ExtremeWare Software Command Reference Guide

Software Version 7.1.0

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: October 17, 2003
Part number: 100115-00 Rev 06

Authors: Hugh Bussell, Julie Laccabue, Megan Mahar, Richard Small

Production: Hugh Bussell

Contents

Chapter 18 BGP Commands

Chapter 20 IPX Commands

Chapter 25 MPLS Commands

Appendix B Troubleshooting Commands

Index of Commands

Preface

This preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the complete syntax for all the commands available in the currently-supported versions of the ExtremeWare® software running on either modular or stand-alone switches from Extreme Networks®. This also includes commands that support specific modules such as the ARM, MPLS or PoS modules.

This guide is intended for use as a reference by network administrators who are responsible for installing and setting up network equipment. It assumes knowledge of Extreme Networks switch configuration. For conceptual information and guidance on configuring Extreme Networks switches, see the *ExtremeWare Software User Guide* for your version of the ExtremeWare software.

Terminology

When features, functionality, or operation is specific to a modular or stand-alone switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the “switch.”

Conventions

and list conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

Command Titles

For clarity and brevity, the command titles omit variables, values, and optional arguments. The complete command syntax is displayed directly below the command titles.

Related Publications

The publications related to this one are:

- ExtremeWare release notes
- *ExtremeWare Software User Guide*
- *ExtremeWare 7.1.0 Software Quick Reference Guide*
- *Extreme Networks Consolidated Hardware Guide*

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

http://www.extremenetworks.com/

1 Command Reference Overview

Introduction

This guide provides details of the command syntax for all ExtremeWare commands as of ExtremeWare version 7.1.0.

NOTE

ExtremeWare 7.1.0 only supports Extreme Networks products that contain the "i" or "3" series chipset. This includes the BlackDiamond, Alpine, and Summit "i" series platforms, but does not include the Summit e-series and Summit 200 series platforms.

This guide does not provide feature descriptions, explanations of the technologies, or configuration examples. For information about the various features and technologies supported by Extreme Networks switches, see the installation and user guides for your product. This guide does not replace the installation and user guides; this guide supplements the installation and user guides.

Audience

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of the following:

- Local area networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- Internet Protocol (IP) concepts
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) concepts
- Border Gateway Protocol (BGP-4) concepts
- IP Multicast concepts
- Distance Vector Multicast Routing Protocol (DVMRP) concepts
- Protocol Independent Multicast (PIM) concepts
- Internet Packet Exchange (IPX) concepts

- Server Load Balancing (SLB) concepts
- Simple Network Management Protocol (SNMP)

This guide also assumes that you have read the Installation and User Guide for your product.

Structure of this Guide

This guide documents each ExtremeWare command. Related commands are grouped together and organized into chapters based on their most common usage. The chapters reflect the organization of the *ExtremeWare Software User Guide*. If a specific command is relevant to a wide variety of functions and could be included in a number of different chapters, we have attempted to place the command in the most logical chapter. Within each chapter, commands appear in alphabetical order. You can use the Index of Commands to locate specific commands if they do not appear where you expect to find them.

For each command, the following information is provided:

- **Command Syntax**—The actual syntax of the command. The syntax conventions (the use of braces or curly brackets, for example) are defined in the section "Understanding the Command Syntax" on page 49.
- **Description**—A brief (one sentence) summary of what the command does.
- **Syntax Description**—The definition of any keywords and options used in the command.
- **Default**—The defaults, if any, for this command. The default can be the default action of the command if optional arguments are not provided, or it can be the default state of the switch (such as for an enable / disable command).
- **Usage Guidelines**—Information to help you use the command. This may include prerequisites, prohibitions, and related commands, as well as other information.
- **Example**—Examples of the command usage, including output, if relevant.
- **History**—The version of ExtremeWare in which the command was introduced, and version(s) where it was modified, if appropriate.
- **Platform Availability**—The platforms on which the command is supported.

NOTE

Commands designated as "available on all platforms" are supported on both Summit chipset-based, "i"-series, and "3" series platforms. Summit e-series devices are not included.

Understanding the Command Syntax

When entering a command at the prompt, ensure that you have the appropriate privilege level. Most configuration commands require you to have the administrator privilege level.

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. Table 3 summarizes command syntax symbols.

Table 3: Command Syntax Symbols

Symbol	Description
angle brackets < >	Enclose a variable or value. You must specify the variable or value. For example, in the syntax `configure vlan <vlan name> ipaddress <ip_address>` you must supply a VLAN name for `<vlan name>` and an address for `<ip_address>` when entering the command. Do not type the angle brackets.
square brackets [ ]	Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax `use image [primary | secondary]` you must specify either the primary or secondary image when entering the command. Do not type the square brackets.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax `configure snmp community [read-only | read-write] <string>` you must specify either the read or write community string in the command. Do not type the vertical bar.
braces { }	Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax `reboot {<date> <time> | cancel}` you can specify either a particular date and time combination, or the keyword `cancel` to cancel a previously scheduled reboot. If you do not specify an argument, the command will prompt asking if you want to reboot the switch now. Do not type the braces.

Command Completion with Syntax Helper

The CLI has a built-in syntax helper. If you are unsure of the complete syntax for a particular command, enter as much of the command as possible and press [Tab]. The syntax helper provides a list of options for the remainder of the command, and places the cursor at the end of the command you have entered so far, ready for the next option.

If the command is one where the next option is a named component, such as a VLAN, access profile, or route map, the syntax helper will also list any currently configured names that might be used as the next option. In situations where this list might be very long, the syntax helper will list only one line of names, followed by an ellipses to indicate that there are more names than can be displayed.

The syntax helper also provides assistance if you have entered an incorrect command.

Abbreviated Syntax

Abbreviated syntax is the shortest unambiguous allowable abbreviation of a command or parameter. Typically, this is the first three letters of the command. If you do not enter enough letters to allow the switch to determine which command you mean, the syntax helper will provide a list of the options based on the portion of the command you have entered.

NOTE

When using abbreviated syntax, you must enter enough characters to make the command unambiguous and distinguishable to the switch.

Names

All named components of the switch configuration must have a unique name. Names must begin with an alphabetical character and are delimited by whitespace, unless enclosed in quotation marks.

Command Shortcuts

All named components of the switch configuration must have a unique name. Components are named using the `create` command. When you enter a command to configure a named component, you do not need to use the keyword of the component. For example, to create a VLAN, you must enter a unique VLAN name:

```
create vlan engineering
```

Once you have created the VLAN with a unique name, you can then eliminate the keyword `vlan` from all other commands that require the name to be entered. For example, instead of entering the modular switch command

```
configure vlan engineering delete port 1:3,4:6
```

you could enter the following shortcut:

```
configure engineering delete port 1:3,4:6
```

Similarly, on the stand-alone switch, instead of entering the command

```
configure vlan engineering delete port 1-3,6
```

you could enter the following shortcut:

```
configure engineering delete port 1-3,6
```

Modular Switch Numerical Ranges

Commands that require you to enter one or more port numbers on a modular switch use the parameter `<portlist>` in the syntax. A `<portlist>` can be one port on a particular slot. For example,

```
port 3:1
```

A `<portlist>` can be a range of numbers. For example,

```
port 3:1-3:3
```

You can add additional slot and port numbers to the list, separated by a comma:

```
port 3:1,4:8,6:10
```

You can specify all ports on a particular slot. For example,

```
port 3:*
```

indicates all ports on slot 3.

You can specify a range of slots and ports. For example,

```
port 2:3-4:5
```

indicates slot 2, port 3 through slot 4, port 5.

Stand-alone Switch Numerical Ranges

Commands that require you to enter one or more port numbers on a stand-alone switch use the parameter `<portlist>` in the syntax. A portlist can be a range of numbers, for example:

```
port 1-3
```

You can add additional port numbers to the list, separated by a comma:

```
port 1-3,6,8
```

Line-Editing Keys

Table 4 describes the line-editing keys available using the CLI.

Table 4: Line-Editing Keys

Key(s)	Description
Backspace	Deletes character to left of cursor and shifts remainder of line to left.
Delete or [Ctrl] + D	Deletes character under cursor and shifts remainder of line to left.
[Ctrl] + K	Deletes characters from under cursor to end of line.
Insert	Toggles on and off. When toggled on, inserts text and shifts previous text to right.
Left Arrow	Moves cursor to left.
Right Arrow	Moves cursor to right.
Home or [Ctrl] + A	Moves cursor to first character in line.
End or [Ctrl] + E	Moves cursor to last character in line.
[Ctrl] + L	Clears screen and movers cursor to beginning of line.
[Ctrl] + P or Up Arrow	Displays previous command in command history buffer and places cursor at end of command.
[Ctrl] + N or Down Arrow	Displays next command in command history buffer and places cursor at end of command.
[Ctrl] + U	Clears all characters typed from cursor to beginning of line.
[Ctrl] + W	Deletes previous word.

Command History

ExtremeWare “remembers” the last 49 commands you entered. You can display a list of these commands by using the following command:

```
history
```

2 Commands for Accessing the Switch

This chapter describes:

- Commands used for accessing and configuring the switch including how to set up user accounts, passwords, date and time settings, and software licenses
- Commands used for configuring the Domain Name Service (DNS) client
- Commands used for checking basic switch connectivity

ExtremeWare supports the following two levels of management:

- User
- Administrator

A user-level account has viewing access to all manageable parameters, with the exception of:

- User account database
- SNMP community strings

A user-level account can use the `ping` command to test device reachability and change the password assigned to the account name.

An administrator-level account can view and change all switch parameters. It can also add and delete users and change the password associated with any account name. The administrator can disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged on by way of the Telnet connection is notified that the session has been terminated.

The DNS client in ExtremeWare augments certain ExtremeWare commands to accept either IP addresses or host names. For example, DNS can be used during a Telnet session when you are accessing a device or when using the `ping` command to check the connectivity of a device.

The switch offers the following commands for checking basic connectivity:

- `ping`
- `traceroute`

The `ping` command enables you to send Internet Control Message Protocol (ICMP) echo messages to a remote IP device. The `traceroute` command enables you to trace the routed path between the switch and a destination endstation.

clear session

```
clear session <number>
```

Description

Terminates a Telnet session from the switch.

Syntax Description

number	Specifies a session number from `show session` output to terminate.

Default

N/A.

Usage Guidelines

An administrator-level account can disconnect a management session that has been established by way of a Telnet connection. You can determine the session number of the session you want to terminate by using the `show session` command. The `show session` output displays information about current Telnet sessions including:

- The session number
- The login date and time
- The user name
- The type of Telnet session

Depending on the software version running on your switch, additional session information may be displayed. The session number is the first number displayed in the `show session` output.

Example

The following command terminates session 4 from the system:

```
clear session 4
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure account

```
configure account <user account> {encrypted} {<password>}
```

Description

Configures a user account password.

Syntax Description

user account	Specifies a user account name.
encrypted	This option is for use only by the switch when generating an ASCII configuration file. Specifies that the password should be encrypted when the configuration is uploaded to a file. Should not be used through the CLI.
password	Specifies a user password. Supported in ExtremeWare 4.x and ExtremeWare 6.0.x only. In ExtremeWare 6.1 and later, the switch will prompt for entry of the password interactively.

Default

N/A.

Usage Guidelines

You must create a user account before you can configure a user account. Use the `create account` command to create a user account.

You must have administrator privileges to change passwords for accounts other than your own. User names and passwords are case-sensitive.

The `encrypted` option is used by the switch when generating an ASCII configuration file (using the `upload configuration` command), and parsing a switch-generated configuration file (using the `download configuration` command). Do not select the encrypted option in the CLI.

For ExtremeWare 6.1 and higher:

- The password cannot be specified on the command line. Instead, the switch will interactively prompt you to enter the password, and will then prompt you to reenter the password to verify that you have entered it correctly.

For ExtremeWare 6.0 and higher:

- Passwords must have a minimum of 1 character and can have a maximum of 30 characters.

For ExtremeWare 4.x:

- Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.

Example

The following command defines a new password for the account *admin*:

```
configure account admin
```

The switch responds with a password prompt:

```
password:
```

Your keystrokes will not be echoed as you enter the new password. After you enter the password, the switch will then prompt you to reenter it.

