.
- **`domaingroup`** *`domain-group-name`* – Name of a configured list of domain names.
- *`ipaddr`*`[`*`/mask-length`*`]` – IP address and, optionally, the mask length. The default IP address mask length is 32 bits.
- **`iplist`** *`name`* – Name of a configured list of IP addresses.
- **`idgroup`** *`name`* – Name of a configured group of user IDs. When users log in, the EX device resolves their user names to IP addresses using the IP-to-ID function of IDsentrie.
- **`except`** *`option`* – Excludes individual items from the match filter. The *option* can be any of the other **dip** options described above.

dmac *macaddr* – Destination MAC address. Enter the address in the following format: aaaa.bbbb.cccc

dport – Destination protocol ports. The ports can be specified by one of the following:

> *protocol-port* – Destination protocol port number.
>
> **portlist** *name* – Name of a configured list of protocol ports.
>
> **except** *option* – Excludes individual items from the match filter. The *option* can be either of the other **dport** options described above.

dscp – Enter the DiffServ Code Point for one of the following DSCP values: , or EF). The ports can be specified by one of the following:

> *assured forwarding phb:*
> AF11 - AF43
>
> *class selector forwarding phb:*
> cs1 - cs7
>
> *default phb:*
> default
>
> *expedited forwarding phb:*
> ef

prot {**tcp** | **udp** | **icmp**} – IP protocol.

sip *ipaddr* – Destination IP address(es). The options are the same as those for **dip**. (See above.)

smac *macaddr* – Source MAC address. Enter the address in the following format: *aaaa.bbbb.cccc*

sport *protocol-port* – Source protocol port number. The options are the same as those for **dport**. (See above.)

vlan *vlan-id* – VLAN ID.

qos Enables you to configure more QoS settings without returning to the global configuration level of the CLI first.

[**no**] **report** Enables or disables reporting for the class.

Default

None

Mode

Configuration mode

Usage

All traffic that matches the rules under the class belongs to the class.

If you specify the category when entering this command to edit an existing traffic class, the category of the class will be changed to the category you specify. The category name must be specified when creating a new traffic class.

The class will be used to create policy. Policy reference the class by class name.

The **no** form of the command deletes the specified traffic class. If you do not specify a traffic class name, the command deletes all traffic classes.

QoS classes are of two types: predefined and user defined. On a new EX device, only predefined classes exist. If you change the definition of a predefined class, it becomes a user defined class. Changes include category and rules.

A QoS class cannot be deleted if it is referred to by a policy.

The "Others" class can not be deleted. This class is used for traffic that does not match any of the other classes defined in the system.

Example

The following command creates a class named "test" and places it in category "Misc":

```
EX(config)#qos class test category Misc
```

Example

The following commands configure and display some match rules:

```
EX(config-class)#match prot tcp sip 192.168.3.2 sport 21
EX(config-class)#match prot tcp sport 80
EX(config-class)#show qos class test
qos class test category Misc     (None)
   match (0)  prot tcp sip 192.168.3.2 sport 21
   match (1)  prot tcp sport 80
```

Example

The following commands create a class where the source IP range is from the 192.168.230.0/24 network, and exclude host 192.168.230.30 from this class.

```
EX(config)#qos class 230net category misc
EX(config-class)#match sip 192.168.230.0/24
EX(config-class)#match sip except 192.168.230.30
```

Related Commands

`qos policy`

qos domaingroup

Create a domain group. A domain group can be used to define source or destination IP addresses in QoS match rules.

Syntax Description

```
[no] qos domaingroup domain-name
```

This command changes the CLI to the configuration level for the specified domain group, where the following domain-group related command is available:

`[no] domain-name`	Adds a domain name to the current domain group. Wildcard characters ***** and **?** are supported.

Default

None

Mode

Configuration mode

Usage

If you use wildcard characters in the domain name, the EX device finds matching domain names by examining DNS request and reply packets. This requires the DNS traffic to be forwarded to the EX device.

qos idgroup

Create an ID group. An ID group can be used to define source or destination IP addresses in QoS match rules.

Syntax Description

```
[no] qos idgroup name
```

This command changes the CLI to the configuration level for the specified ID group, where the following ID-group related command is available:

Command	Description
`[no] member user-id`	Adds a member to the current ID group. The user ID is used in IDsentrie or in a statically configured IP2ID mapping.

Note: If a statically configured mapping is found, the static mapping will be used even if the EX device is configured to obtain IP-to-ID mappings from IDsentrie.

Default

None

Usage

The normal form of this command creates a new or edits an existing ID group and changes the CLI to the configuration level for the ID group.

The **no** form of this command removes the specified ID group. If you do not specify an ID group name, all ID groups are removed after user confirmation.

An ID group is a group of users. You can use the ID group name as the source or destination IP address in match rules.

ID groups require user names to be mapped to client IP addresses. You can create the mappings manually or use the companion A10 product, IDsentrie, to provide the mappings dynamically.

To configure either type of IP-to-ID mapping, use the **ip2id** command.

Example

The following command creates an ID group named "test":

```
EX(config)#qos idgroup test
```

Example

The following command adds user "omro@a10networks.com" to the current ID group:

```
EX(config-qos-idgroup)#member omro@a10networks.com
```

Related Commands **ip2id**

qos interface

Create or delete QoS interfaces.

Syntax Description

```
qos interface name

no qos interface [name [name ...]]
```

Parameter	Description
name	QoS interface name.

This command changes the CLI to the configuration level for the specified QoS interface, where the following QoS-interface related commands are available:

Command	Description
[no] port *interface-type*	Binds physical interfaces to the QoS interface.

When you bind a physical to a QoS interface, all traffic through the physical interface also belongs to the QoS interface.

The command changes the CLI to configuration level for the QoS interface, where the following QoS-interface related commands are available.

The *interface-type* can be one of the following:

ethernet *if-number* [**to** *if-number*] – Binds one or more Ethernet data interfaces to the QoS interface.

management – Binds the management interface to the QoS interface.

`[no] qos policy {ingress | egress} policy-name`

Applies a policy to ingress or egress traffic on the QoS interface.

`ingress | egress` – Traffic direction to which to apply the policy. The **ingress** option applies the policy to traffic coming into the interface from outside. The **egress** option applies the policy to traffic leaving the interface.

`policy-name` – Policy name.

The sum of the bandwidth settings in the policy and child-policy cannot exceed the shape rate of the applied interface.

`[no] shape rate`

Shapes the rate of traffic leaving the QoS interface, in kbps per second.

Default

None. When you create a QoS interface, it does not have any Ethernet interfaces by default.

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing QoS interface and changes the CLI to the configuration level for the interface.

The **no** form of this command removes the specified QoS interface. If you do not specify an interface name, all QoS interfaces are removed after user confirmation.

Example The following command creates QoS interface “vt”:

```
EX(config)#qos interface vt
EX(config-qos-intf)#
```

Example The following command binds two Ethernet interfaces to QoS interface “vt”:

```
EX(config)#qos interface vt
EX(config-qos-intf)#port ethernet 1
EX(config-qos-intf)#port ethernet 2
EX(config-qos-intf)#port ethernet 3
```

The above three commands are the same as the following single command:

```
EX(config-qos-intf)#port ethernet 1 to 3
```

Example The following command applies policy “test” to ingress traffic received on the current QoS interface:

```
EX(config-qos-intf)#qos policy ingress test
```

Example The following command shapes the rate of egress traffic sent out the current QoS interface to 100 kbps.

```
EX(config-qos-intf)#shape 100
```

qos ip limit

Limit the bandwidth and maximum number of connections allowed for IP clients.

Syntax Description [**no**] **qos ip limit** *iplist-name bandwidth-limit* [*connection-limit*]

Parameter	Description
iplist-name	Name of a configured IP address list.
bandwidth-limit	Maximum bandwidth, in Kbps, allowed for each client in the IP address list. You can specify 0-500000 Kbps.
connection-limit	Maximum rate of new connections allowed for each client in the IP address list. You can specify 0-4096.

Default None

Mode Configuration mode

Usage

The normal form of this command creates a new or edits an existing IP limit.

The **no** form of this command removes the specified IP limit. If you do not specify an IP address list name, all IP limits are removed after user confirmation.

Example

The following command creates an IP limit for clients in IP address list "iplist1":

```
EX(config)#qos ip limit iplist1 25000
```

qos iplist

Create an IP address list. An IP address list can be used to define source or destination IP addresses in QoS match rules.

Syntax Description

```
[no] qos iplist name
```

Parameter	Description
name	Name of the list, 1-31 characters.

This command changes the CLI to the configuration level for the specified IP list, where the following IP-list related command is available:

Command	Description
[no] **ip** *ip-address1* {{*subnet-mask* | */mask-length*} | **to** *ip-address2*}	Adds a range of IP addresses to the current IP list. *ip-address1* – First IP address of the IP range. *subnet-mask* | */mask-length* – Subnet mask or mask length. If you use this option, all addresses in the subnet (all addresses that match the mask) are included in the list. *ip-address2* – Last IP address of the IP range.

Default

The EX device does not have an IP lists by default.

Mode

Configuration mode

Usage The normal form of this command creates a new or edits an existing IP list, and changes to the configuration level for the list.

The **no** form of this command removes the specified list. If you do not specify a list name, all IP lists are removed after user confirmation.

Example The following command creates an IP address list named “test”:

```
EX(config)#qos iplist test
EX(config-qos-iplist)#
```

Example The following command adds some address ranges to the current IP list and displays the results:

```
EX(config-qos-iplist)#ip 192.168.3.2 to 192.168.3.10
EX(config-qos-iplist)#ip 192.168.3.20 to 192.168.3.30
EX(config-qos-iplist)#ip 192.168.3.15
EX(config-class)#show this

qos iplist test
  ip 192.168.3.2 to 192.168.3.10
  ip 192.168.3.15
  ip 192.168.3.20 to 192.168.3.30
```

qos policy

Create or delete a QoS policy for traffic management.

Syntax Description [**no**] **qos policy** *policy-name*

Parameter	Description
policy-name	Policy name, 1-31 characters.

This command changes the CLI to the configuration level for the specified QoS policy, where the following policy-related commands are available:

Command	Description
[**no**] {**category** *category-name* | **class** *class-name*} [**precedence** *prec-value*]	Adds a traffic category or class to the current QoS policy. The *prec-value* is a numeric value used to prioritize the action groups within a policy. Before

comparing traffic against a policy, the EX device internally reorders the action groups based on precedence. The EX device then compares the traffic against the action groups, and takes the action specified in the first policy group that matches the QoS class (or category) in the traffic. You can specify 1-10. The highest (most preferred) precedence is 1.

The command changes the CLI to configuration level for the class, where the following class-related commands are available.

`[no] bandwidth total` *`options`* – Limits the bandwidth for egress traffic leaving the QoS interface, for the entire class.

`min` *`min-rate`* `|` **`percent`** *`num`* – The minimum rate of the class. This is the bandwidth that will be reserved for the class. You can specify the rate in Kbps (0-8000000) ***or*** as a percentage (**percent** 0-100).

`max` *`max-rate`* `|` **`percent`** *`num`* – The maximum rate of the class. This is the maximum rate that can be reached by borrowing from a sibling class if there is bandwidth left. You can specify the rate in Kbps (0-8000000) ***or*** as a percentage (**percent** 0-100).

Note: If you plan to set percentage values, use the **min** command first. If you set only the minimum percentage, the maximum percentage is set to the same value as the minimum percentage by default.

`priority` *`priority-value`* – Class priority for bandwidth. If there is insufficient bandwidth available, classes with lower priorities have higher bandwidth priority than classes with higher priority values.

`qlen` *`queue-length`* – Number of packets that can be queued for the class if its current rate is over the bandwidth rate. Packets are dropped if the number of packets that need to be queued exceeds the queue length.

`[no] bandwidth perip` *`options`* – sets bandwidth guarantees and limits for individual IP flows within a traffic class, and dynamically allocate bandwidth equally among active flows.

> **`external | internal`** – Traffic direction to which this action group applies:
>
> – **external**: outside IP address connected to an EX external interface
>
> – **internal**: inside IP address connected to an EX internal interface
>
> **`max`** `{`*`max-rate`* `|` **`unlimited`**`}` – Amount of bandwidth, measured in Kbps, reserved for the Max Number of IPs. You can specify 0-8000000 or **unlimited**.
>
> **`maxip`** `{`*`num`* `|` **`unlimited`**`}`
> `[`**`overflow`** *`options`*`]` – Number of IP addresses for which bandwidth will be guaranteed. Bandwidth is allocated in equal portions up to the maximum rate to all IP addresses up to the maximum. You can specify 0-65535 or **unlimited**.
>
> Additional IP addresses can get bandwidth only if you use the **overflow** option. The **max** option specifies the maximum bandwidth allowed for additional IP addresses, 0-8000000 or **unlimited**. The **min** option specifies the amount of bandwidth guaranteed for additional IP addresses, 0-8000000.
>
> **`min`** *`min-rate`* – Amount of bandwidth, measured in Kbps, reserved for **maxip**. You can specify 0-8000000.

`[`**`no`**`]` **`connection`** `{`**`total`** `|`
`perip` `{`**`internal`** `|` **`external`**`}}`
– Specify one of the following connection limits:

> **`max-active`** *`num`* – Maximum number of active connections (0-1000000).
>
> **`max-rate`** *`num`* – Maximum number of connections per second (0-1000000).

For each of the above options, you can specify the action to take when the connection limit is exceeded:

> **`action`** `{`**`drop`** `|` **`reject`**`}`

Drop means packets from the new connection request are silently dropped. **Reject** means the EX appliance sends a TCP RST (TCP reset flag) to the client.

[no] drop – Drops all traffic of this class.

The bandwidth, connection, drop, and limit actions are exclusive of one another.

```
[no] limit rate
[conform conform-action
  {transmit | drop |
   set-dscp-transmit
     dscp-value}]
[exceed exceed-action
  {transmit | drop |
   set-dscp-transmit
     dscp-value}]
```

Limits the rate of incoming traffic for the current class and specifies the actions to take for conforming and excess traffic.

rate – The permitted rate of incoming traffic for the class.

conform-action – Action to take for traffic within the specified limit. You can specify one of the following:

transmit – Transmit the traffic.

drop – Drop the traffic.

set-dscp-transmit – Set the DSCP value in the traffic, then transmit the traffic.

exceed-action – Action to take for traffic that exceeds the specified limit. The available options are the same as those for *conform-action*.

The bandwidth, limit, and drop actions are exclusive of one another.

[no] mark dscp *dscp-value*

Changes the differentiated services code point (DSCP) value of packets that belongs to this traffic class. The *dscp-value* is the value to mark in the DSCP field in the IP headers. Enter **mark dscp ?** to list the available DSCP values.

`[no] policy policy-name` – Creates a child policy under this class, which creates a hierarchical policy. All packets processed for the class are processed for the child policy also.

Adding a policy to another policy creates a hierarchical policy. The policy you add here becomes a child policy. The traffic class to which you are adding the policy becomes the parent class of the child policy.

`qos` Enables you to configure more QoS settings without returning to the global configuration level of the CLI first.

Default

The EX device does not have any default QoS policies. When you add a policy, the policy has the following default settings:

- **class** or **category** – When you create a QoS policy, a “default” traffic class is automatically created for the policy. Traffic that does not match any of the traffic classes you add to the policy will match the default class instead. The default precedence value for each class is 10 (lowest precedence).

  When you add a class to the policy, the class has the following default settings within the policy.

  - **bandwidth** – The default max-rate is the value you specify for the min-rate. The default priority value is 0. The default queue length is 1024. Per-IP shaping is disabled by default.
  - **connection** – None
  - **drop** – Traffic is not dropped.
  - **limit** – The default conform action is **transmit**. The default exceed action default is **drop**.
  - **mark** – None
  - **policy** – None

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing QoS policy and changes the CLI to the configuration level for the policy.

The **no** form of this command removes the specified QoS policy. If you do not specify a policy name, all QoS policies are removed after user confirmation.

Rules for Bandwidth Rates

If you specify the rates as percentages:

- The percent is the parent-class or the shape-rate percentage of the interface.
- If the policy of the class is a child policy of a class, the percent is the percent of the bandwidth of its parent class. If the parent class is not configured with bandwidth, the percent will be its parent class percent, and so on.
- If the policy of the class has no parent class, the percent will be the shape rate of the interface that the policy is applied to.
- If the class is in a sub-policy, the actual rate will not exceed the rate of the parent class.

The bandwidth, limit, and drop actions are exclusive of one another.

The difference between the bandwidth and limit actions is that bandwidth queues excess packets whereas the limit action does not queue any packets. For this reason, A10 recommends that you use the limit action for ingress traffic and the bandwidth action for egress traffic.

Example The following command creates a policy named “test”:

```
EX(config)#qos policy test
```

Example The following command adds class “http” to the current policy:

```
EX(config-policy)#class http
```

Example The following command allows 100 percent of the bandwidth to the “http” class within the current policy:

```
EX(config-policy-class)#bandwidth min 100
```

Example The following command sets the conform and exceed actions for the current traffic class:

```
EX(config-policy-class)#limit 200 conform set-dscp-transmit AF43 exceed
set-dscp-transmit 34
```

Example The following command marks the DSCP value in packets in the current traffic class:

```
EX(config-policy-class)#mark dscp ef
```

qos portlist

Create a port list. A port list can be used to define source or destination protocol ports in QoS match rules.

Syntax Description `[no] qos portlist name`

Parameter	Description
name	Name of the list, 1-31 characters.

This command changes the CLI to the configuration level for the specified port list, where the following port-list related command is available:

Command	Description
[no] port *portnum* [**to** *portnum*]	Specifies a protocol port or range of ports in the list. To specify a range, enter the lowest port number in the range, followed by **to** and the highest port number in the range.

Default None

Mode Configuration mode

Example The following command configures a port list containing ports 2048-2054:

```
EX(config)#qos portlist portlist1
EX(config-qos-portlist)#port 2048 to 2054
```

qos resource-limit

Limit the number of auto-created classes.

Syntax Description

```
qos resource-limit class auto-created number num
```

Parameter	Description
num	Max limit imposed on auto-created classes, ranges from 0-5120, based upon model.

Default

Varies based upon model.

Mode

Configuration mode

Usage

The EX appliance's traffic classes are pre-defined by the system, or they can be manually configured by the user, or automatically created using the auto-detect feature (which is enabled by default) and creates classes based upon VLAN, interface, internal subnet, or IP-protocol.

However, deploying the EX appliance in complicated networks that have many TCP flows can result in the autodetect feature creating too many auto-created classes (and using up resources). To prevent this outcome, use the `resource-limit` command to place a limit on the number of classes that can be created by the auto-detect feature.

Example

The following command restricts the number of auto-created classes to no more than half (512) of the total number available (1,024) on an EX 1100. This should keep some classes available for manually-created classes.

```
EX(config)#qos resource-limit class auto-created number 512
```

qos schedule

Schedule application of a policy to a QoS interface.

Syntax Description

```
[no] qos schedule policy-name on intf-name
{ingress | egress} hh1:mm1 hh2:mm2 [day [day ...]]
```

Parameter	Description
policy-name	Policy to be scheduled.
intf-name	QoS interface name.
ingress | egress	Traffic direction.
hh1:mm1	Start time.

hh2:*mm2*	End time.
day	Day of the week (Sun, Mon, Tue, ... Sat).

Mode

Configuration mode

Usage

If a policy is already applied to the interface before this policy is applied by the schedule, the former policy will be replaced for the duration of the policy schedule, then restored after the scheduled policy's schedule ends.

While a scheduled policy is in effect, the **show qos interface** command will still list the configured policy rather than the scheduled policy. However, the statistics counters will show statistics for the currently applied policy, which is the scheduled policy.

Example

The following commands schedule some policies and show the schedule:

```
EX(config)#qos schedule http on vt egress 01:01 02:02 Mon Web Fri
EX(config)##qos schedule http on vt egress 03:03 04:04 Tue Thu
EX(config)#qos schedule http on vt egress 07:07 08:08
EX(config)#qos schedule http on vt ingress 01:01 02:02
EX(config)#qos schedule http on vt ingress 04:04 05:05
EX(config)#qos schedule http on vt ingress 10:10 11:11
EX(config)#show qos schedule
qos schedule http on vt ingress 01:01 02:02 Mon Web Fri
qos schedule http on vt ingress 04:04 05:05 Tue Thu
qos schedule http on vt ingress 10:10 11:11
qos schedule http on vt egress 01:01 02:02
qos schedule http on vt egress 03:03 04:04
qos schedule http on vt egress 07:07 08:08
```

qos statistic memory

Limit the memory used for traffic statistics.

Syntax Description

qos statistic memory *Mbytes*

Parameter	Description
Mbytes	Number of MB to use for traffic statistics, 1-64.

Default

N/A

Mode

Configuration mode

Example

The following command limits the amount of memory that can be used for traffic statistics to 8 MB:

```
EX(config)#qos statistic memory 8
```

qos tcp-optimization

Optimize the flow of TCP traffic across the network.

Syntax Description `[no] qos tcp-optimization enable`

Default Disabled. When disabled, the EX will drop packets when the sending device transmits too much traffic.

Mode Configuration mode

Usage Enabling TCP optimization feature enables sending and receiving devices to better coordinate the transmission of data for more efficient use of network resources.

Example The following command enables the TCP Window Adjustment feature:

```
EX(config)#qos tcp-optimization enable
```

qos view

Configure a QoS view for reporting. A view is a named set of QoS categories.

Syntax Description `[no] qos view name`

Parameter	Description
name	Name of the list, 1-31 characters.

This command changes the CLI to the configuration level for the specified QoS view, where the following view-related command is available:

Command	Description
[no] include *category-name*	Specifies a QoS category to add to the view.

Default When you create a new view, it contains no categories by default.

The EX device has the following views by default:

- application – This view contains the following categories:
  - Others
  - Application
  - Misc
  - Database

  - DirectoryService
  - Email
  - File
  - Messaging
  - Multimedia
  - P2P
  - Session
  - Security
  - VOIP
- extif – This view contains the extif category, which contains the QoS external interfaces configured on the device. Each QoS external interface is a separate class within the extif category.
- intif – This view contains the intif category, which contains the QoS internal interfaces configured on the device. Each QoS internal interface is a separate class within the intif category.
- subnet – This view contains the subnet category, which contains local (private) IP subnets configured on the device.
- vlan – This view contains the vlan category, which contains the VLANs configured on the device.

These default views can not be modified or deleted. However, if you do not want the EX device to automatically add classes to the default views, you can disable class auto-detection. (See “qos autodetect” on page 114.)

Mode

Configuration mode

Report Commands

report alert-rule

Configure traffic alert rules.

Syntax Description

```
report alert-rule {total-rate | user-rate |
user-connection} rule-name

no report alert-rule {total-rate | user-rate |
user-connection} {all | rule-name}
```

Parameter	Description
total-rate	Sets a limit for the total traffic rate. The alert will be raised if the total traffic rate exceeds the limit.
user-rate	Sets a limit for user traffic rate. The alert will be raised if any user's traffic rate exceeds the limit.
user-connection	Sets a limit for user connections. The alert will be raised if new user-sponsored connections within a certain time period exceed the limit.
rule-name	Name of the rule, 1-255 characters.
all	Valid only with the **no** form of the command. This option removes all alert rules.

The **total-rate**, **user-rate**, and **user-connection** parameters change the CLI to the configuration level for the alert rule, where the following alert-rule related commands are available:

Command	Description
connection *num*	Maximum number of connections allowed within the duration period, for a single user. Maximum number of connections allowed within the duration period, for a single user.
duration *minutes*	Configures the duration time for the rate limit or connection limit. If the average rate or number of new connections exceeds the limit within the specified duration, the alert is generated. You can specify 0-2147483647 minutes.

[no] email [append] *email-address* [*email-address...*]

Configures email addresses to which to send email for generated reports.

The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option.

To remove individual addresses from the list, use the **no** form of the command.

If no email addresses are specified for the report template, the default email address will be used. The default email address is configured by the **report email** command.

[no] enable-email

Enables or disables sending email.

ignore-ip *ipaddr*

Excludes the specified IP address from the alert.

name *string*

Renames the alert rule. The name can be 1-31 characters long.

notify-interval *minutes*

Specifies the amount of time the EX device will wait between sending alerts generated by this alert rule. You can specify 0-2147483647 minutes.

rate *rate-value*

Specifies the maximum allowed traffic for a total traffic alert rule or user traffic alert rule. You can specify 1-8000000 kbits/s.

report

Enables you to configure additional report settings, without the need to return to the global configuration level of the CLI.

Default

Report templates do not have any alert rules by default.

When you create an alert rule, it has the following default settings:

- **connection** – not set
- **duration** – not set
- **email** – email addresses configured for the report template
- **enable-email** – email setting for the report template
- **ignore-ip** – not set

- **name** – name used when the alert was created
- **notify-interval** – not set
- **rate** – not set

Mode Configuration mode

Usage The normal form of the command creates a new alert rule and changes the CLI to the configuration level for the rule.

The **no** form of the command removes the specified alert rule. If you use the **all** option instead of a rule name, all alert rules are removed.

Example The following command creates a total-rate alert rule named “limit-total-traffic”:

```
EX(config)#report alert-rule total-rate limit-total-traffic
EX(config-alert-rule)#
```

Example The following command sets the rate in the current alert rule to 1024 kbits/s:

```
EX(config-alert-rule)#rate 1024
```

Related Commands **show report alert-rule**, **show traffic alert**

report email

Configure the default email address for report templates and alert rules.

Syntax Description

```
report email [append] email-address
[email-address ...]

[no] report email [email-address ...]
```

Default N/A

Mode Configuration mode

Usage The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option.

To remove individual addresses from the list, use the **no** form of the command.

You also can configure email address lists in individual report templates and alert rules. In this case, the email address list configured in an individual report template or alert rule overrides the default email address list configured here.

Example

The following commands configure a default email address, then add another address to the list:

```
EX(config)#report email test1@a10networks.com
EX(config)#report email append test2@a10networks.com
```

report enable

Enable report statistics.

Syntax Description

```
[no] report enable
{
class [{all | class-name}
  [internal-talker | external-talker | talker]] |
others-ip-port
tcp |
url [path]
}
```

Parameter	Description
`class {all | class-name}`	Enables report statistics for all classes or a specific class. Optionally, you can specify the traffic direction: **internal-talker** – Enables report statistics only for internal talkers. **external-talker** – Enables report statistics only for external talkers. **talker** – Enables report statistics for internal and external talkers.
`others-ip-port`	Enables report statistics for the “Others” class, by IP address and protocol port.
`tcp`	Enables report statistics for TCP traffic.
`url [path]`	Enables report statistics for URLs and, optionally, individual pathnames on the URLs**.**

Default

All reports are enabled by default.

Mode

Configuration mode

Example The following command enables report statistics for internal talkers in all classes:

```
EX(config)#report enable class all internal-talker
```

report export

Export a generated report file to a remote host using a file transfer protocol.

Syntax Description

```
report export {tftp | ftp | scp | rcp}
```

Export generated report files using one of the following file transfer methods:

Parameter	Description
tftp	Trivial File Transfer Protocol. This is a light-weight version of FTP. Remote file path of tftp, with format: **tftp://***host***[:***port***]/***file*
ftp	File Transfer Protocol (standard protocol for copying files over TCP/IP network). Remote file path of FTP, with format: **ftp://[***user***:***pass***@]***host***[:***port***]/***file*
scp	Secure Copy (based on SSH). Remote file path of scp, with format: **scp://[***user***:***pass***@]***host***[:***port***]/***file*
rcp	Unix 'remote copy' command. Remote file path of rcp, with format: **rcp://[***user***@]***host***/***file*

Default N/A

Mode Configuration mode

Usage In addition to sending EX reports by email, the EX appliance can export generated report files using file transfer protocols.

Example The following command uses the Unix remote copy command to copy the file “sample-file” to the server “example.com”:

```
EX(config)#report export rcp://jsmith@example.com/sample-file
```

report favorite abuser

Configure a favorite (template) for abuser reports.

Abuser reports show statistics for users who were in the abuser class during the report period. Users are placed in the abuser class when their network activity exceeds the thresholds specified by the configured abuser criteria.

By default, the 10 most active abusers are listed by username. You can change the number of abusers listed, or choose to list users by IP address instead of username.

Syntax Description

```
[no] report favorite abuser template-name
```

Parameter	Description
template-name	Specifies the name of the abuser report template.

This command changes the CLI to the configuration level for the specified report template, where the following template-related commands are available:

Command	Description
content abuser top base-on {**ip** | **user**} [**top-num** *num*]	Specifies the number of abusers to include in the report, and whether to list them by IP address or username. You can specify 1-100 users, with a default of 10.
[**no**] **email** [**append**] *email-address* [*email-address...*]	Defines the email addresses to which to send generated reports. The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option. To remove individual addresses from the list, use the **no** form of the command. If no email addresses are specified for the report template, the default email address will be used.

The default email address is configured by the **report email** command.

[no] export

Defines the file transfer protocol to use to send generated reports. (See “report export” on page 139 for details.)

[no] format {html | pdf | xml | csv}

Defines the document format for the generated report. Options are HTML, PDF, XML, and CSV. The default is PDF.

[no] period {minutes | hours | days | weeks | months} *num*

Time span for the report. Enter a period type (minute, or hour, and so on), and then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {now | *mm/dd/yyyy hh:mm***}**

Specifies when the time span for the report ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

[no] schedule enable

Enables the schedule. Use the other schedule commands to configure the schedule. The schedule takes effect after you enable it.

[no] schedule start-time {now | *mm/dd/yyyy***}**

Defines the start time for the report generation. You can choose to generate reports immediately or at some point in the future, by specifying the month, day and year.

[no] schedule end-time *mm/dd/yyyy*

Defines the end time for the report generation. Specify the month, day, and year to designate an end time for the report generation. If no end-time value is specified, the default 3-hour period will be used.

[**no**] **schedule per-days** *num-days* **time** *hh*:*mm* [*hh*:*mm* ...]	Defines the daily frequency with which the report will be generated. For example, to generate the report every other day at 2 p.m., you would enter the following command: **schedule per-days 2 time 14:00**
[**no**] **schedule per-weeks** *num-weeks* **at** {*day* ...} **time** *hh*:*mm* [*hh*:*mm* ...]	Defines the weekly frequency with which the report will be generated. For example, to generate the report every week on Friday at 5 p.m., you would enter the following command: **schedule per-weeks 1 at Friday time 17:00** The *day* can be one or more of the following: **Sunday** **Monday** **Tuesday** **Wednesday** **Thursday** **Friday** **Saturday**
[**no**] **schedule per-months** *num-months* **at** {*date* [...]} **time** *hh*:*mm* [*hh*:*mm* ...]	Defines the monthly frequency with which the report will be generated. For example, to generate the report every 2 months on the last day of the month at command: , you would enter the following command: **schedule per-months 2 at last-day-of-month time 24:00**

The *date* can be one or more of the following:

The date, **1-31.**

last-day-of-month

Default

There are no default template criteria. When you configure a favorite template, some of the values have defaults, as described above.

Mode

Configuration mode

Example

The following command changes the document format to HTML:

```
EX(config)#report favorite abuser abuser-1 format html
```

report favorite others

Configure a favorite (template) for others reports.

Others reports show activity for the Others traffic class. By default, overall statistics are shown for all IP addresses and Layer 4 protocol ports, by source address. You can narrow the scope of the report by entering a specific IP address or protocol port. You also can enable statistics for the following:

- Top services (listed by IP address and protocol port)
- Top IP addresses
- Top protocol ports

Syntax Description

```
[no] report favorite others template-name
```

Parameter	Description
template-name	Specifies the name of the others report template.

This command changes the CLI to the configuration level for the specified report template, where the following template-related commands are available:

Command	Description
[no] content others-class overall range {destination | source} [conn-dir {inbound | outbound}]	Provides overall statistics.

	range {**destination** | **source**} – Specify whether to include source IP addresses or destination IP addresses. **conn-dir** {**inbound** | **outbound**} – Optionally, limits the output to inbound connections or outbound connections. By default, statistics are shown for both directions.
`[no] content others-class ip-port range {destination	source} [conn-dir {inbound	outbound}] [top-num` *`num`*`]`	Provides statistics for services (identified by Layer 3 IP address plus Layer 4 protocol port). **range** {**destination** | **source**} – Following the scope option, you must specify whether to include source IP addresses or destination IP addresses. **conn-dir** {**inbound** | **outbound**} – Optionally, limits the output to inbound connections or outbound connections. By default, statistics are shown for both directions. **top-num** *num* – Optionally, limits the output to only the most active traffic. The *num* can be 1-100.
`[no] content others-class ip range {destination	source} [conn-dir {inbound	outbound}] [top-num` *`num`*`]`	Provides statistics for IP addresses. **range** {**destination** | **source**} – Following the scope option, you must specify whether to include source IP addresses or destination IP addresses. **conn-dir** {**inbound** | **outbound**} – Optionally, limits the output to inbound connections or out-

bound connections. By default, statistics are shown for both directions.

top-num *num* – Optionally, limits the output to only the most active traffic. The *num* can be 1-100. The default value for *num* is 10.

[**no**] **content others-class port range** {**destination** | **source**} [**conn-dir** {**inbound** | **outbound**}] [**top-num** *num*]

Provides statistics for protocol ports.

range {**destination** | **source**} – Following the scope option, you must specify whether to include source IP addresses or destination IP addresses.

conn-dir {**inbound** | **outbound**} – Optionally, limits the output to inbound connections or outbound connections. By default, statistics are shown for both directions.

top-num *num* – Optionally, limits the output to only the most active traffic. The *num* can be 1-100. The default value for *num* is 10.

[**no**] **email** [**append**] *email-address* [*email-address...*]

Defines the email addresses to which to send generated reports.

The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option.

To remove individual addresses from the list, use the **no** form of the command.

If no email addresses are specified for the report template, the default email address will be used. The default email address is configured by the **report email** command.

[no] **export**

Defines the file transfer protocol to use to send generated reports. (See “report export” on page 139 for details.)

[no] **format** {**html** | **pdf** | **xml** | **csv**}

Defines the document format for the generated report. Options are HTML, PDF, XML, and CSV. The default is PDF.

[no] **period** {**minutes** | **hours** | **days** | **weeks** | **months**} *num*

Time span for the report. Enter a period type (**minute**, or **hour**, and so on), and then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {**now** | *mm/dd/yyyy* *hh*:*mm*}

Specifies when the time span for the report ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

[no] **schedule enable**

Enables the schedule. Use the other schedule commands to configure the schedule. The schedule takes effect after you enable it.

[no] **schedule start-time** {**now** | *mm/dd/yyyy*}

Defines the start time for the report generation. You can choose to generate reports immediately or at some point in the future, by specifying the month, day and year.

[no] **schedule end-time** *mm/dd/yyyy*

Defines the end time for the report generation. Specify the month, day, and year to designate an end time for the report generation. If no end-time is specified, the default 3-hour period is used.

[**no**] **schedule per-days** *num-days* **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the daily frequency with which the report will be generated. For example, to generate the report every other day at 2 p.m., you would enter the following command: command: **schedule per-days 2 time 14:00**

[**no**] **schedule per-weeks** *num-weeks* **at** {*day* ...} **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the weekly frequency with which the report will be generated. For example, to generate the report every week on Friday at 5 p.m., you would enter the following command: **schedule per-weeks 1 at Friday time 17:00**

The *day* can be one or more of the following:

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

[**no**] **schedule per-months** *num-months* **at** {*date* [...]} **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the monthly frequency with which the report will be generated. For example, to generate the report every 2 months on the last day of the month at command: , you would enter the following command:
schedule per-months 2 at last-day-of-month time 24:00

The *date* can be one or more of the following:

The date, **1-31.**

last-day-of-month

`[no] scope`
`[ip ipaddr`
`[port portnum]`
	Narrows the scope of the report by limiting it to a specific internal IP address or port. If you specify an IP address, you can optionally further restrict the output using a specific port, ranging from 1 - 65535. If you specify a port number, you can optionally further restrict the output by specifying an IP address.

Default

There are no default template criteria. When you configure a favorite template, some of the values have defaults, as described above.

Mode

Configuration mode

Example

The following command sets the time period during which statistics are gathered to 2 days:

```
EX(config)#report favorite others others-1 period days 2
```

report favorite tcp

Configure a favorite (template) for TCP reports.

TCP performance reports shows graphs and statistics for the following:

- Efficiency
- Round-trip-time (RTT)
- Connection health (Conn-Health)

By default, statistics are shown for all classes, and for both packet and connection directions. You can narrow the scope of the report by selecting individual classes, and by selecting inbound or outbound for the packet or connection direction.

Syntax Description

`[no] report favorite tcp template-name`

Parameter	Description
template-name	Specifies the name of the TCP report template.

This command changes the CLI to the configuration level for the specified report template, where the following template-related commands are available:

Command	Description
content tcp efficiency [**packet-dir** {**inbound** | **outbound**}]	Determines that report content will include TCP transmission efficiency statistics. You can optionally define the traffic packet direction. By default, statistics are shown for both directions.
content tcp conn-health [**conn-dir** {**inbound** | **outbound**}]	Determines that report content will include TCP connection health statistics. You can optionally define the traffic packet direction. By default, statistics are shown for both directions.
content tcp rtt	Determines that report content will include TCP round trip time statistics.
[**no**] **email** [**append**] *email-address* [*email-address...*]	Defines the email addresses to which to send generated reports. The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option. To remove individual addresses from the list, use the **no** form of the command. If no email addresses are specified for the report template, the default email address will be used. The default email address is configured by the **report email** command.
[**no**] **export**	Defines the file transfer protocol to use to send generated reports. (See "report export" on page 139 for details.)