```
Reenter password:
```

Assuming you enter it successfully a second time, the password is now changed.

In ExtremeWare 4.1.19, the following command defines a new password, *Extreme1*, for the account *admin*:

```
configure account admin Extreme1
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure banner

```
configure banner
```

Description

Configures the banner string that is displayed at the beginning of each login prompt of each session.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Press [Return] at the beginning of a line to terminate the command and apply the banner. To clear the banner, press [Return] at the beginning of the first line.

For ExtremeWare 6.0 and higher:

- You can enter up to 24 rows of 79-column text that is displayed before the login prompt of each session.

For ExtremeWare 2.0 and ExtremeWare 4.x:

- You can enter up to 24 rows of 80-column text that is displayed before the login prompt of each session.

Example

The following command adds a banner, *Welcome to the switch*, before the login prompt:

```
configure banner [Return]
Welcome to the switch
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure banner netlogin

```
configure banner netlogin
```

Description

Configures the network login banner that is displayed at the beginning of each login prompt of each session.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The network login banner and the switch banner cannot be used at the same time. If you configure a Network Login banner, users do **not** see the normal banner. If no banner is configured, the Extreme logo is displayed. The network login banner displays in HTML. No links or images are supported.

Press [Enter] to enter text on a new line. Press [Enter] twice to finish entering the network login banner. You can enter up to 1024 characters in the banner.

Example

The following command adds the banner “Welcome to your switch” in 8 point purple Arial before the login prompt:

```
configure banner netlogin [Enter]
<font face="Arial" size=8 color=534579></font>Welcome to your switch
[Enter]
[Enter]
```

History

This command was introduced in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure dns-client add

```
configure dns-client add <ipaddress>
```

Description

Adds a DNS name server to the available server list for the DNS client.

Syntax Description

ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

Up to three DNS name servers can be configured in ExtremeWare versions prior to 6.2.1. In ExtremeWare 6.2.1 and later, eight DNS name servers can be configured.

Example

The following command specifies that the switch use the DNS server 10.1.2.1:

```
configure dns-client add 10.1.2.1
```

History

This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 6.2.1 to support up to eight DNS name servers.

Platform Availability

This command is available on all platforms.

configure dns-client add domain-suffix

```
configure dns-client add domain-suffix <domain_name>
```

Description

Adds a domain name to the domain suffix list.

Syntax Description

domain_name	Specifies a domain name.

Default

N/A.

Usage Guidelines

The domain suffix list can include up to six items. If the use of all previous names fails to resolve a name, the most recently added entry on the domain suffix list will be the last name used during name resolution. This command will not overwrite any exiting entries. If a null string is used as the last suffix in the list, and all other lookups fail, the name resolver will attempt to look up the name with no suffix.

Example

The following command configures a domain name and adds it to the domain suffix list:

```
configure dns-client add domain-suffix xyz_inc.com
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure dns-client add name-server

```
configure dns-client add name-server <ipaddress>
```

Description

Adds a DNS name server to the available server list for the DNS client.

Syntax Description

ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

Up to three DNS name servers can be configured in ExtremeWare versions prior to 6.2.1. In ExtremeWare 6.2.1 and later, eight DNS name servers can be configured.

Example

The following command specifies that the switch use the DNS server 10.1.2.1:

```
configure dns-client add name-server 10.1.2.1
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure dns-client default-domain

```
configure dns-client default-domain <domain_name>
```

Description

Configures the domain that the DNS client uses if a fully qualified domain name is not entered.

Syntax Description

domain_name	Specifies a default domain name.

Default

N/A.

Usage Guidelines

Sets the DNS client default domain name to `domain_name`. The default domain name will be used to create a fully qualified host name when a domain name is not specified. For example, if the default default domain name is set to “food.com” then when a command like “`ping dog`” is entered, the ping will actually be executed as “`ping dog.food.com`”.

Example

The following command configures the default domain name for the server:

```
configure dns-client default-domain xyz_inc.com
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure dns-client delete

```
configure dns-client delete <ipaddress>
```

Description

Removes a DNS name server from the available server list for the DNS client.

Syntax Description

ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

None

Example

The following command removes a DNS server from the list:

```
configure dns-client delete 10.1.2.1
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure dns-client delete domain-suffix

```
configure dns-client delete domain-suffix <domain_name>
```

Description

Deletes a domain name from the domain suffix list.

Syntax Description

domain_name	Specifies a domain name.

Default

N/A.

Usage Guidelines

This command randomly removes an entry from the domain suffix list. If the deleted item was not the last entry in the list, all items that had been added later are moved up in the list. If no entries in the list match the domain name specified, an error message will be displayed.

Example

The following command deletes a domain name from the domain suffix list:

```
configure dns-client delete domain-suffix xyz_inc.com
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure dns-client delete name-server

```
configure dns-client delete name-server <ipaddress>
```

Description

Removes a DNS name server from the available server list for the DNS client.

Syntax Description

ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes a DNS server from the list:

```
configure dns-client delete name-server 10.1.2.1
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure idletimeouts

```
configure idletimeouts <minutes>
```

Description

Configures the time-out for idle HTTP, console, and Telnet sessions.

Syntax Description

minutes	Specifies the time-out interval, in minutes. Range is 1 to 240 (1 minute to 4 hours).

Default

Default time-out is 20 minutes.

Usage Guidelines

This command configures the length of time the switch will wait before disconnecting idle HTTP, console, or Telnet sessions. The idletimeouts feature must be enabled for this command to have an effect (the idletimeouts feature is disabled by default).

In ExtremeWare v 6.2.0, the time-out interval was specified in seconds, not minutes.

Example

The following command sets the time-out for idle HTTP, login and console sessions to 10 minutes:

```
configure idletimeouts 10
```

History

This command was first available in ExtremeWare 6.2.

This command was modified in ExtremeWare 6.2.1 to change the time-out value specification to minutes.

Platform Availability

This command is available on all platforms.

configure time

```
configure time <date> <time>
```

Description

Configures the system date and time.

Syntax Description

date	Specifies the date in `mm/dd/yyyy` format.
time	Specifies the time in `hh:mm:ss` format.

Default

N/A.

Usage Guidelines

The format for the system date and time is as follows:

```
mm/dd/yyyy hh:mm:ss
```

The time uses a 24-hour clock format. The AM hours range from 1 through 11, and the PM hours range from 12 through 23.

For ExtremeWare 6.0 and higher:

- You cannot set the year past 2036.

For ExtremeWare 2.0 and 4.x:

- You cannot set the year past 2023.

Example

The following command configures a system date of February 15, 2002 and a system time of 8:42 AM and 55 seconds:

```
configure time 02/15/2002 08:42:55
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure timezone

```
configure timezone {name <std_timezone_ID>} <GMT_offset>
{autodst {name <dst_timezone_ID>} {<dst_offset>}
{begins [every <floatingday> | on <absoluteday>] {at <time_of_day>}
{ends [every <floatingday> | on <absoluteday>] {at <time_of_day>}}}
| noautodst}
```

Description

Configures the Greenwich Mean Time (GMT) offset and Daylight Saving Time (DST) preference.

Syntax Description

GMT_offset	Specifies a Greenwich Mean Time (GMT) offset, in + or - minutes.
std-timezone-ID	Specifies an optional name for this timezone specification. May be up to six characters in length. The default is an empty string.
autodst	Enables automatic Daylight Saving Time.
dst-timezone-ID	Specifies an optional name for this DST specification. May be up to six characters in length. The default is an empty string.
dst_offset	Specifies an offset from standard time, in minutes. Value is in the range of 1 to 60. Default is 60 minutes.
floating_day	Specifies the day, week, and month of the year to begin or end DST each year. Format is: <week><day><month> where: • <week> is specified as [first | second | third | fourth | last] or 1-5 • <day> is specified as [sunday | monday | tuesday | wednesday | thursday | friday | saturday] or 1-7 (where 1 is Sunday) • <month> is specified as [january | february | march | april | may | june | july | august | september | october | november | december] or 1-12 Default for beginning is first sunday april; default for ending is last sunday october.
absolute_day	Specifies a specific day of a specific year on which to begin or end DST. Format is: <month>/<day>/<year> where: • <month> is specified as 1-12 • <day> is specified as 1-31 • <year> is specified as 1970 - 2035 The year must be the same for the begin and end dates.
time_of_day	Specifies the time of day to begin or end Daylight Saving Time. May be specified as an hour (0-23) or as hour:minutes. Default is 2:00.
noautodst	Disables automatic Daylight Saving Time.

Default

Autodst, beginning every first Sunday in April, and ending every last Sunday in October.

Usage Guidelines

Network Time Protocol (NTP) server updates are distributed using GMT time. To properly display the local time in logs and other timestamp information, the switch should be configured with the appropriate offset to GMT based on geographic location.

The `gmt_offset` is specified in +/- minutes from the GMT time.

Automatic DST changes can be enabled or disabled. The default configuration, where DST begins on the first Sunday in April at 2:00 AM and ends the last Sunday in October at 2:00 AM, applies to most of North America, and can be configured with the following syntax:
`configure timezone <gmt_offst> autodst`.

As of ExtremeWare 6.2.1, the starting and ending date and time for DST may be specified, as these vary in time zones around the world.

- Use the `every` keyword to specify a year-after-year repeating set of dates (e.g. the last Sunday in March every year)
- Use the `on` keyword to specify a non-repeating, specific date for the specified year. If you use this option, you will need to specify the command again every year.
- The `begins` specification defaults to `every first sunday april`.
- The `ends` specification defaults to `every last sunday october`.
- The `ends` date may occur earlier in the year than the `begins` date. This will be the case for countries in the Southern Hemisphere.
- If you specify only the starting or ending time (not both) the one you leave unspecified will be reset to its default.
- The `time_of_day` specification defaults to `2:00`
- The timezone IDs are optional. They are used only in the display of timezone configuration information in the `show switch` command.

To disable automatic DST changes, re-specify the GMT offset using the `noautodst` option:
`configure timezone <gmt_offst> noautodst`.

NTP updates are distributed using GMT time. To properly display the local time in logs and other timestamp information, the switch should be configured with the appropriate offset to GMT based on geographical location. Table 5 describes the GMT offsets.