[no] format {html | pdf | xml | csv}

Defines the document format for the generated report. Options are HTML, PDF, XML, and CSV. The default is PDF.

[no] period {minutes | hours | days | weeks | months} *num*

Time span for the report. Enter a period type (**minute**, or **hour**, and so on), and then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {now | *mm/dd/yyyy hh*:*mm*}

Specifies when the time span for the report ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

[no] schedule enable

Enables the schedule. Use the other schedule commands to configure the schedule. The schedule takes effect after you enable it.

[no] schedule start-time {now | *mm/dd/yyyy*}

Defines the start time for the report generation. You can choose to generate reports immediately or at some point in the future, by specifying the month, day and year.

[no] schedule end-time *mm/dd/yyyy*

Defines the end time for the report generation. Specify the month, day, and year to designate an end time for the report generation. If no end-time value is specified, the default 3-hour period will be used.

[**no**] **schedule per-days** *num-days* **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the daily frequency with which the report will be generated. For example, to generate the report every other day at 2 p.m., you would enter the following command: **`schedule per-days 2 time 14:00`**

[**no**] **schedule per-weeks** *num-weeks* **at** {*day* ...} **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the weekly frequency with which the report will be generated. For example, to generate the report every week on Friday at 5 p.m., you would enter the following command: **`schedule per-weeks 1 at Friday time 17:00`**

The *day* can be one or more of the following:

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

[no] **schedule per-months** *num-months* **at** {*date* [...]} **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the monthly frequency with which the report will be generated. For example, to generate the report every 2 months on the last day of the month at command: , you would enter the following command:

schedule per-months 2 at last-day-of-month time 24:00

The *date* can be one or more of the following:

The date, **1-31.**

last-day-of-month

scope class *class-name*

Narrows the scope of the report by limiting it to a specific class.

Default There are no default template criteria. When you configure a favorite template, some of the values have defaults, as described above.

Mode Configuration mode

Example The following command overwrites any existing email addresses associated with the TCP reports with the new email address, jack@example.com:

```
EX(config)#report favorite tcp tcp-1 email jack@example.com
```

report favorite traffic

Configure a favorite (template) for traffic reports.

Traffic reports show graphs and statistics for the following:

- Traffic rate
- Number of connections
- Packet size distribution

For each type of statistic, you can enable the following:

- Overall
- Top 10 Classes
- Top 10 Talkers

The overall option is enabled by default. The top-class, top-internal-talker, and top-external-talker options are disabled by default. The top-num option specifies how many classes or talkers to include. The default is 10.

By default, statistics are shown for all classes, internal talker IPs, and external talker IPs. You can narrow the scope of the report by specifying any of the following:

- Specific classes
- Specific internal talker IP
- Specific external talker IP

Statistics for all (both) inbound and outbound connection and packet directions are shown. For traffic rate, you can change the direction to inbound or outbound connections only. For packet distribution, you can change the connection direction and packet direction individually, to inbound or outbound.

Syntax Description

```
[no] report favorite traffic template-name
```

Parameter	Description
template-name	Specifies the name of the traffic report template.

This command changes the CLI to the configuration level for the specified report template, where the following template-related commands are available:

Command	Description
content rate overall [**conn-dir** {**inbound** | **outbound**}]	Determines that report output will include overall rate statistics. You can optionally define the traffic packet direction. By default, statistics are shown for both directions.
content rate top-class [**view** *view-name*] [**conn-dir** {**inbound** | **outbound**} [**top-num** *num*]	Determines that report output will include top-class rate statistics. You can optionally define the traffic packet direction. By default, statistics are

shown for both directions. You can optionally define how many classes are shown in the report from 1 - 100. By default, the top 10 classes are shown.

content rate top-internal-talker [**conn-dir** {**inbound** | **outbound**}] [**top-num** *num*]

Determines that report output will include top-internal-talker rate statistics. You can optionally define the traffic packet direction. By default, statistics are shown for both directions. You can optionally define how many talkers are shown in the report from 1 - 100. By default, the top 10 talkers are shown.

content rate top-external-talker [**conn-dir** {**inbound** | **outbound**}] [**top-num** *num*]

Determines that report output will include top-external-talker rate statistics. You can optionally define the traffic packet direction. By default, statistics are shown for both directions. You can optionally define how many talkers are shown in the report from 1 - 100. By default, the top 10 talkers are shown.

content connection overall

Determines that report output will include overall connection statistics.

content connection top-class [**view** *view-name*] [**top-num** *num*]

Determines that report output will include top-class connection statistics. You can optionally define how many classes are shown in the report from 1 - 100. By default, the top 10 classes are shown.

content connection top-internal-talker [**top-num** *num*]

Determines that report output will include top-internal-talker connection statistics. You can optionally define how many talkers are shown in the report from 1 - 100. By default, the top 10 talkers are shown.

content connection top-external-talker [**top-num** *num*]

Determines that report output will include top-external-talker connection statistics. You can optionally define how many talkers are shown in the report from 1 - 100. By default, the top 10 talkers are shown.

content packet-distribution overall [**conn-dir** {**inbound** | **outbound**}] [**packet-dir** {**inbound** | **outbound**}]

Determines that report output will include overall packet-distribution statistics. You can optionally change the connection direction and packet direction individually, to inbound or outbound. By default, statistics are shown for both directions.

content packet-distribution top-class [**view** *view-name*] [**large-packet-size** *size*] [**conn-dir** {**inbound** | **outbound**}] [**packet-dir** {**inbound** | **outbound**}] [**top-num** *num*]

Determines that report output will include top-class packet distribution statistics. You can further refine the report output using the following optional parameters:

	view – The view name. **large-packet-size** – Limit the report to include statistics for packets equal to or greater than the length you specify (256, 512, or 1024 bytes). The default large packet size is 1024. **conn-dir** – Limit the report to include inbound or outbound connections. By default, statistics are shown for both directions. **packet-dir** – Limit the report to include inbound or outbound packet direction. By default, statistics are shown for both directions. **top-num** – You can optionally define how many classes are shown in the report, from 1 - 100. By default, the top 10 classes are shown.
`content packet-distribution top-internal-talker [large-packet-size size] [conn-dir {inbound | outbound}] [packet-dir {inbound | outbound}] [top-num num]`	Determines that report output will include top-internal-talker packet distribution statistics. You can further refine the report output using the following optional parameters: **large-packet-size** – Limit the report to include statistics for packets equal to or greater than the length you specify (256, 512, or 1024 bytes). The default large packet size is 1024. **conn-dir** – Limit the report to include inbound or outbound connections. By default, statistics are shown for both directions.

packet-dir – Limit the report to include inbound or outbound packet direction. By default, statistics are shown for both directions.

top-num – You can optionally define how many classes are shown in the report from 1 - 100. By default, the top 10 classes are shown.

[**no**] **email** [**append**] *email-address* [*email-address...*]

Defines the email addresses to which to send generated reports.

The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option.

To remove individual addresses from the list, use the **no** form of the command.

If no email addresses are specified for the report template, the default email address will be used. The default email address is configured by the **report email** command.

[**no**] **export**

Defines the file transfer protocol to use to send generated reports. (See “report export” on page 139 for details.)

[**no**] **format** {**html** | **pdf** | **xml | csv**}

Defines the document format for the generated report. Options are HTML, PDF, XML, and CSV. The default is PDF.

[**no**] **period** {**minutes** | **hours** | **days** | **weeks** | **months**} *num*

Time span for the report. Enter a period type (**minute**, or **hour**, and so on), and then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {now | *mm/dd/yyyy hh*:*mm*}

Specifies when the time span for the report ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

[no] schedule enable

Enables the schedule. Use the other schedule commands to configure the schedule. The schedule takes effect after you enable it.

[no] schedule start-time {now | *mm/dd/yyyy*}

Defines the start time for the report generation. You can choose to generate reports immediately or at some point in the future, by specifying the month, day and year.

[no] schedule end-time *mm/dd/yyyy*

Defines the end time for the report generation. Specify the month, day, and year to designate an end time for the report generation. If no end-time value is specified, the default 3-hour period will be used.

[no] schedule per-days *num-days* **time** *hh*:*mm* [*hh*:*mm ...*]

Defines the daily frequency with which the report will be generated. For example, to generate the report every other day at 2 p.m., you would enter the following command:

schedule per-days 2 time 14:00

[no] schedule per-weeks *num-weeks* **at** {*day ...*} **time** *hh*:*mm* [*hh*:*mm ...*]

Defines the weekly frequency with which the report will be generated. For example, to generate the report every week on Friday at 5 p.m., you would enter the following command: **schedule per-weeks 1 at Friday time 17:00**

The *day* can be one or more of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

[**no**] **schedule per-months** *num-months* **at** {*date* [*...*]} **time** *hh*:*mm* [*hh*:*mm ...*]

Defines the monthly frequency with which the report will be generated. For example, to generate the report every 2 months on the last day of the month at command: , you would enter the following command:

```
schedule per-months 2 at last-day-of-month time 24:00
```

The *date* can be one or more of the following:

- The date, **1-31.**
- **last-day-of-month**

scope category *category-name*

Narrows the scope of the report by specifying one or more classes of traffic.

scope class *class-name*

Narrows the scope of the report by specifying one or more classes of traffic.

scope class internal-talker *ipaddr*

Narrows the scope of the report by specifying an internal IP address.

external-talker *ipaddr*

Narrows the scope of the report by specifying an external IP address.

Default

There are no default template criteria. When you configure a favorite template, some of the values have defaults, as described above.

Mode

Configuration mode

Example

The following command narrows the scope of the generated report to statistics from internal IP address 10.10.10.1:

```
EX(config)#report favorite traffic traffic-1 scope internal-talker 10.10.0.1
```

report favorite url

Configure a favorite (template) for URL reports.

URL reports show the URLs accessed by internal talkers during the report period, and list the most active internal talker IP addresses. By default, overall statistics are displayed, as well as the 10 most active URLs and the 10 most active internal talkers.

You can narrow the scope of the report by entering a specific URL string, internal talker IP, or both. You also can change the number of URLs or talker IPs listed in the report output.

Syntax Description

```
[no] report favorite url template-name
```

Parameter	Description
template-name	Specifies the name of the URL report template.

This command changes the CLI to the configuration level for the specified report template, where the following template-related commands are available:

Command	Description
content url overall	Displays overall statistics.
content url top-url [**top-num** *num*]	Displays statistics for the most active URLs. You can specify 1-100 URLs, with a default of 10.
content url top-talker [**top-num** *num*]	Displays statistics for the most active talkers. You can specify 1-100 users, with a default of 10.

[**no**] **email** [**append**] *email-address* [*email-address...*]

Defines the email addresses to which to send generated reports.

The **append** option adds new email addresses without overwriting email addresses previously added with this command. To overwrite the previously configured list of email addresses, do not use the **append** option.

To remove individual addresses from the list, use the **no** form of the command.

If no email addresses are specified for the report template, the default email address will be used. The default email address is configured by the **report email** command.

[**no**] **export**

Defines the file transfer protocol to use to send generated reports. (See “report export” on page 139 for details.)

[**no**] **format** {**html** | **pdf** | **xml** | **csv**}

Defines the document format for the generated report. Options are HTML, PDF, XML, and CSV. The default is PDF.

[**no**] **period** {**minutes** | **hours** | **days** | **weeks** | **months**} *num*

Time span for the report. Enter a period type (**minute**, or **hour**, and so on), and then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {**now** | *mm/dd/yyyy hh*:*mm*}

Specifies when the time span for the report ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

[no] **schedule enable**

Enables the schedule. Use the other schedule commands to configure the schedule. The schedule takes effect after you enable it.

[no] **schedule start-time** {**now** | *mm/dd/yyyy*}

Defines the start time for the report generation. You can choose to generate reports immediately or at some point in the future, by specifying the month, day and year.

[no] **schedule end-time** *mm/dd/yyyy*

Defines the end time for the report generation. Specify the month, day, and year to designate an end time for the report generation. If no end-time value is specified, the default 3-hour period will be used.

[no] **schedule per-days** *num-days* **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the daily frequency with which the report will be generated. For example, to generate the report every other day at 2 p.m., you would enter the following command: **schedule per-days 2 time 14:00**

[no] **schedule per-weeks** *num-weeks* **at** {*day* ...} **time** *hh*:*mm* [*hh*:*mm* ...]

Defines the weekly frequency with which the report will be generated. For example, to generate the report every week on Friday at 5 p.m., you would enter the following command: **schedule per-weeks 1 at Friday time 17:00**

The *day* can be one or more of the following:

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

[**no**] **schedule per-months** *num-months* **at** {*date* [*...*]} **time** *hh*:*mm* [*hh*:*mm ...*]

Defines the monthly frequency with which the report will be generated. For example, to generate the report every 2 months on the last day of the month at command: , you would enter the following command:

```
schedule per-months 2 at last-day-of-month time 24:00
```

The *date* can be one or more of the following:

The date, **1-31.**

last-day-of-month

scope url *url-path* [**talker** *ipaddr*]

Narrows the scope of the report by specifying a URL, and optionally, an internal IP address associated with a specific user.

scope talker *ipaddr* [**url** *url-path*]

Narrows the scope of the report by specifying an internal IP address associated with a specific user, and optionally, a URL.

Default

There are no default template criteria. When you configure a favorite template, some of the values have defaults, as described above.

Mode

Configuration mode

Example

The following command creates a favorite URL template that will generate a report listing the top 5 most frequented websites.

```
EX(config)#report favorite url url-1 content url top-url top-num 5
```

report history

Change the amount of time report data is stored on the system.

Syntax Description

```
report history days

[no] report history
```

Parameter	Description
days	Number of days to keep report data, 7-365.

Default

Report data is kept for 30 days by default.

Mode

Configuration mode

Usage

Setting a longer data storage time can support long-term reports and history queries. However, as the report database grows, system performance can be affected. You can use the **show report history** command to monitor report data storage time and database size.

Example

The following command changes the report history length to 90 days:

```
EX(config)#report history 90
```

Related Commands

`show report history`

Application Protocol Logging Commands

applog alias

Assign an alias name to a set of applications.

Syntax Description

```
[no] applog alias alias-name {aim | msnim | yim |
ftp | nfs | cifs | smtp | pop3 | qq | http}
```

Parameter	Description
alias-name	The alias name.
aim	AOL Instant Messenger
msnim	Microsoft Instant Messenger
yim	Yahoo Instant Messenger
ftp	File Transfer Protocol
nfs	Network file system
cifs	Common Internet File System
smtp	Simple Mail Transfer Protocol
pop3	Post Office Protocol v3
qq	Tencent Instant Messaging
http	Hypertext Transfer Protocol

Default None

Mode Configuration mode

Usage You can use application log aliases with **applog** commands that take an application name.

Example The following command creates an alias called “alltypes”:

```
EX(config)#applog alias alltypes aim yim msnim ftp nfs cifs smtp pop3 qq http
```

applog archive enable

Enable archiving of application logs.

Syntax Description

```
[no] applog archive enable [aim] [msnim] [yim]
[ftp] [nfs] [cifs] [smtp] [pop3] [qq] [http]
```

Parameter	Description
`aim`	AOL Instant Messenger
`msnim`	Microsoft Instant Messenger
`yim`	Yahoo Instant Messenger
`ftp`	File Transfer Protocol
`nfs`	Network file system
`cifs`	Common Internet File System
`smtp`	Simple Mail Transfer Protocol
`pop3`	Post Office Protocol v3
`qq`	Tencent Instant Messaging
`http`	Hypertext Transfer Protocol

Default

Disabled

Mode

Configuration mode

Example

The following command enables archiving of HTTP POST actions for Yahoo Instant Messenger and HTTP:

```
EX(config)#applog archive enable yim http
```

applog archive format

Specify the file format in which to save archived application logs.

Syntax Description

```
[no] applog archive format
{pdf | csv | xml | html}
```

Parameter	Description
`pdf`	Portable Document Format
`csv`	Comma-Separated Values
`xml`	Extensible Markup Language
`html`	Hypertext Transfer Protocol

Default HTML

Mode Configuration mode

Example The following command sets the file format for archived application logs to Comma-Separated Values:

```
EX(config)#applog archive format csv
```

applog archive interval

Change the interval at which the EX device archives application logs.

Syntax Description

```
[no] applog archive interval minutes
```

Parameter	Description
minutes	Number of minutes between archives, 1-1440 minutes.

Default 60

Mode Configuration mode

Usage If the application log buffer becomes full before the archive interval expires, the EX device immediately archives the logs and resets the interval timer to 0.

Example The following command changes the application log archive interval to 30 minutes:

```
EX(config)#applog archive interval 30
```

applog archive url

Specify the protocol and remote server for archiving application logs.

Syntax Description

```
[no] applog archive url url
```

Parameter	Description
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and

a password is required, you will still be prompted for the password. To enter the entire URL:

```
tftp://host/file
ftp://[user@]host[:port]/file
scp://[user@]host/file
rcp://[user@]host/file
```

Default None

Mode Configuration mode

Usage The archive files are named using the following convention:

```
applog_archive-year-mm-dd-hh-mm-ss.format.tar.gz
```

To use this naming convention, just press Enter when prompted to enter a filename.

Example The following command configures the EX device to use FTP to send application log archives to server 1.1.1.2:

```
EX(config)#applog archive url ftp:
Address or name of remote host []?1.1.1.2
User name []?exadmin
Password []?*********
File name [/]?<<Press Enter>>
```

applog bind

Bind a filter with applications to be logged.

Syntax Description

```
[no] applog bind filter-name
[alias alias-name] |
[aim] [msnim] [yim] [ftp] [nfs] [cifs] [smtp]
[pop3] [qq] [http]
```

Parameter	Description
filter-name	The filter name.
alias alias-name	Alias group of application types.
aim	AOL Instant Messenger
msnim	Microsoft Instant Messenger

yim	Yahoo Instant Messenger
ftp	File Transfer Protocol
nfs	Network file system
cifs	Common Internet File System
smtp	Simple Mail Transfer Protocol
pop3	Post Office Protocol v3
qq	Tencent Instant Messaging
http	Hypertext Transfer Protocol

Mode Configuration mode

Example The following command binds filter “testfilter” to AIM.

```
EX(config)#applog bind testfilter aim
```

applog enable

Globally enable or disable all application logging actions, without changing the application logging configuration.

Syntax Description

```
[no] applog enable [application [actions]]
```

Parameter	Description
aim [*actions*]	Enables or disables logging of AOL Instant Messenger (AIM) actions: **logon** – Logon action **logoff** – Logoff action
cifs [*actions*]	Enables or disables logging of Common Internet File System (CIFS) actions: **setup** – CIFS setup message **tconnect** – CIFS tconnect message **open** – CIFS open file action **read** – CIFS read file action **write** – CIFS write file action **create** – CIFS create new file action **mkdir** – CIFS make directory action **rmdir** – CIFS remove directory action **rename** – CIFS rename action

`delete` – CIFS delete file action

`logoff` – CIFS logoff action

`ftp` `[`*`actions`*`]` Enables or disables logging of File Transfer Protocol (FTP) actions:

`logon` – FTP logon message

`password` – FTP password message

`rmdir` – FTP remove directory action

`mkdir` – FTP make directory action

`retrieve` – FTP retrieve new file action

`store` – FTP store action

`rename` – FTP rename action

`execute` – FTP execute action

`delete` – FTP delete action

`http` `[`*`actions`*`]` Enables or disables logging of Hypertext Transfer Protocol (HTTP) actions:

`post` – HTTP POST action

`msnim` `[`*`actions`*`]` Enables or disables logging of Microsoft Instant Messenger (MSNIM) actions:

`logon` – Logon action

`logoff` – Logoff action

`nfs` `[`*`actions`*`]` Enables or disables logging of Network File System (NFS) actions:

`mount` – NFS mount action

`umount` – NFS unmount action

`read` – NFS read file action

`write` – NFS write file action

`rename` – NFS rename action

`lookup` – NFS lookup file handle action

`create` – NFS create new file action

`mkdir` – NFS make directory action

`rmdir` – NFS remove directory action

`remove` – NFS delete file action

`readdir` – NFS read directory action

pop3 [*actions*]	Enables or disables logging of Post Office Protocol v3 (POP3) actions: **mail** – POP3 mail action
qq [*actions*]	Enables or disables logging of Tencent Instant Messaging actions: **logon** – Logon action **logoff** – Logoff action
smtp [*actions*]	Enables or disables logging of Simple Mail Transfer Protocol (SMTP) actions: **mail** – SMTP mail action
yim [*actions*]	Enables or disables logging of Yahoo Instant Messenger (YIM) actions: **logon** – Logon action **logoff** – Logoff action

Default Logging of all applications and all application actions is enabled by default.

Mode Configuration mode

Example The following command disables logging of all CIFS application actions:

```
EX(config)#no applog enable cifs
```

Related Commands **applog filter, applog bind**

applog filter

Configure an application logging filter.

Syntax Description [**no**] **applog filter** *filter-name*

Parameter	Description
filter-name	The filter name, 1-31 characters.

This command changes the CLI to the configuration level for the specified application log filter, where the following filter-related commands are available:

Command	Description
`[no] include` *`ip-address {subnet-mask | /mask-length}`*	Specifies an IP address range to include in the application log filter.
`[no] exclude` *`ip-address {subnet-mask | /mask-length}`*	Specifies an IP address range to exclude from the application log filter.

Default

None

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing application log filter uniquely identified by *filter-name*, and enters the configuration level for the filter.

The **no** form of this command deletes the specified application log filter.

Example

The following command creates an application log filter named “testfilter”:

```
EX(config)#applog filter testfilter
EX(config-filter)#
```

Example

The following command sets 192.168.46.0 255.255.255.0 as an included IP range:

```
EX(config-filter)#include 192.168.46.0 /24
```

Example

The following command sets 192.168.46.0 255.255.255.0 as an included IP range:

```
EX(config-filter)#include 192.168.46.0 /24
```

Firewall Load Balancing Commands

fwlb enable

Set the placement of the EX Series Secure WAN Manager in an FWLB sandwich topology.

Syntax Description

```
[no] fwlb enable {inside | outside}
```

Parameter	Description
inside	The EX device is on the inside (private) side of the firewall nodes. The EX device load balances ***outbound*** connections through the FWLB nodes.
outside	The EX device is on the outside (public) side of the FWLB nodes. The EX device load balances ***inbound*** connections through the FWLB nodes.

Default

None

Mode

Configuration mode

Example

The following command sets the EX device's FWLB placement as outside:

```
EX(config)#fwlb enable outside
```

fwlb group

Create, edit, or delete an FWLB group.

Syntax Description

```
fwlb group name

no fwlb group [name [name ...]]
```

Parameter	Description
name	FWLB group name, 1-31 characters.

This command changes the CLI to the configuration level for the specified FWLB group, where the following group-related commands are available:

Command	Description
[no] bind default qos class	Binds the virtual "match-all" QoS class to FWLB group. If the default class is already bound to

another group, the class is unbound from the other group when you bind it to this group.

[no] bind node *name* [*name* ...]

Adds FWLB nodes to the FWLB group. There is no limit to number of nodes in an FWLB group. FWLB nodes must be configured before you can add them to a group.

[no] bind qos class *class* [*class* ...]

Binds a traffic class to the FWLB group. Traffic that matches a QoS class bound to the group will be load balanced among the nodes in the group. You can bind multiple classes to a group. A given QoS class can be bound to only one FWLB group.

If you bind a class that is already bound to another group, the class is unbound from the other group.

The QoS classes must be configured (using the **traffic class** command) before you can bind them to a group.

method {round-robin | weighted-round-robin | least | weighted-least}

Changes the FWLB group's load balancing method.

[no] persistent [age *seconds* **| by destination]**

Enables persistence of FWLB sessions. When you enable persistence, the EX device always sends traffic for a given connection to the same node. After the node is selected for the first packet in a connection, traffic for the same or similar connections (in terms of IP address) is sent to the same node.

age *seconds* – Specifies the number of seconds sessions remain persistent. You can specify 60-86400 seconds. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.

by destination – Changes persistence from source-IP-based persistence to destination-IP-based persistence.

Default

The EX device does not have any FWLB groups by default. When you create one, the group has the following default settings:

- **bind default qos class** – not bound
- **bind node** – none
- **bind qos class** – none
- **method** – round-robin
- **persistent** – disabled

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing FWLB load balancing group uniquely specified by *name*, and enters the configuration level for the group.

The **no** form of this command removes existing FWLB groups. If you do not specify a name, all FWLB load balancing groups are removed after user confirmation.

There is no **default** form of this command.

The total number of firewall load balancing groups, transparent cache switching groups, and service groups can be up to 256. No individual limit is put on each type of group.

The following command creates a new FWLB group:

```
EX(config)#fwlb group WebServiceFwGrp
EX(config-fwlb group: WebServiceFwGrp)#
```

Example

The following command adds FWLB nodes “SanJoseHQ” and “BeijingBranch” to FWLB load balancing group "fw-grp":

```
EX(config-fwlb group: WebServiceFwGrp)#bind node SanJoseHQ BeijingBranch
```

Example

The following command binds QoS class “http” with FWLB group “fw-grp”:

```
EX(config-fwlb group:WebServiceFwGrp)#bind qos class http
```

fwlb node

Create, edit, or delete an FWLB node.

Syntax Description

```
fwlb node name
[ip-address {subnet-mask | /mask-length}]

no fwlb node [name [name ...]]
```

Parameter	Description
name	Node name, 1-31 characters.
ip-address	IP address of the node.
subnet-mask | *lmask-length*	Network mask or mask length.

This command changes the CLI to the configuration level for the specified FWLB node, where the following node-related commands are available:

Command	Description
[**no**] **bind health monitor** *name*	Binds a health monitor to the FWLB node. Each FWLB node must have a health monitor. The monitor is used to check the node's status and to mark the status as "Running" or "Stopped", depending on the success or failure of the health check. Stopped nodes are not available for load balancing. A monitor must be configured (using the health monitor command) before you can bind it to a node.
[**no**] **connection limit** *limit*	Changes the FWLB node's connection limit. You can specify 0-1000000; 0 means no limit. The connection limit puts a hard limit on the number of concurrent connections supported by this node. No more connections will be sent through a node if its current number of connections is already equal to or greater than the configured limit. A node's current connection number can be greater than the configured limit in the following cases: – The node's connection limit is changed to a number smaller than its current number of connections. – New connections are coming from the node; that is, the EX Series Secure WAN Manager is passively counting connections, rather than actively sending them to the node.

`[no] disable`	Disables the FWLB node. Disabled nodes are not available for load balancing.
`[no] weight` *`weight`*	Changes the FWLB node's weight. The weight can be 1-255. The weight is used in weighted load balancing methods such as **weighted-round-robin** and **weighted-least-connection**. Higher weights are favored over lower weights**.**

Default

The EX device does not have any FWLB nodes by default. When you create one, the node has the following default settings:

- **bind health monitor** – ping
- **connection limit** – 0 (no limit)
- **disable** – FWLB nodes are enabled by default.
- **weight** – 1

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing FWLB node, and enters the configuration level for the node.

The IP address and network mask or mask length are required only when you create a new node. If you are editing an existing node, you only need to specify the name.

The **no** form of this command removes the specified FWLB node(s). If you do not specify a node name, all FWLB nodes are removed.

There is no **default** form of this command.

The total number of firewalls, caches, and servers can be up to 1024.

An FWLB node must be directly connected with the EX Series Secure WAN Manager (without intermediate routers).

The IP address can *not* be the same as any IP address already configured for an FWLB node.

The node's IP address and network mask define the neighbourhood of the FWLB node. FWLB traffic destined to this neighbourhood is not load balanced.

Example

The following command creates a new FWLB node called “SanJoseHQ” with IP address and mask length 10.0.0.2/32:

```
EX(config)#fwlb node SanJoseHQ 10.0.0.2 /32
EX(config-fwlb node:SanJoseHQ)#
```

Example

The following command changes the FWLB node’s connection limit to 10000:

```
EX(config-fwlb node:SanJoseHQ)#connection limit 10000
```

Example

The following command binds health monitor “http” to the FWLB node:

```
EX(config-fwlb node:SanJoseHQ)#bind health monitor http
```

fwlb peer

Specify the EX device on the other side of the FWLB nodes.

Syntax Description

fwlb peer *ip-address* {*subnet-mask* | */mask-length*}

Parameter	Description
ip-address	IP address of the other EX device.
subnet-mask | */mask-length*	Network mask or mask length.

Default

None

Mode

Configuration mode

Usage

The normal form of this command specifies the IP address and mask of the peer EX device in an FWLB sandwich topology.

The **no** form of this command clears the peer address and mask.

Load balancing features will ***not*** be applied to traffic destined for the other EX device itself.

Example

The following command specifies the peer IP address and mask:

```
EX(config)#fwlb peer 10.0.0.1 /24
```

IPS Commands

ips group

Create, edit, or delete Intrusion Prevention System (IPS) groups.

Syntax Description

ips group *group-name*

no ips group [*group-name*]

Parameter	Description
group-name	IPS group name, length 1-31.

Default

The EX device has a default IPs group named “default”. To display the settings in the default IPS group, use the **show default | sec ips** command. (See the example below.)

Mode

Configuration mode

Usage

An IPS group is a container for IPS filters, and can be applied to physical interface. Each interface can have only one IPS group.

The normal form of this command creates a new (or edits an existing) IPS group, and enters the configuration level for the group.

The **no** form of this command deletes an existing IPS filter group, or all IPS filter groups.

There is no **default** form of this command.

The EX device supports a maximum of 30 IPS groups.

Example

The following command displays the default IPS group:

```
EX#show default | sec ips
ips group default
 exceed rate source threshold 2000 interval 1000 hold 120 log
 icmp ping maxlength
 ip land log drop
 tcp checkflag log drop
 tcp flood threshold 2000 interval 100 hold 120 log
 tcp synflood threshold 30000 interval 1000 log
 tcp synfragment log drop
 udp flood threshold 2000 interval 100 hold 120 log
```

Example The following command creates an IPS filter group named “ips1”:

```
EX(config)#ips group ips1
EX(config-ips-group)#
```

The IPS commands you can enter at the configuration level for the IPS group are described in “IPS Group Commands” on page 181.

ips hold

Block (“hold”) packets coming from specific source IP addresses.

Syntax Description

```
[no] ips hold ip-address
{subnet-mask | /mask-length} [log]
```

Parameter	Description
ip-address	IP address.
subnet-mask | /mask-length	Network mask or mask length.
log	Enables logging.

Default No IPS hold is defined by default.

Mode Configuration mode

Usage The normal form of this command creates an IPS hold entry to block all traffic from the specified IP host or subnet.

The **no** form of this command removes the IPS hold from the specified IP addresses).

You can configure a maximum of 128 IPS hold entries.

Example The following command creates an IPS hold IP for the 192.168.3.x subnet:.

```
EX(config)#ips hold 192.168.3.0 255.255.255.0
```

ips log record enable

Enable logging of IPS events.

Syntax Description

```
[no] ips log record enable
```

Default Disabled

Mode Configuration mode

IPS Group Commands

The IPS configuration commands you can use at the configuration level for an IPS group are described in this section.

exceed rate destination

Configure an IPS filter to protect against distributed denial-of-service (DDoS) attacks. In a DDoS attack, malicious traffic can come from hundreds of hosts, known as “zombie agents”, that are surreptitiously under the control of an attacker.

Setting an exceed rate destination filter can ensure that the EX device allows only an acceptable number of concurrent connection requests.

Syntax Description

```
[no] exceed rate destination
[threshold threshold
  [interval milliseconds
    [hold seconds
      [log]]]]
```

Parameter	Description
`threshold`	Maximum number of connections allowed for the same destination IP address. You can specify 1-999999. The default is 2000.
`milliseconds`	Number of milliseconds during which no more than the specified threshold of connections are allowed for the same destination IP address. You can specify 1-65535 milliseconds. The default is 1000.
`seconds`	Number of seconds to withhold packets that try to establish new connections to a destination IP address that has reached its threshold. Connection attempts are dropped during the hold period. You can specify 0-65535 seconds. If you specify 0, packets are not withheld. The default is 120.
`log`	Enables logging.

Default None

Mode IPS configuration mode

Usage

The normal form of this command adds a DDoS destination filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example

The following command adds a DDoS destination filter to the current IPS group:

```
EX(config-ips-group)#exceed rate destination threshold 20 interval 1000 log
drop
```

exceed rate source

Configure an IPS filter to protect against excessive concurrent connections from the same source IP address. This type of filter can protect against attacks such as a Nimda virus attack.

Syntax Description

```
[no] exceed rate source
[threshold threshold
  [interval milliseconds
    [hold seconds
      [log]]]]
```

Parameter	Description
threshold	Maximum number of connections allowed for the same source IP address. You can specify 1-999999. The default is 2000.
milliseconds	Number of milliseconds during which no more than the specified threshold of connections are allowed for the same source IP address. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold packets that try to establish new connections from a source IP address that has reached its threshold. Connection attempts are dropped during the hold period. You can specify 0-65535 seconds. If you specify 0, packets are not withheld. The default is 120.
log	Enables logging.

Default

None

Mode

IPS configuration mode

Usage

The normal form of this command adds a DDoS source filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example

The following command adds a DDoS source filter to the current IPS group:

```
EX(config-ips-group)#exceed rate source threshold 20 interval 1000 log drop
```

icmp address sweep

Configure an IPS filter to protect against reconnaissance attempts using ICMP address sweeps.

An ICMP address sweep is a series of ICMP echo requests sent to a range of IP addresses. When a host replies to the request, this confirms the host's IP address to the hacker.

If the EX device receives more than 5 ICMP echo packets from the same source to different destinations, within the specified interval, the EX device drops further ICMP echo packets from that source for the period specified by the hold time.

Syntax Description

```
[no] icmp address sweep
[interval milliseconds [hold seconds [log]]]
```

Parameter	Description
milliseconds	Number of milliseconds during which no more than 5 ICMP echo packets are allowed from the same source to different destinations. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold ICMP echo packets from the same source, after the threshold is exceeded. ICMP echo packets from the same source are dropped during the hold period. You can specify 0-65535 seconds. If you specify 0, packets are not withheld. The default is 120.
log	Enables logging.

Default

None

Mode

IPS configuration mode

Usage

The normal form of this command adds an ICMP address sweep filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example

The following command adds an ICMP address sweep filter to the current IPS group:

```
EX(config-ips-group)#icmp address sweep interval 1000 hold 130 log
```

icmp broadcast

Configure an ICMP broadcast filter to protect against ICMP broadcast packets, which are used by attackers for reconnaissance of target networks and hosts.

Syntax Description

```
[no] icmp broadcast [echo request]
{drop | log | drop log}
```

Parameter	Description
`echo request`	Protects against ICMP echo requests sent to a subnet broadcast address. Echo replies from hosts in the network can be used by an attacker to gather information about the network.
`drop`	Drops ICMP broadcast packets.
`log`	Enables logging.

Default

None

Mode

IPS configuration mode

Usage

The normal form of this command adds an ICMP broadcast filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example

The following command adds an ICMP broadcast filter to the current IPS group:

```
EX(config-ips-group)#icmp broadcast log drop
```

icmp flood

Configure an IPS filter to protect against ICMP floods.

Syntax Description

```
[no] icmp flood
[threshold threshold
  [interval millisecond
    [hold seconds [log]]]]
```

Parameter	Description
threshold	Maximum number of ICMP packets to the same destination IP address that are allowed within the specified interval. You can specify 1-999999 packets. The default is 2000.
milliseconds	Number of milliseconds during which the number of ICMP packets specified by the threshold are allowed for the same destination IP address. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold ICMP packets addressed to the destination, after the threshold is exceeded. ICMP packets addressed to the destination are dropped during the hold period. You can specify 0-65535 seconds. If you specify 0, packets are not withheld. The default is 120.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an ICMP flood filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds an ICMP flood filter to the current IPS group:

```
EX(config-ips-group)#icmp flood threshold 100 interval 1000 hold 120 log drop
```

icmp ping maxlength

Configure an ICMP ping filter to drop ICMP ping packets longer than the specified maximum number of bytes.

Excessively long ICMP ping packets can cause DoS, with symptoms such as halting or restarting on the target host.

Generally, this type of attack occurs in conjunction with fragmented packets, where the attacker sends the last fragment with an offset such that the ping packets are longer than 65535 bytes (the default byte length allowed by the filter), causing 16-bit variables to overflow.

Syntax Description

```
[no] icmp ping maxlength [bytes [log]]
```

Parameter	Description
bytes	Maximum length allowed for ICMP ping packets, 512-1472 bytes. The default is 1472.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an ICMP ping filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds an ICMP ping filter to the current IPS group:

```
EX(config-ips-group)#icmp ping maxlength 1200 log drop
```

icmp type

Configure an ICMP type filter to specify the valid ranges of ICMP type and code values. This type of filter protects against attacks using combinations of ICMP type and code (subtype) that can be used to gain information about a host or network.

For example, an ICMP timestamp message (type 13) elicits a timestamp reply from Unix systems, but not from Microsoft systems, therefore indicating to the attacker the types of systems in the network.

If the type or the code in the packet is larger than the configured Type/Code, the packet will be dropped.

Those packets for which type and code are both smaller than the configured Type/Code, are allowed to pass.

Syntax Description

```
icmp type [type-num code subtype-num [drop] [log]]

no icmp type
```

Parameter	Description
type-num	ICMP packet type, 0-40.
subtype-num	ICMP packet code, 0-15.

drop	Drops packets in which the type or code is larger than the specified type and code.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an ICMP type filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds an ICMP type filter to the current IPS group:

```
EX(config-ips-group)#icmp type 3 code 11 log drop
```

ip

Configure IPS filters to drop suspicious IP packets.

Syntax Description

```
[no] ip
{
fragment |
land |
loose source route option |
malformed option |
max known protocol protocol-num |
option |
record route option |
security option |
stream option |
strict source route option |
timestamp option |
}
drop [log]
```

Parameter	Description
fragment	Protects against fragmented packets. Fragmented packets can be used to attack hosts running IP stacks that have known vulnerabilities in their fragment reassembly code.
land	Protects against spoofed SYN packets containing the same IP address as the source and destination. Flooding a system with such empty connec-

tions can overwhelm the system, causing Denial of Service (DoS).

loose source route option
Protects against packets that specify an IP address that must be used as one of the hops to reach the destination. Attackers can use information in messages sent by routers to learn about the address scheme and topology of a target network.

malformed option
Protects against packets with incomplete or malformed options in the header. This type of packet is always invalid and should not be forwarded.

max known protocol *protocol-num*
Logs all packets whose protocol numbers are higher than the specified maximum protocol number.

option
Protects against all packets containing any IP option.

record route option
Protects against packets that record the route used to forward them. Attackers can use route information to learn about the address scheme and topology of a target network.

security option
Protects against packets containing the IP security option, which is obsolete. Because the option is no longer used, packets containing the option are most likely from malicious sources.

stream option
Protects against packets that use the stream option. This option is obsolete, therefore its presence can indicate a malicious source.

strict source route option
Protects against packets that specify each hop to use for forwarding to the destination. Attackers can use information in messages sent by routers to learn about the address scheme and topology of a target network.

timestamp option
Protects against packets that use the timestamp option. This option is rarely used, therefore its presence can indicate a malicious source.

drop	Drops traffic that matches the specified filter type. (The filter type is specified by using one of the options above.)
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an IPS filter.

The **no** form of this command removes the filter.

Example The following command adds an IP land filter to the current IPS group:

```
EX(config-ips-group)#ip land log drop
```

port scan

Configure an IPS filter to protect against reconnaissance attempts using protocol port scans. During a port scan, an attacker sends a series of packets with the same source and destination IP addresses, but to different TCP or UDP ports.

Syntax Description

```
[no] port scan
[interval milliseconds
  [hold seconds
    [log]]]]
```

Parameter	Description
milliseconds	Number of milliseconds during which no more than 6-1 TCP or UDP ports can be addressed in packets from the same source and addressed to the same destination IP address. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold further TCP or UDP packets with the same pair of source and destination IP addresses, after the threshold is exceeded. TCP or UDP packets with the same IP address pair are dropped during the hold period. You can specify 0-65535 seconds. If you specify 0, packets are not withheld. The default is 120.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds a port scan filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds a port scan filter to the current IPS group:

```
EX(config-ips-group)#port scan interval 1000 log
```

tcp checkflag

Configure a TCP checkflags filter to protects against TCP packets with the following flag settings, which typically are used by attackers for reconnaissance:

- No flags set
- FIN flag only
- SYN and FIN flags
- FIN with no ACK
- FIN, SYN, and ACK

Syntax Description

```
tcp checkflag
{drop | clearsession | reset | resetclient |
resetserver}
[log]

no tcp checkflag
```

Parameter	Description
drop	Drops the TCP packet.
clearsession	Drops the TCP packet and removes the session from the EX session table, but does not send a reset to either the client or the server.
reset	Drops the TCP packet, sends a reset to both the client and the server, and removes the session from the EX session table.
resetclient	Drops the TCP packet, sends a reset to the client, and removes the session from the EX session table.
resetserver	Drops the TCP packet, sends a reset to the server, and removes the session from the EX session table.

log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds a TCP SYN fragment filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following commands adds a TCP checkflag filter to the current IPS group:

```
EX(config-ips-group)#tcp checkflag log drop
```

tcp flood

Configure an IPS filter to protect against TCP floods.

Syntax Description

```
[no] tcp flood
[threshold threshold
  [interval milliseconds
    [hold seconds
      [log]]]]
```

Parameter	Description
threshold	Maximum number of TCP packets to the same destination IP address that are allowed within the specified interval. You can specify 1-999999 packets. The default is 2000.
milliseconds	Number of milliseconds during which the number of TCP packets specified by the threshold are allowed for the same destination IP address. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold TCP packets addressed to the destination, after the threshold is exceeded. TCP packets addressed to the destination are dropped during the hold period. You can specify 0-65535 seconds. The default is 0, which means packets are not withheld.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an TCP flood filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds a TCP flood filter to the current IPS group:

```
EX(config-ips-group)#tcp flood threshold 100 interval 1000 hold 120 log drop
```

tcp synflood

Configure transaction rate limiting to protect against TCP SYN floods.

An attacker can cause a TCP SYN flood by sending TCP SYN (connection) requests to a host faster than the host can acknowledge them, causing DoS on the host. Generally, the source IP address of the TCP SYN packets is spoofed.

Syntax Description

```
tcp synflood
[threshold threshold interval milliseconds [log]]
```

Syntax Description

```
no tcp synflood
```

Parameter	Description
threshold	Maximum number of TCP SYN packets to the same destination IP address that are allowed within the specified interval. You can specify 1-999999 packets. The default is 2000. If this number or more TCP SYN packets are received for the same destination within the interval, the EX device creates a SYN cookie.
milliseconds	Number of milliseconds during which that number of TCP SYN packets specified by one less than the threshold value are allowed for the same destination IP address. You can specify 1-65535 milliseconds. The default is 1000.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an TCP SYN flood filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example

The following command adds a TCP SYN flood filter to the current IPS group:

```
EX(config-ips-group)#tcp synflood threshold 100 interval 1000 log
```

tcp synfragment

Configure an IPS filter to respond to TCP SYN fragments.

During a TCP SYN fragment attack, the targeted host stores the TCP SYN fragments in order to reassemble them and presumably complete the connections. Eventually, the SYN fragments for uncompleted connections fill the host’s memory buffer, causing the host to stop working properly.

Syntax Description

```
[no] tcp synfragment
{drop | clearsession | reset | resetclient |
resetserver}
[log]
```

Parameter	Description
`drop`	Drops the TCP SYN packet.
`clearsession`	Drops the TCP SYN packet and removes the session from the EX session table, but does not send a reset to either the client or the server.
`reset`	Drops the TCP SYN packet, sends a reset to both the client and the server, and removes the session from the EX session table.
`resetclient`	Drops the TCP SYN packet, sends a reset to the client, and removes the session from the EX session table.
`resetserver`	Drops the TCP SYN packet, sends a reset to the server, and removes the session from the EX session table.
`log`	Enables logging.

Default

None

Mode

IPS configuration mode

Usage

The normal form of this command adds a TCP SYN fragment filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example

The following commands adds a TCP SYN fragment filter to the current IPS group:

```
EX(config-ips-group)#tcp synfragment log drop
```

udp address sweep

Configure an IPS filter to protect against reconnaissance attempts using USP address sweeps.

A UDP sweep is a series of UDP packets from the same source but to different IP addresses, within the specified interval. Because this traffic pattern is unusual, it is considered to be a signature of reconnaissance for an attack.

If the EX device receives more than 5 UDP packets from the same source to different destinations, within the specified interval, the EX device drops further UDP packets from that source for the period specified by the hold time.

Syntax Description

```
[no] udp address sweep
[interval milliseconds [hold seconds [log]]]
```

Parameter	Description
milliseconds	Number of milliseconds during which no more than 5 UDP packets are allowed from the same source to different destinations. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold UDP packets from the same source, after the threshold is exceeded. UDP packets from the same source are dropped during the hold period. Number of seconds to withhold further TCP or UDP packets with the same pair of source and destination IP addresses, after the threshold is exceeded. TCP or UDP packets with the same IP address pair are dropped during the hold period. You can specify 0-65535 seconds. If you specify 0, packets are not withheld. The default is 120.
log	Enables logging.

Default

None

Mode

IPS configuration mode

Usage

The normal form of this command adds a UDP address sweep filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds a UDP address sweep filter to the current IPS group:

```
EX(config-ips-group)#udp address sweep interval 1000 log
```

udp broadcast echo request

Configure an IPS filter to protect against UDP echo requests sent to a subnet broadcast address. Echo replies from hosts in the network can be used by an attacker to gather information about the network.

Syntax Description

```
[no] udp broadcast echo request
{drop | log | drop log}
```

Parameter	Description
drop	Drops the UDP echo request packet.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds a UDP broadcast echo request filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds a UDP broadcast echo request filter to the current IPS group:

```
EX(config-ips-group)#udp broadcast echo request log drop
```

udp flood

Configure an IPS filter to protect against UDP floods.

Syntax Description

```
[no] udp flood
[threshold threshold
  [interval milliseconds
    [hold seconds
      [log]]]]
```

Parameter	Description
threshold	Maximum number of UDP packets to the same destination IP address that are allowed within the specified interval. You can specify 1-999999 packets. The default is 2000.
milliseconds	Number of milliseconds during which the number of UDP packets specified by the threshold are allowed for the same destination IP address. You can specify 1-65535 milliseconds. The default is 1000.
seconds	Number of seconds to withhold UDP packets addressed to the destination, after the threshold is exceeded. UDP packets addressed to the destination are dropped during the hold period. You can specify 0-65535 seconds. The default is 0, which means packets are not withheld.
log	Enables logging.

Default None

Mode IPS configuration mode

Usage The normal form of this command adds an UDP flood filter to the current IPS group.

The **no** form of this command removes the filter from the IPS group.

Example The following command adds a UDP flood filter to the current IPS group:

```
EX(config-ips-group)#udp flood threshold 100 interval 1000 hold 120 log drop
```

Server Load Balancing Commands

slb group

Create, edit, or delete an SLB group.

Syntax Description

```
slb group {tcp | udp | any} group

no slb group
[{tcp | udp | any} [group [group ...]]]
```

Parameter	Description
tcp	TCP-port-based SLB group.
udp	UDP-port-based SLB group.
any	Node-based SLB group.
group	SLB group name, 1-31 characters.

This command changes the CLI to the configuration level for the specified SLB group, where the following group-related commands are available:

Command	Description
[**no**] **bind port** *node-name* *port-num* [*port-num* ...]	Binds an SLB node to the SLB group. *node-name* – Server node name. *port-num* – Protocol port number.

Note: This command is available only for SLB groups with transport protocol type “tcp” or “udp”.

[**no**] **method** {**round-robin** | **weighted-round-robin** | **least** | **weighted-least**}	Changes the SLB group’s load balancing method.
[**no**] **persistent** [**age** *seconds*]	Enables persistence of SLB sessions. When you enable persistence, the EX device always sends traffic from a given IP address to the same node. After the node is selected for the first packet in a connection, traffic for the same or similar con-

nections (in terms of IP address) is sent to the same node.

age *seconds* – Specifies the number of seconds sessions remain persistent. You can specify 60-86400 seconds. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.

Default

The EX device does not have any SLB groups by default. When you create an SLB group, it has the following default settings:

- **bind port** – none
- **method** – round-robin
- **persistent** – disabled

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing SLB group uniquely specified by transport protocol (**tcp**, **udp**, or **any**) and *name*, and enters the configuration level for the group.

The **no** form of this command removes the specified SLB group. If you do not specify a group name, all SLB groups are removed after user confirmation.

There is no **default** form of this command.

An EX device can have up to 256 groups, including FWLB groups, CLB groups, and SLB groups. No individual limit (above 256) is put on each type of group.

Example

The following command creates a new SLB group called “WebServerGrp” that can have ports on any transport protocol type:

```
EX(config)#slb group any WebServerGrp
EX(config-slb group any:WebServerGrp)#
```

Example

The following command adds an SLB node to the current SLB group:

```
EX(config-slb group any:WebServerGrp)#bind node apache
```

slb node

Create, edit, or delete an SLB real server.

Syntax Description

```
slb node name
[ip-address {subnet-mask | /mask-length}]

no slb node [name [name ...]]
```

Parameter	Description
name	Server node name, 1-31 characters.
ip-address	IP address of the server. Specify the real IP address, not the virtual IP address.
subnet-mask | */mask-length*	Network mask or mask length.

This command changes the CLI to the configuration level for the specified SLB node, where the following node-related commands are available:

Command	Description
[**no**] **bind health monitor** *name*	Binds a health monitor to the node. Each SLB node must have a health monitor. The monitor is used to check the node's status and to mark the status as "Running" or "Stopped", depending on the success or failure of the health check. Stopped nodes are not available for load balancing. A monitor must be configured (using the health monitor command) before you can bind it to a node.
[**no**] **connection limit** *limit*	Change the maximum number of concurrent connections allowed on the SLB node. You can specify 0-1000000; 0 means no limit. The connection limit puts a hard limit on the number of concurrent connections supported by this node. No more connections will be sent to the node if the number of current connections is already equal to or larger than the configured limit.

A node’s number of current connections can be larger than the configured limit in the following cases:

– The node’s connection limit is changed to a number lower than the number of current connections.

– New connections are coming from the node; that is, the EX Series Secure WAN Manager is passively counting connections, rather than actively sending new connections to the node.

[**no**] **disable**

Disables the node. Disabled nodes are not available for load balancing.

[**no**] **port** {**tcp** | **udp**} *portnum*

Adds a TCP or UDP protocol port. The port number can be 1-65535. There can be up to 2048 ports, but no individual limit is set for the number of ports per node.

This command changes the CLI to configuration level for the port, where the following port-related commands are available:

[**no**] **connection limit** *limit* – Changes the SLB port’s connection limit. You can specify 0-1000000; 0 means no limit. This setting overrides the connection limit set for the SLB node. For more information about connection limiting, see the description above.

[**no**] **disable** – Disables the port. Disabled ports are not available for load balancing.

[**no**] **weight** *weight* – Changes the SLB port’s weight. A port’s weight is used in weighted load balancing methods such as weighted-round-robin and weighted-least-connection. Higher weights are favored over lower weights**.**

[**no**] **weight** *weight*

Changes the SLB node’s weight. A node’s weight is used in weighted load balancing methods such as weighted-round-robin and weighted-least-connection. Higher weights are favored over lower weights**.**

Default

The EX device does not have any SLB nodes by default. When you create an SLB node, it has the following default settings:

- **bind health monitor** – ping
- **connection limit** – 0 (no limit)
- **disable** – SLB nodes are enabled by default.
- **port** – None. When you add a port, the port has the following default settings:
  - **connection limit** – 0 (no limit). However, if a connection limit is set on the SLB node, the node’s connection limit becomes the default limit for the port.
  - **disable** – SLB ports are enabled by default.
  - **weight** – 1
- **weight** – 1

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing SLB node (real server), and enters the configuration level for the server. The IP address and mask are required for new servers. If you are editing an existing node, only the name is required. If you enter a different IP address or mask, the new value replaces the older value.

The **no** form of this command removes the specified SLB nodes. If you do not specify a node name, all SLB nodes are removed after user confirmation.

There is no **default** form of this command.

The EX device can have up to 1024 nodes, including FWLB, CLB, and SLB. There is no limit (up to 1024) on how many nodes of each type the device can have.

The IP address of the node must be unique.

Example

The following command creates a new SLB node called “apache” with IP address 10.0.0.2/24:

```
EX(config)#slb node apache 10.0.0.2 /24
EX(config-slb node:apache)#
```

Example

The following command binds health monitor “http” to the current SLB node:

```
EX(config-slb node:apache)#bind health monitor http
```

Example The following command changes the current SLB node’s connection limit to 1000:

```
EX(config-slb node:apache)#connection limit 1000
```

Example The following command creates a new port on the current node:

```
EX(config-slb node:apache)#port tcp 80
EX(config-slb node:apache-rport:TCP 80)#
```

Related Commands **health monitor**

slb virtual server

Create, edit, or remove an SLB virtual server.

Syntax Description

```
[no] slb virtual server name
[ip-address {subnet-mask | /mask-length}]
```

Parameter	Description
name	Virtual server node name, 1-31 characters.
ip-address	Virtual IP address of the virtual server. This is the IP address to which clients will send requests.
subnet-mask | /mask-length	Network mask or mask length.

This command changes the CLI to the configuration level for the specified SLB virtual server, where the following virtual-server related commands are available:

Command	Description
[no] nat ippool *ippool-name*	Binds an IP address pool to the virtual server to use for Network Address Translation (NAT). The IP address pool must be configured before you can bind to the virtual server. If an IP pool is assigned to the virtual server (using the **nat ippool** command), the NAT addresses come from the pool. If an IP pool is not assigned to the virtual server, the VIP address will be used as the source address.

[**no**] **permit ping** [**if-real-server-available**]

Allows the EX device to reply to pings for the VIP address. The **if-real-server-available** option replies only if at least one real server is up. Without this option, the EX device replies to pings for the VIP even if all real servers are down.

[**no**] **port** {**tcp** *portnum* | **udp** *portnum* | *protocol-name* | *protocol-number*} *group-name*

Adds virtual ports to the virtual server.

There can be up to 1024 virtual ports configured in the EX Series Secure WAN Manager. There is no limit (up to 1024) on how many virtual ports can be on one virtual server.

If you enter **tcp** or **udp**, you must also enter a port number. If you specify port number 0, traffic that matches the virtual IP address and protocol matches on any port number.

For other protocols, you can specify the protocol name or number, 0-138. To add all protocols, enter **all**.

For a list of supported protocols, enter the following command: **port ?**

group-name – SLB group name.

This command changes the CLI to configuration level for the port, where the following port-related commands are available:

[**no**] **nat ippool** *ippool-name* – Binds an IP address pool to the port. This setting overrides the NAT setting on the virtual server.

[**no**] **port** – Adds another port to the virtual server.

[**no**] **snat** – Enables source NAT on the virtual server. This setting overrides the NAT setting on the virtual server.

`[no] snat`	Enables source NAT on the virtual server. If an IP pool is assigned to the virtual server (using the **nat ippool** command), the NAT addresses come from the pool. If an IP pool is not assigned to the virtual server, the VIP address will be used as the source address.

Default

The EX device does not have any SLB virtual servers by default. When you create an SLB virtual server, it has the following default settings:

- **nat** – Source NAT is disabled on virtual servers by default.
- **permit** – Replies to pings sent to the VIP are disabled by default.
- **port** – None. When you add a port, the port has the following default settings:
    - **nat** – NAT setting on the virtual server
    - **snat** – SNAT setting on the virtual server
- **snat** – Source NAT is disabled on virtual servers by default.

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing virtual server, and changes to the configuration level for the virtual server. The IP address and mask are required when you create the virtual server. They are not required if you are editing an existing server. If you do specify the address and mask when editing a server, the new address and mask replace the previous ones.

The **no** form of this command removes the specified virtual server. If you do not specify a virtual server name, all virtual servers are removed after user confirmation.

There is no **default** form of this command.

There can be up to 256 virtual servers.

Example

The following command creates a new virtual server named “VirtualServer” with IP address and mask 10.0.0.254/24:

```
EX(config)#slb virtual server VirtualServer 10.0.0.254 /24
EX(config-slb virtual server:VirtualSer...)#
```

Example

The following command binds IP address pool “pool1” to the current virtual server:

```
EX(config-slb virtual server:VirtualSer...)#nat ippool pool1
```

Example

The following command creates a new virtual port on the current virtual server:

```
EX(config-slb virtual server:VirtualSer...)#port tcp 80 WebServerGrp
```

Health Monitor Commands

health external

Use an external program for health monitoring.

Syntax Description

```
health external
{delete program-name |
import [description] url |
export program-name url}
```

Parameter	Description
program-name	Program file name, 1-31 characters.
description	Description of the program file, 1-63 characters.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: **tftp://***host***/***program-name* **ftp://**[*user*@]*host*[:*port*]**/***program-name* **scp://**[*user*@]*host***/***program-name* **rcp://**[*user*@]*host***/***program-name*

Default N/A

Mode Configuration mode

Usage To manage the external program, use the **health external** command.

Example The following example imports external program “mail.tcl” from FTP server 192.168.0.1:

```
EX(config)#health external import "checking mail server"
ftp://192.168.0.1/mail.tcl
```

Related Commands show health external

health method

Configure a health method.

Syntax Description

```
health method method-name method-options
```

Parameter	Description
method *method-name*	Method name, 1-31 characters.
icmp [**transparent** *ipaddr*]	Sends an ICMP echo request to the server. Expects ICMP echo reply message. The **transparent** *ipaddr* option checks the health of a multilink path. The *ipaddr* specifies the IP address of the device at the other end of the path. For example, for FWLB, the *ipaddr* is EX on the other side of the firewall. In an HA FWLB configuration, the *ipaddr* is the floating IP address of the HA group on the other side of the firewall. For LLB, the *ipaddr* is the device at the other end of a load-balanced link.
tcp **port** *port-num* [**halfopen**]	Sends a connection request (TCP SYN) to the specified TCP port on the server. Expects TCP SYN ACK in reply. By default, the EX responds to the SYN ACK by sending an ACK. To configure the EX device to send a RST (Reset) instead, use the **halfopen** option.
udp **port** *port-num*	Sends a packet with a valid UDP header and a garbage payload to the specified UDP port on the server. Expects either of the following: – server reply from the specified UDP port, with any type of packet. – server does not reply at all. The server fails the health check only if the server replies with an ICMP Error message.

http [**port** *port-num*] [**url** *string*] [**username** *name*] [**expect** {*string* | **response-code** *code-list*}]	Sends an HTTP GET or HEAD request to the specified TCP port and URL. Expects OK message (200). The **url** option specifies the page to which to send the request. Unless anonymous login is used, the **username** must be specified. The **expect** option specifies a response code or string expected from the server, in which case this value is also expected. To specify a range of response codes, use a dash (-) between the low and high numbers of the range. Use commas to delimit individual code numbers or separate ranges.
ftp [[**username** *name* **password** *string*] **port** *port-num*]	Sends an FTP login request to the specified port. Expects OK message, or Password message followed by OK message. Unless you use anonymous login, the username and password must be specified in the health check configuration.
snmp [**community** *string*] [**oid** *oid-name*] [**operation** {**get** | **getnext**}] [**port** *port-num*]	Sends an SNMP Get or Get Next request to the specified OID, from the specified community. Expects reply with the value of the OID. The OID can be **sysDescr**, **sysUpTime**, **sysName**, or another name in ASN.1 style.
smtp **domain** *domain-name* **port** *port-num*	Sends an SMTP Hello message to the specified server in the specified domain. Expects reply with OK message (reply code 250).

dns
domain *domain-name*
port *port-num*

Sends a lookup request to the specified port number for the specified domain name. Expects reply with code 0.

pop3
port *port-num*
username *name*
password *string*

Sends a POP3 user login request with the specified username and password. Expects reply with OK message.

radius
port *port-num*
secret *string*
username *name*
password *string*

Sends a Password Authentication Protocol (PAP) request to the specified port to authenticate the specified username. Expects Access Accepted message (reply code 2). The **secret** option specifies the shared secret required by the RADIUS server.

ldap
[**binddn** *name*
password
string]
[**overssl**]
[**port** *port-num*]

Sends an LDAP Bind request. Expects reply containing result code 0. The **binddn** option species the Distinguished Name and the **password** option specifies the password for the Distinguished Name. The **overssl** option uses SSL (TLS) for the health check.

rtsp
port *port-num*
rtspurl *string*

Sends a request to the specified port for information about the file specified by **rtspurl**. Expects reply with information about the specified file.

sip
[**port** *port-num*]]

Sends a SIP request to the SIP port. Expects 200 OK in response. The request is an OPTION request.

external port *port-num* **program** *program-name* [**arguments** *argument-string*]	Runs an external program (for example, a Tcl script) and bases the health status on the outcome of the program.
https [**port** *port-num*] [**expect** {*string* | **response-code** *code-list*}] [**url** *string*] [**username** *name* **password** *string*]	Similar to an HTTP health check, except SSL is used to secure the connection.

Default

When configuring a health method, some of the values have defaults, as described above.

Mode

Configuration mode

Example

The following example configures a health monitor named “PING1” that uses the ping method. The command checks the health of a multilink path by sending an ICMP echo request to the IP address (10.0.0.1) of the device, located at the other end of the path.

```
EX(config)#health method PING1 icmp transparent 10.10.10.1
```

Related Commands **health monitor**

health monitor

Configure a health monitor.

Syntax Description

```
[no] health monitor monitor-name
```

Parameter	Description
monitor-name	Health monitor name, 1-31 characters.

This command changes the CLI to the configuration level for the specified health monitor, where the following health-monitor configuration commands are available:

Command	Description
interval *seconds*	Number of seconds between each use of the health monitor, 15-180 seconds.
method *method-name*	Name of a configured health method, 1-31 characters. (To configure a health method, use the **health method** command.)
min-active-cnt *number*	Minimum threshold of successful methods. You can specify 0-10, with 0 denoting that all must be successful.
retry *number*	Maximum number of times the same health check will be sent to an unresponsive server before determining that the server is down. You can specify 1-4.
timeout *seconds*	Number of seconds the EX waits for a reply to a health check, 1-12 seconds.

Default

When you add a health monitor, it has the following default settings:

- **interval** – 30
- **method** – not set
- **min-active-cnt** – 0 (all)
- **retry** – 3
- **timeout** – 5

By default, the EX device has one configured Layer 3 health method, “ping”.

Mode

Configuration mode

Usage

To bind a health monitor to a node, use the following command at the configuration level for the node: **bind health monitor** *monitor-name*

Example

The following example configures the health monitor named “myping” that uses the ping method. The commands also change the interval from 30 seconds to 20 seconds.

```
EX(config)#health monitor myping
EX(config-health-monitor)#method ping
EX(config-health-monitor)#interval 20
```

Related Commands

health method, bind health monitor

Transparent Cache Switching Commands

clb group

Create, edit, or delete a CLB group.

Syntax Description

```
[no] clb group name
```

Parameter	Description
name	CLB group name, 1-31 characters.

This command changes the CLI to the configuration level for the specified CLB group, where the following group-related commands are available:

Command	Description
`[no] bind node node-name [node-name ...]`	Binds CLB nodes to the CLB group. CLB nodes must be configured before you can bind them to a group. CLB nodes must be configured before you can bind them to a group.
`[no] bind qos class class [class ...]`	Binds QoS classes to the CLB group. Traffic that matches a QoS class bound to the group will be load balanced among the nodes in the group. You can bind multiple classes to a group. A given QoS class can be bound to only one CLB group. If you bind a class that is already bound to another group, the class is unbound from the other group. The QoS classes must be configured (using the **traffic class** command) before you can bind them to a group.
`[no] method {round-robin | weighted-round-robin | least | weighted-least}`	Changes the load balancing method for the CLB group.

`[no] persistent [age seconds]`

Enables persistence of CLB sessions. When you enable persistence, the EX device always sends traffic from a given IP address to the same node. After the node is selected for the first packet in a connection, traffic for the same or similar connections (in terms of IP address) is sent to the same node.

age *seconds* – Specifies the number of seconds sessions remain persistent. You can specify 60-86400 seconds. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.

Default

The EX device does not have any CLB groups by default. When you create a CLB group, it has the following default settings:

- **bind node** – none
- **bind qos class** – none
- **method** – round robin
- **persistent** – disabled

Default

None

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing CLB group uniquely specified by “*name*”, and enters the configuration level for the group.

The **no** form of this command removes the specified CLB group. If you do not specify a group name, all CLB groups are removed after user confirmation.

There is no **default** form of this command.

An EX device can have up to 256 groups, including FWLB groups, CLB groups, and SLB groups. No individual limit (above 256) is put on each type of group.

Example

The following command creates a new CLB group called “SquidCacheGrp”:

```
EX(config)#clb group SquidCacheGrp
EX(config-clb group:SquidCacheGrp)#
```

Example

The following command binds CLB node “SquidCache” to the current CLB group:

```
EX(config-clb group:SquidCacheGrp)#bind node SquidCache
```

Example

The following command binds QoS class “http” with the current CLB group:

```
EX(config-clb group:SquidCacheGrp)#bind qos class http
```

clb node

Create, edit, or delete a Cache Load Balancing (CLB) node.

Syntax Description

```
clb node name
[ip-address {subnet-mask | /mask-length}]

no clb node [name [name ...]]
```

Parameter	Description
name	CLB node name, 1-31 characters.
ip-address	IP address of the CLB node.
subnet-mask | /mask-length	Network mask or mask length.

This command changes the CLI to the configuration level for the specified CLB node, where the following node-related commands are available:

Command	Description
[no] **bind health monitor** *name*	Binds a health monitor to the CLB node. Each CLB node must have a health monitor. The monitor is used to check the node’s status and to mark the status as “Running” or “Stopped”, depending on the success or failure of the health check. Stopped nodes are not available for load balancing. A monitor must be configured (using the **health monitor** command) before you can bind it to a node.
[no] **connection limit** *limit*	Changes the CLB node’s connection limit. You can specify 0-1000000; 0 mean no limit. The connection limit puts a hard limit on the number of concurrent connections supported by

this node. No more connections sent to a node if the number of current connections is already equal to or greater than the configured limit.

A node's number of current connections can be greater than the configured limit in the following cases:

– The node's connection limit is changed to a number lower than the current number connections on the node.

– New connections are coming from the node; that is, the EX Series Secure WAN Manager is passively counting connections, rather than actively sending them to the node.

`[no] disable` Disables the CLB node. Disabled nodes are not available for load balancing.

`[no] weight` *`weight`* Changes the weight of the CLB node. You can specify 1-255. The weight is used in weighted balancing methods such as weighted-round-robin and weighted-least-connection. Higher weights are favored over lower weights**.**

Default

The EX device does not have any CLB nodes by default. When you create a CLB node, it has the following default settings:

- **bind health monitor** – ping
- **connection limit** – 0 (no limit)
- **disable** – CLB nodes are enabled by default.
- **weight** – 1

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing CLB node, and enters the configuration level for the node.

The IP address and mask are required when you create a node. They are not required when you are editing one.

The **no** form of this command removes the specified CLB nodes. If you do not specify a node name, all CLB nodes are removed.

There is no **default** form of this command.

There can be up to 1024 nodes on an EX device, including firewall, cache, and server nodes. There is no limit (above 1024) on the number of nodes of each type.

CLB nodes must be directly connected to the EX device (without intermediate routers).

The IP address can not be the same as any IP address already configured for a CLB node.

Example

The following command creates a new CLB node called “SquidCache” with IP address 10.0.0.2:

```
EX(config)#clb node SquidCache 10.0.0.2 /24
EX(config-clb node:SquidCache)
```

Example

The following command binds health monitor “http” to the current CLB node:

```
EX(config-clb node:SquidCache)#bind health monitor http
```

Example

The following command changes the connection limit of the current CLB node to 1000:

```
EX(config-clb node:SquidCache)#connection limit 1000
```

Related Commands `health monitor, show clb node, clear clb node`

aFleX Commands

aflex check

Check the syntax of an aFleX script.

Syntax Description **`aflex check`** *`aflex-name`*

Mode Configuration mode

aflex copy

Save a local copy of an aFlex script.

Syntax Description **`aflex cop`** *`aflex-name new-aflex-name`*

Mode Configuration mode

aflex delete

Delete an aFleX script.

Syntax Description **`aflex delete`** *`aflex-name`*

Mode Configuration mode

aflex export

Export an aFleX script from the EX device to a remote device.

Syntax Description **`aflex export`** *`aflex-name url`*

Parameter	Description
aflex-name	Filename of the aFleX script.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL:

```
tftp://host/file
ftp://[user@]host[:port]/file
scp://[user@]host/file
rcp://[user@]host/file
```

Mode Configuration mode

aflex import

Import an aFleX script onto the EX device.

Syntax Description **aflex import** *aflex-name url*

Parameter	Description
aflex-name	Filename of the aFleX script.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: **tftp:**//*host*/*file* **ftp:**//[*user*@]*host*[:*port*]/*file* **scp:**//[*user*@]*host*/*file* **rcp:**//[*user*@]*host*/*file*

Mode Configuration mode

aflex max-filesize

Specify the maximum file size for aFleX scripts on the EX device.

Syntax Description [**no**] **aflex max-filesize** *Kbytes*

Parameter	Description
KBytes	Maximum size an individual aFleX script can be, in Kbytes. You can specify 16-128 Kbytes.

Default 32 Kbytes

Mode Configuration mode

IP Commands

dnat name

Enable destination Network Address Translation (NAT) for inbound traffic by mapping one or more external IP addresses to a single internal IP address.

Syntax Description

```
[no] dnat name dnat-name
```

Parameter	Description
dnat-name	Name of DNAT private host.

This command changes the CLI to the configuration level for the specified DNAT, where the following commands are available:

Command	Description
[no] external ip *ip-addr* **[port** *num***]**	Add external host IP address. Optionally, add external host port number with value ranging from 0 - 65535.
[no] internal *ip-addr* **[port** *num***]**	Add internal host IP address. Optionally, add internal host port number with value ranging from 0 - 65535.

Default

None

Mode

Configuration mode

Usage

The command allows up to eight external IP addresses and ports to be mapped to a single internal IP address and port. This DNAT implementation does not rely on QoS classes, so they can be reserved for other uses.

Example

The following command creates a destination NAT profile with the name “DNAT1”, and creates an association between external IP address 10.0.0.1 (port 80) and internal IP address 192.168.10.3 (port 20):

```
EX(config)#dnat name DNAT1
EX(config-DNAT)#external ip 10.0.0.1 port 80
EX(config-DNAT)#internal ip 192.168.10.3 port 20
```

dnat qos

Enable destination Network Address Translation (NAT) for inbound traffic based on QoS traffic classes.

Syntax Description

```
[no] dnat qos class
{
default ip-address |
class-name ip-address
}
```

Parameter	Description
default	Name of a QoS default class.
class-name	Name of a QoS traffic class.
ip-address	IP address to use as the destination address.

Default

None

Mode

Configuration mode

Usage

The normal form of this command enables destination NAT for the specified class, using the specified IP address.

The **no** form of this command disables destination NAT for the specified class. If you do not specify a class, destination NAT is disabled for all classes after user confirmation.

Example

The following command enables destination NAT for traffic class “test”, using IP address 10.10.10.1 as the destination address for this class’s traffic:

```
EX(config)#dnat qos class test 10.10.10.1
```

ip http

Configure access parameters for the Graphical User Interface (GUI).

Syntax

```
[no] ip http
{
auto-redir |
port protocol-port |
secure-port protocol-port |
server |
secure-server |
timeout-policy idle minutes
}
```

Parameter	Description
auto-redir	Enables requests for the unsecured port (HTTP) to be automatically redirected to the secure port (HTTPS).
port *protocol-port*	Specifies the protocol port number for the unsecured (HTTP) port.
secure-port *protocol-port*	Specifies the protocol port number for the secure (HTTPS) port.
server	Enables the HTTP server.
secure-server	Enables the HTTPS server.
timeout-policy idle *minutes*	Specifies the number of minutes a Web management session can remain idle before it times out and is terminated by the EX. You can specify 0-60 minutes. To disable the timeout, enter 0.

Default

This command has the following defaults:

- **auto-redir** – enabled
- **port** – 80
- **secure-port** – 443
- **server** – enabled
- **secure-server** – enabled
- **timeout-policy** – 10 minutes

Mode

Configuration mode

Usage

If you disable HTTP or HTTPS access, any sessions on the management GUI are immediately terminated.

Example

The following command disables management access on HTTP:

```
EX(config)#no ip http server
```

ip route *destination-ipaddr*

Configure a static IP route.

Syntax Description

```
[no] ip route destination-ipaddr
{subnet-mask | /mask-length} next-hop-ipaddr
[ethernet port-num] [ve vlan-id] [distance]
```

Parameter	Description
destination-ipaddr {subnet-mask | /mask-length}	Specifies the destination of the route. To configure a default route, specify 0.0.0.0 /0.
next-hop-ipaddr	Specifies the next-hop router to use to reach the route destination. The address must be in the same subnet as the EX device.
ethernet *port-num*	Specifies the physical port out which to send the packets.
ve *vlan-id*	If the outbound interface is a VE, this option specifies the physical port out which to send the packets.
distance	Administrative distance of the route, 1-255. If there are multiple routes to the same destination and all other costs associated with the routes are equal, the route with the lowest administrative distance is used.

Default

None

Mode

Configuration mode

Usage

Use this command to configure IP routes

Example

The following command configures a static route to 11.11.11.0/24 with next hop 192.168.3.1:

```
EX(config)#ip route 11.11.11.0 255.255.255.0 192.168.3.1
```

Example

The following command configures a static route to 12.12.12.0/24 with next hop 192.168.4.1, through Ethernet interface 2, with distance value 100:

```
EX(config)#ip route 12.12.12.0 /24 192.168.4.1 ethernet 2 100
```

Related Commands

show ip route

ip route reply-same-interface

Force replies to a locally received request to be sent on the same interface that received the request.

A locally received packet is a packet whose destination IP address is the address of the EX device itself. For example, HTTP, HTTPS, SSH, TELNET, SNMP, and DNS requests addressed to the EX device are locally received requests.

Syntax Description

```
[no] ip route reply-same-interface
{force | prefer}
```

Parameter Description

`force`	Response to a locally received request is always sent out the interface on which the request was received.
`prefer`	If a route to the reply destination exists and the next hop can be reached through the interface that received the request, the route is used. Otherwise, the same interface is used.

Default

Disabled (Neither **force** nor **prefer** is enabled.) Responses to a locally received packet may be sent out a different interface than the one the packet is received on. This is because a route lookup is performed on locally sent packets to determine the outgoing interface.