Table 5: Greenwich Mean Time Offsets

GMT Offset in Hours	GMT Offset in Minutes	Common Time Zone References	Cities
+0:00	+0	GMT - Greenwich Mean UT or UTC - Universal (Coordinated) WET - Western European	London, England; Dublin, Ireland; Edinburgh, Scotland; Lisbon, Portugal; Reykjavik, Iceland; Casablanca, Morocco
-1:00	-60	WAT - West Africa	Azores, Cape Verde Islands
-2:00	-120	AT - Azores	
-3:00	-180		Brasilia, Brazil; Buenos Aires, Argentina; Georgetown, Guyana;
-4:00	-240	AST - Atlantic Standard	Caracas; La Paz

Table 5: Greenwich Mean Time Offsets (continued)

GMT Offset in Hours	GMT Offset in Minutes	Common Time Zone References	Cities
-5:00	-300	EST - Eastern Standard	Bogota, Columbia; Lima, Peru; New York, NY, Trevor City, MI USA
-6:00	-360	CST - Central Standard	Mexico City, Mexico
-7:00	-420	MST - Mountain Standard	Saskatchewan, Canada
-8:00	-480	PST - Pacific Standard	Los Angeles, CA, Cupertino, CA, Seattle, WA USA
-9:00	-540	YST - Yukon Standard	
-10:00	-600	AHST - Alaska-Hawaii Standard	
		CAT - Central Alaska	
		HST - Hawaii Standard	
-11:00	-660	NT - Nome	
-12:00	-720	IDLW - International Date Line West	
+1:00	+60	CET - Central European	Paris, France; Berlin, Germany; Amsterdam, The Netherlands; Brussels, Belgium; Vienna, Austria; Madrid, Spain; Rome, Italy; Bern, Switzerland; Stockholm, Sweden; Oslo, Norway
		FWT - French Winter	
		MET - Middle European	
		MEWT - Middle European Winter	
		SWT - Swedish Winter	
+2:00	+120	EET - Eastern European, Russia Zone 1	Athens, Greece; Helsinki, Finland; Istanbul, Turkey; Jerusalem, Israel; Harare, Zimbabwe
+3:00	+180	BT - Baghdad, Russia Zone 2	Kuwait; Nairobi, Kenya; Riyadh, Saudi Arabia; Moscow, Russia; Tehran, Iran
+4:00	+240	ZP4 - Russia Zone 3	Abu Dhabi, UAE; Muscat; Tblisi; Volgograd; Kabul
+5:00	+300	ZP5 - Russia Zone 4	
+5:30	+330	IST – India Standard Time	New Delhi, Pune, Allahabad, India
+6:00	+360	ZP6 - Russia Zone 5	
+7:00	+420	WAST - West Australian Standard	
+8:00	+480	CCT - China Coast, Russia Zone 7	
+9:00	+540	JST - Japan Standard, Russia Zone 8	
+10:00	+600	EAST - East Australian Standard	
		GST - Guam Standard	
		Russia Zone 9	
+11:00	+660		
+12:00	+720	IDLE - International Date Line East	Wellington, New Zealand; Fiji, Marshall Islands
		NZST - New Zealand Standard	
		NZT - New Zealand	

Example

The following command configures GMT offset for Mexico City, Mexico and disables automatic DST:

```
configure timezone -360 noautodst
```

The following four commands are equivalent, and configure the GMT offset and automatic DST adjustment for the US Eastern timezone, with an optional timezone ID of EST:

```
configure timezone name EST -300 autodst name EDT 60 begins every first sunday april
at 2:00 ends every last sunday october at 2:00

configure timezone name EST -300 autodst name EDT 60 begins every 1 1 4 at 2:00 ends
every 5 1 10 at 2:00

configure timezone name EST -300 autodst name EDT

configure timezone -300 autodst
```

The following command configures the GMT offset and automatic DST adjustment for the Middle European timezone, with the optional timezone ID of MET:

```
configure timezone name MET 60 autodst name MDT begins every last sunday march at 1
ends every last sunday october at 1
```

The following command configures the GMT offset and automatic DST adjustment for New Zealand. The ending date must be configured each year because it occurs on the first Sunday on or after March 5:

```
configure timezone name NZST 720 autodst name NZDT 60 begins every first sunday
october at 2 ends on 3/16/2002 at 2
```

History

This command was first available in ExtremeWare 4.0.

Modified in ExtremeWare 6.2.1 to allow configuration of a beginning and ending time for the automatic DST.

Platform Availability

This command is available on all platforms.

create account

```
create account [admin | user] <username> {encrypted} {<password>}
```

Description

Creates a new user account.

Syntax Description

admin	Specifies an access level for account type `admin`.
user	Specifies an access level for account type `user`.
username	Specifies a new user account name. See “Usage Guidelines” for more information.
encrypted	Specifies an encrypted option.
password	Specifies a user password. See “Usage Guidelines” for more information.

Default

By default, the switch is configured with two accounts with the access levels shown in Table 6:

Table 6: User Account Levels

Account Name	Access Level
admin	This user can access and change all manageable parameters. The admin account cannot be deleted.
user	This user can view (but not change) all manageable parameters, with the following exceptions: • This user cannot view the user account database. • This user cannot view the SNMP community strings. This user has access to the `ping` command.

You can use the default names (*admin* and *user*), or you can create new names and passwords for the accounts. Default accounts do not have passwords assigned to them.

Usage Guidelines

The switch can have a total of 16 user accounts. There must be one administrator account on the system.

You must have administrator privileges to change passwords for accounts other than your own. User names and passwords are case-sensitive.

For ExtremeWare 6.0 and higher:

- User account names must have a minimum of 1 character and can have a maximum of 30 characters.
- Passwords must have a minimum of 0 characters and can have a maximum of 16 characters.

For ExtremeWare 4.x and higher:

- Admin-level users and users with RADIUS command authorization can use the `create account` command.

For ExtremeWare 4.x:

- User account name specifications are not available.
- Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.
- The encrypted option should only be used by the switch to generate an ASCII configuration (using the `upload configuration` command), and parsing a switch-generated configuration (using the `download configuration` command).

Example

The following command creates a new account named John2 with administrator privileges:

```
create account admin john2
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support the encrypted option. In addition, admin-level users with RADIUS command authorization were allowed to use the `create account` command.

Platform Availability

This command is available on all platforms.

delete account

```
delete account <username>
```

Description

Deletes a specified user account.

Syntax Description

username	Specifies a user account name.

Default

N/A

Usage Guidelines

Use the `show accounts` command to determine which account you want to delete from the system. The show accounts output displays the following information in a tabular format:

- The user name
- Access information associated with each user
- User login information
- Session information

Depending on the software version running on your switch and the type of switch you have, additional account information may be displayed.

You must have administrator privileges to delete a user account. There must be one administrator account on the system; the command will fail if an attempt is made to delete the last administrator account on the system.

Do not delete the default administrator account. If you do, it is automatically restored, with no password, the next time you download a configuration. To ensure security, change the password on the default account, but do not delete it. The changed password will remain intact through configuration uploads and downloads.

If you must delete the default account, first create another administrator-level account. Remember to manually delete the default account again every time you download a configuration.

Example

The following command deletes account John2:

```
delete account john2
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable clipaging

```
disable clipaging
```

Description

Disables pausing at the end of each show screen.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

The command line interface (CLI) is designed for use in a VT100 environment. Most show command output will pause when the display reaches the end of a page. This command disables the pause mechanism and allows the display to print continuously to the screen.

NOTE

Press [q] and then press [Return] to force a pause when CLI paging is disabled.

To view the status of CLI paging on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for CLI paging.

Example

The follow command disables clipaging and allows you to print continuously to the screen:

```
disable clipaging
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable idletimeouts

```
disable idletimeouts
```

Description

Disables the timer that disconnects idle sessions from the switch.

Syntax Description

This command has no arguments or variables.

Default

Enabled. Timeout 20 minutes.

Usage Guidelines

When idle time-outs are disabled, console sessions remain open until the switch is rebooted or you logoff. Telnet sessions remain open until you close the Telnet client.

To view the status of idle time-outs on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for idle time-outs.

Example

The following command disables the timer that disconnects all sessions to the switch:

```
disable idletimeouts
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable clipaging

```
enable clipaging
```

Description

Enables the pause mechanism and does not allow the display to print continuously to the screen.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

The command line interface (CLI) is designed for use in a VT100 environment. Most show command output will pause when the display reaches the end of a page.

To view the status of CLI paging on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for CLI paging.

If CLI paging is enabled and you use the `show tech-support` command to diagnose system technical problems, the CLI paging feature is disabled.

Example

The following command enables clipaging and does not allow the display to print continuously to the screen:

```
enable clipaging
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable idletimeouts

```
enable idletimeouts
```

Description

Enables a timer that disconnects Telnet and console sessions after 20 minutes of inactivity.

Syntax Description

This command has no arguments or variables.

Default

Enabled. Timeout 20 minutes.

Usage Guidelines

You can use this command to ensure that a Telnet, HTTP, or console session is disconnected if it has been idle for the required length of time. This ensures that there are no hanging connections.

To view the status of idle time-outs on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for idle time-outs.

In ExtremeWare 6.2 or later, you can configure the length of the time-out interval.

Example

The following command enables a timer that disconnects any Telnet, HTTP, and console sessions after 20 minutes of inactivity:

```
enable idletimeouts
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable license

```
enable license [basic_L3 | advanced_L3 | full_L3 ] <license_key>
```

Description

Enables a particular software feature license.

Syntax Description

basic_L3	Specifies a basic L3 license. (4.x only)
advanced_L3	Specifies an advanced L3 license. (4.x only)
full_L3	Specifies a full L3 license. (6.0, 6.1 and higher)
license_key	Specifies your software license key.

Default

N/A

Usage Guidelines

Specify `license_key` as an integer.

The `unconfigure switch all` command does not clear licensing information. This feature cannot be disabled after the license has been enabled on the switch.

Depending on the software version running on your switch, and the type of switch you have, only the license parameters applicable to your software or switch can be used.

To view the type of license you are currently running on the switch, use the `show switch` command. The license key number is not displayed, but the type of license is displayed in the `show switch` output. The type of license is displayed after the system name, system location, system contact, and system MAC address.

Example

The following command enables a full L3 license on the switch:

```
enable license fullL3
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

history

```
history
```

Description

Displays a list of the previous 49 commands entered on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

ExtremeWare “remembers” the last 49 commands you entered on the switch. Use the `history` command to display a list of these commands.

Example

The following command displays the previous 49 commands entered on the switch:

```
history
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

reboot

```
reboot {time <date> <time> | cancel} {slot <slot number> | msm-a | msm-b}
```

Description

Reboots the switch or the module in the specified slot at a specified date and time.

Syntax Description

date	Specifies a reboot date in mm/dd/yyyy format.
time	Specifies a reboot time in hh:mm:ss format.
cancel	Cancels a previously scheduled reboot.
slot number	Specifies the slot where the module is installed.
msm-a	Specifies a BlackDiamond MSM module installed in slot A.
msm-b	Specifies a BlackDiamond MSM module installed in slot B.

Default

N/A.

Usage Guidelines

If you do not specify a reboot time, the switch will reboot immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the cancel option.

The slot <slot number> option is added to the command to make it possible to reboot a module in a specific slot. When you specify this option, the command applies to the module in the specified slot, rather than to the switch. In general, the modules that can be rebooted have separate images from the ExtremeWare image for the switch.

The modules that can be rebooted are: E1, T1, T3, ARM, ATM, MPLS, PoS, and slave or switch fabric MSM modules.

NOTE

When you configure a timed reboot of an MSM, there is no show output in the CLI to view the configuration.

The E1, T1, and T3 reboot slot command does not support the time or cancel keywords, so this command can only be executed immediately.

Example

The following command reboots the switch at 8:00 AM on April 15, 2002:

```
reboot 04/15/2002 08:00:00
```

The following command reboots the MPLS module in slot number 5:

```
reboot time 10/04/2001 10,46,00 slot 5
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 7.0.0 to include the `slot` option.

This command was modified in ExtremeWare 7.1.0 to include the `msm-a` and `msm-b` options.

Platform Availability

This command is available on all platforms.

show accounts pppuser

```
show accounts pppuser
```

Description

Displays user account information for all users on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

You need to create a user account using the `create account` command before you can display user account information.

To view the accounts that have been created, you must have administrator privileges.

The `show accounts` command displays the following information in a tabular format:

- **User Name**—The name of the user. This list displays all of the users who have access to the switch.
- **Access**—The SNMP community strings. This may be listed as R/W for read/write or RO for read only.
- **Login OK**—The number of logins that are okay.
- **Failed**—The number of failed logins.

Depending on the software version running on your switch, additional or different account information may be displayed.

Example

The following command displays user account information on the switch:

```
show accounts pppuser
```

Output from this command looks similar to the following:

```
User Name       Access LoginOK Failed  PPPUser
---------------- ------ -------  ------ -------
           admin   R/W        3       1
            user   RO         0       0
        dbackman   R/W        0       0
             ron   RO         0       0
         nocteam   RO         0       0
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show banner

```
show banner
```

Description

Displays the user-configured banner string.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to view the banner that is displayed before the login prompt.