Mode

Configuration mode

ip smtp

Set Simple Mail Transfer Protocol (SMTP) parameters.

Syntax Description

```
[no] ip smtp {hostname | ip-address}
  [port port-num]

[no] ip smtp port port-num

[no] ip smtp mailfrom source-address

[no] ip smtp needauthentication

ip smtp username user-name password password

no ip smtp user-name
```

Parameter	Description
hostname | ip-address	SMTP server IP address or hostname.
port-num	SMTP server port.
source-address	Email source address.
user-name	Username required to log into the SMTP server.
password	Password required to log into the SMTP server.
needauthentication	Specifies that the SMTP needs to be authenticated.

Default

No SMTP server is configured by default. When you configure one, it has the following default settings:

- *port-num* – 25
- *source-address* – not set
- *user-name* – not set
- *password* – not set
- **needauthentication** – disabled

Mode

Configuration mode

Example

The following commands set SMTP server 192.168.0.1 and specify that it needs authentication. The username and password required for logging into the server are specified, and email source address name@email_domain.com is specified.

```
EX(config)#ip smtp 192.168.0.1
EX(config)#ip smtp needauthentication
EX(config)#ip smtp username username1 password password1
EX(config)#ip smtp mailfrom username@email_domain.com
```

ippool

Configure an IP address pool for Network Address Translation (NAT).

Syntax Description

[**no**] **ippool** *ippool-name*

Parameter	Description
ippool-name	Pool name, 1-31 characters.

This command changes the CLI to the configuration level for the specified IP pool, where the following pool-related commands are available:

Command	Description
`[no] ip ip-address [to ip-address]`	Adds an IP address or range to the pool. *ip-address* – Specifies the first address in the range. **to** *ip-address* – Specifies the last address in the range. The IP addresses in the pool are configured as local addresses on the EX device.

Default

None

Mode

Configuration mode

Usage

The normal form of this command creates a new or edits an existing IP address pool identified by *name*, and enters the configuration level for the pool.

The **no** form of this command deletes the specified IP pool. If you do not specify a pool name, all IP pools are removed after user confirmation.

The IP addresses in the pool are configured as local addresses on the EX device.

Example

The following command creates an IP address pool named “test”:

```
EX(config)#ippool test
EX(config-IP pool)#
```

Example

The following commands add IP address 192.168.3.13 and IP range 192.168.3.50 – 192.168.3.60 to pool “test”:

```
EX(config-IP pool)#ip 192.168.3.13
EX(config-IP pool)#ip 192.168.3.50 to 192.168.3.60
```

DNS Commands

dns enable

Enable the Domain Name System (DNS) service on the EX device.

Syntax Description `[no] dns`

Default The DNS service and DNS proxy are both enabled by default.

Mode Configuration mode

Example The following command disables the DNS service:

```
EX(config)#no dns enable
```

dns except-interface

Disable listening for DNS server or proxy traffic on EX interfaces.

Syntax Description

```
[no] dns except-interface [proxy]
{ethernet port-num | ve ve-num}
```

Parameter	Description
`proxy`	Disable listening for DNS proxy traffic. Without this option, listening is disabled for DNS server traffic.

Default Listening for DNS traffic is enabled on all interfaces by default.

Mode Configuration mode

Example The following command disables listening for DNS server traffic on VE 4:

```
EX(config)#dns except-interface ve 4
```

Example The following command disables listening for DNS proxy traffic on Ethernet interface 7:

```
EX(config)#dns except-interface proxy ethernet 7
```

dns local-domain

Configure local domain settings.

Syntax Description `[no] dns local-domain domain-name`

Parameter	Description
domain-name	Sets the local domain name on the EX device.

This command changes the CLI to the configuration level for the specified domain, where the following domain-related commands are available:

Command	Description
cname *domain-name* to *alias* [**ttl** *seconds*]	Configures a Canonical Name (CNAME) record, by mapping the specified *domain-name* to the specified *alias*. To configure aging for the CNAME (alias) sent in DNS replies, use the **ttl** option. You can specify 0-2592000 seconds. To disable aging, specify 0 seconds.
host *name* **ip** *ip-address* [**ttl** *secs*]	Adds a host to the domain. To configure aging for Address (A) records sent in reply to requests for the host IP address, use the **ttl** option. You can specify 0-2592000 seconds. To disable aging, specify 0 seconds.

Note: To configure an Address (A) record for the base domain name, enter “” as the name. For example: **`host "" ip 10.10.10.1`**

Command	Description
mx *name* **priority** *num* [**ttl** *secs*]	Configures a Mail Exchange (MX) record. The *name* is the fully-qualified domain name of the mail server for the zone. The **priority** option specifies the order in which the mail server should attempt to deliver mail to the MX hosts. The MX with the lowest priority value has the highest priority and is tried first. The priority can be 0-65535. There is no default.

	To configure aging, use the **ttl** option. You can specify 0-2592000 seconds. To disable aging, specify 0 seconds.
name *name*	Renames the domain.

Default None. When you configure a local domain, the default TTL for A and MX records is 600 seconds.

Mode Configuration mode

Example The following commands add a local domain called “mycorp.com”, add some hosts to it, and configure an MX record for the domain:

```
EX(config)#dns local-domain example.com
Created new domain example.com
EX(config-domain:example.com)#host ws1 ip 10.10.10.12
EX(config-domain:example.com)#host ws2 ip 10.10.10.14
EX(config-domain:example.com)#mx idsentrie.example.com
```

dns proxy-server

Configure the EX device to act as a DNS proxy.

Syntax Description [**no**] **dns proxy-server** *ip-address* **domain** *domain-name*

Parameter	Description
ip-address	Specifies the IP address of the DNS server for which to act as a proxy.
domain-name	Specifies the domain name for which to act as a proxy.

Default None

Mode Configuration mode

Example The following command adds a DNS proxy for DNS server 10.10.10.66 and domain name “example.com”:

```
EX(config)#dns proxy-server 10.10.10.66 domain example.com
```

ip dns

Configure DNS servers and the default domain name (DNS suffix) for hostnames on the EX device.

Syntax

```
[no] ip dns {primary | secondary} ipaddr
[no] ip dns suffix string
```

Parameter	Description
ipaddr	DNS server's IP address.
string	DNS suffix.

Default

None

Mode

Configuration mode

Example

The following commands configure DNS server 1.1.1.1 as the primary DNS server and 2.2.2.2 as the secondary DNS server, and set the DNS suffix to "localdomain":

```
EX(config)#ip dns primary 1.1.1.1
EX(config)#ip dns secondary 2.2.2.2
EX(config)#ip dns suffix localdomain
```

RIP CLI Commands

key chain

Enable authentication for routing protocols by identifying a group of authentication keys.

Syntax Description

```
[no] key chain name
```

Parameter	Description
name	Name of the key chain, 1-31 characters.

Default

No key chain exists by default.

Mode

Configuration mode

Usage

Enhanced Routing Information Protocol (RIP) Version 2 uses key chains. You must configure a key chain with keys to enable authentication. Although you can identify multiple key chains, A10 recommends using one key chain per interface per routing protocol.

The normal form of this command creates or edits the specified key chain and enters the configuration level for the command.

The **no** form of this command removes the specified key chain.

Example

The following command creates a key chain named “trees”:

```
EX(config)#key chain trees
EX(config-keychain)#
```

key

Configure a key in a key chain.

Syntax Description

```
[no] key key-id
```

Parameter	Description
key-id	Identification number of the key, 0-2147483647. The key identification numbers do not need to be consecutive. This command changes the CLI to the configuration level for the specified key, where the following key-related command is available:

`[no] key-string` *`string`* – Configures the authentication string of the key, 1-16 characters.

Default

No keys exist by default.

Mode

Key-chain configuration mode

Usage

The normal form of this command creates or edits the specified key.

The **no** form of this command removes the specified key.

It is useful to have multiple keys on a key chain so that the software can sequence through the keys.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the no key chain command.

Example

The following commands add keys to the key chain named “trees”:

```
EX(config)#key chain trees
EX(config-keychain)#key 1
EX(config-keychain-key)#key-string thisiskey1
EX(config-keychain-key)#exit
EX(config-keychain)#key 2
EX(config-keychain-key)#key-string thisiskey2
```

router rip

Enable RIP routing.

Syntax Description

```
[no] router rip
```

Default

RIP is disabled by default.

Mode

Configuration mode

Usage

The normal form of the command enables RIP and changes the CLI to the configuration level for global RIP parameters.

The **no** form of this command disables RIP.

Example

The following command enables RIP:

```
EX(config)#router rip
EX(config-router-rip)#
```

The configuration commands available at the RIP configuration level are described below.

network

Configure a RIP network.

Syntax Description

```
[no] network ipaddr {subnet-mask | /mask-length}
```

Default

None

Mode

RIP configuration mode

Usage

RIP routing updates will be sent and received only through interfaces on this network. RIP sends updates to the interfaces in the specified networks. Also, if an interface’s network is not specified, it will not be advertised in any RIP update.

Example

The following command configures RIP network 10.10.10.0 /8:

```
EX(config-router-rip)#network 10.10.10.10 /8
```

passive-interface

Description

Disable route advertisements from being sent on an interface.

Syntax

```
[no] passive-interface
{ethernet port-num | management | ve vlan-id}
```

Default

Route advertisements are enabled. (No interfaces are passive.)

Mode

RIP configuration mode

Example

The following command disables RIP route advertisements from being sent out VE 4:

```
EX(config-router-rip)#passive-interface ve 4
```

redistribute

Description Enable distribution of RIP routes into other route types.

Syntax

```
[no] redistribute {connected | ospf | static}
```

Default Disabled. By default, RIP routes are not redistributed.

Mode RIP configuration mode

Example The following command enables redistribution of RIP routes into OSPF:

```
EX(config-router-rip)#redistribute ospf
```

RIP Interface Commands

ip rip authentication

Configure the RIP authentication mode used on the current interface.

Syntax Description

```
[no] ip rip authentication
{mode md5 | string text}
```

Parameter	Description
mode md5	Uses Message Digest 5 (MD5) for authentication.
string *text*	Uses a simple text password for authentication. The password string can be 1-16 characters with no blanks.

Default Plain text authentication (**string** *text*).

Mode Interface configuration mode

Usage Authentication is supported only in RIPv2.

Example The following command sets the RIP authentication mode on the interface to MD5:

```
EX(config-if:ethernet1)#ip rip authentication
mode md5
```

ip rip authentication key-chain

Specify the key chain to use for MD5 authentication for RIP on the current interface.

Syntax Description

```
[no] ip rip authentication key-chain chain-name
```

Parameter	Description
chain-name	Set of passwords.

Mode

Interface configuration mode

Usage

Authentication is supported only in RIPv2.

Example

The following command configures the current interface to accept and send any key belonging to the key chain named “trees”:

```
EX(config-if:ethernet1)#ip rip authentication key-chain trees
```

Related Commands

key chain

ip rip poisoned-reverse

Enable poison-reverse, which sets the current interface to block information about RIP routes from being advertised out of the interface from which the route information originated.

Syntax Description

```
[no] ip rip poisoned-reverse
```

Default

Disabled. The default loop prevention algorithm is split horizon.

Mode

Interface configuration mode

Usage

The normal form of this command disables split-horizon and enables poison-reverse.

The **no** form of the command disables poison-reverse and enables split-horizon.

Example

The following command enables poison-reverse:

```
EX(config-if:ethernet1)#ip rip poisoned-reverse
```

OSPF CLI Commands

router ospf

Enable OSPF routing.

Syntax Description

```
[no] router ospf
```

Default

OSPF is disabled by default.

Mode

Configuration mode

Usage

The normal form of the command enables OSPF and changes the CLI to the configuration level for global OSPF parameters.

The **no** form of this command disables OSPF.

Example

The following command enables OSPF:

```
EX(config)#router ospf
EX(config-router-ospf)#
```

The configuration commands available at the RIP configuration level are described below.

area

Configure an OSPF area.

Syntax Description

```
[no] area ip-address
{stub | authentication [message-digest]}
```

Parameter	Description
ip-address	Identifies the area.
stub	Indicates that the area is a stub area.
authentication [message-digest]	Enables use of authentication. If you use the **message-digest** option, MD5 is used. If you omit this option, a plain text key is used.

Default

None

Mode

OSPF configuration mode

Usage

If a stub area is configured on the EX device, the same area must be configured as a stub area on all other OSPF routers in the same OSPF area.

Example

The following command configures a stub area with area ID 10.2.4.5:

```
EX(config-router-ospf)#area 10.2.4.5 stub
```

default-metric

Set the numeric cost that is assigned to OSPF routes by default. The metric (cost) is added to routes when they are redistributed.

Syntax Description

```
[no] default-metric metric-value
```

Parameter	Description
metric-value	1-16777214

Default

None. The metric of redistributed connected and static routes is set to 0.

Mode

OSPF configuration mode

Usage

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a **default metric** provides a reasonable substitute and enables the redistribution to proceed.

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Example

The following commands make OSPF compatible with RFC 1583:

```
EX(config-router-ospf)#default-metric 10
EX(config-router-ospf)#redistribute rip
```

Related Commands

redistribute

network area

Description Configure an OSPF network.

Syntax

```
[no] network
ip-address {subnet-mask | /mask-length}
area ip-address
```

Default None

Mode OSPF configuration mode

Usage The *ip-address* and mask arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the mask argument allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument.

Example The following command configures an OSPF network:

```
EX(config-router-ospf)#network 192.168.1.0 /24 area 1
```

passive-interface

Description Disable Link-State Advertisements (LSAs) from being sent on an interface.

Syntax

```
[no] passive-interface
{ethernet port-num | management | ve vlan-id}
```

Default LSAs are enabled. (No interfaces are passive.)

Mode OSPF configuration mode

Usage On passive interfaces, all received packets are processed as normal and OSPF does not send either multicast or unicast OSPF packets.

Example The following command configures a passive interface on the Virtual Ethernet (VE) interface on VLAN 3:

```
EX(config-router-ospf)#passive-interface ve 3
```

redistribute

Enable distribution of OSPF routes into other route types.

Syntax Description

```
[no] redistribute
{connected | rip | static}
[metric-type {1 | 2} metric num]
```

Parameter	Description
`metric` *num*	Metric for the default route.
`metric-type {1 | 2}`	External link type associated with the default route advertised into the OSPF routing domain: **1** – Type 1 external route **2** – Type 2 external route

Default Disabled. By default, OSPF routes are not redistributed.

Mode OSPF configuration mode

Example The following command enables redistribution of OSPF routes into RIP:

```
EX(config-router-ospf)#redistribute rip
```

router-id

Description Set the value used by the EX device to identify itself when exchanging route information with other OSPF routers.

Syntax

```
[no] router-id ip-address
```

Default The default router ID is the highest-numbered IP address configured on any of the EX Ethernet interfaces.

Mode OSPF configuration mode

Usage The EX device has only one router ID. The address does not need to match an address configured on the device; however, the address must be unique within the routing domain.

New or changed router IDs require a restart of the EX device OSPF process. To restart the OSPF process, use the following command: **clear ip ospf process**

Example

The following commands set the router ID to 2.2.2.2 and reload OSPF to place the new router ID into effect:

```
EX(config-router-ospf)#router-id 2.2.2.2
EX(config-router-ospf)#clear ip ospf process
```

OSPF Interface Commands

ip ospf authentication

Specify the authentication type to use for OSPF on the current interface.

Syntax Description

```
[no] ip ospf authentication
[message-digest | null]
```

Parameter	Description
`message-digest`	Specifies that message-digest authentication will be used.
`null`	No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.

Default

The interface default is no authentication (null authentication).

Mode

Interface configuration mode

Usage

If you enter the `authentication` command without either of the options above, a simple key is used for authentication.

Before using the **ip ospf authentication** command, configure a password for the interface using the **ip ospf authentication-key** command. If you use the **ip ospf authentication message-digest** command, configure the message-digest key for the interface with the **ip ospf message-digest-key** command.

For backward compatibility, authentication type for an area are still supported. If the authentication type is not specified for an interface, the authentication type for the area will be used. (The area default is null authentication.)

Example

The following command enables MD5 authentication:

```
EX(config-if:ethernet1)#ip ospf authentication message-digest
```

Related Commands **area authentication**, **ip ospf authentication-key**, **ip ospf message-digest-key**

ip ospf authentication-key

Specify the password used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers.

Syntax Description

```
[no] ip ospf authentication-key password
```

Parameter	Description
password	String of 1-8 characters with no blanks.

Default No password is specified.

Mode Interface configuration mode

Usage The password created by this command is used as a key that is inserted directly into the OSPF header when the EX device originates OSPF packets. A separate password can be assigned to each network on a per-interface basis. All neighbours on the same network must have the same password to be able to exchange OSPF information.

Example The following command configures an authentication key with password "ospfpwd":

```
EX(config-if:ethernet1)#ip ospf authentication-key ospfpwd
```

Related Commands **area authentication**, **ip ospf authentication**, **ip ospf message-digest-key**

ip ospf cost

Explicitly specify the cost of sending a packet on the current interface.

Syntax Description

```
[no] ip ospf cost interface-cost-value
```

Parameter	Description
interface-cost-value.	Numeric cost for using the interface, 1-65535.

Default No default cost is predefined.

Mode Interface configuration mode

Example The following example sets the interface cost value to 65:

```
EX(config-if:ethernet1)#ip ospf cost 65
```

ip ospf dead-interval

Set the number of seconds that neighbor OSPF routers will wait for a new OSPF Hello packet from the EX device before declaring this OSPF router (the AX Series) to be down.

Syntax Description

```
[no] ip ospf dead-interval seconds
```

Parameter	Description
seconds	Specifies the interval, 1-65535 seconds. The same value must be used on all OSPF nodes on the network.

Default Four times the length of the hello interval. The default hello interval is 10 seconds and the default dead interval is 40 seconds.

Mode Interface configuration mode

Usage The dead interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Example The following command sets the OSPF dead interval to 60 seconds:

```
EX(config-if:ethernet1)#ip ospf dead-interval 60
```

Related Commands **ip ospf hello-interval**

ip ospf hello-interval

Set the number of seconds between transmission of OSPF Hello packets on this interface.

Syntax Description

```
[no] ip ospf hello-interval seconds
```

Parameter	Description
seconds	Specifies the interval, 1-65535 seconds. The value must be the same for all nodes on a specific network.

Default 10 seconds

Mode

Interface configuration mode

Usage

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Example

The following command sets the interval between hello packets to 15 seconds:

```
EX(config-if:ethernet1)#ip ospf hello-interval 15
```

Related Commands

`ip ospf dead-interval`

ip ospf message-digest-key

Specify a set of MD passwords used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers.

Syntax Description

```
[no] ip ospf message-digest-key key-id md5 key
```

Parameter	Description
key-id	An identifier in the range from 1 to 255.
key	Alphanumeric password of up to 16 bytes, with no blanks.

Default

OSPF MD5 authentication is disabled.

Mode

Interface configuration mode

Usage

This command applies only to MD authentication. Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *key* value.

Example

The following command creates key 19 with password “8ry4567”:

```
EX(config-if:ethernet1)#ip ospf message-digest-key 19 md5 8ry4567
```

Related Commands

`area authentication`, **`ip ospf authentication-key`**

ip ospf priority

Set the eligibility of this OSPF router to be elected as the designated router (DR) or backup designated router (BDRs) for the routing domain.

Syntax Description

```
[no] ip ospf priority number-value
```

Parameter	Description
number-value	Number that specifies the priority of the router, 0-255. 1 is the lowest priority and 255 is the highest priority.

Default

The default priority is 1.

Mode

Interface configuration mode

Usage

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multi-access networks (in other words, not to point-to-point networks).

Example

The following command sets the router priority value to 8:

```
EX(config-if:ethernet1)#ip ospf priority 8
```

ip ospf retransmit-interval

Set the number of seconds between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface.

Syntax Description

```
[no] ip ospf retransmit-interval seconds
```

Parameter	Description
seconds	Time (in seconds) between retransmissions. The time must be longer than the expected round-trip delay between any two routers on the attached network. The range is 1-65535 seconds.

Default

5 seconds

Mode

Interface configuration mode

Usage When a router sends an LSA to its neighbour, it keeps the LSA until it receives an acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

Example The following command sets the retransmit interval value to 38 seconds:

```
EX(config-if:ethernet1)#ip ospf retransmit-interval 38
```

ip ospf transmit-delay

Set the number of seconds it takes to transmit Link State Update packets (route updates) on this interface. This amount is added to the ages of LSAs sent in the updates.

Syntax Description

```
[no] ip ospf transmit-delay seconds
```

Parameter	Description
seconds	Time required to send a link-state update, 1-65535 seconds

Default 1 second

Mode Interface configuration mode

Usage Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified by *seconds* before transmission. The value assigned should take into account the transmission and propagation delays for the interface. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Example The following command sets the retransmit delay value to 5 seconds:

```
EX(config-if:ethernet1)#ip ospf transmit-delay 5
```

Ethernet Interface Configuration Commands

external

Configure the current interface as an external interface.

Syntax Description

```
[no] external
```

Default

No interfaces are configured as external interfaces by default.

Mode

Interface configuration mode

Example

The following command configures the current interface as an external interface:

```
EX(config-if:ethernet4)#external
```

ip address

Assign an IP address to the current interface, either manually or using a DHCP server.

Syntax Description

```
[no] ip address
{
ip-address {subnet-mask | /mask-length}
  [secondary] | dhcp [options]
}
```

Parameter	Description
ip-address	Statically assigned IP address.
subnet-mask | /mask-length	Network mask or mask length.
secondary	Indicates that this address is a secondary address.
dhcp [options]	Get the IP and network information from a DHCP server, and optionally, choose to retrieve information about the routers, static-routes, domain-name, and the domain-name-servers.

Mode

Interface configuration mode

Usage

You can assign an IP address manually or from a DHCP server to an EX interface. If a static IP address is manually assigned while the EX device is configured in transparent mode, then the interface is removed from transparent mode and is no longer associated with the device’s global IP address.

To route between transparent mode and gateway mode, assign a Virtual Ethernet (VE) interface to the transparent ports.

Example

The following command adds IP address 4.4.4.4 /24 to Ethernet interface 4:

```
EX(config-if:ethernet4)#ip address 4.4.4.4 /24
```

Related Commands

`interface`

ip nat ippool

Enable IP source Network Address Translation (NAT) on the current interface.

Syntax Description

```
[no] ip nat [ippool ippool-name]
```

Parameter	Description
ippool-name	Pool name.

Mode

Interface configuration mode

Example

The following command enables IP source NAT with IP pool “pool1”:

```
EX(config-if:ethernet4)#ip nat ippool pool1
```

Example

This second example provides a CLI command that tells the EX to use source NAT, even if no IP Pool has been specified. Traffic output from interface ethernet 3 will do Source NAT using the IP address assigned to that interface.

```
EX(config-if:ethernet3)#ip nat
```

Related Commands

`ippool`

ip renew

Renew the lease on an IP address assigned by a DHCP server.

Syntax Description

```
ip renew
```

Default

No IP addresses are assigned by a DHCP server by default.

Mode

Interface configuration mode

Example

The following command renews the lease on a DHCP-assigned IP address:

```
EX(config-if:ethernet3)#ip renew
```

ips

Apply an IPS group to a physical interface.

Syntax Description

```
[no] ips group-name
```

Parameter	Description
group-name	IPS filter group name.

Default

No IPS filter groups are applied to interfaces.

Mode

Interface configuration mode

Usage

The normal form of this command applies the specified IPS group to the physical interface.

The **no** form of this command removes the specified IPS filter group from the interface.

Each interface can have only one IPS group. IPS groups can be applied only to physical interfaces. They cannot be applied to virtual interfaces.

Example

The following command applies IPS filter group “ips1” to the current Ethernet interface:

```
EX(config-if:ethernet1)#ips ips1
```

mtu

Change the maximum transmission unit (MTU) on the current interface.

Syntax Description

```
[no] mtu bytes
```

Default

1500

Mode

Interface configuration mode

permit

Control access to the current interface.

Syntax Description

```
[no] permit {ssh | telnet | http | snmp | ping |
trust_host}
```

Default

Access by SSH, HTTP, and PING are enabled by default.

Mode

Interface configuration mode

Usage

The **trust_host** option allows access only by trusted hosts configured in admin accounts. (See “admin” on page 261.)

Example

The following command enables Telnet access on Ethernet interface 4:

```
EX(config-if:ethernet4)#permit telnet
```

shutdown

Shut down the current interface.

Syntax Description

```
[no] shutdown
```

Default

By default, interfaces are not shut down.

Mode

Interface configuration mode

Example

The following command shuts down the current interface:

```
EX(config-if:ethernet4)#shutdown
```

speedduplex

Set the maximum speed and duplex mode on the current interface.

Syntax Description

```
[no] speedduplex {10full | 100full| 10half |
100half | auto}
```

Parameter	Description
10Full	Configured speed is 10Mbit/s and the duplex mode is full-duplex.
100Full	Configured speed is 100Mbit/s and the duplex mode is full-duplex.

1000Full	Configured speed is 1 Gbit/s and the duplex mode is full-duplex.
10Half	Configured speed is 10Mbit/s and the duplex mode is half-duplex.
100Half	Configured speed is 100Mbit/s and the duplex mode is half-duplex.
auto	Port speed and duplex mode are auto-negotiated by the two ends of the link.

Default **auto**

Mode Interface configuration mode

Example The following command configures Ethernet interface 4 to operate at 100Mbit/s in full-duplex mode:

```
EX(config-if:ethernet4)#speedduplex 100Full
```

bypass

Configure port bypass.

Note: This command applies only to models EX 1100 and EX 2110.

Syntax Description `[no] bypass interface-pair {1 | 2 | all}`

Parameter	Description
1 | 2 | all	Specifies the bypass pair to enable: **1** – Enables hardware bypass on Ethernet interfaces 1 and 2. **2** – Enables hardware bypass on Ethernet interfaces 3 and 4. **all** – Enables hardware bypass on both pairs (1-2, 3-4).

Default Hardware bypass is disabled when the EX device is powered on.

Mode Configuration mode

Usage When hardware bypass is enabled, the EX device forwards traffic received on an interface in a bypass pair out the other interface in the pair at Layer 2, without processing the traffic. This is equivalent to the hardware bypass function when the EX device is powered off.

bypass-on-shutdown

The feature is an enhancement to the hardware bypass feature. By enabling bypass-on-shutdown, you can configure the EX appliance to reduce the amount of time (i.e. "limbo period") during which control of traffic is transferred from the EX software to the hardware bypass feature.

Note: This command applies only to models EX 1100 and EX 2110.

Syntax Description

```
[no] bypass-on-shutdown interface-pair {1 | 2 |
all}
```

Parameter	Description
`1	2	all`	Specifies the bypass pair to enable: **1** – Enables hardware bypass on Ethernet interfaces 1 and 2. **2** – Enables hardware bypass on Ethernet interfaces 3 and 4. **all** – Enables hardware bypass on both pairs (1-2 and 3-4) of Ethernet interfaces.

Default

The bypass-on-shutdown feature is disabled by default.

Mode

Configuration mode

Usage

When the EX is powered on, the EX software is actively processing traffic. However, if the EX device is powered down, the EX software relinquishes control and the hardware bypass feature takes over. The EX's hardware bypass feature allows the device to continue passing traffic (in an unintelligent fashion) even after the system has been powered off. This allows traffic to continue flowing through the box without help from the EX software.

During the switchover scenario, there is a "limbo period" that exists as control of traffic is passed from the EX software to the hardware bypass feature. During this hand-off, packets are dropped and TCP connections are terminated, which can obviously be disruptive to network users.

This limbo period typically lasts for about 12 seconds during shut-down, but to minimize disruption, the limbo period can be reduced to about 4 seconds by using the **bypass-on-shutdown** command.

The command allows you to enable the feature on paired ports (1 and 2), or paired ports (3 and 4), or you can enable the feature on both sets of ports.

Example

To enable the **bypass-on-shutdown** command on both sets of paired ports, use the following command:

```
EX(config)#bypass-on-shutdown interface-pair all
```

High Availability (HA) Commands

ha full-sync

Manually synchronize the HA Master's configuration with the configuration on an HA Backup.

Note: To enable automatic configuration synchronization, see Figure , "ha sync-peer," on page 254.

Syntax Description **ha full-sync**

Mode Configuration mode

Usage Before using this command, use the **ha sync-peer** command to specify the IP address of the Backup EX device.

When you use this option, the EX device copies its running-config and startup-config to the specified Backup, to replace the running-config and startup-config.

Manual synchronization can be performed only from the HA Master to an HA Backup. Configurations cannot be synchronized from a Backup to another Backup or to a Master.

Example The following command copies the startup-config and running-config to the HA peer:

```
EX(config)#ha sync-peer 10.10.10.4
EX(config)#ha full-sync
```

ha master-down-timeout

Increase or decrease the amount of time used by the backup device to determine if the master is dead and failover should occur.

Syntax Description [**no**] **ha master-down-timeout** *number-of-intervals*

Mode Configuration mode

Usage Use the master down timeout to increase or decrease the amount of time used by the backup device to determine when the master is dead and failover should occur. The total time is determined by multiplying the basic HA timer interval by a configurable number, ranging from 1-60, with a default value of 3. If the backup does not receive a response from the master during the specified number of timer intervals, then the backup declares that the master is dead and takes over.

Note: The interval time is set in the vgroup, and the timer command is set in seconds. The default interval time is 1 second.

Usage CLI syntax appears below.

Example The following command multiplies the configured time interval times 10.

```
EX(config)#ha master-down-timeout 10
```

ha sync-peer

Specify the IP address of an HA peer.

Syntax Description `[no] ha sync-peer ip-address`

Mode Configuration mode

Usage This option is required for configuration synchronization (**ha full-sync**) and session synchronization (**ha sync-session**).

Example The following command specifies the IP address of an HA peer:

```
EX(config)#ha sync-peer 10.10.10.4
EX(config)#ha full-sync
```

ha sync-session

Enable automatic synchronization of sessions from the Master to Standby EX device.

Syntax Description `[no] ha sync-session`

Default Disabled

Mode Configuration mode

Usage This option requires the configurations on the EX devices in the HA pair to be the same.

Session synchronization provides stateful failover for active sessions. If a failover occurs, active sessions that have been synchronized continue uninterrupted. Clients experience little or no service interruption.

Session synchronization applies to the following types of connections:

- Forwarded IP with session (TCP, UDP, ICMP, other IP)
- IP NAT and NAT ALG connections
- Connections to internal servers such as IPsec of PPTP VPN, SSL VPN, internal email, or web server

The following state information is synchronized:

- Link information (persistence info, session and link association, and so on)
- NAT info (source be source or destination NAT, or both)
- Layer 2 though Layer 7 Information

Session synchronisation applies to the following features:

- Outbound LLB
- Inbound LLB in combination with DNAT or SLB
- Transparent bridge mode
- CLB
- FWLB
- QoS Policy

ha sync-timeout

Set the time required to complete a full configuration synchronization operation.

Syntax Description

```
[no] ha sync-timeout timeout-value
```

Mode

Configuration mode

Usage

Use this command to set the time required to complete a full configuration synchronization operation. By default, the sync-timeout command is set to 2 minutes. However, depending on the environment, a full sync may actually take longer to complete.

Example

The following command specifies the IP address of an HA peer:

```
EX(config)#ha sync-timeout 5
```

vgroup

Create, edit or delete a virtual group for High Availability (HA).

Syntax Description

```
[no] vgroup group-id
```

Parameter	Description
group-id	The virtual group ID, 1-255.

This command changes the CLI to the configuration level for the specified HA virtual group, where the following group-related commands are available:

Command	Description
[**no**] **activate**	Activates the virtual group.
[**no**] **disable-port-hold-time** *ms*	Specifies the number of milliseconds (ms) during which to flap (disable, then re-enable) the HA interface following HA failover. Flapping the interface forces the other devices connected to the EX devices to more quickly relearn their MAC and ARP entries for the EX. Until the other devices relearn the MAC and ARP entries, the entries will still refer to the EX device that is no longer Master. You can specify 100-10000 ms.

Note: This command applies only to Virtual Ethernet (VE) interfaces, and only in transparent mode.

Command	Description
[**no**] **heartbeat** {**ethernet** *port-num* | **management**}	Sets the HA heartbeat interface. A valid heartbeat interface is a physical Ethernet interface. In gateway (route) mode, if no heartbeat interface is configured or the interface goes down, the virtual group will send advertisements to the other EX device using network links. Each virtual group can have a maximum of 3 heartbeat interfaces.

[**no**] **ip** *ip-address* {*subnet-mask* | /*mask-length*}

Configures a virtual IP address within the HA virtual group.

The IP address must be a valid host IP address and can not be the same as a real IP address configured on the interface.

Each virtual group can have a maximum of 8 virtual IP addresses.

[**no**] **preempt**

Enables this EX device to become the active EX device for the virtual group by pre-empting a lower priority active EX device.

[**no**] **priority** *priority-value* [**weight** *weight-value*]

Sets the HA priority of the virtual group.

The virtual group with the highest priority will become active; others will become standbys.

If the interface bound to the virtual group fails, the group’s priority is reduced by the weight value of the bound interface.

The p*riority-value* can be 1-255. The *weight-value* can be 1-255. The sum of the weight values must be less than the priority value.

[**no**] **tag** *number*

Sets the tag value for the virtual group. The *number* specifies the tag number, 0-255. Virtual groups that have the same tag value will be treated as one group. To release a virtual group, reset its tag value to 0.

[**no**] **timer** *number*

Sets the heartbeat interval for the virtual group. The *number* specifies the interval and can be 1-255 seconds.

[**no**] **track interface ethernet** *port-num* [**weight** *weight-value*]

Tracks other physical interfaces in the virtual group. If the tracked interface fails, the priority value of the current interface is reduced by the amount of the tracked interface’s weight.

The *weight-value* can be 1-255. The sum of the weight value must be less than the priority value.

[no] track service *service* **weight** *weight-value*

Tracks background services in the virtual group. The *service* can be one of the following

log – Log service (includes syslog and kernel log)

hm – Health monitor service

web – Web service

ssh – SSH service

report – Report service

routing – Routing service (includes routing manager, OSPF and RIP)

system – Health monitor service (includes IP2ID, DNS, system timer, and SNMP)

If a tracked service fails, the priority value will be reduced by the amount of the failed service's weight.

Each service has its own default *weight-value*, 1-255. (See the “Default” section below.) The sum of the weight values must be less than the priority value.

Default

The EX device does not have any HA virtual groups by default. When you create an HA virtual group, it has the following default settings:

- **activate** – Virtual groups are disabled by default.
- **disable-port-hold-time** – 2000 ms
- **heartbeat ethernet** – none
- **ip** – none
- **preempt** – enabled
- **priority** – The default *priority-value* is 100. The default *weight-value* is 10.
- **tag** – 0
- **timer** – 1 second

- **track interface ethernet** – Depends on whether the configuration is for gateway mode or transparent mode:
  - Gateway mode – None.
  - Transparent mode – All physical interfaces in the VLAN will be tracked automatically.

  The default *weight-value* is the weight of the physical interface on which the virtual group is configured.
- **track service** – None. When you add tracking of a service, the default weight depends on the service:
  - **log** – 10
  - **hm** – 5
  - **web** – 5
  - **ssh** – 5
  - **report** – 5
  - **routing** – 5
  - **system** – 5

Mode Interface configuration mode

Usage The normal form of this command creates a new or edits an existing HA virtual group and enters the configuration level for the group.

The **no** form of this command removes the virtual group.

An EX device can have a maximum of 32 HA virtual groups.

Example The following command creates HA virtual group 1:

```
EX(config-if:ethernet1)#vgroup 1
   Add virtual group ok.
EX(config-if:ethernet1-vgroup:1)#
```

Example The following command configures Ethernet interface 2 as a HA heartbeat interface:

```
EX(config-if:ethernet1-vgroup:1)#heartbeat ethernet 2
```

Example The following command configures a virtual IP address for the current HA virtual group:

```
EX(config-if:ethernet1-vgroup:1)#ip 192.168.1.1
```

Example The following command changes the HA priority and weight for the current virtual group:

```
EX(config-if:ethernet1-vgroup:1)#priority 120 weight 20
```

Example The following command adds tracking for the SSH service and increases the weight of the service to 20:

```
EX(config-if:ethernet1-vgroup:1)#track service ssh weight 20
```

Example The following command activates the current virtual group:

```
EX(config-if:ethernet1-vgroup:1)#activate
```

Related Commands `show vrrp`

Admin Configuration Commands

admin

Use to add a new admin user or to delete an exist admin user.

Syntax Description

```
[no] admin admin-username [password password]
```

Parameter	Description
admin-username	Admin username, 1-31 characters.
password	Sets the password, 1-63 characters.

This command changes the CLI to the configuration level for the specified admin account, where the following admin-related commands are available:

Command	Description
admin	Enters the configuration level for another admin account. If you are configuring multiple admin accounts, this command simplifies navigation of the CLI because you do not need to return to the global Config level to begin configuration of the next account.
disable	Disables the admin account.
enable	Enables the admin account.
password *string*	Sets the password, 1-63 characters.
privilege *priv-level*	Sets the privilege level for the account: **read** – The admin can access the User EXEC and Privileged EXEC modes of the CLI only. **write** – The admin can access all levels of the CLI but cannot configure other admin accounts.
show this	Displays information about the current admin account. The output is the same as the output of **show admin** *name* **detail**, where *name* is the name of this admin account.
trusted-host *ipaddr* *{subnet-mask | /mask-length}*	Specifies the host or subnet address from which the admin is allowed to log onto the EX device.
rename *new-name*	Changes the admin name.

`unlock` Unlocks the account. Use this option if the admin has been locked out due to too many login attempts with an incorrect password. (To configure lockout parameters, see "admin lockout" on page 263.)

Default The system has a default admin account, with username "admin" and password "a10". The default admin account has write privileges and can log on from any host or subnet address. The default admin account is the only account that has root access, which allows configuration of other admin accounts.

Other admin accounts have the following defaults:

- **enable** / **disable** – Admin accounts are enabled by default as soon as you add them.
- **password** – "a10". This is the default for the "admin" account and for any other admin account you configure.
- **privilege** – **read**
- **trusted-host** – 0.0.0.0 /0, which allows access from any host or subnet.
- **unlock** – N/A. Admin accounts are unlocked by default. They can become locked based on **admin lockout** settings.

Mode Configuration mode

Usage The normal form of the command adds a new or edits an existing admin account, and changes the CLI to the configuration level for the account.

The system's default "admin" account can be modified but it can not be deleted.

Example The following command adds admin user "adminuser1" with password "1234":

```
EX(config)#admin adminuser1 password 1234
EX(config-admin:adminuser1)#
```

Example The following command restricts the current admin account's logins to occur only from the 1.1.1.0 subnet:

```
EX(config-admin:adminuser1)#trusted-host 1.1.1.0 255.255.255.0
```

Example The following command shows information about the “adminuser99” account:

```
EX(config-admin:adminuser99)#show this
  User Name              ...... adminuser99
  Status                 ...... Enabled
  Privilege              ...... Read only
  Trusted Host(Netmask)  ...... Any
  Lock Status            ...... No
  Lock Time              ......
  Unlock Time            ......
  Password Type          ...... Encrypted
  Password               ...... $1$5a786dfc$QRQ1Pw2xO9wUmQYetSihc.
```

Related Commands **admin lockout, show admin**

admin lockout

Set lockout parameters for admin sessions.

Syntax

```
[no] admin lockout
{duration minutes | enable | reset-time minutes |
threshold number}
```

Parameter	Description
duration *minutes*	Number of minutes a lockout remains in effect. After the lockout times out, the admin can try again to log in. You can specify 0-1440 minutes. To keep accounts locked until you or another authorized administrator unlocks them, specify 0.
enable	Enables the lockout feature.
reset-time *minutes*	Number of minutes the EX device remembers failed login attempts. You can specify 1-1440 minutes.
threshold *number*	Number of consecutive failed login attempts allowed before an administrator is locked out. You can specify 1-10.

Default The lockout feature is disabled by default. This command has the following defaults:

- **duration** – 10 minutes
- **reset-time** – 10 minutes
- **threshold** – 5

Mode

Configuration mode

Example

This following command enables admin lockout:

```
EX(config)#admin lockout enable
```

ldap server

Set LDAP parameters, for authenticating administrative access to the EX device.

Syntax Description

```
[no] ldap server {hostname | ipaddr}
port protocol-port
cn cn dn dn
```

Parameter	Description
hostname | ipaddr	LDAP server’s hostname or IP address.
protocol-port	Protocol port on which the server listens for LDAP requests, 1-65535.
cn	LDAP common name identifier; for example: “cn” or “uid”.
dn	LDAP distinguished name (dn).

Default

None

Mode

Configuration mode

Example

The following command configures LDAP server 192.168.1.1:

```
EX(config)#ldap server 192.168.1.1 port 389 cn cn dn dc=my,dc=com
```

radius

Configure two or more RADIUS servers to authenticate administrative accounts.

Syntax

```
[no] radius server {hostname | ipaddr}
[acct-port port]
[auth-port protocol-port]
[secret secret-string]
```

Parameter	Description
hostname | *ipaddr*	Hostname or IP address of the RADIUS server.
acct-port *protocol-port*	Specify the RADIUS server's port.
auth-port *protocol-port*	Specify the RADIUS server's port.
secret *secret-string*	Password required by the RADIUS server for authentication requests. The shared secret is used to validate RADIUS requests and replies. The value entered here must match what is configured on the RADIUS server.

Default

No RADIUS servers are configured by default. The default RADIUS protocol ports are 1812 for authentication and 1813 for accounting.

Mode

Configuration mode

Usage

The EX supports two or more RADIUS servers. One is designated as the primary, the next is designated as the secondary, tertiary, etc. You can use the `show radius server` command to list all configured RADIUS servers. The first server listed in the output is the primary, the second one listed is the secondary, and so on.

The RADIUS protocol supports the "Service Type" attribute, which defines the administrative read and write privileges. The "Service Type" attribute can have the following values:

- **1 – Login -** user can execute non-privileged (read-only) commands
- **6 – Administrative -** user can execute privileged (read/write) commands
- **7 – NAS Prompt -** user can execute non-privileged (read-only) command

The EX also supports the "A10-Admin-Privilege” option, which can also be used to determine administrative privileges. There are two acceptable values: (1) Read only and (2) Read & Write.

If both the "A10-Admin-Privilege” and RADIUS “Service Type” administrative privileges are configured, then the priority is given to the "A10-Admin-Privilege”.

Example

The following command configures the EX device to use RADIUS server 10.10.1.86 to authenticate administrative access:

```
EX(config)#radius server 10.10.1.86 secret radpwd
```

Example

The following command removes the RADIUS server 10.10.10.15:

```
EX(config)#no radius server 10.10.10.15
```

authentication type

Set the authentication method used to authenticate administrative access to the EX device.

Syntax Description

```
[no] authentication type local {ldap | radius}
```

Parameter	Description
`local`	Use the EX local admin database (admin entries in the configuration file) for authentication. If the admin username and password match an entry in the config file, then the admin is granted access.
`ldap`	Use an external LDAP server for authentication.
`radius`	Use external RADIUS server for authentication.

Default

By default, only local authentication is used.

Mode

Configuration mode

Usage

Local authentication is required and is always used first, even if you use the **ldap** or **radius** option too. If the username or password does not match a username and password configured on the EX device, the device checks for the username and password on an external server, if **ldap** or **radius** is specified. However, if the username or password does not match and **ldap** or **radius** *is not* specified, authentication fails.

System Management Commands

Description Create a static ARP entry.

Syntax

```
[no] arp ipaddr mac-address
[interface {ethernet num | ve ve-num | management}
[vlan vlan-id]]
```

Parameter	Description
ipaddr	IP address of the static entry.
mac-address	MAC address of the static entry.
interface *interface-type*	Specifies the Ethernet interface.
vlan *vlan-id*	If the EX device is deployed in transparent mode, and the interface is a tagged member of multiple VLANS, use this option to specify the VLAN for which to add the ARP entry.

Mode Configuration mode

backup

Backup up a configuration file.

Syntax Description

```
backup {startup-config | running-config}
{
daily hh:mm |
monthly date hh:mm |
once |
weekly day hh:mm
}
[with-timestamp]
[with-version]
url
```

Parameter	Description
startup-config | running-config	Specifies the configuration file to back up.
daily *hh*:*mm*	Saves a backup of the specified configuration once a day, at the specified time.

monthly *date hh*:*mm*
Saves a backup of the specified configuration once a month, on the specified date (1-31).

once
Immediately saves a backup of the specified configuration.

weekly *day hh*:*mm*
Saves a backup of the specified configuration once a week, on the specified day and time. The can be one of the following: **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, or **Sat**.

with-timestamp
Adds a timestamp to the backup filename.

with-version
Adds the software version to the backup filename.

url
File transfer protocol, username (if required), and directory path.

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL:

```
tftp://host/file
ftp://[user@]host[:port]/file
scp://[user@]host/file
rcp://[user@]host/file
```

Default

Automatic configuration backups are disabled. When you use this command to immediately save a backup or to schedule one, the **with-timestamp** and **with-version** options are disabled by default for the backup.

Mode

Configuration mode

Example

The following command immediately backs up the startup-config:

```
EX(config)#backup once tftp://1.1.1.1/back_file
```

Related Commands

restore

banner

Set the banner configuration

Syntax Description

```
banner [exec line | login line]
```

Parameter	Description
exec	The EXEC mode banner
login	The login banner
line	Banner text

Default

The default login banner is as follows: “Welcome to EX”

The default EXEC banner is as follows: “[type ? for help]”

Mode

Configuration mode

Usage

Use this command to configure banner information.

Example

The following commands set the login banner to “welcome to login mode” and set the exec banner to “welcome to exec mode”:

```
EX(config)#banner exec welcome to exec mode
EX(config)#banner login welcome to login mode
```

check config

Check whether the configuration is right.

Syntax Description

```
check config
```

Default

None

Mode

Configuration mode

Example

The following command checks the configuration:

```
EX(config)#check config
The config is right
```

clock set

Set the clock.

Syntax Description

```
clock set time day month year
```

Parameter	Description
time	Format hh:mm:ss (24 hr.)
day	Format 1-31 - day of month
month	Format January, February, etc.
year	Format 2007, 2008, etc.

Mode

Privileged EXEC mode

Usage

Use this command to set the time and date on the system clock.

Example

The following commands set the time and date to 05:08:000 October 31, 2006 and verify the change:

```
EX#clock set 05:12:000 31 Oct 2006
EX#show clock
05:12:50.636 PST Tue Oct 31 2006
```

Related Commands

show clock, clock timezone

clock timezone

Set the clock timezone.

Syntax Description

```
clock timezone timezone
```

Parameter	Description
timezone	Specifies the timezone. To display a list of valid timezone values, enter the following command: **clock timezone ?**

Default

Europe/Dublin

Mode

Configuration mode

Usage

Use this command to configure the timezone. Use the help form to view a list of available timezones.

Example The following commands display the available timezones and set the timezone to the equivalent of Pacific Standard Time (PST):

```
EX(config)#clock timezone ?
  Pacific/Midway               (GMT-11:00)Midway Island, Samoa
  Pacific/Honolulu             (GMT-10:00)Hawaii
  America/Anchorage            (GMT-09:00)Alaska
  America/Los_Angeles          (GMT-08:00)Pacific Time(US & Canada)
  America/Tijuana              (GMT-08:00)Tijuana, Baja California
  America/Phoenix              (GMT-07:00)Arizona
  America/Shiprock             (GMT-07:00)Mountain Time(US & Canada)
  America/Chicago              (GMT-06:00)Central Time(US & Canada)
  America/Mexico_City          (GMT-06:00)Mexico City
  America/Regina               (GMT-06:00)Saskatchewan
...
EX(config)#clock timezone America/Los_Angeles
```

Related Commands **show clock, clock set**

copy

Copy the running config to disk or copy the startup-config to memory.

Syntax Description

```
copy running-config startup-config
copy startup-config running-config
```

Default None

Mode Configuration mode

Usage The **copy running-config startup-config** command is equivalent to the **write memory** command.

Example The following command copies the running configuration from memory to the startup-config file on disk:

```
EX(config)#copy running-config startup-config
```

Related Commands **write memory**

database

Reconstruct or reset the traffic statistics database.

Syntax Description

```
database {reconstruct | reset}
{flow | traffic-stat | url}
```

Parameter	Description
reconstruct	Reconstruct the database.
reset	Clears the statistics counters.
flow	Traffic flow database.
traffic-stat	Traffic statistic database.
url	URL database.

Default None

Mode Configuration mode

enable-password

Set the enable password, which secures access to the Privileged EXEC mode (also called the Enable level) of the CLI.

Syntax Description

```
enable-password string
```

Parameter	Description
string	The password string.

Default None

Mode Configuration mode

Example The following command sets the enable password to “123456”:

```
EX(config)#enable-password 123456
```

Related Commands **enable**

flow asymmetric

Asymmetric routing can occur when packets take a path through the network from point A to point B and then use a different return path to return from point B to point A. This asymmetry can prevent the two-way visibility required by some applications to process their connection-oriented (TCP) flows. In prior releases, this lack of bi-directional visibility could prevent the EX appliance from being able to properly handle asymmetric flows.

The EX appliance supports asymmetric routing so that asymmetric flows can pass through the device unimpeded.

Syntax Description

```
[no] flow asymmetric
```

Default

This feature is enabled by default. To disable support for asymmetric routing, use the **no** form of this command.

Mode

Configuration mode

Usage

Asymmetric flows may have trouble being properly classified by classes that rely on L7 protocols for their match criteria. Some classification protocols must analyze packets in both directions in order to properly classify them, but when dealing with asymmetric flows, they only have traffic visibility in one direction. Please keep this in mind when using the “show flow” command, as the output may not accurately reflect the traffic you would expect to see if there are asymmetric flows on the EX appliance.

Example

Asymmetric routing is enabled by default. To disable the feature, use the following command:

```
EX(config)#no flow asymmetric
```

flow passby qos class

Set a QoS traffic class as a passby class. Traffic matching a passby class is simply forwarded, without any EX feature being applied.

Syntax Description

```
[no] flow passby qos class name [name [name ...]]
```

Parameter	Description
name	Name of a QoS class.

Default

N/A

Mode

Configuration mode

Usage

The normal form of this command sets one or more QoS traffic classes as passby classes.

The **no** form of this command removes the passby setting from the specified traffic class. If you do not specify a class name, the passby setting is removed from all traffic classes.

Example

The following command sets QoS class “http” as a passby class:

```
EX(config)#flow passby qos class http
```

flow semi-session

Enable (or disable) sessionless TCP flows to pass through the EX appliance, or change the default time period for which sessionless TCP flows can pass after the EX comes online.

Syntax Description

```
[no] flow semi-session [timeout minutes]
```

Parameter	Description
timeout *minutes*	You can specify 0-60 minutes. Selecting 0 will cause the EX to always allow sessionless TCP flows to pass through the device unimpeded.

Default

By default, the EX will allow sessionless TCP traffic to pass through for the first 5 minutes after the EX appliance comes online. This interval can be modified as needed.

Mode

Configuration mode

Usage

The **flow semi-session** command can be used to prevent the EX from terminating sessionless TCP flows after the device first comes online.

If this feature is disabled, booting the EX device in a network with many TCP-based flows will cause those flows to be terminated because the EX will not be able to find an associated session in the session pool. The EX will drop packets until a new connection is established.

Example

By default, the sessionless passthrough feature is enabled for the first 5 minutes after the EX comes online. If you wish to disable the feature, use the following command:

```
EX(config)#no flow semi-session
```

Example

You can change the amount of time the EX will allow sessionless TCP flows to pass after the EX comes online. To alter the duration from the default value of 5 minutes to one hour, use the following command:

```
EX(config)#flow semi-session timeout 60
```

hostname

Set the EX device’s hostname.

Syntax Description

```
[no] hostname string
```

Default

EX

Mode

Configuration mode

Usage

The CLI command prompt also is changed to show the new hostname.

Example

The following command sets the hostname to “WANbalancer”:

```
EX(config)#hostname WANbalancer
WANbalancer(config)#
```

idle *protocol-or-class* timeout

Set the maximum number of seconds a TCP session can remain idle before the EX device terminates it.

Syntax Description

```
[no] idle
{icmp | ip proto num | qos class name | tcp | udp}
timeout seconds
```

Parameter	Description
icmp	Sets the idle timeout for ICMP sessions.
ip proto *num*	Sets the idle timeout for sessions of the specified IP protocol, 1-255.
qos class *name*	Sets the idle timeout for sessions in the specified QoS class.
tcp	Sets the idle timeout for TCP sessions.
udp	Sets the idle timeout for UDP sessions.
seconds	Maximum number of seconds a session can remain idle. You can specify an interval from 10-655340 seconds, in 10-second intervals. For example, 655330 is valid, but 655333 is not.

Default

The default depends of the session type:

- TCP – 600 seconds
- All other session types – 50 seconds

Mode

Configuration mode

Usage

When a new connection begins, the Layer 4 idle timeout is used. If the traffic is then classified into a QoS traffic class, the idle timeout is selected as follows:

- If the idle timeout is configured for both the traffic class and the protocol, the idle timeout configured for the class is used.
- If a session is classified into more than one class, the longest idle timeout configured for the session's classes is used.

Usage

Changes to the idle timeout configuration are applied to existing sessions by gradually updating the age time of each session.

ip2id idsentrie

Configure the EX device to obtain IP-to-ID mappings dynamically from an IDsentie or IDaccess device:

Syntax Description

```
[no] ip2id IDsentrie host {hostname | ip-address}
port port
[xmlport port]
username user-name password password
[interval minutes]
[latest minutes]
```

Parameter	Description
host *hostname* | *ip-address*	IP address or hostname of the IDsentrie or IDaccess device.
port *port*	Protocol port number used to communicate with the IDsentrie or IDaccess device, 1-65535. The same port number must be configured on the IDsentrie.
xmlport *port*	Protocol port number used to communicate with the XML interface on the IDsentrie or IDaccess device, 1-65535. The same port number must be configured on the IDsentrie or IDaccess device.
username *user-name*	Admin name to log onto the IDsentrie or IDaccess device.
password *password*	Admin password to log onto the IDsentrie or IDaccess device.

interval *minutes*	Interval at which IP-to-ID entries are retrieved from the IDsentrie or IDaccess device. Entries are updated on a periodic basis specified by the configured interval, 1-60 minutes. The default is 5 minutes.
latest *minutes*	Specifies how far back to retrieve records. For example, if you use 5 minutes (the default), records that were active within the last 5 minutes are retrieved. This parameter ensures that records that were active after the previous request interval but that are no longer active, are retrieved. You can specify 1 to 60 minutes.

Note: To ensure that all records are retrieved, set the **latest** parameter to the same value as the "Process account activity logs every" parameter on the EX appliance or IDaccess. (The "Process account activity logs every" parameter is set on the Identity Management General tab, accessed by selecting Identity Management > General.)

Default Not configured

Mode Configuration mode

Example The following command configures the EX device to use IDsentie 192.168.1.1 to obtain IP-to-ID mappings:

```
EX(config)#ip2id IDsentie host 192.168.1.1 port 80 username us1 password pas
```

ip2id static

Configure static IP-to-ID mappings.

Syntax Description

```
[no] ip2id static ip-address user-name
```

Parameter	Description
ip-address	IP address.
user-name	Username (ID) to map to the IP address.

Mode Configuration mode

Usage You can enter more than one IP-to-ID mapping on the same command line.

Example The following command config maps IP address 1.1.1.1 to user ID "user1":

```
EX(config)#ip2id static 1.1.1.1 user1
```

language

Set the language used in the GUI.

Syntax Description

```
[no] language {english | simple-chinese |
traditional-chinese | japanese | korean}
```

Default

English

locale

Set the CLI locale.

Syntax Description

```
locale {test | locale}
```

Default

en_US.UTF-8

Mode

Configuration mode

Usage

Use this command to configure the locale or to test the supported locales.

Example

The following commands test the Chinese locales and set the locale to zh_CN.GB2312:

```
EX(config)#locale test zh_CN
EX(config)#locale zh_CN.GB2312
```

logging buffered

Configure the size of the local logging buffer.

Syntax Description

```
logging buffered maximum-messages
```

Parameter	Description
maximum-messages	Logging buffer size, 10000-50000.

Default

30,000 messages

Mode

Configuration mode

Usage

The following command configures the size of the local logging buffer:

Example

The following command sets the logging buffer size to 20,000 messages:

```
EX(config)#logging buffered 20000
```

logging console

Configure the log message levels sent to the console.

Syntax Description

```
logging console severity-level
```

Parameter	Description

severity-level	Specifies the severity levels to log. You can enter the name or the number of the severity level.
	{**0**|**emergency**}
	{**1**|**alert**}
	{**2**|**critical**}
	{**3**|**error**}
	{**4**|**warning**}
	{**5**|**notification**}
	{**6**|**information**}
	{**7**|**debugging**}

Default

The default level is error.

Mode

Configuration mode

Usage

Sending low-level messages such as information or debugging messages to the console can affect system performance.

Example

This following command sets the log message level sent to the console to notification:

```
EX(config)#logging console notification
```

logging email

Configure the log message levels to sent by email.

Syntax Description

```
logging email severity-level
```

Parameter	Description

severity-level	Specifies the severity levels of log messages to send by email. You can enter the name or the number of the severity level.
	{**0** | **emergency**}
	{**1** | **alert**}
	{**2** | **critical**}
	{**5** | **notification**}

Default

Disabled

Mode

Configuration mode

Usage

All messages at the specified log level and higher are emailed. For example, if you specify alert (1), all alert and emergency messages are emailed.

Use the **logging email-address** command to specify the email addresses to which to send the log messages.

Example

The following command sets the log message level to be emailed to emergency messages only:

```
EX(config)#logging email emergency
```

logging email-address

Specify the email addresses to which to send event messages.

Syntax Description

```
[no] logging email-address email-address [...]
```

Parameter	Description
email-address	Specifies an email address. You can enter more than one address on the command line. Use a space between each address.

Default

None

Mode

Configuration mode

Usage

A maximum of 10 email addresses are supported.

Use the **logging email** command to specify the log severity levels to send by email.

Example

The following command sets two email addresses to which to send log messages:

```
EX(config)#logging email-address admin1@example.com admin2@example.com
```

Related Commands **logging email, ip smtp**

logging export

Export buffered log messages to a remote device.

Syntax Description **logging export [all]** *url*

Parameter	Description
all	Includes system support messages.
	Name of the file to use on the target server.
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: **tftp://***host/file* **ftp://**[*user*@]*host*[:*port*]**/***file* **scp://**[*user*@]*host***/***file* **rcp://**[*user*@]*host***/***file*

Default

None

Mode

Configuration mode

Usage

This command builds a compressed archive package file (tar, gzip) of the buffered log, and transfers it to the specified destination.

Example

The following command exports the buffered log to FTP server 192.168.0.2 using the anonymous user account:

```
EX(config)#logging export ftp://192.168.0.2/
```

Related Commands

`logging buffered`

logging facility

Enable logging facilities.

Syntax Description

```
[no] logging facility facility-name
```

Parameter	Description
facility-name.	Name of a log facility: **local0** **local1** **local2** **local3** **local4** **local5** **local6** **local7**

Default

The default facility is local0.

Mode

Configuration mode

Example

The following command enables logging facility local7:

```
EX(config)#logging facility local7
```

logging flow-control enable

Control handling of log messages when the logging buffer is full.

Syntax Description

```
[no] logging flow-control enable
```

Default

Disabled

Mode

Configuration mode

Usage

When flow control is disabled, messages are dropped.

When flow control is enabled, messages are saved on an external data store.

Older messages replace newer ones. Depending on the state of logging flow control, the oldest messages are deleted or copied to an external data store to make room for new messages.

Example The following command enables logging flow control:

```
EX(config)#logging flow-control enable
```

logging host

Specify an external syslog server to which to send log messages.

Syntax

```
[no] logging host ipaddr [port protocol-port]
```

Parameter	Description
ipaddr	IP address of the syslog server.
port *protocol-port*	Protocol port number to which to send messages.

Default The default protocol port is 514.

Mode Configuration mode

Usage A maximum of 2 syslog servers are supported.

Example The following command configures log server 192.168.10.10:

```
EX(config)#logging host 192.168.10.10
```

Related Commands **logging syslog**

logging monitor

Configure the log message level to send to monitor (Telnet and SSH) CLI sessions.

Syntax Description

```
logging monitor severity-level
```

Parameter	Description
severity-level	Specifies the severity levels to log. You can enter the name or the number of the severity level.

{**0**|**emergency**}
{**1**|**alert**}
{**2**|**critical**}
{**3**|**error**}
{**4**|**warning**}
{**5**|**notification**}
{**6**|**information**}
{**7**|**debugging**}

Default

debugging

Mode

Configuration mode

Example

The following command sets the log message level to send to monitor sessions to emergency only:

```
EX(config)#logging monitor emergency
```

logging syslog

Configure the log message levels to send to external syslog servers.

Syntax Description

```
logging syslog severity-level
```

Parameter	Description

severity-level	Specifies the severity levels to log. You can enter the name or the number of the severity level.
	{**0**|**emergency**}
	{**1**|**alert**}
	{**2**|**critical**}
	{**3**|**error**}
	{**4**|**warning**}
	{**5**|**notification**}
	{**6**|**information**}
	{**7**|**debugging**}

Default

Disabled

Mode

Configuration mode

Usage To configure the external syslog server, use the **logging host** command.

Example The following command sets the log message level to send to external syslog servers to emergency only:

```
EX(config)#logging syslog emergency
```

logging trap

Configure the severity levels for which to send traps:

Syntax Description

```
logging trap severity-level
```

Parameter	Description

severity-level	Specifies the severity levels to log. You can enter the name or the number of the severity level.
	{**0**|**emergency**}
	{**1**|**alert**}
	{**2**|**critical**}

Default Disabled

Mode Configuration mode

Example The following command sets the trap level to emergency only:

```
EX(config)#logging trap emergency
```

Related Commands **snmp-server**

ntp

Configure Network Time Protocol (NTP) parameters.

Syntax Description

```
[no] ntp server {hostname | ipaddr} [minutes]

[no] ntp {disable | enable}
```

Parameter	Description
hostname | *ipaddr*	Hostname or IP address of the NTP server.
minutes	Synchronization interval, which specifies how often the EX device polls the NTP server for

	updated time information. You can specify 1-518400 minutes.
disable	Disables synchronization with the NTP server.
enable	Enables synchronization with the NTP server.

Default NTP synchronization is disabled by default. If you enable it, the default interval is 1440 minutes.

Mode Configuration mode

Example The following commands configure NTP server 22.22.22.22, change the synchronization interval to 500 minutes, and enable NTP:

```
EX(config)#ntp server 22.22.22.22 500
EX(config)#ntp enable
```

restore

Restore the startup-config file from a backup. The restored configuration takes effect following a reboot.

Syntax Description

```
restore url
```

Parameter	Description
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: **tftp://***host/file* **ftp://**[*user*@]*host*[**:***port*]**/***file* **scp://**[*user*@]*host/file* **rcp://**[*user*@]*host/file*

Mode Configuration mode

Usage Do not save the configuration (**write memory**) after restoring the startup-config. If you do, the startup-config will be replaced by the running-config and you will need to restore the startup-config again.

To place the restored configuration into effect, reboot the EX device.

The **no** form of this command is invalid.

Example

The following command uses TFTP to restore the configuration from a backup file on a remote server:

```
EX(config)#restore tftp://1.1.1.1/backup_1
```

Related Commands

backup

reload

Reload the system or to cancel a pending reload.

Syntax

```
reload
[text |
in [hh:]mm [text] |
at hh:mm [month day | day month] [text] |
cancel]
```

Parameter	Description
text	Reason for the reboot, 1-255 characters long.
in [*hh*:]*mm*	Schedule a reboot to take effect in the specified minutes or hours and minutes. The reboot must take place within approximately 24 hours.
at *hh*:*mm*	Schedule a reboot to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reboot is scheduled to take place at the specified time and date. If you do not specify the month and day, the reboot takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reboot for command: .
month	Name of the month, any number of characters in a unique string.
day	Number of the day, 1-31.
cancel	Cancel a scheduled reboot.

Default

None

Mode

Privileged EXEC mode

Usage

Use this command to reload the system or to cancel a pending reload.

Example The following command schedules a reboot for 12:00 p.m.:

```
EX#reload at 12:00
```

raid

Enter the configuration level for RAID.

Syntax

```
raid
```

CAUTION! RAID configuration should be performed only by or with the assistance of A10 Networks. A10 strongly advises that you do not experiment with these commands.

shutdown

Schedule a system shutdown or cancel a pending shutdown.

Syntax

```
shutdown {at hh:mm | in hh:mm | cancel [text]}
```

Parameter	Description
at	Shutdown at a specific time/date (*hh*:*mm*)
in	Shutdown after time interval (*mmm* or *hh*:*mm*)
cancel	Cancel pending shutdown
text	Reason for shutdown

Default None

Mode Privileged EXEC mode

Usage Use this command to shutdown the system.

Example The following command schedules a system shutdown to occur at 11:59 p.m.:

```
EX#shutdown at 23:59
```

snmp-server community

Configure an SNMP community string.

Syntax

```
[no] snmp-server community
read ro-community-string
[oid oid-value]
[remote {hostname | ipaddr mask-length}]
```

Parameter	Description
ro-community-string	The read-only community string.
oid *oid-value*	Object ID. This option restricts the objects that the EX device returns in response to GET requests. Values are returned only for the objects within or under the specified OID.
remote {*hostname* | *ipaddr mask-length*}	Restricts SNMP access to a specific host or subnet. When you use this option, only the specified host or subnet can receive SNMP data from the EX device by sending a GET request to this community.

Default

The configuration does not have any default SNMP communities. When you configure one, all OIDs are allowed by default and all remote hosts are allowed by default.

Mode

Configuration mode

Usage

All SNMP communities are read-only. Read-write communities are not supported.

The **no** form removes the read-only community string.

Example

The following commands enable SNMP, define community string "A10_EX", and restrict access to hosts in subnet 10.10.20.x/24 and to EX MIB objects only:

```
EX(config)#snmp-server enable
EX(config)#snmp-server community read A10_EX oid ExMgmt remote 10.10.20.0 24
```

Related Commands

snmp user

snmp-server contact

Configure SNMP contact information.

Syntax

```
[no] snmp-server contact contact-name
```

Parameter	Description
contact-name	The contact person's name.

Default Empty string

Mode Configuration mode

Usage The **no** form removes the contact information.

Example The following command defines the contact person as "snmp-admin":

```
EX(config)#snmp-server contact snmp-admin
```

Related Commands **snmp-server location**

snmp-server enable

Enable the EX device to accept SNMP MIB data queries and to send SNMP v1/v2c traps.

Syntax Description

```
[no] snmp-server enable [traps]
```

Default The SNMP service is disabled by default and all traps are disabled by default.

Mode Configuration mode

Example The following command enables the SNMP service and all EX traps:

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

snmp-server group

Configure an SNMP group.

Syntax Description

```
[no] snmp-server group group-name {v1 | v2c | v3
{auth | noauth | priv}} read view-name
```

Parameter	Description
group-name	Specifies the name of the SNMP group.
v1	Uses the least secure of the security models.
v2c	Uses the second-least secure of the security models.
v3	Uses the most secure of the security models.
auth	Uses packet authentication but does not encrypt the packets. (This is the authNoPriv security level.)
noauth	Does not use any authentication of packets. (This is the noAuthNoPriv security level.)
priv	Uses packet authentication and encryption. (This is the authPriv security level.)
view-name	Specifies the name of a read-only view for accessing the MIB object values.

Default The configuration does not have any default SNMP groups.

Mode Configuration mode

Example The following commands add SNMP v3 group “group1” with authPriv security and read-only view “view1”:

```
EX(config)#snmp-server group group1 v3 priv read view1
```

Related Commands **snmp-server view**

snmp-server host

Configure an SNMP v1/v2c trap receiver.

Syntax

```
[no] snmp-server host trap-receiver
[version {v1 | v2c}]
community-string
[udp-port port-num]
```

Parameter	Description
trap-receiver	Hostname or IP address of the remote device to which traps will be sent.
version {v1 | v2c}	SNMP version. If you omit this option, the trap receiver can use SNMP v1 or v2c.

community-string	Community string for the traps.
port-num	UDP port to which the EX device will send the traps.

Default No SNMP hosts are defined. When you configure one, the default SNMP version is v2c and the default UDP port is 162.

Mode Configuration mode

Example The following command configures SNMP trap receiver 100.10.10.12 to use community string “public” and UDP port 166 for SNMP v2c traps.

```
EX(config)#snmp-server host 100.10.10.12 public udp-port 166
```

snmp-server location

Configure SNMP location information.

Syntax

```
[no] snmp-server location location
```

Parameter	Description
location	The location of this EX device.

Default Empty string

Mode Configuration mode

Usage The **no** form removes the location information.

Example The following command configures the location as “A10-HQ”:

```
EX(config)#snmp-server location A10-HQ
```

Related Commands **snmp-server contact**

snmp-server user

Configure SNMP user-based groups.

Syntax

```
[no] snmp-server user username group groupname
{v1 | v2 | v3 [auth {md5 | sha} password
[encrypted]]}
```

Parameter	Description
username	Specifies the SNMP user name.
groupname	Specifies the group to which the SNMP user belongs.
v1 | **v2c**	Specifies SNMP version 1 or v2c.
v3 [**auth** {**md5** | **sha**} *password* [**encrypted**]]	Specifies SNMP version 3 and the authentication to use. **md5** | **sha** – HMAC MD5 (**md5**) or HMAC SHA (**sha**). *password* [**encrypted**] – Password for SNMP messages. To encrypt the password, use the **encrypted** option.

Default

No SNMP users are configured by default. When you configure one, all remote hosts are allowed by default. For v3, there is no authentication by default.

Mode

Configuration mode

Usage

The SNMP group must be configured before you can use it in this command.

Example

The following command adds an SNMP user belonging to group “group1”. The SNMP version is 3 and the authentication method is HMAC MD5. The password is “12345678”. The password is not encrypted.

```
EX(config)#snmp-server user user1 group group1 v3 auth md5 12345678
```

Related Commands

snmp-server group

snmp-server view

Configure an SNMP view.

Syntax Description

```
[no] snmp-server view view-name oid [oid-mask]
{included | excluded}
```

Parameter	Description
view-name	SNMP views name.
oid	MIB view family name or OID.

oid-mask	OID mask. Use hex octets, separated by '.'.
included	MIB family is included in the view.
excluded	MIB family is excluded from the view.

Default None

Mode Configuration mode

Example The following command adds and SNMP view:

```
EX(config)#snmp-server view view1 1.3.6 included
```

tcpdump

Create and manage files containing network traffic.

Syntax Description

```
tcpdump write dump-file-name
[-adeflnNOpqRStuvxX] [-c count]
[-C file-size] [-F file]
[-i interface] [-m module] [-r file]
[-s snaplen] [-T type] [-U user] [-w file]
[-E algo:secret] [expression]
```

```
tcpdump
{list |
read dump-file-name |
export dump-file-name url |
remove dump-file-name}
```

Parameter	Description
write	Copies network traffic to a file.
list	Displays a list of the saved TCP dump files.
read	Displays the contents of the specified TCP dump file.
export *url*	Copies a TCP dump file to a remote server. The *url* specifies the file transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL:

	tftp://*host/file* **ftp:**//[*user*@]*host*[:*port*]/*file* **scp:**//[*user*@]*host/file* **rcp:**//[*user*@]*host/file*
remove	Erases the specified TCP dump file.

Default None

Mode Privileged EXEC mode

Usage Use these commands to collect traffic samples to analyze.

This command prints the headers of packets that match the specified options. By default, packets are printed to the terminal. To save the packets to a file instead, use the **-w** flag. To read packets from a saved TCP dump file, use the **-r** flag.

Unless you use the **-c** flag, the command will continue capturing packets until you interrupt the capture by pressing ctrl-C.

Example The following command starts a TCP dump file named “tcpdumpfile” that will capture 10 packets:

```
EX#tcpdump write tcpdumpfile -c 10
tcpdump: WARNING: fpga0: no IPv4 address assigned
tcpdump: listening on fpga0, link-type EN10MB (Ethernet), capture size 96 bytes
```

tcp-reset

Configure TCP reset settings.

Syntax Description `[no] tcp-reset [window seconds]`

Parameter	Description
window *seconds*	Specifies the number of seconds after bootup during which the EX device sends TCP resets for all TCP packets that are beyond session creation. This behavior immediately informs any host applications that previously had connections that the connections are broken and need to be re-established. You can specify 0-86400 seconds. If you specify 0, TCP resets are disabled.

Default The default is 0 seconds (disabled).

Mode

Configuration mode

Usage

The TCP reset option sends a TCP reset (RST) to the endpoints of a TCP session through the EX device, when the session is cleared on the EX device. This option helps the endpoints of the TCP session to clear the session more quickly. Without this option, the other devices might not clear the session until it times out on those devices, even though the session has already been cleared on the EX device.

terminal

Set the terminal configuration.

Syntax

```
[no] terminal {auto-size | editing |
history [size number] | idle-timeout minutes |
length number | width lines}
```

Parameter	Description
auto-size	Automatically adjusts the length and width of the terminal display.
editing	Enables command editing.
history [**size** *number*]	Enables the command history and specifies the number of commands it can contain, 0-1000.
idle-timeout *minutes*	Specifies the number of minutes a CLI session can be idle before it times out and is terminated, 0-60 minutes. To disable timeout, enter 0.
length *number*	Specifies the number of lines to display per page, 0-512. To disable paging, enter 0.
width *lines*	Specifies the number of columns to display, 0-512. To use an unlimited number of columns, enter 0.

Default

This command has the following defaults:

- **auto-size** – enabled
- **editing** – enabled
- **history** – enabled, for up to 256 commands
- **idle-timeout** – 10 minutes

- **length** – 24 lines
- **width** – 80 columns

Mode Configuration mode

Example The following example sets the idle-timeout to 30 minutes:

```
EX(config)#terminal idle-timeout 30
```

trunk

Configure a trunk group, which is a single logical link consisting of multiple physical Ethernet interfaces.

Syntax

```
[no] trunk num
```

This command changes the CLI to the configuration level for the specified trunk, where the following trunk-related commands are available:

Command	Description
`[no] bind [management] ethernet portnum [to portnum] [ethernet portnum] ...`	Adds ports to the trunk and enables them.
`[no] disable [management] ethernet portnum [to portnum] [ethernet portnum] ...`	Disables ports in the trunk but does not remove them from the trunk.
`[no] method lb-method`	Specifies the method used to load-balance traffic across the interfaces in the trunk. You can specify one of the options listed in Table 1.