Example

The following command displays the switch banner:

```
show banner
```

Output from this command looks similar to the following:

```
Extreme Networks Summit48i Layer 3 Switch
############################################################
  Unauthorized Access is strictly prohibited.
  Violators will be persecuted
############################################################
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show dns-client

```
show dns-client
```

Description

Displays the DNS configuration.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the DNS configuration:

```
show dns-client
```

Output from this command looks similar to the following:

```
Number of domain suffixes: 2
Domain Suffix 1:        njudah.local
Domain Suffix 2:        dbackman.com
Number of name servers: 2
Name Server 1:  172.17.1.104
Name Server 2:  172.17.1.123
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show switch

```
show switch
```

Description

Displays the current switch information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

The `show switch` command displays:

- sysName, sysLocation, sysContact
- MAC address
- License type
- System mode
- Diagnostics mode (BlackDiamond switch only)
- RED configuration
- DLCS state
- Backplane load sharing (BlackDiamond switch only)
- System health check
- Recovery mode
- Transceiver diagnostics
- FDB-scan diagnostics
- MSM failover information (BlackDiamond switch only)
- Watchdog state
- Reboot loop information
- Current date, time, system boot time, and time zone configuration
- Configuration modified information
- Any scheduled reboot information
- Scheduled upload/download information
- Operating environment (temperature, fans, and power supply status)
- Software image information (primary/secondary image, date/time, version)

- NVRAM configuration information (primary/secondary configuration, date/time, size, version)
- PACE configuration information
- Software licensing information
- MSM information (BlackDiamond switch only)
- Mode of switch operation (Alpine 3802 only)

This information may be useful for your technical support representative if you have a problem.

Depending on the software version running on your switch, additional or different switch information may be displayed.

Example

The following command displays current switch information:

```
show switch
```

Output from this command looks similar to the following:

```
SysName:          Alpine3804
SysLocation:      Extreme Networks HQ
SysContact:       Carlos_Beronio
System MAC:       00:01:30:23:C1:00

License:          Full L3
System Mode:      802.1Q EtherType is 8100 (Hex).   CPU Tx-Priority = High

RED Probability:  0
DLCS:             Enabled

SysHealth Check:  Enabled.   Alarm Level = Log
Recovery Mode:    All - System-dump/Reboot
Transceiver Diag: Enabled.    Failure action:  log only
Fdb-Scan Diag:    Enabled.    Failure action:  log only
System Watchdog:  Enabled
Reboot Loop Prot: Disabled

Current Time:     Tue Jun 10 07:39:40 2003
Timezone:         [Auto DST Enabled] GMT Offset: 0 minutes, name is GMT.
                  DST of 60 minutes is currently not in effect, name is not set.
                  DST begins every first Sunday April at 2:00
                  DST ends every last Sunday October at 2:00
Boot Time:        Wed Jun 4 11:52:38 2003
Config Modified:  Mon Jun 9 15:09:44 2003
Next Reboot:      None scheduled
Timed Upload:     None scheduled
Timed Download:   None scheduled

Temperature:      Normal.    All fans are operational.
Power supply:     Upper (PSU-A) not present,   Lower (PSU-B) OK
Image Selected:   Primary
Image Booted:     Primary

Primary EW Ver:   7.0.0b61 [unknown-ssh]
Secondary EW Ver: 7.1.0b34 [non-ssh]
```

```
Module            Image Selected    Image Booted
------            --------------    ------------
SMM               Secondary         Secondary
Slot 2 (WM4T1)    Secondary         Secondary


Config Selected:  Primary
Config Booted:    Primary
Primary Config:   Created by EW Version:
                  7.1.0 Build 34  [38]
                  7928 bytes saved on Wed Jun 4 11:54:03 2003
Secondary Config: Created by EW Version:
                  6.2.2 Build 56 [38]
                  2900 bytes saved on Thu Jan 30 04:21:10 2003
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1.8 to display the mode of switch operation—extended, standard, or auto—for the Alpine 3802.

This command was modified in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

traceroute

```
traceroute <host name/ip> {from <source IP address>} {ttl <number>} {port
<port number>}
```

Description

Enables you to trace the routed path between the switch and a destination endstation.

Syntax Description

host name/ip	Specifies the hostname or IP address of the destination endstation.
from <source IP address>	Uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used. (6.1 and higher)
ttl <number>	Configures the switch to trace up to the time-to-live number of the switch. (6.1 and higher)
port <port number>	Specifies the UDP port number. (6.1 and higher)

Default

N/A.

Usage Guidelines

To use the `host name` parameter, you must first configure DNS.

Each router along the path is displayed.

Example

The following command enables the traceroute function to a destination of 123.45.67.8:

```
traceroute 123.45.67.8
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support the `hostname` parameter.

This command was modified in ExtremeWare 6.1 to support the `from`, `ttl`, and `port` parameters.

Platform Availability

This command is available on all platforms.

3 Commands for Managing the Switch

This chapter describes:

- Commands for configuring Simple Network Management Protocol (SNMP) parameters on the switch
- Commands for managing the switch using Telnet and web access
- Commands for configuring Simple Network Time Protocol (SNTP) parameters on the switch

SNMP

Any network manager running the Simple Network Management Protocol (SNMP) can manage the switch, if the Management Information Base (MIB) is installed correctly on the management station. Each network manager provides its own user interface to the management facilities.

The following SNMP parameters can be configured on the switch:

- **Authorized trap receivers**—An authorized trap receiver can be one or more network management stations on your network. The switch sends SNMP traps to all trap receivers. Entries in this list can be created, modified, and deleted using the RMON2 trapDestTable MIB variable, as described in RFC 2021.
- **Authorized managers**—An authorized manager can be either a single network management station, or a range of addresses (for example, a complete subnet) specified by a prefix and a mask. The switch can have a maximum of eight authorized managers.
- **Community strings**—The community strings allow a simple method of authentication between the switch and the remote Network Manager. The default read-only community string is *public*. The default read-write community string is *private*. The community strings for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps.
- **System contact (optional)**—The system contact is a text field that enables you to enter the name of the person(s) responsible for managing the switch.
- **System name**—The system name is the name that you have assigned to this switch. The default name is the model name of the switch (for example, Summit1).
- **System location (optional)**—Using the system location field, you can enter an optional location for this switch.

The following can also be configured on the switch for version 6.0 and higher:

- **SNMP read access**—The ability to read SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.
- **SNMP read/write access**—The ability to read and write SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.

Telnet

Telnet allows you to access the switch remotely using TCP/IP through one of the switch ports or a workstation with a Telnet facility. If you access the switch via Telnet, you will use the command line interface (CLI) to manage the switch and modify switch configurations.

Simple Network Time Protocol

ExtremeWare supports the client portion of the Simple Network Time Protocol (SNTP) Version 3 based on RFC1769. SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. When enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean time (GMT) offset and the use of Daylight Saving Time. These features have been tested for year 2000 compliance.

ExtremeWare Vista

ExtremeWare Vista is a device management software running in the switch that allows you to access the switch over a TCP/IP network using a standard web browser. ExtremeWare Vista provides a subset of the CLI commands available for configuring and monitoring the switch. If a particular command is not available using ExtremeWare Vista, you must use the CLI to access the desired functionality.

configure snmp access-profile readonly

```
configure snmp access-profile readonly [<access-profile> | none]
```

Description

Assigns an access profile that limits which stations have read-only access to the switch.

Syntax Description

access-profile	Specifies a user defined access profile.
none	Cancels a previously configured access profile.

Default

All users have access until an access profile is created and specified.

Usage Guidelines

The ability to read SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.

You must create and configure an access profile before you can use this command. You create an access profile using the `create access-profile` command. You configure an access profile using the `configure access-profile` command.

Use the none option to remove a previously configured access profile.

Read community strings provide read-only access to the switch. The default read-only community string is public. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 32 characters.

To view the SNMP read-only access communities configured on the switch, use the `show management` command. The `show management` command displays information about the switch including the encrypted names and the number of read-only communities configured on the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp access-profile readonly` command, use the `unconfigure management` command.

Example

The following command allows the user defined access profile *admin* read-only access to the switch:

```
configure snmp access-profile readonly admin
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure snmp access-profile readwrite

```
configure snmp access-profile readwrite [<access-profile> | none]
```

Description

Assigns an access profile that limits which stations have read/write access to the switch.

Syntax Description

access-profile	Specifies a user defined access profile.
none	Cancels a previously configured access profile.

Default

All users have access until an access profile is specified.

Usage Guidelines

The ability to read SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.

You must create and configure an access profile before you can use this command. You create an access profile using the `create access-profile` command. You configure an access profile using the `configure access-profile` command.

Use the none option to remove a previously configured access profile.

Read/write community strings provide read and write access to the switch. The default read/write community string is *private*. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 32 characters.

To view the SNMP read/write access communities configured on the switch, use the `show management` command. The `show management` command displays information about the switch including the names and the number of read/write communities configured on the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp access-profile readwrite` command, use the `unconfigure management` command.

Example

The following command allows the user defined access profile *management* read/write access to the switch:

```
configure snmp access-profile readwrite management
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure snmp add community

```
configure snmp add community [readonly | readwrite] {encrypted}
<alphanumeric string>
```

Description

Adds an SNMP read or read/write community string.

Syntax Description

readonly	Specifies read-only access to the system.
readwrite	Specifies read and write access to the system.
encrypted	Specifies encryption, for use only by the switch when uploading or downloading a configuration. Should not be used through the CLI.
alphanumeric string	Specifies an SNMP community string name. See “Usage Guidelines” for more information.

Default

The default read-only community string is *public*. The default read/write community string is *private*.

Usage Guidelines

Community strings provide a simple method of authentication between a switch and a remote network manager. Read community strings provide read-only access to the switch. The default read-only community string is *public*. Read-write community strings provide read and write access to the switch. The default read/write community string is *private*.

An authorized trap receiver must be configured to use the correct community strings on the switch for the trap receiver to receive switch-generated traps. In some cases, it may be useful to allow multiple community strings so that all switches and trap receivers are not forced to use identical community strings. The `configure snmp add community` command allows you to add multiple community strings in addition to the default community string.

An SNMP community string can contain up to 32 characters.

To change the value of the default read/write and read-only community strings, use the `configure snmp community` command.

The `encrypted` option is intended for use by the switch when generating an ASCII configuration file (using the `upload configuration` command), or parsing a switch-generated configuration (using the `download configuration` command). Do not select the encrypted option in the CLI.