TABLE 1 Load Balance Trunk Load Balancing Methods

Load Balancing Method	Unicast Traffic Is Load-Balanced Based On...
src-mac	Source MAC address
dst-mac	Destination MAC address
src-dst-mac	Source and destination MAC addresses
src-ip	Source IP address
dst-ip	Destination IP address
src-dst-ip	Source and destination IP addresses
src-port	Source Layer 4 protocol port
dst-port	Destination Layer 4 protocol port
src-dst-port	Source and destination Layer 4 protocol ports
vlanID	VLAN ID
src-ip-port	Source IP protocol port
dst-ip-port	Destination IP protocol port
src-dst-ip-port	Source and destination IP protocol ports
src-ip-vlan	Source IP address and VLAN ID
dst-ip-vlan	Destination IP address and VLAN ID
src-dst-ip-vlan	Source and destination IP address and vlan ID
src-ip-port-vlan	Source IP address, source Layer 4 protocol port, and VLAN ID
dst-ip-port-vlan	Destination IP address, source Layer 4 protocol port, and VLAN ID
src-dst-ip-port-vlan	Source and destination IP address, source Layer 4 protocol port, and VLAN ID

Default N/A

Mode Configuration mode

Usage The EX device supports a maximum of 4 trunks. Each trunk can contain a maximum of 8 physical Ethernet interfaces. An Ethernet interface can be a member of only a single trunk.

When you add an Ethernet interface to a trunk, the following settings are replaced with those set on the trunk:

- IP address
- MAC address
- Speed configuration
- Mode (duplex, half-duplex, and so on)
- MTU size

Operations such as setting an IP interface or VLAN are performed on the lead member of the trunk, which is the lowest-numbered interface. For example, to configure an IP interface on a trunk containing ports 1-4, add the interface to port 1.

Multicast traffic is load balanced as follows:

- Multicast traffic that includes Layer 4 information – load balanced based on source IP address, source Layer 4 protocol port, destination IP address, and destination Layer 4 protocol port
- Multicast traffic without Layer 4 information – load balanced based on source and destination IP addresses
- Non-IP multicast traffic – load balanced based on source and destination MAC addresses

Notes

- It is recommended not to use an HA interface in a trunk. If an interface in a trunk is also configured for High Availability (HA), HA operations can change interface settings such as MAC address and IP address. In this case, the interface's HA settings may conflict with the trunk settings.
- When configuring a trunk, be careful if adding the management interface to the trunk. If you add the interface your GUI or CLI management session is using to a trunk, your management session will end and you will lose management access on that interface.

vlan

Create, edit, or delete a Virtual LAN (VLAN).

Syntax Description

```
[no] vlan vlan-id
```

Parameter	Description
vlan-id	VLAN ID, 1-4094.

This command changes the CLI to the configuration level for the specified VLAN, where the following VLAN-related commands are available:

Command	Description
[**no**] **tagged ethernet** *port-num* [**ethernet** *port-num* ... | **to** *port-num*]	Adds tagged member interfaces to the VLAN. Tagging allows an interface to belong to more than one VLAN.
[**no**] **untagged ethernet** *port-num* [**ethernet** *port-num* ... | **to** *port-num*]	Adds untagged member interfaces to the VLAN. Untagged interfaces can belong to only one VLAN.

Default

By default, no VLANs are configured on the EX device.

Mode

Configuration mode

Usage

VLANs logically segment the EX device into different LANs.

VLAN IDs 0 and 4095 are reserved. You cannot configure these VLANs.

You can configure up to 64 VLANs on an EX device.

If an IP address is configured on an interface, the interface cannot be added to a VLAN.

Example

The following command adds VLAN 9 and enters the configuration level for it:

```
EX(config)#vlan 9
EX(config-vlan:9)#
```

Example

The following command adds Ethernet interfaces 1-12 to VLAN 2 as tagged members of the VLAN:

```
EX(config-vlan:2)#tagged ethernet 1 to 12
```

Example

The following command adds Ethernet interfaces 1-12 to VLAN 2 as untagged members of the VLAN:

```
EX(config-vlan:2)#untagged ethernet 1 to 12
```

Related Commands

show vlans, **show mac vlan**

update cf

Copy the currently running system image from the hard disk to the compact flash (CF) card.

Syntax Description

```
update cf
```

Mode

Configuration mode

Example

The following command updates the CF card:

```
EX(config)#update cf
```

Related Commands

`show cf`

upgrade app-protocol library

Upgrade the L7 signature library module without performing a full software upgrading (which requires a reboot and can impact traffic).

Syntax Description

```
upgrade app-protocol library url
```

Parameter	Description
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: **tftp://***host***/***file* **ftp://**[*user*@]*host*[**:***port*]**/***file* **scp://**[*user*@]*host***/***file* **rcp://**[*user*@]*host***/***file*

Default

None

Mode

Configuration mode

Usage

The EX device supports non-disruptive Layer 7 signature library updates that do not require reboot of the box. As new signatures are added to the library, the library can be updated at a convenient time, and existing traffic flows are unaffected.

Example The following command upgrades the library using SCP:

```
EX(config)#upgrade app-protocol library scp://root:joe@10.10.10.3/L7sigFile
```

upgrade system

Upgrade the system.

Syntax Description **upgrade system** *url*

Parameter	Description
url	File transfer protocol, username (if required), and directory path. You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL: **tftp://***host***/***file* **ftp://**[*user*@]*host*[**:***port*]**/***file* **scp://**[*user*@]*host***/***file* **rcp://**[*user*@]*host***/***file*

Default None

Mode Configuration mode

Usage Make sure to save the configuration first. You can use the **write memory** or **copy running-config startup-config** command.

Example The following command upgrades the system by loading a file using SCP:

```
EX(config)#upgrade scp://root:123456@192.168.3.33/upgradefile
```

Example The following example uses TFTP to upgrade the system image:

```
EX(config)#upgrade tftp://192.168.1.144/ax2k_upg_1_2_0_107.tgz
```

write memory

Save the running configuration in memory to the startup-config file on disk.

Syntax Description **write memory**

Default None

Mode

Configuration mode

Example

The following command saves the configuration:

```
EX(config)#write memory
```

write terminal

Display the running configuration (running-config) on the terminal.

Syntax Description

`write terminal`

Default

None

Mode

Privileged EXEC mode

Usage

This command is equivalent to **show running-config**.

Example

The following command displays the running configuration:

```
EX#write terminal
Building configuration...

Current configuration : 16051 bytes
!Configuration last updated at 19:51:58 IST Mon Mar 31 2008
!Configuration last saved at 01:49:55 GMT Wed Mar 12 2008

version 2.1.0
!
hostname EX2100
!
clock timezone Europe/Dublin
!
no ntp enable
!
vlan 10
 untagged ethernet 3 ethernet 4
!
ips group ips1
 icmp ping maxlength
!
interface ethernet 1
 speedduplex auto
--MORE--
```

Related Commands

`show running-config`

Show Commands

show abuser-log

Display the logging messages for abusers.

Syntax Description

```
show abuser-log
[
start-time mm/dd/yyyy hh:mm:ss |
end-time mm/dd/yyyy hh:mm:ss |
start-id num |
end-id num |
ip address |
mac address |
user name |
host name |
criteria name |
action filter value
]
```

Parameter	Description
start-time *mm/dd/yyyy hh*:*mm*:*ss*	Shows only entries posted at or later than the specified date and time.
end-time *mm/dd/yyyy hh*:*mm*:*ss*	Shows only entries posted earlier than or at the specified date and time.
start-id *num*	Starting ID with value ranging from 0-2,147,483,647.
end-id *num*	Starting ID with value ranging from 0-2,147,483,647.
ip *address*	IP address filter.
mac *address*	MAC address filter.
user *name*	Username filter.
host *name*	Hostname filter.
criteria *name*	Criteria name filter value. Wildcard characters ***** and **?** are supported.

action *filter value*	Displays log entries only for actions that match the fallin or fallout filter value. The filter value is a string and can contain ? (match any one character) and * (match any string of characters) wildcard characters.

Default None

Mode All

show admin

Show information about admin accounts.

Syntax Description **show admin** [*admin1* [*admin2*...]] [**detail**]

Parameter	Description
detail	Displays detailed information.

Mode All

Example The following commands show summary information about all admin accounts, then show detailed information about account “adminuser99”:

```
EX(config)#show admin
UserName                        Status    Privilege
-------------------------------------------------------
admin                           Enabled   Root
adminuser99                     Enabled   Read only

EX(config)#show admin adminuser99 detail
  User Name               ...... adminuser99
  Status                  ...... Enabled
  Privilege               ...... Read only
  Trusted Host(Netmask)   ...... Any
  Lock Status             ...... No
  Lock Time               ......
  Unlock Time             ......
  Password Type           ...... Encrypted
  Password                ...... $1$5a786dfc$QRQ1Pw2xO9wUmQYetSihc.
```

show aflex

Display information for the aFleX scripts on the EX device.

Syntax Description

show aflex [*filename*]

Parameter	Description
filename	Displays the aFleX script file. If you omit this option, the list of aFleX script files is displayed instead.

Mode

All

Example

The following command shows a list of the aFleX scripts on the EX device:

```
EX(config)#show aflex
Total aFlex number: 1
Max aFlex file size: 32K
Name                             Syntax   Qos class
------------------------------------------------------------
http-manual                      Check    Bind
```

In this example, only one aFleX script is on the EX device. The display shows the following information for each aFleX script:

- Syntax – Indicates whether the script passed the syntax check performed by the EX device when you imported the script or configured it using the GUI.
- QoS class – Indicates whether the aFleX script is bound to a match rule for a QoS class.

Example

The following command shows the contents of the script file:

```
EX(config)#show aflex http-manual
Name:                    http-manual
Syntax:                  Check
Qos class:               Bind
Statistics:
    Event CLIENT_DATA          execute 0 times (0 failures, 0 aborts)
    Event SERVER_DATA          execute 0 times (0 failures, 0 aborts)
Content:
when CLIENT_DATA {
    if { [IP::addr [IP::client_addr] equals 192.168.3.39] } {
        matchaflex
        return
    } elseif { [IP::addr [IP::server_addr] equals 192.168.3.39] } {
        matchaflex
        return
    } elseif { [TCP::payload] contains "a10networks.com"} {
        matchaflex
        return
    }
    if { [UDP::payload] starts_with "OK" } {
        matchaflex
        return
    }
}

when SERVER_DATA {
    if { [IP::protocol] == 50 } {
        matchaflex
        return
    }
}
```

The script filename, syntax status, and QoS class binding status are shown at the top of the output, followed by the contents of the script file.

show applog

Show application log messages stored in the local buffer.

Syntax Description

```
show applog
[setting]
[archive]
[start-time mm/dd/yyyy hh:mm:ss]
[end-time mm/dd/yyyy hh:mm:ss]
[app-user filter-value]
[user filter-value]
[action filter-value]
[action-detail filter-value]
[alias alias-name]
[aim] [msnim] [yim] [ftp] [nfs] [cifs] [smtp]
[pop3] [qq] [http]
```

Parameter	Description
setting	Displays the configured application log settings.
archive	Displays the application log archive statistics.
start-time *mm/dd/yyyy hh*:*mm*:*ss*	Specifies the beginning of the time span for which to display application log entries.

end-time *mm/dd/yyyy hh*:*mm*:*ss*

Specifies the end of the time span for which to display application log entries.

app-user *filter-value*

Displays log entries only for application user names that match the filter value. The filter value is a string and can contain **?** (match any one character) and ***** (match any string of characters) wildcard characters.

user *filter-value*

Displays log entries only for user names that match the filter value. The filter value is a string and can contain **?** (match any one character) and ***** (match any string of characters) wildcard characters.

action *filter-value*

Displays log entries only for actions that match the filter value. The filter value is a string and can contain **?** (match any one character) and ***** (match any string of characters) wildcard characters.

action-detail *filter-value*

Displays log entries only for application details that match the filter value. The filter value is a string and can contain **?** (match any one character) and ***** (match any string of characters) wildcard characters.

alias *alias-name*

Displays log entries only for application names that are mapped to the specified alias.

aim

Displays log entries only for AOL Instant Messenger.

msnim

Displays log entries only for Microsoft Instant Messenger.

yim

Displays log entries only for Yahoo Instant Messenger.

ftp

Displays log entries only for File Transfer Protocol.

nfs

Displays log entries only for Network file system.

cifs Displays log entries only for Common Internet File System.

smtp Displays log entries only for Simple Mail Transfer Protocol.

pop3 Displays log entries only for Post Office Protocol v3.

qq Displays log entries only for Tencent Instant Messaging.

http Displays log entries only for HTTP.

Mode All

Usage The EX device can store up to 50000 log messages in the local buffer.

Related Commands **applog alias**

show arp

Display ARP table entries.

Syntax Description **show arp** [*ip-address* [*ip*-address…]]

Default None

Mode All

Example The following command displays MAC entries:

```
EX#show arp
IP Address          MAC Address          Type          Interface
--------------------------------------------------------------
192.168.12.1        0009.0F03.DD7B       Dynamic       ve10
192.168.12.18       0090.0B0A.D921       Dynamic       ve10
192.168.12.99       0290.0B0A.D921       Dynamic       ve10
...
```

Related Commands **arp**

show bypass

Display the current port bypass settings.

Note: This command applies only to models EX 1100 and EX 2110.

Syntax Description `show bypass interface-pair [1 | 2 | all]`

Parameter	Description
`1 | 2 | all`	Specifies the bypass pair: **1** – Displays the hardware bypass state for Ethernet interfaces 1 and 2. **2** – Displays the hardware bypass state for Ethernet interfaces s 3 and 4. **all** – Displays the hardware bypass state for both pairs (1-2, 3-4).

Mode All

Example The following command shows the current settings for port bypass:

```
EX#show bypass interface-pair
Interface                      Bypass
-------------------------------------
1,2                            Enabled
3,4                            Disabled
```

Related Commands `bypass interface-pair`

show cf

Display the system image version installed on the compact flash (CF). If the EX device is unable to boot from the hard disk (HD), the EX device attempts to boot from the CF instead.

Syntax Description `show cf`

Mode All

Example The following command shows the system image version installed on the CF:

```
EX#show cf
Software Version: 2.1.0
Build: 722
```

show clb group

Display information about a CLB group.

Syntax Description

show clb group [*name* [*name* ...]] [**detail**]

Parameter	Description
name	CLB group name.
detail	Displays detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

If you are at the configuration level for a CLB group, you also can display information about the group by entering the **show this** command.

Example

The following commands display information about CLB group “Squid-CacheGrp”:

```
EX(config)#show clb group SquidCacheGrp
Name                 Method               # of nodes
SquidCacheGrp        Round Robin          2
EX(config)#show clb group SquidCacheGrp detail
Name:                SquidCacheGrp
Method:              Round Robin
Persistent:          Disabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show clb node

Display information about CLB nodes.

Syntax Description

show clb node [*name* [*name* ...]] [**detail**]

Parameter	Description
name	CLB node name.
detail	Displays detailed information.

Default

None

Mode All

Usage There is no **no** or **default** form of this command.

If you are at the configuration level for a CLB node, you also can display information about the node by entering the **show this** command.

Example The following commands display information for CLB node “SquidCache”:

```
EX(config)#show clb node SquidCache
Name            Type       IP              Status     Curr Conn  Total Conn
SquidCache      Cache      10.0.0.2        Stopped    0          0
EX(config)#show clb node detail SquidCache
Name:                SquidCache
Type:                Cache
Status:              Stopped
IP Addr:             10.0.0.2
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show clock

Display the time, timezone, and date.

Syntax Description

```
show clock [detail]
```

Parameter	Description
detail	Shows the clock source, which can be one of the following: – Time source is NTP – Time source is user configuration

Default None

Mode All

Example The following command shows clock information for an EX device:

```
EX#show clock detail
20:27:16 Europe/Dublin Sat Apr 28 2007
Time source is NTP
```

Example

If a dot appears in front of the time, the EX device has been configured to use NTP but NTP is not synchronized. The clock was in sync, but has since lost contact with all configured NTP servers.

```
EX#show clock
.20:27:16 Europe/Dublin Sat Apr 28 2007
```

Example

If an asterisk appears in front of the time, the clock is not in sync or has never been set.

```
EX#show clock
*20:27:16 Europe/Dublin Sat Apr 28 2007
```

show coredump

Display a core dump.

Syntax Description

```
show coredump
```

Default

None

Mode

All

Example

The following command shows the first page of output for a core dump:

```
EX#show coredump

-------------------a10wa core dump information------------------------

-------------------file 1------------------------
GNU gdb 6.6
Copyright (C) 2006 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i686-pc-linux-gnu"...
Using host libthread_db library "/lib/libthread_db.so.1".
Core was generated by `./a10wa'.
Program terminated with signal 11, Segmentation fault.
#0  0xffffe410 in __kernel_vsyscall ()
(gdb)   6 process 3399  0xffffe40e in __kernel_vsyscall ()
  5 process 3400  0xffffe40e in __kernel_vsyscall ()
  4 process 3401  0xffffe40e in __kernel_vsyscall ()
  3 process 3402  0xffffe40e in __kernel_vsyscall ()
  2 process 3403  0xffffe40e in __kernel_vsyscall ()
* 1 process 3394  0xffffe410 in __kernel_vsyscall ()
(gdb) [Switching to thread 1 (process 3394)]#0  0xffffe410 in __kernel_vsyscall
()
--MORE--
```

show cpu

Display current CPU usage.

Syntax Description

```
show cpu [interval]
```

Parameter	Description
`interval`	Periodically samples CPU utilization and continues until you press Ctrl+C. Without this this option, samples for the most recent 1-second, 5-second, 10-second, 30-second, and 60-second intervals are shown.

Default

None

Mode

All

Example

The following command shows CPU usage statistics for intervals as far back as the last 60 seconds:

```
EX#show cpu
Time:18:08:43.375 PST Mon Nov 24 2008
            1Sec    5Sec    10Sec   30Sec   60Sec
--------------------------------------------------------
CPU    0    4.8%    4.7%    4.8%   11.3%    9.8%
CPU    1    0.0%    0.0%    0.0%    0.0%    0.0%
CPU    2    0.0%    0.0%    0.0%    0.0%    0.0%
CPU    3    0.0%    0.0%    0.0%    0.0%    0.0%
```

Example

The following command shows continual real-time CPU usage statistics:

```
EX#show cpu interval
CPU Number: 4
CPU Usage: (press ^C to quit)
-----------------------------
CPU0    CPU1    CPU2    CPU3
5.8%    0.0%    0.1%    0.0%
5.5%    0.0%    0.0%    0.0%
6.1%    0.0%    0.0%    0.0%
6.5%    0.0%    0.0%    0.0%
5.5%    0.0%    0.5%    0.0%
6.1%    0.0%    0.0%    0.0%
6.0%    0.0%    0.0%    0.0%
2.6%    0.0%    0.0%    0.0%
6.5%    0.0%    0.0%    0.0%
...
```

show debug

Display debug information.

Syntax Description

```
show debug
[packet capture dump [dump-file] detail]
```

Default None

Mode All

Example The following command lists the debug options that are currently enabled:

```
EX#show debug
SYS
  SYSTEM session debugging is on
  SYSTEM config debugging is on
  SYSTEM process debugging is on
  SYSTEM monitor debugging is on
  SYSTEM time debugging is on
  SYSTEM dns debugging is on
  SYSTEM dhcp debugging is on
  SYSTEM other debugging is on
MGMT
  MGMT system debugging is on
```

show default

Display the default configuration settings of the EX device.

Syntax Description

```
show default
```

Default None

Mode All

Example The following command displays the health monitor settings that are configured by default:

```
EX#show default | section health
health method ping icmp
health monitor ping method ping
```

Note: The “**| section health**” portion of the command is an output filter. See “Searching and Filtering CLI Output” on page 30.

show disk

Display hard disk usage information.

Syntax Description

```
show disk
```

Default

None

Mode

All

Example

The following command shows hard disk usage information:

```
EX#show disk

Disk Usage: (size is MB)
------------------------
  Total      Used       Free       Usage
  74600      127        74472      0.1%
```

show dnat

Display information about destination Network Address Translation (NAT).

Syntax Description

```
show dnat qos class [class-name]
```

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

Example

The following example displays destination NAT information for QoS traffic class "test".

```
EX(config)#show dnat qos class test
dnat qos class test 10.0.0.10
```

show dns

Display DNS information.

Syntax Description

```
show dns {cache | local-domain [domain-name] |
proxy-server | proxy-setting}
```

Default

None

Mode

All

Example

The following command shows the DNS proxies configured on the EX device:

```
EX(config)#show dns proxy-server
    10.10.10.66  example.com
```

show environment

Display temperature, fan, and power supply status.

Syntax Description

`show environment`

Default

None

Mode

All

Example

The following command shows environment information for an EX device:

```
EX#show environment
Physical CPU1 temperature: 64C / 147F
Physical CPU2 temperature: 63C / 145F
Fan1 speed: 5487 R p.m.
Fan2 speed: 5152 R p.m.
Voltage(+12V): 12.220V
Voltage(+5V): 5.103V
Power1(Upper): ON
Power2(Lower): OFF
```

show flow counters

Display flow counters.

Syntax Description

`show counters`

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

Example The following example displays current global traffic counters.

```
EX>show flow counters
IP ingress:                    2524345871 (bytes) / 3109855 (pkts)
  IP fragments:                  0 (bytes) / 0 (pkts)
  IP broadcast:                  633918 (bytes) / 2805 (pkts)
  Non IP:                        4498560 (bytes) / 74976 (pkts)
  Local:                         7236468 (bytes) / 101983 (pkts)
  ------------------------------------------
  Inbound:                       1760743973 (bytes) / 1722872 (pkts)
  Outbound:                      759975817 (bytes) / 1351649 (pkts)
  Inbound (suspect):             677 (bytes) / 6 (pkts)
  Outbound (suspect):            0 (bytes) / 4 (pkts)
  Internal sameside:             0 (bytes) / 0 (pkts)
  External sameside:             0 (bytes) / 0 (pkts)
  ------------------------------------------
  Inbound connections:           1499 (opened) / 1498 (closed)
  Outbound connections:          30221 (opened) / 30215 (closed)
  Inbound connections (suspect): 2 (opened) / 2 (closed)
  Outbound connections (suspect): 3 (opened) / 3 (closed)
  Internal sameside connections: 0 (opened) / 0 (closed)
  External sameside connections: 0 (opened) / 0 (closed)
```

show flow passby qos class

Displays all passby classes

Syntax Description **show flow passby qos class**

Default None

Mode All

Usage There is no **no** or **default** form of this command.

Example The following command displays all the QoS traffic classes set as passby classes.

```
EX#show flow passby qos class
Passby QoS classes:
   http
```

show flow sessions

Display currently active sessions.

Syntax Description

```
show flow sessions
[age seconds]
[asymmetric]
[counters]
[fwd-dip ip-address]
[fwd-dport port]
[fwd-sip ip-address]
[fwd-sport port]
[max num]
[proto {tcp | udp}]
[rev-dip ip-address]
[rev-dport port]
[rev-sip ip-address]
[rev-sport port]
[semi-session]
```

Parameter	Description
age *seconds*	Current age of the session, 10-655340 seconds.
asymmetric	Shows asymmetric sessions only.
counters	Shows summary connection statistics.
fwd-dip *ip-address*	Destination IP address of the forward direction.
fwd-dport *port*	Destination port of the forward direction.
fwd-sip *ip-address*	Source IP address of the forward direction.
fwd-sport *port*	Source port of the forward direction.
max *num*	Maximum number of sessions to include in the output, 1-100000. The default is 10000.
proto {**tcp** | **udp**}	Protocol of the session, TCP or UDP.
rev-dip *ip-address*	Destination IP address of the reverse direction.
rev-dport *port*	Destination port of the reverse direction.
rev-sip *ip-address*	Source IP address of the reverse direction.
rev-sport *port*	Source port of the reverse direction.

semi-session	Shows semi-sessions only.

Default

N/A

Mode

All

Example

The following command displays currently active sessions:

```
EX#show flow sessions
Proto   Age    Dir    IF     Source                 Destination            Class
TCP     570    fwd(A) eth1   192.168.3.137:1339     119.96.86.160:26000    others
               rev(S) eht2   119.96.86.160:26000    192.168.3.137:1339
```

show fwlb

Display the FWLB placement configuration of the EX device.

Syntax Description

show fwlb

Default

None

Mode

All

Usage

Optional parameters for this command (for example, **group**) are described in other sections.

There is no **no** or **default** form of this command.

Example

The following command displays the FWLB placement information:

```
EX>show fwlb
Fwlb enable:          Enabled
Fwlb peer:            10.10.10.99/255.255.255.255
```

show fwlb group

Display information about FWLB groups.

Syntax Description

show fwlb group [*name* [*name...*]] [**detail**]

Parameter	Description
name	FWLB group name.
detail	Displays detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

If you are at the configuration level for an FWLB group, you also can display information about the group by entering the **show this** command.

Example

The following commands display information about FWLB group “WebServiceFwGrp”:

```
EX(config)#show fwlb group WebServiceFwGrp
Name                 Method                 # of nodes
WebServiceFwGrp      Round Robin            3
EX(config)#show fwlb group WebServiceFwGrp detail
Name:                WebServiceFwGrp
Method:              Round Robin
Persistent:          Disabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show fwlb node

Display information about FWLB nodes.

Syntax Description

`show fwlb node` `[`*`name`*` [`*`name`*` ...]] [`**`detail`**`]`

Parameter	**Description**
name	Firewall node name.
detail	Shows detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

If you are at the configuration level for an FWLB node, you also can display information about the node by entering the **show this** command.

Example

The following commands display information about FWLB node “SanJoseHQ”:

```
EX>show fwlb node SanJoseHQ
Name            Type       IP              Status     Curr Conn  Total Conn
SanJoseHQ       Firewall   10.0.0.2        Stopped    0          0
EX>show fwlb node SanJoseHQ detail
Name:                    SanJoseHQ
Type:                    Firewall
Status:                  Stopped
IP Addr:                 10.0.0.2
Mask:                    255.255.255.255
Connection Limit:        0
Weight:                  1
Health Monitor:          ping
Enable/Disable:          Enabled
Sent:                    0 (bytes) / 0 (packets)
Received:                0 (bytes) / 0 (packets)
Current Connection:      0
Total Connection:        0
```

Example

The following command displays detailed information for the current FWLB node:

```
EX(config-fwlb node:SanJoseHQ)#show this
Name:                    SanJoseHQ
Type:                    Firewall
Status:                  Stopped
IP Addr:                 10.0.0.2
Mask:                    255.255.255.255
Connection Limit:        0
Weight:                  1
Health Monitor:          ping
Enable/Disable:          Enabled
Sent:                    0 (bytes) / 0 (packets)
Received:                0 (bytes) / 0 (packets)
Current Connection:      0
Total Connection:        0
```

show gui

Display the status of “Easy QoS GUI” feature.

Syntax Description `show gui`

Default None

Mode All

Usage

QoS configuration has been divided into two modes: (1) advanced mode and (2) simplified mode. The simplified mode, also referred to as "Easy QoS GUI", removes the concepts of ingress and egress and no longer requires QoS Policies to be bound to QoS Interfaces.

New installations will automatically default to the simplified QoS configuration mode, but existing deployments configured using the legacy approach will remain in advanced mode.

Example

To display the QoS configuration mode, use the following command:

```
EX(config)#show gui
GUI Settings:
Simple QoS Policy............Enabled
```

show ha

Show the status of HA synchronization.

Syntax Description

show ha sync

Default

N/A

Mode

All

Example

The following command displays the HA synchronization state on an EX device:

```
EX(config)#show ha sync
HA sync is not activated
```

show health external

Show information about external health monitoring programs.

Syntax Description

show health external
[*program-name* [*program-name* ...]]

Parameter	Description
program-name	Program name.

Default

N/A

Mode

All

Example The following command displays information about all external health monitoring programs imported onto the EX device:

```
EX#show health external
External Program                Description
http_sample.tcl                 The http sample script
ping_sample.tcl                 The ping sample script
```

Related Commands health external

show health method

Display configuration information for health methods.

Syntax Description **show health method** [*name* [*name* ...]]

Parameter	Description
name	Health method name.

Default None

Mode All

Example The following command shows configuration information for health methods “ping” and “http”.

```
EX(config)#show health method ping http
Method Name:   ping
Type:          ICMP

Method Name:   http
Type:          HTTP
Attribute:     port=80
               url="GET /"
```

show health monitor

Display health monitor configuration information.

Syntax Description **show health monitor** [*name* [*name* ...]]

Parameter	Description
name	Health monitor name.

Default None

Mode All

Example

The following commands shows configuration information for monitors “ping” and “http”:

```
EX(config)#show health monitor ping http
Monitor Name     Interval   Retries    Timeout    Method           Status
ping             30         3          5          ping             BUSY
http             30         3          5          http             IDLE
```

show health stat

Display health monitoring statistics.

Syntax Description

`show health stat`

Default

None

Mode

All

Example

The following command shows health monitoring statistics:

```
EX(config)#show health stat
Health monitor statistics
Total run time:               : 307 hours 2868 seconds
Opened socket:                : 184445
Open socket failed:           : 0
Close socket:                 : 184442
Send packet:                  : 110665
Send packet failed:           : 0
Receive packet:               : 0
Receive packet failed         : 0
Retry times:                  : 73776
Timeout:                      : 331986
Unexpected error:             : 0

IP address                    Port  Health monitor  Status Cause(Up/Down/Retry)
------------------------------------------------------------------------------
10.0.0.2                             ping            Down   0/7/73776
192.168.12.10                  8080  tcp-connect     Down   0/15/0
192.168.12.10                        http8080        Down   0/5/0
192.168.12.4                   8080  tcp-connect     Down   0/0/0
192.168.12.4                         http8080        Down   0/0/0
```

show history

Show the CLI command history for the current session.

Syntax Description

```
show history
```

Default None

Mode All

Usage Commands are listed starting with the oldest command, which appears at the top of the list.

Example The following command lists the commands entered during the current CLI session:

```
EX#show history
   en
   show
   show clock
   show cpu
   debug sys all
   debug management all
   show debug
   show disk
   show history
```

show idle

Shows timeout settings for idle sessions.

Syntax Description

```
show idle timeout
{
icmp |
ip proto num |
qos class name |
tcp |
udp
}
```

Parameter	Description
icmp	Displays the idle timeout for ICMP sessions.
ip proto *num*	Displays the idle timeout for IP sessions of the specified IP protocol, 1-255.

qos class *name*	Displays the idle timeout for QoS sessions of the specified class.
tcp	Displays the idle timeout for TCP sessions.
udp	Displays the idle timeout for UDP sessions.

Mode All

show interfaces

Display information about EX interfaces.

Syntax Description

show interfaces
[[**ethernet** [*port-num* ...]] | [**ve** [*vlan-id* ...]] |
brief | **detail**]

Parameter	Description
brief	Displays summary information.
detail	Displays detailed information.

Mode Privileged EXEC mode

Example The following command displays summary information for the device's interfaces:

```
EX#show interface brief
Port        Link Protocol  Dupl  Speed        MAC        IP Address       Total IPs
------------------------------------------------------------------------------
ethernet1    DOWN   UP     FULL  0     0090.0B08.8511  0.0.0.0/0              0
ethernet2    DOWN   UP     FULL  0     0090.0B08.8510  0.0.0.0/0              0
ethernet3    UP     UP     FULL  1000  0090.0B08.850F  0.0.0.0/0              0
ethernet4    UP     UP     FULL  1000  0090.0B08.850E  0.0.0.0/0              0
ethernet5    DOWN   UP     FULL  0     0090.0B08.8549  0.0.0.0/0              0
ethernet6    DOWN   UP     FULL  0     0090.0B08.8548  0.0.0.0/0              0
ethernet7    DOWN   UP     FULL  0     0090.0B08.8547  0.0.0.0/0              0
ethernet8    UP     UP     FULL  100   0090.0B08.8546  192.168.42.1/24        1
ethernet9    DOWN   UP     FULL  0     0090.0B09.89D1  0.0.0.0/0              0
--MORE--
```

Example The following command displays detailed information about Ethernet interfaces 3 and 4:

```
EX#show interface ethernet 3 4 detail
ethernet3 is up, line protocol is up
  Hardware is Ethernet, address is 0090.0B08.850F
  No ip address assigned
  MTU is 1500 bytes, Bandwidth is 1000 Mbit
  Full-Duplex, speed is 100 Mb/s, auto negotiation enabled
  RX packets:907768 errors:0 dropped:0 overruns:0 frame:0
  TX packets:810379 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:100
  RX bytes:808160689 (770.7 M), TX bytes:328905781 (313.7 M)
  QoS shaping rate: 1000 Kbps
      Average rate: 0 Kbps
      Queue length: 0
      Dropped packets: 0

ethernet4 is up, line protocol is up
  Hardware is Ethernet, address is 0090.0B08.850E
  No ip address assigned
  MTU is 1500 bytes, Bandwidth is 1000 Mbit
  Full-Duplex, speed is 1000 Mb/s, auto negotiation enabled
  RX packets:796785 errors:0 dropped:0 overruns:0 frame:0
  TX packets:901858 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
--MORE--
```

Related Commands **interface**

show ip

Display IP configuration information.

Syntax Description

```
show ip
{
dns |
http |
interface
  [ethernet port-num [port-num ...] |
   ve vlan-id [vlan-id ...] | detail] |
ospf [neighbor] |
rip |
route [ospf | rip |
  ip-address {subnet-mask | /mask-length} |
reply-same-interface [sessions | stats]] |
smtp
}
```

Default None

Mode All

Example The following commands show DNS, HTTP, and SMTP configuration information:

```
EX#show ip dns
DNS suffix: localdomain
Primary server: 1.1.1.1
Secondary server: 2.2.2.2
EX#show ip http
HTTP:
         Idle TimeOut.............10 minutes
         Http Port................80
         Https Port...............443
         Auto Redirect............Enabled
         Https....................Enabled
         Http.....................Enabled
EX#show ip smtp
SMTP:
         SMTP SERVER .............<Not configured>
         SMTP PORT................25
```

Example The following commands show sessions information and statistics for management reply traffic routed using the **reply-same-interface** option.

```
EX#show ip route reply-same-interface sessions
Proto Age           Local             Destination       Interface
TCP   20     172.21.116.81:40155  216.190.168.95:443    ethernet3
TCP   50     172.21.116.81:26289   217.70.54.211:2608   ethernet3
TCP   40     172.21.131.21:64350     8.22.48.67:80      ethernet4
TCP   50     172.21.131.21:64206     8.22.48.67:80      ethernet4
ICMP  10      12.10.182.40:49825    12.175.178.9:0      ethernet1
ICMP  40      12.10.182.40:23307     12.229.87.1:8      ethernet1
TCP   40      12.10.182.40:36719    24.68.41.137:62127  ethernet1
UDP   30     172.21.131.21:64332    58.251.60.53:8000   ethernet4
UDP   30     172.21.116.81:33378     68.94.156.1:53     ethernet3
...

EX#show ip route reply-same-interface stats
Connection number: 262144
Connection free:   262116
Connection used:   28
Connection memory: 8388608
Box number:        256
Box size:          1024
Box memory:        2048
Hash size:         262144
Hash memory:       2097152
```

show ip2id cache

Show the IP-to-ID mappings in the ID-to-ID cache.

Syntax Description

```
show ip2id cache
```

Default

None

Mode

All

show ippool

Display information about IP address pools.

Syntax Description

```
show ippool [name]
```

Default

None

Mode

All

Usage

The output is the same as the output of **show ippool** *name*, where *name* is the name of this IP pool.

There is no **no** or **default** form of this command.

If you are at the configuration level for the IP pool, you also can display information about the pool by entering the **show this** command.

Example

The following example displays information about IP pool “test”.