Example

The following command adds a read/write community string with the value *extreme*:

```
configure snmp add community readwrite extreme
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure snmp add trapreceiver

```
configure snmp add trapreceiver <ip address> {port <number>} community
{hex} <community string> {from <source ip address>} {mode [enhanced |
standard]} trap-group {auth-traps{,}} {bgp-traps{,}} {extreme-traps{,}}
{link-up-down-traps{,}} {ospf-traps{,} {ping-traceroute-traps{,}}
{rmon-traps{,}} {security-traps{,}} {smart-traps{,}} {stp-traps{,}}
{system-traps{,}} {vrrp-traps{,}}
```

Description

Adds the IP address of a trap receiver to the trap receiver list and specifies which SNMPv1/v2c traps are to be sent.

Syntax Description

ip address	Specifies an SNMP trap receiver IP address.
port <number>	Specifies a UDP port to which the trap should be sent. Default is 162.
hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
community string	Specifies the community string of the trap receiver.
source ip address	Specifies the IP address of a VLAN to be used as the source address for the trap
enhanced	Specifies enhanced traps, which contain extra varbinds at the end.
standard	Specifies standard traps, which do not constrain the extra varbinds.
auth-traps	Specifies that authentication traps will be sent to the trap receiver.
bgp-traps	Specifies that BGP traps will be sent to the trap receiver.
extreme-traps	Specifies that Extreme Networks specific traps will be sent to the trap receiver.
link-up-down-traps	Specifies that link state traps will be sent to the trap receiver.
ospf-traps	Specifies that OSPF traps will be sent to the trap receiver.
ping-traceroute-traps	Specifies that ping and traceroute traps will be sent to the trap receiver.
rmon-traps	Specifies that RMON traps will be sent to the trap receiver.
security-traps	Specifies that security traps will be sent to the trap receiver.
smart-traps	Specifies that Extreme Networks smart traps will be sent to the trap receiver.
stp-traps	Specifies that STP traps will be sent to the trap receiver.
system-traps	Specifies that system traps will be sent to the trap receiver.
vrrp-traps	Specifies that VRRP traps will be sent to the trap receiver.

Default

Trap receivers are in enhanced mode by default, and the version is SNMPv2c by default.

Usage Guidelines

The IP address can be unicast, multicast, or broadcast.

An authorized trap receiver can be one or more network management stations on your network. Authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. The switch sends SNMP traps to all trap receivers configured to receive the specific trap group. If no trap groups are specified, all traps will be sent to the receiver. Entries in this

list can be created, modified, and deleted using the RMON2 trapDestTable MIB variable, as described in RFC 2021.

Table 7 lists the currently defined SNMP trap groups. From time to time, new trap groups may be added to this command.

Table 7: SNMP Trap Groups

Trap Group	Notifications	MIB Subtree
stp-traps	newRoot topologyChange	dot1dBridge, 1.3.6.1.2.1.17
bgp-traps	bgpEstablished bgpBackwardTransition extremeBgpPrefixReachedThreshold extremeBgpPrefixMaxExceeded	bgpTraps, 1.3.6.1.2.1.15.7 extremeBgpTrapsPrefix, 1.3.6.1.4.1.1916.4.2.0
ospf-traps	ospfIfStateChange ospfVirtIfStateChange ospfNbrStateChange ospfVirtNbrStateChange ospfIfConfigError ospfVirtIfConfigError ospfIfAuthFailure ospfVirtIfAuthFailure ospfIfRxBadPacket ospfVirtIfRxBadPacket ospfTxRetransmit ospfVirtIfTxRetransmit ospfOriginateLsa ospfMaxAgeLsa ospfLsdbOverflow ospfLsdbApproachingOverflow	ospfTraps, 1.3.6.1.2.1.14.16.2
ping-traceroute-traps	pingTestFailed pingTestCompleted tracerouteTestFailed tracerouteTestCompleted	pingNotifications, 1.3.6.1.2.1.80.0 traceRouteNotifications, 1.3.6.1.2.1.81.0
vrrp-traps	vrrpTrapNewMaster vrrpTrapAuthFailure	vrrpNotifications, 1.3.6.1.2.1.68.0
system-traps	extremeOverheat extremeFanFailed extremeFanOK extremePowerSupplyFail extremePowerSupplyGood extremeModuleStateChange extremeHealthCheckFailed extremeCpuUtilizationRisingTrap extremeCpuUtilizationFallingTrap coldStart warmStart	1.3.6.1.4.1.1916.0.6 1.3.6.1.4.1.1916.0.7 1.3.6.1.4.1.1916.0.8 1.3.6.1.4.1.1916.0.10 1.3.6.1.4.1.1916.0.11 1.3.6.1.4.1.1916.0.15 1.3.6.1.4.1.1916.4.1.0.1 1.3.6.1.4.1.1916.4.1.0.2 1.3.6.1.4.1.1916.4.1.0.3 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.5.2
extreme-traps	extremeEsrpStateChange extremeEdpNeighborAdded extremeEdpNeighborRemoved extremeSlbUnitAdded extremeSlbUnitRemoved	1.3.6.1.4.1.1916.0.17 1.3.6.1.4.1.1916.0.20 1.3.6.1.4.1.1916.0.21 1.3.6.1.4.1.1916.0.18 1.3.6.1.4.1.1916.0.19
smart-traps	extremeSmartTrap	1.3.6.1.4.1.1916.0.14
auth-traps	AuthenticationFailure extremeInvalidLoginAttempt	1.3.6.1.6.3.1.1.5.5 1.3.6.1.4.1.1916.0.9

Table 7: SNMP Trap Groups (continued)

Trap Group	Notifications	MIB Subtree
link-up-down-traps	linkDown linkUp	1.3.6.1.6.3.1.1.5.3 1.3.6.1.6.3.1.1.5.4
rmon-traps	risingAlarm fallingAlarm	rmon-traps, 1.3.6.1.2.1.16.0
security-traps	extremeMacLimitExceeded extremeUnauthorizedPortForMacDetected extremeMacDetectedOnLockedPort extremeNetloginUserLogin extremeNetloginUserLogout extremeNetloginAuthFailure	1.3.6.1.4.1.1916.4.3.0.1 1.3.6.1.4.1.1916.4.3.0.2 1.3.6.1.4.1.1916.4.3.0.3 1.3.6.1.4.1.1916.4.3.0.4 1.3.6.1.4.1.1916.4.3.0.5 1.3.6.1.4.1.1916.4.3.0.6

To view the SNMP trap receivers configured on the switch, use the `show management` command. The `show management` command displays information about the switch including the destination and community of the SNMP trap receivers configured on the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp add trapreceiver` command, use the `unconfigure management` command.

For version 7.1 and higher:

- Only the trap groups specified will be sent to the receiver.

  ExtremeWare 7.1 introduced support for SNMPv3, and the concept of trap groups was added to allow SNMPv1/v2c users to access a simplified version of the capabilities of SNMPv3. The trap groups are pre-defined and cannot be modified. See chapter 3, “Managing the Switch”, in the *ExtremeWare Software User Guide* for more detail about trap groups.

For version 6.0 and higher:

- A maximum of sixteen trap receivers can be configured for each switch.

For version 4.x:

- A maximum of six trap receivers can be configured for each switch.

Example

The following command adds the IP address 10.101.0.100 as a trap receiver with community string *purple*:

```
configure snmp add trapreceiver 10.101.0.100 community purple
```

The following command adds the IP address 10.101.0.105 as a trap receiver with community string *green*, using port 3003:

```
configure snmp add trapreceiver 10.101.0.105 port 3003 community green
```

The following command adds the IP address 10.101.0.105 as a trap receiver with community string *blue*, and IP address 10.101.0.25 as the source:

```
configure snmp add trapreceiver 10.101.0.105 community blue from 10.101.0.25
```

The following command adds port 9990 at the IP address 10.203.0.22 as a trap receiver with the community string *public*, and the receiver should be sent standard traps for the trap groups for BGP and Extreme Networks:

```
configure snmp add trapreceiver ipaddress 10.203.0.22 port 9990 community public mode
standard trap-group extreme-traps, bgp-traps
```

History

This command was first available in ExtremeWare 1.0.

This command was modified in ExtremeWare 6.2.1 to support the `port`, `community`, and source (`from`) options.

This command was modified in ExtremeWare 6.2.2 to add the `mode` options.

This command was modified in ExtremeWare 7.1.0 to add trap groups and the `version` option.

Platform Availability

This command is available on all platforms.

configure snmp community

```
configure snmp community [readonly | readwrite] {encrypted} <alphanumeric
string>
```

Description

Configures the value of the default SNMP read or read/write community string.

Syntax Description

readonly	Specifies read-only access to the system.
readwrite	Specifies read and write access to the system.
encrypted	Specifies encryption, for use only by the switch when uploading or downloading a configuration. Should not be used through the CLI.
alphanumeric string	Specifies an SNMP community string name. See “Usage Guidelines” for more information.

Default

The default read-only community string is *public*. The default read/write community string is *private*.

Usage Guidelines

This command has been superseded by the `configure snmp add community` command and can be used only to modify the first read-only or read-write community string which, are normally the default public and private community strings.

The community strings allow a simple method of authentication between the switch and the remote network manager. There are two types of community strings on the switch. Read community strings provide read-only access to the switch. The default read-only community string is *public*. Read-write community strings provide read and write access to the switch. The default read/write community string is *private*.

It is recommended that you change the values of the default read/write and read-only community strings. You use the `configure snmp community` command to change the value of the default community strings. An SNMP community string can contain up to 32 characters.

The `encrypted` option is intended for use by the switch when generating an ASCII configuration file (using the `upload configuration` command), or parsing a switch-generated configuration (using the `download configuration` command). Do not select the encrypted option in the CLI.

For version 6.2:

- A total of sixteen community strings can be configured on the switch. You can add additional community strings (in addition to the default community stings) using the `configure snmp add community` command.

Example

The following command sets the read/write community string to *extreme*:

```
configure snmp community readwrite extreme
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure snmp delete community

```
configure snmp delete community [readonly | readwrite] {encrypted} [all |
<alphanumeric string>]
```

Description

Deletes an SNMP read or read/write community string.

Syntax Description

readonly	Specifies read-only access to the system.
readwrite	Specifies read and write access to the system.
encrypted	Specifies an encrypted option.
all	Specifies all of the SNMP community stings.
alphanumeric string	Specifies an SNMP community string name. See “Usage Guidelines” for more information.

Default

The default read-only community string is *public*. The default read/write community string is *private*.

Usage Guidelines

The community strings allow a simple method of authentication between the switch and the remote network manager. There are two types of community strings on the switch. Read community strings provide read-only access to the switch. The default read-only community string is *public*. read/write community strings provide read and write access to the switch. The default read/write community string is *private*. Sixteen read-only and sixteen read-write community strings can be configured on the switch, including the defaults. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 32 characters.

It is recommended that you change the defaults of the read/write and read-only community strings.

Use the `configure snmp add` command to configure an authorized SNMP management station.

The `encrypted` option should only be used by the switch to generate an ASCII configuration (using the `upload configuration` command), and parsing a switch-generated configuration (using the `download configuration` command). Do not select the encrypted option in the CLI.

For version 6.0 and 6.1:

- A total of eight community strings can be configured on the switch.

For version 4.x:

- SNMP community strings can contain up to 126 characters.

For version 2.0:

- The `add` parameter is included in the command syntax. It is available only in version 2.0.
- SNMP community strings can contain up to 127 characters.

Example

The following command adds a read/write community string named *extreme*:

```
configure snmp add community readwrite extreme
```

History

This command was first available in ExtremeWare 2.0.

Support for the add parameter was discontinued in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure snmp delete trapreceiver

```
configure snmp delete trapreceiver [{<ip address> {port <number>}} | {all}]
```

Description

Deletes a specified trap receiver or all authorized trap receivers.

Syntax Description

ip address	Specifies an SNMP trap receiver IP address.
port <number>	Specifies the port associated with the receiver.
all	Specifies all SNMP trap receiver IP addresses.

Default

The default port number is 162.

Usage Guidelines

Use this command to delete a trap receiver of the specified IP address, or all authorized trap receivers.

Beginning in ExtremeWare 7.1.0, this command deletes only the first SNMPv1/v2c trap receiver whose IP address and port number match the specified value.

If a trap receiver has been added multiple times with different community strings, the `community` option specifies that only the trap receiver entry with the specified community string should be removed.

Example

The following command deletes the trap receiver 10.101.0.100 from the trap receiver list:

```
configure snmp delete trapreceiver 10.101.0.100
```

The following command deletes entries in the trap receiver list for 10.101.0.100, port 9990:

```
configure snmp delete trapreceiver 10.101.0.100 port 9990
```

Any entries for this IP address with a different community string will not be affected.

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.1 to support the `community` option.

This command was modified in ExtremeWare 7.1.0 for SNMPv3 compatibility.

Platform Availability

This command is available on all platforms.

configure snmp sysContact

```
configure snmp syscontact <alphanumeric string>
```

Description

Configures the name of the system contact.

Syntax Description

alphanumeric string	Specifies a system contact name.

Default

N/A.

Usage Guidelines

The system contact is a text field that enables you to enter the name of the person(s) responsible for managing the switch. A maximum of 255 characters is allowed.

To view the name of the system contact listed on the switch, use the `show switch` command. The `show switch` command displays switch statistics including the name of the system contact.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp syscontact <alphanumeric string>` command, use the `unconfigure management` command.