```
EX(config-IP pool)#show ippool test
ippool test
   ip 192.168.3.13
   ip 192.168.3.50 to 192.168.3.60
```

show ips action

Show IPS actions taken by the EX device.

Syntax Description

```
show ips action
```

Default

None

Mode

All

show ips counters

Show counters for IPS filters.

Syntax Description

show ips counters
[**ethernet** *portnum* [**ethernet** *portnum* ...]]

Default

None

Mode

Privileged EXEC mode

Example

The following command shows counters for all Ethernet interfaces:

```
EX#show ips counters
IPS Statistics of the system is:
    hold source ip :                            0
    ping of death :                             0
    unknown protocol :                          0
    ip land :                                   0
    syn fragment :                              0
    tcp check flag :                            0
    icmp broadcast echo request :               0
    udp broadcast echo request :                0
    icmp broadcast :                            0
    ip record route option :                    0
    ip strict source route option :             0
    ip security option :                        0
    ip loose source route :                     0
    ip malformed option :                       0
    ip with option :                            0
    ip time stamp option :                      0
    ip stream option :                          0
    ip fragment packet :                        0
    syn flood :                                 0
    icmp type :                                 0
    icmp flood :                                0
    tcp flood :                                 0
    udp flood :                                 0
    icmp address sweep :                        0
    udp address sweep :                         0
    port scan :                                 0
    exceed rate destination :                   0
    exceed rate source :                        0
```

show l7 cache

Display traffic flows in the EX device’s Layer 7 cache.

After the EX device classifies a new flow of traffic, an entry for the traffic flow is placed in the cache. The EX device uses the cache entry to optimize forwarding of subsequent traffic in the flow.

Syntax Description

```
show l7 cache [ip ipaddr [port protocol-port]]
```

Parameter	Description
ip *ipaddr*	Server IP address.
port protocol-port	Protocol port on the server.

Default

None

Mode

All

Example

The following command shows Layer 7 cache entries for server 192.168.1.51:

```
EX#show l7 cache ip 192.168.1.51
Server IP                  Port       Protocol
192.168.1.51               80         http
192.168.1.51               443        ssl
```

show llb

Display LLB configuration information.

Syntax Description

```
show llb
```

Default

None

Mode

All

Usage

Optional parameters for this command (for example, **group**) are described in other sections.

There is no **no** or **default** form of this command.

If you are at the configuration level for an LLB domain, you also can display information about the domain by entering the **show this** command.

Example

The following command displays global LLB configuration information:

```
EX#show llb
Proximity mask:                        255.255.240.0
rtt agetime:                           300
Default group:
```

show llb domain

Display information for LLB domains.

Syntax Description

show llb domain [*domain* [*domain* ...]] [**detail**]

Parameter	Description
domain	Domain name fragment, 1-127 characters.
detail	Shows detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

Example

The following commands display information for domain "a10networks.com":

```
EX>show llb domain a10networks.com
Domain                   Policy     # of hosts
a10networks.com          Include    0
EX#show llb domain a10networks.com detail
Domain:                  a10networks.com
Policy:                  Include
```

show llb link

Display information about LLB links.

Syntax Description

show llb link [*name* [*name* ...]] [**detail**]

Parameter	Description
name	LLB link name. If you omit this option, information is displayed for all configured LLB links.
detail	Shows detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

If you are at the configuration level for an LLB link, you also can display information about the link by entering the **show this** command.

Example

The following commands display information about link “ISP1”:

```
EX>show llb link ISP1
Name            Gateway              Status     Curr Conn  Total Conn
ISP1            10.10.10.1           Down       0          0
EX>show llb link ISP1 detail
Name:                ISP1
Status:              Down
Gateway:             10.10.10.1
Mask:                255.255.255.0
Source NAT           Enable
Bandwidth:           1000 (kbps)
Price:               unlimited        1000
Connection Limit:    0
Weight:              1
Health Monitor:
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (pkts)
Received:            0 (bytes) / 0 (pkts)
Upstream:            0 (kbps) / 0 (pps)
Downstream:          0 (kbps) / 0 (pps)
Current Connection:  0
Connetion/sec:       0
Total Connection:    0
```

Example

The following example displays the current LLB link’s detailed information.

```
EX(config-llb link:ISP1)#show this
Name:                ISP1
Status:              Down
Gateway:             10.10.10.1
Mask:                255.255.255.0
Source NAT           Enable
Bandwidth:           1000 (kbps)
Price:               unlimited        1000
Connection Limit:    0
Weight:              1
Health Monitor:
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (pkts)
Received:            0 (bytes) / 0 (pkts)
Upstream:            0 (kbps) / 0 (pps)
Downstream:          0 (kbps) / 0 (pps)
```

```
Current Connection:  0
Connetion/sec:       0
Total Connection:    0
```

show llb group

Display LLB group information.

Syntax Description

show llb group [*name* [*name* ...]] [**detail**]

Parameter	Description
name	LLB group name. If you omit this option, information about all groups is displayed.
detail	Shows detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

If you are at the configuration level for an LLB group, you also can display information about the group by entering the **show this** command.

Example

The following commands display information about LLB group “llb-group-1”:

```
EX>show llb group llb-group-1
Name                    Method                  # of links
llb-group-1             Round Robin             3
EX>show llb group llb-group-1 detail
Name:                   llb-group-1
Method:                 Round Robin
Persistent:             Disabled
Sent:                   0 (bytes) / 0 (packets)
Received:               0 (bytes) / 0 (packets)
Curr Conn:              0
Total Conn:             0
```

show llb persistent

Show information for LLB persistence.

Syntax Description

show llb persistent {*group-name* {*link-name*}}

show llb rtt

Display collected RTT information.

Syntax Description

```
show llb rtt [link name [ipaddr] | ipaddr]
```

Parameter	Description
name	Name of an LLB link.
ipaddr	IP address whose RTT is to be displayed.

Default

None

Mode

All

Usage

RTT collection is enabled only after **round-trip-time** is set as the load balancing method for an LLB group.

RTT information ages out based on the setting of the **llb rtt agetime** command.

There is no **no** or **default** form of this command.

Example

The following command displays RTT information for IP address 10.0.0.2:

```
EX>show llb rtt 10.0.0.2
Prefix                            Gateway             RTT (ms)
255.255.240.0                     10.10.10.1          27
```

Related Commands

`llb group`, `method` (`llb group`), `llb rtt agetime`

show locale

Display the configured CLI locale.

Syntax Description

```
show locale
```

Default

None

Mode

All

Example

The following command shows the locale configured on an EX device:

```
EX#show locale
en_US.UTF-8
```

show log

Display the logging configuration or messages in the logging buffer.

Syntax Description

```
show log
[
setting |
system |
ips |
start-time mm/dd/yyyy hh:mm:ss |
end-time mm/dd/yyyy hh:mm:ss |
detail string |
severity-level
]
```

Parameter	Description
setting	Shows the configuration settings for the system log.
system	Shows log entries related to the running system, and not related to IPS. These logs can be due to user logins, general messages related to processing failures, configuration-related information, and so on.
ips	Shows log entries for packets that matched and were dropped by Intrusion Protection System (IPS) filters.
start-time *mm/dd/yyyy* *hh*:*mm*:*ss*	Shows only entries posted at or later than the specified date and time.
end-time *mm/dd/yyyy* *hh*:*mm*:*ss*	Shows only entries posted earlier than or at the specified date and time.
detail *string*	Filters the list to display only the entries that contain the specified string, 1-127 characters. You can use the following wildcards in the string: **?** – Matches any single character ***** – Matches any string of characters

severity-level Specifies the severity levels to log. You can enter the name or the number of the severity level.

{**0** | **emergency**}

{**1** | **alert**}

{**2** | **critical**}

{**3** | **error**}

{**4** | **warning**}

{**5** | **notification**}

{**6** | **information**}

{**7** | **debugging**}

Default None

Mode All

Example The following command show system log settings:

```
EX#show log setting
Console logging: level error
Buffer logging: level debugging
Email logging: disable
Trap logging: disable
Syslog logging: disable
Monitor logging: level debugging

Syslog host: NULL
Syslog email address: NULL
Syslog facility: local0
Log flow-control disable

Log Buffer (30000 items):
```

Example The following command show system log entries that contain the string “report:, generated at or later than 2 p.m. on March 30, 2008:

```
EX#show log system detail *report* start-time 03/30/2008 14:00:00
Mar 31 19:00:39    err      Sending email failed for scheduled report based on
report template test1
Mar 31 18:00:39    err      Sending email failed for scheduled report based on
report template test1
Mar 31 17:00:40    err      Sending email failed for scheduled report based on
report template test1
Mar 31 16:00:40    err      Sending email failed for scheduled report based on
report template test1
Mar 31 15:00:39    err      Sending email failed for scheduled report based on
report template test1
```

```
Mar 31 14:00:40    err      Sending email failed for scheduled report based on
report template test1
Mar 31 13:00:39    err      Sending email failed for scheduled report based on
report template test1
Mar 31 12:00:38    err      Sending email failed for scheduled report based on
report template test1
Mar 31 11:00:37    err      Sending email failed for scheduled report based on
report template test1
Mar 31 10:00:37    err      Sending email failed for scheduled report based on
report template test1
```

show mac

Show MAC entries in the run-time forwarding database.

Syntax

show mac [**vlan** *vlan-id* [*macaddr*]]

Option	Description
vlan *vlan-id*	Shows the MAC table entries only for the specified VLAN.
macaddr	Shows the MAC table entry only for the specified MAC address within the specified VLAN.

Example

The following command shows the MAC entries for VLAN 10:

```
EX#show mac vlan 10
VLAN   Interface    MAC Address        Type         Aging Timer
-----------------------------------------------------------------
10     ethernet3    0090.0B08.850F     Static       0.0
10     ethernet4    0030.1BB9.EA00     Dynamic      0.16
10     ethernet4    0030.1BB9.E990     Dynamic      23.16
10     ethernet4    0090.0B08.850E     Static       0.0
10     ethernet4    0290.0B0A.D921     Dynamic      22.1
10     ethernet3    0009.0F03.DD7B     Dynamic      0.0
10     ethernet4    0030.1BBA.3340     Dynamic      18.20
10     ethernet4    0030.1BB9.E98F     Dynamic      98.74
10     ethernet4    0090.0B0A.D921     Dynamic      0.73
-----------------------------------------------------------------
Total entries: 9
```

Related Commands

show vlans

show memory

Display memory usage information.

Syntax Description `show memory`

Default None

Mode All

Example The following command shows memory usage statistics:

```
EX#show memory

Memory Usage: (size is KB)
--------------------------
         Total      Used       Free       Buffers    Cached     Usage
Memory:  1032736    777740     254996     220088     88904      45.3%
```

show ntp

Show the Network Time Protocol (NTP) configuration and status.

Syntax Description `show ntp {status | associations [detail]}`

Parameter	Description
status	Shows NTP status information (enabled or disabled).
associations	Shows the NTP server IP address and synchronization interval.

Default None

Mode All

Example The following commands configure NTP and show NTP information:

```
EX(config)#ntp server 72.232.103.184
EX(config)#ntp enable
EX(config)#show clock
18:43:32.071 PDT Tue Jul 1 2008
EX(config)#show ntp status
NTP sync status: enabled
```

show packet

Show packet drop counters.

Syntax Description **show packet drop counters**

Default None

Mode All

show port (on real servers)

Display information about SLB ports on the current SLB node.

Note: This command is available at the configuration level for SLB nodes.

Syntax Description **show port** [{**tcp** | **udp**} [*port* [*port* ...]]] [**detail**]

Parameter	Description
port	Port number, 1-65535.
detail	Displays detailed information.

Default None

Mode SLB real server configuration mode

Usage There is no **no** or **default** form of this command.

If you are at the configuration level for an SLB port, you also can display information about the port by entering the **show this** command.

Example The following commands display information about a specific SLB port on the current node:

```
EX(config-slb node:apache)#show port tcp 80
Node            Protocol        Port       Status     Curr Conn  Total Conn
apache          TCP             80         Running    0          0
EX(config-slb node:apache)#show port tcp 80 detail
Node:                apache
Protocol:            TCP
Port:                80
Status:              Running
Connection Limit:    0
Weight:              1
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (packets)
```

```
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show port (on virtual servers)

Display information about virtual ports on the current virtual server.

Note: This command is available at the configuration level for SLB virtual servers.

Syntax Description

```
show port [{tcp | udp} [port [port ...]]] [detail]
```

Parameter	Description
port	Port number or well-known port name.
detail	Displays detailed information.

Default None

Mode SLB virtual server configuration mode

Usage There is no **no** or **default** form of this command.

Example The following command displays information about a specific port on the virtual server:

```
EX(config-slb virtual server:VirtualSer...)#show port tcp 80 detail
Virtual Server:      VirtualServer
Protocol:            TCP
Port:                80
Service:             WebServerGrp
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show process

Display system process information.

Syntax Description

```
show process
```

Default None

Mode All

Example The following command displays system process information:

```
EX#show process
  PID  PPID %CPU %MEM    VSZ   RSS   STACKP TTY      START   TIME STAT COMMAND
    1     0  0.0  0.0   1480   516 bfe64130 ?        Mar27   0:45 S    init
    2     1  0.0  0.0      0     0 00000000 ?        Mar27   0:00 S    migration/0
    3     1  0.0  0.0      0     0 00000000 ?        Mar27   0:00 SN   ksoftirqd/0
    4     1  0.0  0.0      0     0 00000000 ?        Mar27   0:00 S    watchdog/0
    5     1  0.0  0.0      0     0 00000000 ?        Mar27   0:00 S    migration/1
...
```

show qos abuser

Show information about QoS abuser criteria.

Syntax Description **show qos abuser** [**criteria** [*criteria-name* ...]]

Mode All

show qos autodetect

Show the status (enable or disabled) for system-defined classes, such as vlan or internal-subnet.

Syntax Description **show qos autodetect**

Mode All

Example The following command shows the QoS autodetect options that are enabled:

```
EX#show qos autodetect
qos autodetect vlan
   enable
qos autodetect internal-interface
   enable
qos autodetect external-interface
   enable
qos autodetect internal-subnet
   disable
```

show qos category

Show QoS categories.

Syntax Description **show qos category** [*name* ...]

Mode All

show qos class

Show the QoS class configuration.

Syntax Description

```
show qos class
[class-name [class-name …]] |
[SystemConfigured] | [UserConfigured]
```

Parameter	Description
class-name	Shows configuration information for the specified class.
SystemConfigured	Shows configuration information for all classes configured by the system.
UserConfigured	Shows configuration information for all classes configured by EX admins.

Default

None

Mode

Privileged EXEC mode

Usage

If you are at the configuration level for a class, you also can display information about the class by entering the **show this** command.

Example

The following command shows configuration information for traffic class “flv”:

```
EX(config)#show qos class flv
qos class flv                      category Multimedia   (Policy defined)
   match (0) application http.content-type ~ "flash"
   match (1) application http.content-type ~ "flv"
   match (2) application http.content-type ~ "fcs"
   match (3) dport 1935
```

Related Commands

qos class

show qos domaingroup

Show QoS domain groups and the IP addresses associated with them.

Syntax Description

`show qos domaingroup` `[`*`name`*` ...]`

Example

The following command shows the domain names and IP addresses in domain group “dgroup1”:

```
EX#show qos domaingroup dgroup1
qos domain group dgroup1
       domain www.a10networks.com.cn
              ip 192.168.3.1
              ip  192.168.3.12
```

Note: IP addresses are listed only if they are returned in replies to DNS queries for the domain names.

show qos idgroup

Show QoS ID groups.

Syntax Description

`show qos idgroup` `[`*`name`*` ...]`

Mode

All

show qos interface

Show QoS interface configuration or counters.

Syntax Description

`show qos interface`
`[`*`name`*` [`*`name`*` ...] [`**`statistics`**` [`*`options`*`]]]`

Parameter	Description
name	QoS interface name.
statistics [*options*]	Displays detailed information. The following options are available. The options are nested. **egress | ingress** – Specifies the traffic direction. *class-name* – Specifies a hierarchical class name, in the following format: *class/subclass/subsubclass*.

perip [*ipaddr* | **top** *num*] – Lists information for specific IP addresses. For the **top** option, *num* can be 1-1000.

Default None

Mode Privileged EXEC mode

Usage If you are at the configuration level for the QoS interface, you also can display information about the interface by entering the **show this** command.

Example The following command shows configuration information for QoS interface “vt”:

```
EX(config)#show qos interface vt
qos interface vt
  port ethernet 1
     port ethernet 2
   shape 1000000
qos policy egress ftp
```

Example The following command shows statistics for QoS interface “bw-in”:

```
EX#show qos interface bw-in statistics

qos interface bw-in
  shape interface bw-in 20000
     Average Rate: 3177 Kbps
     Queue length: 0
     Dropped packets: 37
  bw-in ingress policy FW:
     Class: DNS-Permit prec 9
       Current rate:  0 Kbps
       Average rate : 0 Kbps
       Peak rate:  17 Kbps
       Active sessions : 1
     Class: dns prec 10
       Current rate:  0 Kbps
       Average rate : 0 Kbps
       Peak rate:  0 Kbps
       Active sessions : 0
       Dropped packets:  70080
     Class: default-class prec 10
       Current rate:  224 Kbps
       Average rate : 178 Kbps
       Peak rate:  20251 Kbps
       Active sessions : 798
...
```

Related Commands **qos interface**, **port ethernet**, **qos policy**, **shape**

show qos ip limit

Show QoS IP limits.

Syntax Description

```
show qos ip limit
[[ipaddress [ipaddr] | ip-list-name ...]
counters]
```

Mode

All

show qos iplist

Show the IP addresses in IP lists.

Syntax Description

```
show qos iplist [name [name ...]]
```

Parameter	Description
name	IP list name.

Default

N/A

Mode

Privileged EXEC mode

Usage

If you are at the configuration level for an IP list, you also can display information about the list by entering the **show this** command.

Example

The following command shows the IP addresses in IP list “test”:

```
EX#show qos iplist test
qos iplist test
  ip 192.168.9.2 to 192.168.9.10
  ip 192.168.9.15
  ip 192.168.9.20 to 192.168.9.30
```

show qos policy

Show policy configuration.

Syntax Description

```
show qos policy [policy-name [policy-name ...]]
```

Default

None

Mode

Privileged EXEC mode

Usage

If you are at the configuration level for the policy, you also can display information about the policy by entering the **show this** command.

Example

The following command shows the configuration of policy “test”:

```
 EX(config)#show qos policy test
qospolicy test
   class test prec 10
   class default-class prec 10
```

Related Commands

`qos policy`

show qos portlist

Show QoS port lists.

Syntax Description

```
show qos portlist [name ...]
```

Mode

All

show qos resource-limit

Show configured limit on the number of QoS classes that can be created by auto-detection feature, as a means of partitioning the available classes.

Syntax Description

```
show qos resource-limit class auto-created number
```

Mode

All

Example

The following command shows the maximum number of classes that can be created using auto-detection.

```
EX(config)#resource-limit class auto-created number
Resource limit for Auto-created class number
Current: 512
Maximum: 1024
```

show qos schedule

Show the QoS policy schedule.

Syntax Description

```
show qos schedule
```

Default

N/A

Mode Privileged EXEC mode

Example The following commands schedule some policies and show the schedule:

```
EX(config)#qos schedule http on vt egress 01:01 02:02 Mon Web Fri
EX(config)#qos schedule http on vt egress 03:03 04:04 Tue Thu
EX(config)#qos schedule http on vt egress 07:07 08:08
EX(config)#qos schedule http on vt ingress 01:01 02:02
EX(config)#qos schedule http on vt ingress 04:04 05:05
EX(config)#qos schedule http on vt ingress 10:10 11:11
EX(config)#show qos schedule
qos schedule http on vt ingress 01:01 02:02 Mon Web Fri
qos schedule http on vt ingress 04:04 05:05 Tue Thu
qos schedule http on vt ingress 10:10 11:11
qos schedule http on vt egress 01:01 02:02
qos schedule http on vt egress 03:03 04:04
qos schedule http on vt egress 07:07 08:08
```

show qos statistic memory

Display memory usage information for traffic statistics.

Syntax Description **`show qos statistic memory`**

Mode All

Example The following command shows memory usage information for traffic statistics:

```
EX(config)#show qos statistic memory
Type                     Memory         Blocks

Class                     914 KB          117
User                      416 Bytes         2
Other IP port               0 Bytes         0
Total memory              915 KB          119
Configure memory            8 MB
```

show qos tcp-window-adjust

Show whether TCP-window-adjust is enabled or disabled.

Syntax Description **`show qos tcp-window-adjust`**

Mode All

Usage The TCP Window Adjustment feature optimizes the flow of TCP packets across the network by modifying the window size in the header of an ACK packet as it passes through the EX appliance. The feature is disabled by default.

show qos top

Show traffic counters for QoS classes or categories, sorted by highest average rate.

Syntax Description

```
show qos top
{
category [sort-by | view] |
class [sort-by | view] |
num
}
```

Parameter	Description
category	Name of category.
class	Name of class.
num	Number of classes or categories for which to display counters, 1-63.

Default

By default, statistics for the 10 busiest classes are displayed.

Mode

Privileged EXEC mode

Usage

Statistics for both inbound and outbound traffic directions are displayed. Outbound means the packet comes in through the inside interface and is sent out by the outside interface. Inbound means the packet comes in through the outside interface and is sent out by the inside interface.

The exception is for same-side sessions. One inside interface on the server side is considered to be an outside interface.

Example

The following command shows counters for the busiest classes:

```
EX(config)#show qos top class

Top ten classes
qos class ssh :
   Inbound:  Curren rate: 86045Kbps, average rate: 59256Kbps, peak rate :95803Kbps
   Outbound: Curren rate: 1665 Kbps, average rate: 1208 Kbps, peak rate :2038 Kbps
qos class telnet :
   Inbound:  Curren rate: 51   Kbps, average rate: 352  Kbps, peak rate :1877 Kbps
   Outbound: Curren rate: 24   Kbps, average rate: 204  Kbps, peak rate :1081 Kbps
qos class http :
   Inbound:  Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :353  Kbps
   Outbound: Curren rate: 0    Kbps, average rate: 0    Kbps, peak rate :179  Kbps
```

show qos view

Show QoS views.

Syntax Description

```
show qos view [name ...]
```

Mode All

show radius

Display information about any currently running RADIUS servers.

Syntax Description

```
show radius server
```

Mode Privileged EXEC mode

Example The following command displays RADIUS server information:

```
EX(config)#show radius server
   Host                                       Authentication port    Accounting port
   192.168.10.10                               1812                   1813
```

show raid

Display RAID status.

Syntax Description

```
show raid
```

Mode All

Example The following command displays RAID status:

```
EX#show raid
Device: md0
   Primary Disk: Active
   Secondary Disk: Active
Device: md1
   Primary Disk: Active
   Secondary Disk: Active
```

show reload

Display scheduled system reboots.

Syntax Description

```
show reload
```

Default None

Mode All

Example The following command shows a scheduled reboot on the EX device:

```
EX#show reboot
Reboot scheduled for 04:20:00 PST Sun Apr 20 2008 (in 63 hours and 16 minutes)
by admin on 192.168.1.144
Reboot reason: Outlook_upgrade
```

Related Commands `reload`

show report alert-rule

Show alert rule information.

Syntax Description

```
show report alert-rule
[total-rate | user-rate | user-connection]
[rule-name]
```

Default N/A

Mode All

Usage If you specify an alert rule name, detailed information is displayed for the rule. If you do not specify an alert rule name, the configured alert rules are listed.

Example The following command lists all configured alert rules:

```
EX#show report alert-rule
Name            Type            Limit           Duration(min)   Notify Inter-
val(min)
==============================================================================
dang            Total Rate      0 Kbits/S       0               0
limit-total-traffic Total Rate      0 Kbits/S       0               0
```

Example The following command shows information for alert rule “limit-total-traffic”:

```
EX#show report alert-rule total-rate limit-total-traffic

     Alert rule type: Total rate
     Alert rule name: limit-total-traffic
       Boundary rate: 0 Kbits/S
            Duration: 0 minutes
     Notify Interval: 0 minutes
        Email Status: Enable
       Email Address: test1@a10networks.com,test2@a10networks.com
```

Related Commands `report alert-rule`

show report email

Show the email addresses to which reports are sent.

Syntax Description `show report email`

Mode All

show report history

Show the settings for report history.

Syntax Description `show report history`

Mode All

show resources

Show statistics for resource usage.

Syntax Description `show resources {application | lb | memory}`

Default None

Mode All

Example The following command shows the resource usage statistics for load balancing:

```
EX>show resources lb
Buffer Total:                            12288
Buffer Free:                             11409
Buffer Requested:                        4294241
Buffer Released:                         4293362
Buffer Ran out:                          0
Buffer No action:                        0
Buffer Double Released:                  0
Connection Total:                        1048576
Connection Free:                         1048575
Connection Requested:                    1
Connection Released:                     0
Connection Ran out:                      0
Connection Double Released:              0
```

```
------------------------------------------------
Link Slot Max:                           131
Link Slot Free:                          128
Link Configured:                         3
Node Slot Max:                           259
Node Slot Free:                          253
Node Configured:                         6
Real Port Slot Max:                      515
Real Port Slot Free:                     513
...
```

show resources lb

Display internal resource usage statistics.

Syntax Description `show resources lb`

Default None

Mode All

Usage There is no **no** or **default** form of this command.

This command is used primarily for debugging.

Example The following example displays internal resources usage statistics.

```
EX>show resources lb
Buffer Total:                            8192
Buffer Free:                             7561
Buffer Requested:                        3336171
Buffer Released:                         3335540
Buffer Ran out:                          0
Buffer No action:                        0
Buffer Double Released:                  0
Connection Total:                        1048576
Connection Free:                         1048567
Connection Requested:                    63525
Connection Released:                     63516
Connection Ran out:                      0
Connection Double Released:              0
------------------------------------------------
Link Slot Max:                           131
Link Slot Free:                          130
Link Configured:                         1
Node Slot Max:                           259
Node Slot Free:                          254
Node Configured:                         5
Real Port Slot Max:                      515
Real Port Slot Free:                     513
Real Port Configured:                    2
Group Slot Max:                          131
Group Slot Free:                         126
Group Configured:                        5
Virtual Server Slot Max:                 131
Virtual Server Slot Free:                127
Virtual Server Configured:               2
Virtual Port Slot Max:                   515
Virtual Port Slot Free:                  514
Virtual Port Configured:                 1
Domain Slot Max:                         64
Domain Slot Free:                        62
Domain Configured:                       2
```

show running-config

Display the running configuration.

Syntax Description `show running-config`

Default None

Mode All

Usage This command shows the configuration commands running in memory.

Example The following command shows the running configuration:

```
EX#show running-config
Building configuration...

Current configuration : 16051 bytes
!Configuration last updated at 19:51:58 IST Mon Mar 31 2008
!Configuration last saved at 01:49:55 GMT Wed Mar 12 2008

version 2.1.0
!
hostname EX2100
!
clock timezone Europe/Dublin
!
no ntp enable
!
vlan 10
 untagged ethernet 3 ethernet 4
!
ips group ips1
 icmp ping maxlength
!
```

```
interface ethernet 1
 speedduplex auto
--MORE--
```

show session admin

Display information about the currently active admin sessions.

Syntax Description **show session admin**

Default None

Mode All

Example The following command displays the currently active admin sessions:

```
EX#show session admin
ID    User Name   Start Time                    Source IP        Type   Cfg Mode
*19    admin       22:24:40 IST Mon Mar 31 2008   192.168.1.144     CLI     No
```

show shutdown

Display scheduled system shutdowns.

Syntax Description **show shutdown**

Default None

Mode All

Example The following command shows a scheduled shutdown on an EX device:

```
EX#show shutdown
Shutdown scheduled for 12:00:00 PST Sat Jan 19 2008 (in 358 hours and 23 min-
utes) by admin on 192.168.1.144
Shutdown reason: Scheduled shutdown
```

Related Commands **shutdown**

show slb group

Display information about SLB groups.

Syntax Description

```
show slb group
[{tcp | udp | any} [name [name ...]]] [detail]
```

Parameter	Description
tcp	Show groups with the TCP transport protocol type.
udp	Show groups with the **udp** transport protocol type.
any	Show groups with the **any** transport protocol type.
name	SLB group name.
detail	Displays detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

If you are at the configuration level for an SLB group, you also can display information about the group by entering the **show this** command.

Example

The following commands display SLB group information:

```
EX>show slb group
Name                 Type       Method               # of nodes/ports
WebServerGrp         Any        Weight Round Robin   2
WebServerGrp2        Any        Round Robin          3
EX(config)#show slb group any WebServerGrp detail
Name:                WebServerGrp
Type:                Any
Method:              Weight Round Robin
Persistent:          Disabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
Nodes:               apache
                     apache2
```

show slb node

Display information about SLB nodes.

Syntax Description

show slb node [*name* [*name* ...]] [**detail**]

Parameter	Description
name	SLB node name.
detail	Displays detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

Example

The following commands display information about a specific SLB node:

```
EX(config)#show slb node apache
Name            Type       IP              Status     Curr Conn  Total Conn
apache          Server     10.0.0.2        Stopped    0          0
EX(config)#show slb node apache detail
Name:                apache
Type:                Server
Status:              Stopped
IP Addr:             10.0.0.2
Mask:                255.255.255.0
Connection Limit:    0
Weight:              1
Health Monitor:      ping
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
Ports:
Node            Protocol        Port       Status     Curr Conn  Total Conn
apache          TCP             80         Running    0          0
```

show slb port

Display information about SLB ports.

Syntax Description

show slb port
[*name* [{**tcp** | **udp**} [*port* [*port* ...]]]] [**detail**]

Parameter	Description
name	SLB node name.
port	Protocol port number or well-known port name.
detail	Displays detailed information.

Default None

Mode All

Usage There is no **no** or **default** form of this command.

Example The following commands display information about a specific SLB port:

```
EX(config)#show slb port apache tcp 80
Node            Protocol        Port       Status     Curr Conn  Total Conn
apache          TCP             80         Running    0          0
EX(config)#show slb port apache tcp 80 detail
Node:                apache
Protocol:            TCP
Port:                80
Status:              Running
Connection Limit:    0
Weight:              1
Enable/Disable:      Enabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show slb virtual port

Display information about virtual ports.

Syntax Description

```
show slb virtual port
[name [{tcp | udp} [port [port ...]]]] [detail]
```

Parameter	Description
name	Virtual server name.
tcp	Displays information about TCP virtual ports.
udp	Displays information about UDP virtual ports.
port	Port number or well-known port name.
detail	Displays detailed information.

Default None

Mode All

Usage There is no **no** or **default** form of this command.

Example The following command displays detailed information for TCP port 80 on virtual server “VirtualServer”:

```
EX#show slb virtual port VirtualServer tcp 80 detail
Virtual Server:      VirtualServer
Protocol:            TCP
Port:                80
Service:             WebServerGrp
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
```

show slb virtual server

Displays information of SLB virtual server(s).

Syntax Description

```
show slb virtual server [name [name ...]] [detail]
```

Parameter	Description
name	Virtual server name.
detail	Displays detailed information.

Default None

Mode All

Usage The normal form of this command displays information of SLB virtual server(s); or if no "*name*" is specified, displays information for all SLB virtual servers. If "**detail**" is present, displays detailed information, or else just a summary.

There is no "**no**" or "**default**" form of this command.

If you are at the configuration level for an SLB virtual server, you also can display information about the virtual server by entering the **show this** command.

Example The following commands display information about virtual server “Virtual Server”:

```
EX(config)#show slb virtual server VirtualServer
Name                 Virtual IP      # of ports
VirtualServer        10.0.0.254      1
EX(config)#show slb virtual server VirtualServer detail
Name:                VirtualServer
Virtual IP:          10.0.0.254
Mask:                255.255.255.0
snat                 Disabled
Sent:                0 (bytes) / 0 (packets)
Received:            0 (bytes) / 0 (packets)
Current Connection:  0
Total Connection:    0
Ports:               TCP 80, WebServerGrp
```

show startup-config

Display the startup-config file.

Syntax Description **`show startup-config`**

Default None

Mode All

Usage This command shows the configuration commands saved on disk.

Example The following command displays the startup-config file:

```
EX#show startup-config
Building configuration...

Startup configuration : 15376 bytes
!Configuration last updated at 18:46:39 GMT Mon Mar 17 2008
!Configuration last saved at 01:49:55 GMT Wed Mar 12 2008

version 2.1.0
!
hostname EX
!
clock timezone Europe/Dublin
!
no ntp enable
!
vlan 10
 untagged ethernet 3 ethernet 4
!
!
interface ethernet 1
 speedduplex auto
 permit ssh http ping
```

```
!
--MORE--
```

show tcp-reset

Show TCP-reset settings.

Syntax Description `show tcp-reset`

show techsupport

Display system information for use when troubleshooting.

Syntax Description `show techsupport`

Default None

Mode All

show terminal

Show the terminal settings.

Syntax Description `show terminal`

Default None

Mode All

Example The following examples show terminal information

```
EX#show terminal
Idle-timeout is 00:10:00
Length: 29 lines, Width: 91 columns
Editing is enabled
History is enabled, history size is 256
Auto size is enabled
Terminal monitor is off
```

show throughput

Show aggregate-level throughput, connections per second, and packet per second data.

Syntax Description

```
show throughput
```

Mode

All

Example

The following command shows throughput statistics:

```
EX#show throughput
          total      inbound    outbound   sameside   sameside
                                           internal   external
==============================================================
bits/s    1.8G       455M       458M       502M       504M
packets/s 244K       38K        39K        83K        83K
conns/s   445        0          0          225        220
```

show traffic abuser

Show traffic statistics for network abusers.

Syntax Description

```
show traffic abuser top base-on {ip | user}
[criteria name]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Parameter	Description
ip | user	Specifies whether to list statistics by IP address or by user ID.
criteria *name*	Show reports based on specific set of abuser criteria. You can define the fall-in or fall-out criteria using the **qos abuser criteria** command.
period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {**now** | *mm/dd/yyyy* *hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.
top-num *num*	Specifies how many abusers to display, beginning with the most prolific. You can specify 1-100.

Mode All

show traffic alert

Show traffic alert records.

Syntax Description

```
show traffic alert
[alert-id]
[total-rate]
[user-rate]
[user-connection]
[period {minutes | hours | days | weeks | months}
  num]
[before {now | mm/dd/yyyy hh:mm}]
[rule-name [rule-name]]
```

Parameter	Description
alert-id	ID assigned to the alert by the EX device when the alert was generated.
total-rate	Shows only total-rate alerts.
user-rate	Shows only user-rate alerts.
user-connection	Shows only user-connection alerts.
period {**minutes** | **hours** | **days** | **weeks** | **months**} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {**now** | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.
rule-name	Shows only the alerts generated based on the specified alert name.

Mode All

show traffic class

Show traffic class statistics.

Syntax Description

```
show traffic class class-name
[view view-name]
[conn-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
class-name	Name of the traffic class. If you do not specify a class name, statistics are shown for all classes.
view *view-name*	Name of the QoS view. Statistics are shown only for the classes within the categories in the specified view.

Note: The view option applies only to top-class statistics.

conn-dir {**inbound** | **outbound**}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.

period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (minute, or hour, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.
before {now | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

Mode

All

Usage

If you specify a class name, the command shows traffic details for the class. If you do not specify a class name, the command shows statistics for the top classes (the most active classes).

show traffic connection

Show traffic connection statistics.

Syntax Description

```
show traffic connection overall
[scope
  {class class-list | internal-talker ipaddr |
   external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Syntax Description

```
show traffic connection top-class
[view view-name]
[conn-dir {inbound | outbound}]
[scope
  {class class-list | internal-talker ipaddr |
   external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Syntax Description

```
show traffic connection
  {top-internal-talker | top-external-talker}
[conn-dir {inbound | outbound}]
[scope
  {class class-list | internal-talker ipaddr |
   external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Parameter	Description
`overall`	Displays overall connection statistics.
`top-class`	Displays statistics for the most active classes.
`top-internal-talker`	Displays statistics for the most active internal talker.
`top-external-talker`	Displays statistics for the most active external talker.
scope {class *class-list* **| internal-talker** *ipaddr* **| external-talker** *ipaddr***}**	Specifies the scope of the output. You can specify either or both of the following options: **class** *class-list* – A single class name or a list of class names. To list more than one class name, use a forward slash between each class name, with no blank spaces. For example: *classname1/class-name2/class-name3* **internal-talker** *ipaddr* – IP address of an internal talker. **external-talker** *ipaddr* – IP address of an external talker.
period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter

	hour 2. By default, statistics for the most recent 3 hours are shown.
before {**now** | *mm/dd/yyyy* *hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.
view *view-name*	Name of the QoS view. Statistics are shown only for the classes within the categories in the specified view.
conn-dir {**inbound** | **outbound**}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
top-num *num*	Specifies how many items to display, beginning with the most active. You can specify 1-100.

Mode All

show traffic external-talker

Show traffic statistics for external talkers.

Syntax Description

```
show traffic external-talker ipaddr
[view view-name]
[conn-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
ipaddr	Specifies the external IP address.
view *view-name*	Name of the QoS view. Statistics are shown only for the classes within the categories in the specified view.

conn-dir {inbound | outbound}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (minute, or hour, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.
before {now | *mm/dd/yyyy hh***:***mm***}**	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

Mode All

show traffic internal-talker

Show traffic statistics for internal talkers.

Syntax Description

```
show traffic internal-talker ipaddr
[view view-name]
[conn-dir {inbound | outbound}] |
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
ipaddr	Specifies the internal IP address.

view *view-name*

Name of the QoS view. Statistics are shown only for the classes within the categories in the specified view.

conn-dir {inbound | outbound}

Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet:

– If the first packet is received on a QoS internal interface, the direction is outbound.

– If the first packet is received on a QoS external interface, the direction is inbound.

If you omit this option, statistics are shown for both directions.

period {minutes | hours | days | weeks | months} *num*

Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {now | *mm/dd/yyyy hh*:*mm*}

Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

Mode All

show traffic others-class {dst | src} ip

Show IP statistics for the Others traffic class.

Syntax Description

```
show traffic others-class {dst | src} ip
[ip-address]
[top-num num]
[port protocol-port]
[conn-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
dst | src	Specifies whether to display statistics for destination IP addresses or source IP addresses.
ip-address	Displays statistics only for the specified IP address.
top-num *num*	Specifies how many talkers to display, beginning with the most active. You can specify 1-100.
port *protocol-port*	Displays statistics only for the specified protocol port.
conn-dir {**inbound** | **outbound**}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
period {**minutes** | **hours** | **days** | **weeks** | **months**} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**.
before {**now** | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**.

Mode All

show traffic others-class {dst | src} ip-port

Show IP port statistics for the Others traffic class.

Syntax Description

```
show traffic others-class {dst | src} ip-port
[top-num num]
[conn-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
dst | src	Specifies whether to display statistics for destination IP ports or source IP ports.
top-num *num*	Specifies how many talkers to display, beginning with the most active. You can specify 1-100.
conn-dir {inbound | outbound}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**.
before {now | *mm/dd/yyyy* *hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**.

Mode

All

show traffic others-class {dst | src} port

Show port statistics for the Others traffic class.

Syntax Description

```
show traffic others-class {dst | src} port
[protocol-port]
[top-num num]
[ip ip-address]
[conn-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
dst | src	Specifies whether to display statistics for destination ports or source ports.
protocol-port	Displays statistics only for the specified protocol port.
top-num *num*	Specifies how many talkers to display, beginning with the most active. You can specify 1-100.
ip-address	Displays statistics only for the specified IP address.
conn-dir {inbound | outbound}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**.

before {**now** | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**.