Example

The following command defines FredJ as the system contact:

```
configure snmp syscontact fredj
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure snmp sysLocation

```
configure snmp syslocation <alphanumeric string>
```

Description

Configures the location of the switch.

Syntax Description

alphanumeric string	Specifies the switch location.

Default

N/A.

Usage Guidelines

Use this command to indicate the location of the switch. A maximum of 255 characters is allowed.

To view the location of the switch on the switch, use the `show switch` command. The `show switch` command displays switch statistics including the location of the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp syslocation <alphanumeric string>` command, use the `unconfigure management` command.

Example

The following command configures a switch location name on the system:

```
configure snmp syslocation englab
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure snmp sysName

```
configure snmp sysname <alphanumeric string>
```

Description

Configures the name of the switch.

Syntax Description

alphanumeric string	Specifies a device name.

Default

The default sysname is the model name of the device (for example, Summit1).

Usage Guidelines

You can use this command to change the name of the switch. A maximum of 32 characters is allowed. The sysname appears in the switch prompt.

To view the name of the system listed on the switch, use the show switch command. The show switch command displays switch statistics including the name of the system.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the configure snmp sysname <alphanumeric string> command, use the unconfigure management command.

Example

The following command names the switch:

```
configure snmp sysname engineeringlab
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add access

```
configure snmpv3 add access {hex} <group name> {sec-model [snmpv1 | snmpv2
| usm]} {sec-level [noauth | authnopriv | authpriv]} {read-view {hex}
<view name>} { write-view {hex} <view name>} {notify-view {hex}
<view name>} {volatile}
```

Description

Create (and modify) a group and its access rights.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
group name	Specifies the group name to add or modify.
sec-model	Specifies the security model to use.
snmpv1	Specifies the SNMPv1 security model.
snmpv2	Specifies the SNMPv2c security model.
usm	Specifies the SNMPv3 User-based Security Model (USM).
sec-level	Specifies the security level for the group.
noauth	Specifies no authentication (and implies no privacy) for the security level.
authnopriv	Specifies authentication and no privacy for the security level.
authpriv	Specifies authentication and privacy for the security level.
read-view	Specifies the read view name.
write-view	Specifies the write view name.
notify-view	Specifies the notify view name.
volatile	Specifies volatile storage.

Default

The default values are:

- sec-model—USM
- sec-level—noauth
- read view name—defaultUserView
- write view name— “”
- notify view name—defaultUserView
- non-volatile storage

Usage Guidelines

Use this command to configure access rights for a group. All access groups are created with a unique default context, “”, as that is the only supported context.

There are a number of default (permanent) groups already defined. These groups are: *admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv, v1v2c_ro, v1v2c_rw.*

- The default groups defined (permanent) are *v1v2c_ro* for security names *snmpv1* and *snmpv2c*, *v1v2c_rw* for security names *snmpv1* and *snmpv2c*, *admin* for security name *admin*, and *initial* for security names *initial*, *initialmd5*, *initialsha*, *initialmd5Priv* and *initialshaPriv*.
- The default access defined (permanent) are *admin*, *initial*, *v1v2c_ro*, *v1v2c_rw*, and *v1v2cNotifyGroup*.

Example

In the following command, access for the group *defaultROGroup* is created with all the default values: security model usm, security level noauth, read view *defaultUserView*, no write view, notify view *defaultUserView*, and storage nonvolatile.

```
configure snmpv3 add access defaultROGroup
```

In the following command, access for the group *defaultROGroup* is created with the values: security model USM, security level authnopriv, read view *defaultAdminView*, write view *defaultAdminView*, notify view *defaultAdminView*, and storage nonvolatile.

```
configure snmpv3 add access defaultROGroup sec-model usm sec-level authnopriv
read-view defaultAdminView write-view defaultAdminView notify-view defaultAdminView
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add community

```
configure snmpv3 add community {hex} <community index> name {hex}
<community name> user {hex} <user name> {tag {hex} <transport tag>}
{volatile}
```

Description

Add an SNMPv3 community entry.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
community index	Specifies the row index in the snmpCommunityTable
community name	Specifies the community name.
user name	Specifies the USM user name.
transport tag	Specifies the tag used to locate transport endpoints in SnmpTargetAddrTable. When this community entry is used to authenticate v1/v2c messages, this tag is used to verify the authenticity of the remote entity.
volatile	Specifies volatile storage.

Default

N/A.

Usage Guidelines

Use this command to create or modify an SMMPv3 community in the community MIB.

Example

Use the following command to create an entry with the community index *comm_index*, community name *comm_public*, and user (security) name *v1v2c_user*:

```
configure snmpv3 add community comm_index name comm_public user v1v2c_user
```

Use the following command to create an entry with the community index (hex) of *4:E*, community name (hex) of *EA:12:CD:CF:AB:11:3C*, user (security) name *v1v2c_user,* using transport tag *34872* and `volatile` storage:

```
configure snmpv3 add community hex 4:E name hex EA:12:CD:CF:AB:11:3C user v1v2c_user
tag 34872 volatile
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add filter

```
configure snmpv3 add filter {hex} <profile name> subtree <object
identifier> {/<subtree mask>} type [included | excluded] {volatile}
```

Description

Add a filter to a filter profile.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
profile name	Specifies the filter profile that the current filter is added to.
object identifier	Specifies a MIB subtree.
subtree mask	Specifies a hex octet string used to mask the subtree. For example, f7a indicates 1.1.1.1.0.1.1.1.1.0.1.0.
included	Specifies that the MIB subtree defined by <object identifier>/<mask> is to be included.
excluded	Specifies that the MIB subtree defined by <object identifier>/<mask> is to be excluded.
volatile	Specifies volatile storage.

Default

The default `mask` value is an empty string (all 1s). The other default value is `non-volatile`.

Usage Guidelines

Use this command to create a filter entry in the snmpNotifyFilterTable. Each filter includes or excludes a portion of the MIB. Multiple filter entries comprise a filter profile that can eventually be associated with a target address. Other commands are used to associate a filter profile with a parameter name, and the parameter name with a target address.

This command can be used multiple times to configure the exact filter profile desired.

Example

Use the following command to add a filter to the filter profile *prof1* that includes the MIB subtree *1.3.6.1.4.1/f0*:

```
configure snmpv3 add filter prof1 subtree 1.3.6.1.4.1/f0 type included
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add filter-profile

```
configure snmpv3 add filter-profile {hex} <profile name> param {hex} <param
name> {volatile}
```

Description

Associate a filter profile with a parameter name.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
profile name	Specifies the filter profile name.
param name	Specifies a parameter name to associate with the filter profile.
volatile	Specifies volatile storage.

Default

The default storage type is non-volatile.

Usage Guidelines

Use this command to add an entry to the snmpNotifyFilterProfileTable. This table associates a filter profile with a parameter name. The parameter name is associated with target addresses, and the filter profile is associated with a series of filters, so, in effect, you are associating a series of filters with a target address.

Example

Use the following command to associate the filter profile *prof1* with the parameter name *P1*:

```
configure snmpv3 add filter-profile prof1 param P1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add group user

```
configure snmpv3 add group {hex} <group name> user {hex} <user name>
{sec-model [snmpv1| snmpv2 | usm]} {volatile}
```

Description

Add a user name (security name) to a group.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
group name	Specifies the group name to add or modify.
user name	Specifies the user name to add or modify.
sec-model	Specifies the security model to use.
snmpv1	Specifies the SNMPv1 security model.
snmpv2	Specifies the SNMPv2c security model.
usm	Specifies the SNMPv3 User-based Security Model (USM).
volatile	Specifies volatile storage.

Default

The default values are:

- sec-model—USM
- non-volatile storage

Usage Guidelines

Use this command to associate a user name with a group.

As per the SNMPv3 RFC, a security name is model independent while a username is model dependent. For simplicity, both are assumed to be same here. User names and security names are handled the same. In other words, if a user is created with the user name *username*, the security name value is the same, *username*.

Every group is uniquely identified by a security name and security model. So the same security name can be associated to a group name but with different security models.

Example

Use the following command to associate the user *userV1* to the group *defaultRoGroup* with SNMPv1 security:

```
configure snmpv3 add group defaultRoGroup user userV1 sec-model snmpv1
```

Use the following command to associate the user *userv3* with security model `USM` and storage type `volatile` to the access group *defaultRoGroup*:

```
configure snmpv3 add group defaultRoGroup user userV3 volatile
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add mib-view

```
configure snmpv3 add  mib-view  {hex} <view name> subtree <object
identifier> {/<subtree mask>} {type [included | excluded]} {volatile}
```

Description

Add (and modify) a MIB view.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
view name	Specifies the MIB view name to add or modify.
subtree	Specifies a MIB subtree.
mask	Specifies a hex octet string used to mask the subtree. For example, f7a indicates 1.1.1.1.0.1.1.1.1.0.1.0.
included	Specifies that the MIB subtree defined by <subtree>/<mask> is to be included.
excluded	Specifies that the MIB subtree defined by <subtree>/<mask> is to be excluded.
volatile	Specifies volatile storage.

Default

The default `mask` value is an empty string (all 1s). The other default values are `included` and non-volatile.

Usage Guidelines

Use this command to create a MIB view into a subtree of the MIB. If the view already exists, this command modifies the view to additionally include or exclude the specified subtree.

In addition to the created MIB views, there are three default views. They are of storage type permanent and cannot be deleted, but they can be modified. The default views are: *defaultUserView*, *defaultAdminView*, and *defaultNotifyView*.

Example

Use the following command to create the MIB view *allMIB* with the subtree *1.3* included as non-volatile:

```
configure snmpv3 add mib-view allMIB subtree 1.3
```

Use the following command to create the view *extremeMib* with the subtree *1.3.6.1.4.1.1916* included as non-volatile:

```
configure snmpv3 add mib-view extremeMib subtree 1.3.6.1.4.1.1916
```

Use the following command to create a view *vrrpTrapNewMaster* which excludes VRRP notification.1 and the entry is volatile.

```
configure snmpv3 add mib-view vrrpTrapNewMaster 1.3.6.1.2.1.68.0.1/ff8 type excluded
volatile
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add notify

```
configure snmpv3 add notify {hex} <notify name> tag {hex} <tag> {volatile}
```

Description

Add an entry to the snmpNotifyTable.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
notify name	Specifies the notify name to add.
tag	Specifies a string identifier for the notifications to be sent to the target.
volatile	Specifies volatile storage.

Default

The default storage type is non-volatile.

Usage Guidelines

Use this command to add an entry to the snmpNotifyTable. When a notification is to be sent, this table is examined. For the target addresses that have been associated with the tags present in the table, notifications will be sent, based on the filters also associated with the target addresses.

Example

Use the following command to send notification to addresses associated with the tag *type1*:

```
configure snmpv3 add notify N1 tag type1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add target-addr

```
configure snmpv3 add target-addr {hex} <addr name> param {hex} <param name>
ipaddress <ip address> {transport-port <port>} {from <source IP address>}
{tag-list {hex} <tag>, {hex} <tag>, ...} {volatile}
```

Description

Add and configure an SNMPv3 target address and associate filtering, security, and notifications with that address.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
addr name	Specifies a string identifier for the target address.
param name	Specifies the parameter name associated with the target.
ip address	Specifies an SNMPv3 target IP address.
port	Specifies a UDP port. Default is 162.
source ip address	Specifies the IP address of a VLAN to be used as the source address for the trap
tag	Specifies a string identifier for the notifications to be sent to the target.
volatile	Specifies volatile storage.

Default

The default values are:

- transport-port—port 162
- tag-list—the single tag *defaultNotify*, a pre-defined value in the snmpNotifyTable
- non-volatile storage

Usage Guidelines

Use this command to create an entry in the SNMPv3 snmpTargetAddressTable. The `param` parameter associates the target address with an entry in the snmpTargetParamsTable, which specifies security and storage parameters for messages to the target address, and an entry in the snmpNotifyFilterProfileTable, which specifies filters to use for notifications to the target address.

Example

The following command specifies a target address of *10.203.0.22*, port *9990*, with the name *A1*, and associates it with the security parameters and filter profile *P1*, and the notification tags *type1* and *type2*:

```
configure snmpv3 add target-addr A1 param P1 ipaddress 10.203.0.22 transport-port 9990
tag-list type1, type2
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add target-params

```
configure snmpv3 add target-params {hex} <param name> user {hex} <user
name> mp-model [snmpv1 | snmpv2c | snmpv3] sec-model [snmpv1 | snmpv2c |
usm] {sec-level [noauth | authnopriv | priv]} {volatile}
```

Description

Add and configure SNMPv3 target parameters.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
param name	Specifies the parameter name associated with the target.
user name	Specifies a user.
mp-model	Specifies a message processing model; choose from SNMPv1, SNMPv2, or SNMPv3.
sec-model	Specifies the security model to use.
snmpv1	Specifies the SNMPv1 security model.
snmpv2	Specifies the SNMPv2c security model.
usm	Specifies the SNMPv3 User-based Security Model (USM).
sec-level	Specifies the security level for the group.
noauth	Specifies no authentication (and implies no privacy) for the security level.
authnopriv	Specifies authentication and no privacy for the security level.
authpriv	Specifies authentication and privacy for the security level.
volatile	Specifies volatile storage.

Default

The default values are:

- sec-level—noauth
- non-volatile storage

Usage Guidelines

Use this command to create an entry in the SNMPv3 snmpTargetParamsTable. This table specifies the message processing model, security level, security model, and the storage parameters for messages to any target addresses associated with a particular parameter name.

To associate a target address with a parameter name, see the command “configure snmpv3 add target-addr” on page 122.

Example

The following command specifies a target parameters entry named *P1*, a user name of *guest*, message processing and security model of SNMPv2c, and a security level of no authentication:

```
configure snmpv3 add target-params P1 user guest mp-model snmpv2c sec-model snmpv2c
sec-level noauth
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add user

```
configure snmpv3 add user {hex} <user name> {authentication [md5 | sha]
[hex <hex octet> | <password>]} {privacy [hex <hex octet> | <password>]}
{volatile}
```

Description

Add (and modify) an SNMPv3 user.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
user name	Specifies the user name to add or modify.
MD5	Specifies MD5 authentication.
SHA	Specifies SHA authentication.
authentication	Specifies the authentication password or hex string to use for generating the authentication key for this user.
privacy	Specifies the privacy password or hex string to use for generating the privacy key for this user.
volatile	Specifies volatile storage.

Default

The default values are:

- authentication—no authentication
- privacy—no privacy
- non-volatile storage

Usage Guidelines

Use this command to create or modify an SNMPv3 user configuration.

If hex is specified, supply a 16 octet hex string for MD5, or a 20 octet hex string for SHA.

You must specify authentication if you want to specify privacy. There is no support for privacy without authentication.

The default user names are: *admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv.* The initial password for *admin* is *password*. For the other default users, the initial password is the user name.

Example

Use the following command to configure the user *guest* on the local SNMP Engine with security level noauth (no authentication and no privacy):

```
configure snmpv3 add user guest
```

Use the following command to configure the user *authMD5* to use `MD5` authentication with the password *palertyu:*·

```
configure snmpv3 add user authMD5 authentication md5  palertyu
```

Use the following command to configure the user *authSHApriv* to use `SHA` authentication with the hex key shown below, the privacy password *palertyu*, and `volatile` storage:

```
configure snmpv3 add user authShapriv authentication sha hex
01:03:04:05:01:05:02:ff:ef:cd:12:99:34:23:ed:ad:ff:ea:cb:11 privacy palertyu volatile
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 add user clone-from

```
configure snmpv3 add user {hex} <user name> clone-from {hex} <user name>
```

Description

Create a new user by cloning from an existing SNMPv3 user.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
user name	Specifies the user name to add or to clone from.

Default

- N/A

Usage Guidelines

Use this command to create a new user by cloning an existing one. Once you have successfully cloned the new user, you can modify its parameters using the following command:

```
configure snmpv3 add user {hex} <user name> {authentication [md5 | sha] [hex
<hex octet> | <password>]} {privacy [hex <hex octet> | <password>]} {volatile}
```

Users cloned from the default users will have the storage type of non-volatile. The default names are: *admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv.*

Example

Use the following command to create a user *cloneMD5* with same properties as the default user *initalmd5*. All authorization and privacy keys will initially be the same as with the default user *initialmd5*.

```
configure snmpv3 add user cloneMD5 clone-from initialmd5
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete access

```
configure snmpv3 delete access [all-non-defaults | {{hex} <group name>
{sec-model [snmpv1 | snmpv2c | usm] sec-level [noauth | authnopriv |
priv]}}]
```

Description

Delete access rights for a group.

Syntax Description

all-non-defaults	Specifies that all non-default (non-permanent) security groups are to be deleted.
hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
group name	Specifies the group name to add or modify.
sec-model	Specifies the security model to use.
snmpv1	Specifies the SNMPv1 security model.
snmpv2c	Specifies the SNMPv2c security model.
usm	Specifies the SNMPv3 User-based Security Model (USM).
sec-level	Specifies the security level for the group.
noauth	Specifies no authentication (and implies no privacy) for the security level.
authnopriv	Specifies authentication and no privacy for the security level.
authpriv	Specifies authentication and privacy for the security level.

Default

The default values are:

- sec-model—USM
- sec-level—noauth

Usage Guidelines

Use this command to remove access rights for a group. Use the `all-non-defaults` keyword to delete all the security groups, except for the default groups. The default groups are: *admin*, *initial*, *v1v2c_ro*, *v1v2c_rw*.

Deleting an access will not implicitly remove the related group to user association from the VACMSecurityToGroupTable. To remove the association, use the following command:

```
configure snmpv3 delete group {{hex} <group name>} user [all-non-defaults | {{hex}
<user name> sec-model {sec-model [snmpv1|snmpv2c|usm]}}]
```

Example

The following command deletes all entries with the group name *userGroup*:

```
configure snmpv3 delete access userGroup
```

The following command deletes the group *userGroup* with the security model `snmpv1` and security level of authentication and no privacy (`authnopriv`):

```
configure snmpv3 delete access userGroup sec-model snmpv1 sec-level authnopriv
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete community

```
configure snmpv3 delete community [all-non-defaults | {{hex} <community
index>} | {name {hex} <community name> }]
```

Description

Delete an SNMPv3 community entry.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
community index	Specifies the row index in the snmpCommunityTable
community name	Specifies the community name.
user name	Specifies the USM user name.
all-non-defaults	Specifies that all non-default community entries are to be removed.

Default

N / A.

Usage Guidelines

Use this command to delete an SMMPv3 community in the community MIB. The default entries are *public* and *private*.

Example

Use the following command to delete an entry with the community index *comm_index*:

```
configure snmpv3 delete community comm_index
```

Use the following command to create an entry with the community name (hex) of *EA:12:CD:CF:AB:11:3C*:

```
configure snmpv3 delete community name hex EA:12:CD:CF:AB:11:3C
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete filter

```
configure snmpv3 delete filter [all | [{hex} <profile name> {subtree
<object identifier>}]]
```

Description

Delete a filter from a filter profile.

Syntax Description

all	Specifies all filters.
hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
profile name	Specifies the filter profile of the filter to delete.
object identifier	Specifies the MIB subtree of the filter to delete.

Default

N/A

Usage Guidelines

Use this command to delete a filter entry from the snmpNotifyFilterTable. Specify `all` to remove all entries. Specify a profile name to delete all entries for that profile name. Specify a profile name and a subtree to delete just those entries for that filter profile and subtree.

Example

Use the following command to delete the filters from the filter profile *prof1* that reference the MIB subtree *1.3.6.1.4.1*:

```
configure snmpv3 delete filter prof1 subtree 1.3.6.1.4.1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete filter-profile

```
configure snmpv3 delete filter-profile [all |[{hex}<profile name>
{param {hex}<param name>}]]
```

Description

Remove the association of a filter profile with a parameter name.

Syntax Description

all	Specifies all filter profiles.
hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
profile name	Specifies the filter profile name to delete.
param name	Specifies to delete the filter profile with the specified profile name and parameter name.

Default

The default storage type is non-volatile.

Usage Guidelines

Use this command to delete entries from the snmpNotifyFilterProfileTable. This table associates a filter profile with a parameter name. Specify `all` to remove all entries. Specify a profile name to delete all entries for that profile name. Specify a profile name and a parameter name to delete just those entries for that filter profile and parameter name.

Example

Use the following command to delete the filter profile *prof1* with the parameter name *P1*:

```
configure snmpv3 delete filter-profile prof1 param P1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete group user

```
configure snmpv3 delete group  {{hex} <group name>} user [all-non-defaults
| {{hex} <user name> {sec-model [snmpv1|snmpv2c|usm]}}]
```

Description

Delete a user name (security name) from a group.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
group name	Specifies the group name to add or modify.
all-non-defaults	Specifies that all non-default (non-permanent) users are to be deleted from the group.
user name	Specifies the user name to add or modify.
sec-model	Specifies the security model to use.
snmpv1	Specifies the SNMPv1 security model.
snmpv2	Specifies the SNMPv2c security model.
usm	Specifies the SNMPv3 User-based Security Model (USM).

Default

The default values are:

- sec-model—USM

Usage Guidelines

Use this command to remove the associate of a user name with a group.

As per the SNMPv3 RFC, a security name is model independent while a username is model dependent. For simplicity, both are assumed to be same here. User names and security names are handled the same. In other words, if a user is created with the user name *username*, the security name value is the same, *username*.

Every group is uniquely identified by a security name and security model. So the same security name can be associated to a group name but with different security models.

The default groups are: *admin, initial, v1v2c_ro, v1v2c_rw.*

The default users are: *admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv.*

Example

Use the following command to delete the user *guest* from the group *UserGroup* for the security model snmpv2c:

```
configure snmpv3 delete group UserGroup user guest sec-model snmpv2c
```

Use the following command to delete the user *guest* from the group *userGroup* with the security model USM:

```
configure snmpv3 delete group userGroup user guest
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete mib-view

```
configure snmpv3 delete mib-view [all-non-defaults | {{hex} <view name>
{subtree <object identifier>}}]
```

Description

Delete a MIB view.

Syntax Description

all-non-defaults	Specifies that all non-default (non-permanent) MIB views are to be deleted.
hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
view name	Specifies the MIB view name to add or modify.
subtree	Specifies a MIB subtree.

Default

N/A.

Usage Guidelines

Use this command to delete a MIB view. Views which are being used by security groups cannot be deleted. Use the `all-non-defaults` keyword to delete all the MIB views (not being used by security groups) except for the default views. The default views are: *defaultUserView*, *defaultAdminView*, and *defaultNotifyView*.

Use the `configure snmpv3 add mib-view` command to remove a MIB view from its security group, by specifying a different view.

Example

The following command deletes all views (only the permanent views will not be deleted):

```
configure snmpv3 delete mib-view all-non-defaults
```

The following command deletes all subtrees with the view name *AdminView*:

```
configure snmpv3 delete mib-view AdminView
```

The following command deletes the view *AdminView* with subtree 1.3.6.1.2.1.2

```
configure snmpv3 delete  mib-view AdminView subtree 1.3.6.1.2.1.2
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete notify

```
configure snmpv3 delete notify [{{hex} <notify name>} | all-non-defaults]
```

Description

Delete an entry from the snmpNotifyTable.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
notify name	Specifies the notify name to add.
all-non-defaults	Specifies that all non-default (non-permanent) notifications are to be deleted.