Default N/A

Mode All

show traffic packet-distribution

Show packet distribution statistics.

Syntax Description

```
show traffic packet-distribution overall
[conn-dir {inbound | outbound}]
[packet-dir {inbound | outbound}]
[scope
  {class class-list | internal-talker ipaddr |
   external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Syntax Description

```
show traffic packet-distribution top-class
[view view-name]
[large-packet-size {56+ | 512+ | 1024+}]
[conn-dir {inbound | outbound}]
[packet-dir {inbound | outbound}]
[scope
  {class class-list | internal-talker ipaddr |
   external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Syntax Description

```
show traffic packet-distribution top-internal-
talker
[large-packet-size {56+ | 512+ | 1024+}]
[conn-dir {inbound | outbound}]
[packet-dir {inbound | outbound}]
[scope
  {class class-list | internal-talker ipaddr |
   external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Parameter	Description
overall	Shows overall statistics.
top-class	Shows statistics for top QoS traffic classes.
top-internal-talker	Shows statistics for top internal talkers.
conn-dir {**inbound** | **outbound**}	Traffic connection direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
packet-dir {**inbound** | **outbound**}	Traffic packet direction for which to display statistics. If you omit this option, statistics are shown for both directions.
scope {**class** *class-list* | **internal-talker** *ipaddr* | **external-talker** *ipaddr*}	Specifies the scope of the output. You can specify either or both of the following options: **class** *class-list* – A single class name or a list of class names. To list more than one class name, use a forward slash between each class name, with no blank spaces. For example: *classname1/class-name2/class-name3* **internal-talker** *ipaddr* – IP address of an internal talker. **external-talker** *ipaddr* – IP address of an external talker.

period {**minutes** | **hours** | **days** | **weeks** | **months**} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**.
before {**now** | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**.
view *view-name*	QoS view.
large-packet-size {**56+** | **512+** | **1024+**}	Specifies the minimum packet size to include in the statistics.
top-num *num*	Specifies how many items to display, beginning with the most active. You can specify 1-100.

show traffic rate

Show traffic rate statistics.

Syntax Description

```
show traffic rate overall
[conn-dir {inbound | outbound}]
[scope
  {category name | class class-list | internal-
talker ipaddr |    external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Syntax Description

```
show traffic rate top-category
[view view-name]
[conn-dir {inbound | outbound}]
[scope
  {category name | class class-list | internal-
talker ipaddr |    external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Syntax Description

```
show traffic rate top-class
[view view-name]
[conn-dir {inbound | outbound}]
[scope
  {category name | class class-list | internal-
talker ipaddr |    external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Syntax Description

```
show traffic rate
  {top-internal-talker | top-external-talker}
[conn-dir {inbound | outbound}]
[scope
  {category name | class class-list | internal-
talker ipaddr |    external-talker ipaddr}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Parameter	Description
overall	Displays overall rate statistics.
top-category	Displays statistics for the most active categories.
top-class	Displays statistics for the most active classes.
top-internal-talker	Displays statistics for the most active internal talker.
top-external-talker	Displays statistics for the most active external talker.
conn-dir {inbound | outbound}	Traffic direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound. – If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.

scope {category *name* **|class** *class-list* **| internal-talker** *ipaddr* **| external-talker** *ipaddr***}**

Specifies the scope of the output. You can specify either or both of the following options:

category *name* – A single category name or a list of category names. To list more than one category name, use a forward slash between each category name, with no blank spaces. For example: *catname1/cat-name2/cat-name3*

class *class-list* – A single class name or a list of class names. To list more than one class name, use a forward slash between each class name, with no blank spaces. For example: *classname1/class-name2/class-name3*

internal-talker *ipaddr* – IP address of an internal talker.

external-talker *ipaddr* – IP address of an external talker.

period {minutes | hours | days | weeks | months} *num*

Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**. By default, statistics for the most recent 3 hours are shown.

before {now | *mm/dd/yyyy hh***:***mm***}**

Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**. By default, statistics for the most recent 3 hours are shown.

top-num *num*

Specifies how many items to display, beginning with the most active. You can specify 1-100.

view *view-name*

Name of the QoS view. Statistics are shown only for the classes within the categories in the specified view.

Mode All

show traffic tcp

Show TCP performance statistics.

Syntax Description

```
show traffic tcp efficiency
[class class-name]
[packet-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Syntax Description

```
show traffic tcp conn-health
[class class-name]
[conn-dir {inbound | outbound}]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Syntax Description

```
show traffic tcp rtt
[class class-name]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Parameter	Description
efficiency	Shows TCP transmission efficiency.
conn-health	Shows TCP connection health statistics.
rtt	Shows TCP round-trip-time (RTT) statistics.
class *class-name*	QoS traffic class.
packet-dir {**inbound** | **outbound**}	Traffic packet direction for which to display statistics. If you omit this option, statistics are shown for both directions.
conn-dir {**inbound** | **outbound**}	Traffic connection direction for which to display statistics. The direction of a connection is determined by the QoS interface that receives the first packet: – If the first packet is received on a QoS internal interface, the direction is outbound.

	– If the first packet is received on a QoS external interface, the direction is inbound. If you omit this option, statistics are shown for both directions.
period {minutes | hours | days | weeks | months} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**.
before {now | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**.

Default The default time span is the last 3 hours, ending at the present.

Mode All

show traffic url

Show traffic statistics for URLs.

Syntax Description

```
show traffic url overall
[url url-string]
[talker ipaddr]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
```

Syntax Description

```
show traffic url
  {top-domain | top-sub-domain parent-domain |
   top-sub-path parent-url}
[talker ipaddr]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Syntax Description

```
show traffic url top-talker
[url url-string]
[period {minutes | hours | days | weeks | months}
  num [before {now | mm/dd/yyyy hh:mm}]]
[top-num num]
```

Parameter	Description
overall	Displays overall statistics.
top-domain	Displays statistics for the most active domains.
top-sub-domain *parent-domain*	Displays statistics for the most active sub-domains.
top-sub-path *parent-url*	Displays statistics for the most active sub-domain paths.
top-talker	Displays statistics for the most active talker.
url *url-string*	Displays statistics for the specified URL string.
talker *ipaddr*	Displays statistics for the specified talker.
period {**minutes** | **hours** | **days** | **weeks** | **months**} *num*	Time span for the report. Enter a period type (**minute**, or **hour**, and so on), then enter the quantity. For example, to specify 2 hours, enter **hour 2**.
before {**now** | *mm/dd/yyyy hh*:*mm*}	Specifies when the time span ends. For example, to generate a report for the most recent 2 hours, specify **period hour 2 before now**.
top-num *num*	Specifies how many items to display, beginning with the most active. You can specify 1-100.

Default N/A

Mode All

show trunk

Show trunk (aggregate link) information.

Syntax Description **show trunk** [*num*]

Mode All

show version

Display software, hardware, and firmware version information.

Syntax Description

`show version`

Default

None

Mode

All

Example

The following command shows version information:

```
EX#show version

A10 Networking System Software
Copyright (c) 2004-2006 by A10 Networks, Inc.
Technical Support: http://www.a10networks.com/support
Hardware Model: Edge Accelerator(TM)
Serial Number: EX2K011106390004
 4 online CPUs
 10 Ethernet interfaces
 2 Disks. 153G bytes of disk
 1008M bytes of memory
 118M bytes of CompactFlash

Software Version: 2.1.0
Build: 673

EX2100 starts up at 20:52:07 GMT Thu Mar 27 2008
The uptime is 4 days, 1 hour, 2 minutes
Configuration last updated at 19:51:58 IST Mon Mar 31 2008
Configuration last saved at 01:49:55 GMT Wed Mar 12 2008

Running in regular HD mode
```

show vlans

Show VLAN configuration information.

Syntax Description

`show vlans` *`vlan-id`*

Mode

All

Example

The following command shows the configuration of VLAN 2:

```
EX#show vlans 2

VLAN 2:
-----------------------------------------
Untagged interfaces: ethernet1
   Tagged interfaces: ethernet2
Router interface: ve2
       IP address: 10.10.10.1/24
                Status: Enabled
```

Related Commands

`show mac`

show vrrp

Display Virtual Router Redundancy Protocol (VRRP) information.

Syntax Description

`show vrrp` `[`*`vgroup-num`*`] [`**`detail`**`]`

Parameter	Description
`detail`	Displays detailed information.

Default

None

Mode

All

Usage

There is no **no** or **default** form of this command.

Example

The following commands display summary and detailed VRRP information for virtual group 1:

```
EX#show vrrp 1
   Interface  VrId  Priority  PreE  State   Primary addr     Virtual addr
  ----------------------------------------------------------------------------
   ethernet7  1     90          Y    Backup  0b08.8547        192.168.99.99
```

```
EX#show vrrp detail
   Virtual Group 1
     State is Backup
     Priority
       Setting: 100, Current: 90
     Weight is 10
     Preemption is enabled
     Advertisement interval is 1 sec
     Master Down interval is 3.648000 sec
     Data interface IP is 192.168.99.87
     Primary Address is 0b08.8547
     Virtual IP Address is 192.168.99.99
     Track services
      ---------------------------------
     | Name          | Usage           |
     |---------------------------------|
     | log           |   0/10          |
     | hm            |   0/5           |
     | web           |   0/5           |
     | ssh           |   0/5           |
     | routing       |   0/5           |
     | system        |   0/5           |
      ---------------------------------
     Tag: 0
```

Clear Commands

clear aflex

Clear statistics for aFleX scripts.

Syntax Description

```
clear aflex [script-name]
```

clear applog

Clear application log messages from the local buffer.

Syntax Description

```
clear applog
[archive]
[start-time mm/dd/yyyy hh:mm:ss]
[end-time mm/dd/yyyy hh:mm:ss]
[app-user filter-value]
[user filter-value]
[action filter-value]
[action-detail filter-value]
[alias alias-name]
[aim] [msnim] [yim] [ftp] [nfs] [cifs] [smtp]
[pop3] [qq] [http]
```

For information about the parameters, see “show applog” on page 307.

Mode

Privileged EXEC mode

Example

The following command clears all applog messages for AIM, MSNIM and YIM.

```
EX(config)#do clear applog alias myim
```

Related Commands

applog alias

clear arp

Clear ARP entries.

Syntax Description

```
clear arp
[ip-address | macaddr | ethernet portnum |
ve vlan-id]
```

Mode

Privileged EXEC mode

Example

The following command clears ARP entries for IP Ethernet interface 4.

```
EX(config)#do clear arp ethernet 4
```

clear clb group

Reset CLB group traffic counters.

Syntax Description

```
clear clb group [name [name ...]] counters
```

Parameter	Description
name	CLB group name

Default

None

Mode

Privileged EXEC mode

Usage

This command clears traffic counters for the specified CLB groups. If you do not specify a group name, counters for all CLB groups are cleared after user confirmation.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared. The counter for current connections will age out.

Example

The following command clears traffic counters for CLB group "Squid-CacheGrp":

```
EX#clear clb group SquidCacheGrp counters
```

clear clb node

Reset CLB node traffic counters.

Syntax Description

```
clear clb node [name [name ...]] counters
```

Parameter	Description
name	CLB node name.

Default

None

Mode

Privileged EXEC mode

Usage

This command clears traffic counters for the specified CLB nodes. If you do not specify a node name, traffic counters for all nodes are cleared.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets traffic counters are cleared by this command. The current connection counter will age out.

Example

The following command clears the traffic counters for CLB node “Squid-Cache”:

```
EX#clear clb node SquidCache counters
```

clear coredump

Clear all core dump files.

Syntax Description

```
clear coredump
```

clear debug

Clear debug packet trace logs.

Syntax Description

```
clear debug packet trace
```

clear dns

Clear all DNS cache entries.

Syntax Description

```
clear dns
```

Mode

Privileged EXEC mode

Example

The following command clears all DNS cache entries:

```
EX#clear dns
```

clear flow counters

Reset flow counters.

Syntax Description

```
clear flow counters
```

Default

None

Mode

Privileged EXEC mode

Usage

There is no **no** or **default** form of this command.

This command is used primarily for debugging.

Example

The following command resets the flow counters:

```
EX>clear flow counters
```

clear flow sessions

Clear currently active sessions.

Syntax Description

```
clear flow sessions
[proto {tcp | udp}]
[fwd-sip ip-address]
[fwd-sport port]
[fwd-dip ip-address]
[fwd-dport port]
[rev-sip ip-address]
[rev-sport port]
[rev-dip ip-address]
[rev-dport port]
```

Parameter	Description
proto {**tcp** | **udp**}	Protocol of the session, TCP or UDP.
fwd-sip *ip-address*	Source IP address of the forward direction.
fwd-sport *port*	Source port of the forward direction.
fwd-dip *ip-address*	Destination IP address of the forward direction.
fwd-dport *port*	Destination port of the forward direction.
rev-sip *ip-address*	Source IP address of the reverse direction.
rev-sport *port*	Source port of the reverse direction.
rev-dip *ip-address*	Destination IP address of the reverse direction.
rev-dport *port*	Destination port of the reverse direction.

Default

N/A

Mode

Privileged EXEC mode

Example

The following command clears the currently active sessions whose source IP address in the forward direction is 192.168.12.102:

```
EX#clear flow sessions fwd-sip 192.168.12.102
```

clear fwlb group

Reset FWLB group traffic counters.

Syntax Description

```
clear fwlb group [name [name...]] counters
```

Parameter	Description
name	Firewall group name.

Default

None

Mode

Privileged EXEC mode

Usage

This command clears traffic counters for the specified FWLB groups. If you do not specify a group name, traffic counters are cleared for all FWLB groups.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared. The counter for current connections will age out.

Example

The following command clears traffic counters for FWLB group "WebServiceFwGrp":

```
EX#clear fwlb group WebServiceFwGrp counters
```

clear fwlb node

Reset FWLB node traffic counters.

Syntax Description

```
clear fwlb node [name [name...]] counters
```

Parameter	Description
name	Node name. If you do not specify a name, counters for all FWLB nodes are cleared.

Default

None

Mode Privileged EXEC mode

Usage There is no **no** or **default** form of this command.

Only sent/received bytes/packets traffic counters are cleared by this command. The current connection counter will age out.

Example The following command clears counters for FWLB node “SanJoseHQ”:

```
EX#clear fwlb node SanJoseHQ counters
```

clear health

Clear health monitoring statistics.

Syntax Description

```
clear health
```

clear interface counters

Clear statistics counters for interfaces.

Syntax Description

```
clear interface
[ethernet [port-num ...] | ve [vlan-id ...]] counters
```

Default none

Mode Privileged EXEC mode

Example The following command clears statistics counters for Ethernet interfaces 3 and 4:

```
EX#clear interface ethernet 3 4 counters
```

Related Commands **interface**, **show interfaces**

clear ip2id

Clear all IP-to-ID mappings.

Syntax Description

```
clear ip2id
```

Mode Privileged EXEC mode

Usage

If IP-to-ID mappings are being supplied dynamically by an IDsentrie device, this command also refreshes the mappings by obtaining them from the IDsentrie.

Example

The following command clears all IP-to-ID mappings:

```
EX#clear ip2id
```

clear ips counters

Reset IPS counters.

Syntax Description

```
clear ips counters
[ethernet portnum [ethernet portnum ...]]
```

Default

None

Mode

Privileged EXEC mode

Example

The following command resets the IPS counters:

```
EX#clear ips counters
```

clear l7 blackcache

Clear Layer 7 cache entries classified in the “Others” class.

Syntax Description

```
clear l7 cache [ip ipaddr [port protocol-port]]
```

Parameter	Description
ip *ipaddr*	Server IP address.
port *protocol-port*	Protocol port on the server.

Default

None

Mode

Privileged EXEC mode

Usage

This command clears entries for flows of the “Others” class. To clear cache entries for classes recognized by (known to) the EX device, see “clear l7 cache” on page 392.

Example

The following command clears Layer 7 cache entries of the “Others” class, for server 192.168.1.51:

```
EX#clear l7 blackcache ip 192.168.1.51
```

clear l7 cache

Clear Layer 7 cache entries.

Syntax Description

```
clear l7 cache [ip ipaddr [port protocol-port]]
```

Parameter	Description
ip *ipaddr*	Server IP address.
port *protocol-port*	Protocol port on the server.

Default

None

Mode

Privileged EXEC mode

Usage

This command clears entries from classes recognized by the EX device. To clear cache entries for flows of the “Others” class, see “clear l7 blackcache” on page 391.

Example

The following command clears Layer 7 cache entries for known classes from server 192.168.1.51:

```
EX#clear l7 cache ip 192.168.1.51
```

clear llb group

Reset the LLB group traffic counters.

Syntax Description

```
clear llb group [name [name ...]] counters
```

Parameter	Description
name	LLB group name. If you omit this option, counters for all groups are cleared.

Default

None

Mode

Privileged EXEC mode

Usage

There is no **no** or **default** form of this command.

Various statistics are collected for an LLB link, such as sent/received bytes, packets, current connections, and so on. Only the sent/received bytes and packets are cleared by this command. Other statistics will age out.

Example

The following command clears counters for LLB group "*llb-group-1*":

```
EX#clear llb group llb-group-1 counters
```

clear llb link

Reset LLB link traffic counters.

Syntax Description

```
clear llb link [name [ name ...]] counters
```

Parameter	Description
name	LLB link name. If you omit this option, counters for all LLB links are reset.

Default

None

Mode

Privileged EXEC mode

Usage

Various statistics are collected for an LLB link, such as sent/received bytes, packets, current connections, up/downstream bandwidth usage, connections handled per second, and so on. Only the sent/received bytes and packets are cleared by this command. Other statistics age out.

There is no **no** or **default** form of this command.

Example

The following command clears counters for LLB link ISP1:

```
EX#clear llb link ISP1 counters
```

clear llb rtt

Clear collected LLB RTT information.

Syntax Description

```
clear llb rtt [link name [ipaddr] | ipaddr]
```

Parameter	Description
name	Name of a link.
ipaddr	IP address whose RTT is to be cleared.

Default

N/A

Mode

Privileged EXEC mode

Usage

If you specify a link name and IP address, RTT data is cleared only for that IP address reached through the specified link. If you specify a link name but not an IP address, RTT data is cleared for all IP addresses reached through the link. If you do not specify a link name or IP address, all RTT data is cleared.

Example

The following command clears all RTT data for link ISP1:

```
EX#clear llb rtt link lSP1
```

clear logging

Clear the log entries from the system logging buffer.

Syntax Description

```
clear logging
```

clear ospf

Reset the OSPF process.

Syntax Description

```
clear ospf process
```

clear packet

Clear packet drop counters.

Syntax Description

```
clear packet drop counters
```

clear qos ip limit

Clear statistics for IP limiting.

Syntax Description

```
clear qos ip limit
[[ipaddress [ipaddr] | ip-list-name ...] counters]
```

clear qos policy

Clear policies or policy statistics.

Syntax Description

```
clear qos policy [if-name [ingress | egress]]
```

Parameter	Description
if-name	QoS interface name.

ingress | egress	Traffic direction.

Default None

Mode Privileged EXEC mode

Usage The options you use with the command control whether the command clears statistics counters or removes policies.

If the command **clear qos policy** is used, the counters of all applied policies will be cleared.

If a QoS interface name is specified, the ingress and egress policies will be removed from the interface.

If a QoS interface name and traffic direction are specified, the ingress or egress policy (as specified) will be cleared from the interface.

If you do not specify an interface name but you do specify a traffic direction, counters for all policies applied to that traffic direction are cleared.

Example The following command clears the counters for all policies in the system:

```
EX(config)#clear qos policy
```

Example The following command clears the counters for the ingress policy and egress policy on QoS interface “vt”:

```
EX(config)#clear qos policy vt
```

Example The following command clears the counters for the ingress policy on QoS interface “vt”:

```
EX(config)#clear qos policy vt ingress
```

Related Commands **qos policy**

clear qos shape interface

Clear shaping counters for the specified interface.

Syntax Description

```
clear qos shape interface
{if-name | ethernet port}
```

Parameter	Description
if-name	QoS interface name.
port	Ethernet port number.

Default None

Mode Privileged EXEC mode

Example The following command clears shaping counters on QoS interface “vt”:

```
EX(config)#clear qos shape interface vt
```

Example The following command clears shaping counters on Ethernet interface 1:

```
EX(config)#clear qos shape interface Ethernet 1
```

clear qos top class

Clear top talker statistics counters for traffic classes

Syntax Description

```
clear qos top class [class-name ...]
```

Parameter	Description
class-name	Clears top talker statistics only for the specified traffic classes. If you do not specify a traffic class name, top talker counters for all traffic classes are cleared.

Default None

Mode Privileged EXEC mode

Example The following command clears top talker statistics counters for traffic class http:

```
EX#clear qos top class http
```

clear session

Terminate admin sessions.

Syntax Description

```
clear session admin {all | session-id}
```

Parameter	Description
all	Terminates all admin sessions except yours.

session-id	Terminates the specified admin session. To display the admin session IDs, use the **show session admin** command.

clear slb group

Reset SLB group traffic counters.

Syntax Description

```
clear slb group
[{tcp | udp | any} [name [name ...]]] counters
```

Parameter	Description
tcp	Clears counters for groups with the **tcp** transport protocol type.
udp	Clears counters for groups with the **udp** transport protocol type.
any	Clears counters for groups with the **any** transport protocol type.
name	SLB group name.

Default

None

Mode

Privileged EXEC mode

Usage

The normal form of this command clears traffic counters for the specified SLB groups. If you specify a transport protocol type but not a group name, traffic counters for all groups of that transport protocol type are cleared after user confirmation. If you do not specify a transport protocol type, traffic counters for all SLB groups are cleared after user confirmation.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared. Others counters will age out.

Example

The following command resets traffic counters for SLB group “WebServerGrp”:

```
EX#clear slb group any WebServerGrp counters
```

clear slb node

Reset SLB node traffic counters.

Syntax Description

```
clear slb node [name [name ...]] counters
```

Parameter	Description
name	SLB node name.

Default None

Mode Privileged EXEC mode

Usage The normal form of this command clears traffic counters for the specified SLB node. If you do not specify a node name, traffic counters for all SLB nodes are cleared after user confirmation.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared by this command. Other counters will age out.

Example The following command clears traffic counters for SLB node “apache”:

```
EX#clear slb node apache counters
```

clear slb port

Reset traffic counters for SLB ports.

Syntax Description

```
clear slb port
[name [{tcp | udp} [port [port ...]]]] counters
```

Parameter	Description
name	SLB node name.
port	Protocol port number or well-known port name.

Default None

Mode Privileged EXEC mode

Usage The normal form of this command clears traffic counters for the specified SLB port on the specified node. If you specify a node name but not a port, traffic counters for all ports on the node are cleared after user confirmation. If you do not specify a node name, traffic counters for all ports on all nodes are cleared after user confirmation.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared by this command. Other counters will age out.

Example

The command clears traffic counters for TCP port 80 on SLB node "apache":

```
EX#clear slb port apache tcp 80 counters
```

clear slb virtual port

Reset virtual port traffic counters.

Syntax Description

```
clear slb virtual port
[name [{tcp | udp} [port [port ...]]]] counters
```

Parameter	Description
name	Virtual server name.
tcp	Clears traffic counters for TCP virtual ports.
udp	Clears traffic counters for UDP virtual ports.
port	Port number or well-known port name.

Default

None

Mode

Privileged EXEC mode

Usage

The normal form of this command clears traffic counters for the specified virtual ports. If you specify a transport protocol type but not a virtual server name, traffic counters for all virtual ports of that transport protocol type are cleared after user confirmation. If you do not specify a transport protocol type, traffic counters for all virtual ports are cleared after user confirmation.

There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared by this command. Other counters will age out.

Example

The following command clears traffic counters for TCP virtual port 80 or virtual server "VirtualServer":

```
EX#clear slb virtual port VirtualServer tcp 80 counters
```

clear slb virtual server

Reset virtual server traffic counters.

Syntax Description

```
clear slb virtual server [name [name ...]] counters
```

Parameter	Description
name	Virtual server name.

Default

None

Mode

Privileged EXEC mode

Usage

The normal form of this command clears traffic counters for the specified virtual servers. If you do not enter a virtual server name, counters for all virtual servers are cleared after user confirmation. There is no **no** or **default** form of this command.

Only sent/received bytes/packets are cleared by this command. Other counters will age out.

Example

The following command clears traffic counters for virtual server “VirtualServer”:

```
EX#clear slb virtual VirtualServer counters
```

clear traffic

Clear traffic statistics or alerts.

Syntax Description

```
clear traffic
[
alert
[alert-id]
[before {now | mm/dd/yyyy hh:mm:ss}]
[rule-name name]
[total-rate
  [rule-name name]
  [before {now | mm/dd/yyyy hh:mm:ss}]]
[user-rate
  [rule-name name]
  [before {now | mm/dd/yyyy hh:mm:ss}]]
[user-connection
  [rule-name name]
  [before {now | mm/dd/yyyy hh:mm:ss}]]
]
```

clear trunk

Clear trunk statistics.

Syntax Description

```
clear trunk [num]
```

Debug Commands

debug packet trace filter

Configure a filter to specify the types of packets to trace for troubleshooting.

To configure a packet trace and examine the output:

1. Configure a packet trace filter using the command described in this section.
2. Enable packet tracing. (See "debug packet trace enable" on page 403.)
3. Display the trace data. (See "show debug packet trace" on page 404.)

Note: A10 Networks recommends that you always use a filter for packet traces. Running a packet trace without using a filter can overload the CLI with too much trace output.

Note: The **debug packet trace** commands provide a newer, more flexible alternative to the **debug packet capture** commands, which are not described in this document.

Syntax Description

```
[no] debug packet trace filter
{
arp |
ethernet-protocol |
ip {
    [protocol {ICMP | TCP | UDP | ip-protocol}] |
       [src-host ipaddr] |
       [dest-host ipaddr] |
       [src-host ipaddr] |
       [host ipaddr] |
       [src-port protocol-port] |
       [dst-port protocol-port] |
       [port protocol-port]
    }
}
```

Parameter	Description
arp | *ethernet-protocol* | **ip**	Specifies the type of Ethernet packet to trace: **arp** – Address Resolution Protocol (ARP) packets. *ethernet-protocol* – Ether Type number. You can specify 1-65535, in decimal. For a list of Ether Type numbers, see the following URL: http://www.networksorcery.com/enp/default1001.htm **ip** – Internet Protocol number. For example, TCP is IP protocol 6 and UDP is IP protocol 17. For a list of IP protocol numbers, see the following URL: http://www.iana.org/assignments/protocol-numbers

If you select **ip** as the packet type, the following options are available:

protocol {**ICMP** | **TCP** | **UDP** | *ip-protocol*}	Specifies the IP protocol. The IP protocol number can be 1-255.
src-host *ipaddr*	Specifies the source IP address of packets to trace.
dst-host *ipaddr*	Specifies the destination IP address of packets to trace.
host *ipaddr*	Specifies an IP address in packets to trace. The address can be the source or destination address.
src-port *protocol-port*	Specifies the source Layer 4 protocol port of packets to trace.
dst-port *protocol-port*	Specifies the destination Layer 4 protocol port of packets to trace.
port *protocol-port*	Specifies a Layer 4 protocol port in packets to trace. The port can be the source or destination Layer 4 protocol port.

Default

By default, there is no filter. All packets are included in the trace.

Mode

Privileged EXEC mode

Usage

Configure the filter before enabling packet tracing. The filter remains in effect until you clear it with the **no** form of the command or you configure a new filter. The filter is also cleared if the EX device is rebooted.

The filter applies only to packet traces that you explicitly configure, not to random packet tracing. (For information about random packet tracing, see "debug packet trace random" on page 405.)

Example

The following command configures a packet trace filter to trace all TCP packets to or from protocol port 80:

```
EX#debug packet trace filter ip protocol tcp port 80
```

Example

The following command configures a packet trace filter to trace all IP packets with the source or destination IP address 192.168.1.130:

```
EX#debug packet trace filter ip host 192.168.1.130
```

(For a complete example including trace output, see "show debug packet trace" on page 404.)

debug packet trace enable

Enable admin-configured packet tracing.

Syntax Description

```
debug packet trace enable {info | error}
```

Parameter	Description
`info`	Includes all packets that match the packet trace filter, and records the complete path the packets take through the software during processing.
`error`	Includes only packets that are dropped or contain errors, and indicates the software module that was processing the packet when the drop or error occurred.

Default

Admin-configured tracing is disabled by default. Random packet tracing (see "debug packet trace random" on page 405) is enabled by default.

Mode

Privileged EXEC mode

Usage

Configure a trace filter before enabling packet tracing. (See "debug packet trace filter" on page 401.)

Example The following command enables packet tracing at the information level:

```
EX#debug packet trace enable info
```

(For a complete example including trace output, see “show debug packet trace” on page 404.)

show debug packet trace

Show packet data collected by an admin-configured packet trace.

Syntax Description **show debug packet trace**

Mode All

Usage To configure packet tracing, see “debug packet trace filter” on page 401.

Random packet tracing is separate from admin-configured packet tracing. Trace results from random packet tracing are written to a file that is included in the set of files generated by the **techsupport** command.

Example The following commands configure a packet trace filter, enable packet tracing at the information level, and display the trace data:

```
EX#debug packet trace filter ip host 192.168.1.130
EX#debug packet trace enable info
EX#show debug packet trace

Packet tracing is enabled, level is info
Packet tracing filter:
 Ethernet protocol: IP
 IP protocol: ANY
 IP host: 192.168.1.130
Random packets tracing is disabled, interval: 60 seconds, max: 6.

Jun 14 00:46:48 U 2 fpga3     1e29 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : lb_local_rcv :
Jun 14 00:46:48 U 2 fpga3     1e29 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : lb_process_tcp_packet :
Jun 14 00:46:48 U 2 fpga3     1e29 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : lb_rcv :
Jun 14 00:46:48 U 2 fpga3     1e29 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : swo_l2_switching_rx :
Jun 14 00:46:48 U 2 fpga3     1e29 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : swo_receive_data :
Jun 14 00:46:48 K 0  NULL cb2c1380 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : ip_local_deliver_finish : protocol han-
dler ret: 0
```

```
Jun 14 00:46:48 K 0 fpga3 cb2c1380 TCP 192.168.1.130.4281 >
192.168.1.166.22 2618048203 : tcp_v4_rcv :
--MORE--
```

debug packet trace random

Disable or re-enable random packet tracing.

Syntax Description

```
[no] debug packet trace random
     [interval seconds] [max packets]
```

Parameter	Description
`interval` *`seconds`*	Number of seconds between each sample. You can specify 1-600 seconds.
`max` *`packets`*	Maximum number of packets to capture per interval. You can specify 1-6 packets per interval.

Default

Random packet tracing is enabled by default, and has the following default settings:

- **interval** – 60 seconds
- **max** – 6 packets per interval

Mode

Privileged EXEC mode

Usage

Random packet tracing is separate from admin-configured packet tracing. Trace results from random packet tracing are written to a file that is included in the set of tech support files generated by the **techsupport** command. Trace data from admin-configured traces is displayed on the management terminal. (See “show debug packet trace” on page 404.)

techsupport

Create, list, copy, and clear technical support files that include system information and log files.

Syntax Description

```
techsupport {create | list | export url | clear}
```

Parameter	Description
`create`	Creates the technical support files.
`list`	Displays a list of the technical support files.

export *url* Copies the technical support files to a remote server. The *url* specifies the file transfer protocol, username (if required), and directory path.

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL:

tftp://*host*/*file*

ftp://[*user*@]*host*[:*port*]/*file*

scp://[*user*@]*host*/*file*

rcp://[*user*@]*host*/*file*

clear Erases the technical support files from the EX device.

Default

None

Mode

Configuration mode

Usage

Use these commands to gather system information and export it to a remote server.

The **create** and **export** options are not supported if the EX device is running in recovery mode.

Example

The following commands create technical support files, list them, export them to an external file server, and then erase them from the EX device:

```
EX(config)#techsupport create
EX(config)#techsupport list
TechSupport Files:
-rw-r--r--  1 root root 69502 Mar  5 11:00 techsupport.1204714849
-rw-r--r--  1 root root 69796 Mar  5 11:00 techsupport.1204714850
-rw-r--r--  1 root root 70090 Mar  5 11:00 techsupport.1204714851
EX(config)#techsupport export
tftp://192.168.3.29/techsupport.tgz
Transferring file...
Transfer succeed!
EX(config)#techsupport clear
```

Appendix

List of Supported Applications

The following table lists supported applications for which default classes have been preconfigured on the EX appliance.

Classes can be displayed using the following command:

```
EX(config)#show qos class
```

Categories (and their associated classes) can be displayed using the following command:

```
EX(config)#show qos category
```

Application	Description
100bao	A Chinese P2P application
abacast	AbaCast online audio/video service
aim	America Online Instant Messenger
ares	ARES peer-to-peer protocol
baidux	Baidux peer-to-peer application
bittorrent	BitTorrent protocol (includes BitSpirit)
cifs	Common Internet File System Protocol
clubbox	ClubBox Protocol
cspace	Cspace peer-to-peer protocol
directconnect	Direct Connect peer-to-peer protocol
dns	Domain Name System
emule	Emule edonkey-like peer-to-peer protocol
encrypted-bt	Encrypted BitTorrent protocol
exchange	Microsoft Exchange Protocol
fetion	Fetion messenger
foxy	Peer-to-peer client
freecast	Freecast peer-to-peer media protocol
ftp	File Transport Portocol
furthurnet	Furthurnet peer-to-peer application
gogobox	GoGoBox Protocol
gnutella	GNUTella peer-to-peer protocol

Application	Description
gtalk	Google talk service
h323q931	H323 Q931
h323ras	H323 RAS
http	HyperText Transport Protocol
http.content	HTTP payload, supports wildcard "*" for "~"
http.content-type	Content type for HTTP body, supports wildcard "*" for "~" (eg. "http.content-type = text/html" or using "http.content-type ~ audio" to block online media including WMP, Winamp etc.)
http.header	HTTP header, supports wildcard "*" for "~" (eg. "http.header ~ X-Gnutella-*:*")
http.host	Host name for HTTP header, supports wildcard "*" for "~" (eg. "http.host ~ *.google.com")
http.range	Range of the http document, supports wildcard "*" for "~" (eg. "http.range ~ *")
http.url	Url for HTTP, supports wildcard "*" for "~" (eg. "http.url ~ *.example.com/vedio/*")
http.user-agent	User agent name for HTTP header, supports wildcard "*" for "~" (eg. "http.user-agent ~ iTunes")
huntmine	Huntmine peer-to-peer file sharing application
imap	Internet Message Access Protocol
imesh	iMesh peer-to-peer protocol
isakmp	ISAKMP Protocol
itunes	Apple iTunes music player
krawler	Krawler peer to peer protocol
kazaa	Kazaa peer-to-peer application (includes Kazaa Lite)
kkbox	KKBOX online music service from Taiwan China
kugoo	Chinese peer-to-peer application
ldap	Lightweight Directory Access Protocol
limewire	LimeWire peer-to-peer protocol
lotus	IBM Lotus Notes
megaco	Media Gateway Control (H.248)
mgcp	Media Gateway Control Protocol
msmms	Microsoft Media Server
msnim	Microsoft MSN Messenger
mssql	Microsoft SQL server

Application	Description
mysql	MySQL SQL server
napster	Napster peer-to-peer application
nfs	Network File System protocol
ntp	Network Time Protocol
oracle	Oracle database server
poco	Chinese peer-to-peer application
pop3	Post Office Protocol
pplive	Peer-to-peer online video/audio
ppstream	Peer-to-peer online video/audio
qq	Tencent qq Instant Messaging
qqlive	Peer-to-peer online video/audio
quicktime	Apple QuickTime media player
radius	RADIUS protocol
remote-desktop	Microsoft Remote Desktop Protocol
rtp	Realtime Transport Protocol
rtcp	Realtime Transport Control Protocol
rtsp	Real Time Streaming Protocol, using it to block Real.com online radio
share	Share EX2 peer-to-peer protocol
shareaza	A peer-to-peer client
sharetastic	A peer-to-peer client
sip	Session Initial Protocol, VoIP related
skinny	Cisco's Skinny client control protocol
skype	A popular VoIP client
smtp	Simple Mail Transport Protocol
sopcast	Sopcast peer-to-peer video protocol
soulseek	SoulSeek peer-to-peer application
ssh	Secure Shell Remote Login Protocol
ssl	Secure Socket Layer Protocol
stun	Simple Traversal of UDP through NAT
t120	T.120
telnet	Telnet protocol
tftp	Trivial File Transport Protocol
tvants	TVAnts, peer-to-peer online TV
uusee	UUSee peer-to-peer video protocol
vagaa	A peer-to-peer client

Application	Description
vnc	Virtual Network Computing protocol
winmx	Peer-to-peer protocol
winny	WinNY peer-to-peer protocol
xunlei	Chinese peer-to-peer application
yim	Yahoo Instant Messaging Service
youtube	YouTube online video

Index

Performance by Design

World Headquarters
A10 Networks, Inc.
2309 Bering Dr.
San Jose, CA 95131-1125
USA

http://www.a10networks.com

Tel: +1(408) 325-8662 (main)
Tel: +1(408) 325-8676 (support)
Fax: +1(408) 325-8666

This document is for informational purposes only. A10 Networks MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

A10 Networks may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from A10 Networks, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.