Default

N/A

Usage Guidelines

Use this command to delete an entry from the snmpNotifyTable. When a notification is to be sent, this table is examined. For the target addresses that have been associated with the tags present in the table, notifications will be sent, based on the filters also associated with the target addresses.

There is one default notification that cannot be deleted, *defaultNotify*.

Example

Use the following command to remove the *N1* entry from the table:

```
configure snmpv3 delete notify N1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete target-addr

```
configure snmpv3 delete target-addr [{{hex} <addr name>} | all]
```

Description

Delete SNMPv3 target addresses.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
addr name	Specifies a string identifier for the target address.
all	Specifies all target addresses.

Default

N/A

Usage Guidelines

Use this command to delete an entry in the SNMPv3 snmpTargetAddressTable.

Example

The following command deletes target address named *A1*:

```
configure snmpv3 delete target-addr A1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete target-params

```
configure snmpv3 delete target-params [{{hex} <param name>} | all]
```

Description

Delete SNMPv3 target parameters.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
param name	Specifies the parameter name associated with the target.

Default

N/A

Usage Guidelines

Use this command to delete an entry in the SNMPv3 snmpTargetParamsTable. This table specifies the message processing model, security level, security model, and the storage parameters for messages to any target addresses associated with a particular parameter name.

Example

The following command deletes a target parameters entry named *P1*:

```
configure snmpv3 delete target-params P1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 delete user

```
configure snmpv3 delete user [all-non-defaults | {hex} <user name>]
```

Description

Delete an existing SNMPv3 user.

Syntax Description

all-non-defaults	Specifies that all non-default (non-permanent) users are to be deleted.
hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
user name	Specifies the user name to add or to clone from.

Default

- N/A

Usage Guidelines

Use this command to delete an existing user.

Use the `all-non-defaults` keyword to delete all users, except for the default (permanent) users. The default user names are: *admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv.*

Deleting a user will not implicitly remove the related group to user association from the VACMSecurityToGroupTable. To remove the association, use the following command:

```
configure snmpv3 delete group {{hex} <group name>} user [all-non-defaults | {{hex}
<user name> {sec-model [snmpv1|snmpv2c|usm]}}]
```

Example

The following command deletes all non-default users:

```
configure snmpv3 delete user all-non-defaults
```

The following command deletes the user *guest*:

```
configure snmpv3 delete user guest
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 engine-boots

```
configure snmpv3 engine-boots <(1-2147483647)>
```

Description

Configures the SNMPv3 Engine Boots value.

Syntax Description

(1-2147483647)	Specifies the value of engine boots.

Default

N/A.

Usage Guidelines

Use this command if the Engine Boots value needs to be explicitly configured. Engine Boots and Engine Time will be reset to zero if the Engine ID is changed. Engine Boots can be set to any desired value but will latch on its maximum, 2147483647.

Example

The following command configures Engine Boots to 4096:

```
configure snmpv3 engine-boots 4096
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 engine-id

```
configure snmpv3 engine-id <hex octet>
```

Description

Configures the SNMPv3 snmpEngineID.

Syntax Description

hex octet	Specifies the colon delimited hex octet that serves as part of the snmpEngineID (5-32 octets).

Default

The default `snmpEngineID` is the device MAC address.

Usage Guidelines

Use this command if the `snmpEngineID` needs to be explicitly configured. The first four octets of the ID are fixed to 80:00:07:7C,which represents Extreme Networks Vendor ID. Once the `snmpEngineID` is changed, default users will be reverted back to their original passwords/keys, while non-default users will be reset to the security level of no authorization, no privacy.

In a chassis, the `snmpEngineID` will be generated using the MAC address of the MSM with which the switch boots first. For MSM hitless failover, the same `snmpEngineID` will be propagated to both of the MSMs.

Example

The following command configures the `snmpEngineID` to be 80:00:07:7C:00:0a:1c:3e:11:

```
configure snmpv3 engine-id 00:0a:1c:3e:11
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure snmpv3 target-addr-ext

```
configure snmpv3 target-addr-ext {hex} <addr name> mode [standard |
enhanced] {ignore-mp-model} {ignore-event-community}
```

Description

Configure an entry in the extremeTargetAddrExtTable.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
addr name	Specifies a string identifier for the target address.
enhanced	Specifies enhanced traps, which contain extra varbinds at the end.
standard	Specifies standard traps, which do not contrain the extra varbinds.
ignore-mp-model	Sets the ignore message passing model flag
ignore-event-community	Sets the use Event Community flag to false.

Default

The default values are:

- mode—enhanced
- ignore-mp-model—False, the mp-model is not ignored.
- ignore-event-community—False, the EventCommunity is not ignored.

Usage Guidelines

The command `snmp add trapreceiver` was retained when SNMPv3 support was added to ExtremeWare. This command allows you to set trap receivers without using the details of SNMPv3. However, when the command is executed, it internally sets a per-trap-receiver flag called *ignore-mp-model*, and *ignore-event-community*. This command is never uploaded to the switch, but its equivalent SNMPv3 command, `configure snmpv3 add target-addr`, is uploaded instead. The latter has no tokens for *ignore-mp-model* or *ignore-event-come*. Therefore, upon downloading the configuration, the setting for these objects is lost.

This separate command corresponds to a private SNMP table that was subsequently added. The table contains three objects, *ignoreMPModel*, *useEventCommunity*, and *Mode*. This private table, the extremeTargetAddrExtTable, is an extension to the standard snmpv3TargetAddrTable

Example

The following command that standard traps will be used:

```
configure snmpv3 target-addr-ext A1 mode standard
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure sntp-client server

```
configure sntp-client [primary | secondary] server <host name/ip>]
```

Description

Configures an NTP server for the switch to obtain time information.

Syntax Description

primary	Specifies a primary server name.
secondary	Specifies a secondary server name.
host name/ip	Specifies a host name or IP address.

Default

N/A.

Usage Guidelines

Queries are first sent to the primary server. If the primary server does not respond within 1 second, or if it is not synchronized, the switch queries the second server. If the switch cannot obtain the time, it restarts the query process. Otherwise, the switch waits for the `sntp-client update interval` before querying again.

Example

The following command configures a primary NTP server:

```
configure sntp-client primary server 10.1.2.2
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure sntp-client update-interval

```
configure sntp-client update-interval <seconds>
```

Description

Configures the interval between polls for time information from SNTP servers.

Syntax Description

seconds	Specifies an interval in seconds.

Default

64 seconds.

Usage Guidelines

None.

Example

The following command configures the interval timer:

```
configure sntp-client update-interval 30
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure web login-timeout

```
configure web login-timeout <seconds>
```

Description

Configures the timeout for user to enter username/password in the pop-up window.

Syntax Description

seconds	Specifies an interval in seconds, where <seconds> can range from 30 seconds to 10 minutes (600 seconds).

Default

30 seconds.

Usage Guidelines

The Show for this parameter is displayed by using the following command:

`show management`

Example

The following command configures the interval timer:

`configure sntp-client update-interval 30`

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

disable snmp access

```
disable snmp access {snmp-v1v2c}
```

Description

Selectively disables SNMP on the switch.

Syntax Description

snmp-v1v2c	Disables SNMPv1/v2c access only; does not affect SNMPv3 access.

Default

Enabled.

Usage Guidelines

Disabling SNMP access does not affect the SNMP configuration (for example, community strings). However, if you disable SNMP access, you will be unable to access the switch using SNMP.

To allow access, use the following command:

```
enable snmp access
```

By using the enable and disable commands you can enable all SNMP access, no SNMP access, or only SNMPv3 access. You cannot enable only SNMPv1/v2c access. To enable SNMPv3 only access on the switch, use the following commands:

```
enable snmp access
disable snmp access snmp-v1v2c
```

Example

The following command disables all SNMP access on the switch:

```
disable snmp access
```

History

The `snmp-v1v2c` keyword was added in ExtremeWare 7.1.0

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable snmp dot1dTpFdbTable

```
disable snmp dot1dTpFdbTable
```

Description

Disables SNMP GetNext responses for the dot1dTpFdbTable in the BRIDGE-MIB.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

SNMP Get responses are not affected by this command.

To view the configuration of the dot1dTpFdb table on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state the dot1dTpFdb table.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `disable snmp dot1dTpFdbTable` command, use the `unconfigure management` command.

Example

The following command disables the dot1dTPFdb table:

```
disable snmp dot1dTpFdbTable
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable snmp traps

```
disable snmp traps
```

Description

Prevents SNMP traps from being sent from the switch.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

This command does not clear the SNMP trap receivers that have been configured. The command prevents SNMP traps from being sent from the switch even if trap receivers are configured.

Example

The following command prevents SNMP traps from being sent from the switch to the trap receivers:

```
disable snmp traps
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable snmp traps port-up-down

```
disable snmp traps port-up-down ports [all | mgmt | <portlist>]
```

Description

Prevents SNMP port up/down traps (also known as link up and link down traps) from being sent from the switch for the indicated ports.

Syntax Description

all	Specifies that no link up/down traps should be sent for all ports. This does not include the management port which must be explicitly specified.
mgmt	Specifies that no link up/down traps should be sent for the management port. This option will only appear on platforms that have a management port.
<portlist>	Specifies the list of ports.

Default

Enabled.

Usage Guidelines

This command is used to disable the sending of link up and link down traps for the specified ports. To see which ports do not have such traps disabled, use the *show management* command.

Example

The following command will prevent link up or link down traps from being sent for any port on the switch (except the management port if it has one).

```
disable snmp traps port-up-down all
```

History

This command was first available in ExtremeWare 6.2.2

This command was modified to include the management port in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable snmp traps mac-security

```
disable snmp traps mac-security
```

Description

Prevents SNMP mac-security traps from being sent from the switch for all ports.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command should be used in conjunction with the *configure ports <portlist> limit-learning* command. That command configures a limit on the number of MAC addresses that can be learned on a port(s). After that limit has been reached on a particular port, a trap will be sent by the switch, if a new MAC address appears on that port. In addition, a message will be generated in the syslog and the port will be blackholed.

Example

The following command prevents SNMP mac-security traps from being sent from the switch.

```
disable snmp traps mac-security
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable sntp-client

```
disable sntp-client
```

Description

Disables the SNTP client.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. After the SNTP client has been enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean Time (GMT) offset and the use of Daylight Savings Time (DST).

Example

The following command disables the SNTP client:

```
disable sntp-client
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

disable system-watchdog

```
disable system-watchdog
```

Description

Disables the system watchdog timer.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

The watchdog timer reboots the switch if the CPU becomes trapped in a processing loop. If the watchdog timer is executed, the switch captures information on the cause of the reboot and posts it to the system log.

Example

The following command disables the watchdog timer:

```
disable system-watchdog
```

History

This command was first available in ExtremeWare 6.1.9.

Platform Availability

This command is available on all platforms.

disable telnet

```
disable telnet
```

Description

Disables Telnet services on the system.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

You must be logged in as an administrator to enable or disable Telnet.

Example

With administrator privilege, the following command disables Telnet services on the switch:

```
disable telnet
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable web

```
disable web
```

Description

Disables web access to the switch.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

You can use this command to disable web access to the switch. If you are using ExtremeWare Vista for web access, you must create and configure an access profile before you can use this option. You create an access profile using the `create access-profile` command. You configure an access profile using the `configure access-profile` command.

Example

The following command disables web access to the switch:

```
disable web
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable dhcp ports vlan

```
enable dhcp ports <portlist> vlan <vlan name>
```

Description

Enables DHCP on a specified port in a VLAN.

Syntax Description

portlist	Specifies the ports for which DHCP should be enabled.
vlan_name	Specifies the VLAN on whose ports DHCP should be enabled.

Default

N/A.

Usage Guidelines

None.

Example

The following command enables DHCP for port 9 in VLAN *corp*:

```
enable dhcp ports 9 vlan corp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable snmp access

```
enable snmp access
```

Description

Turns on SNMP support for SNMPv3 and v1/v2c on the switch.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

To have access to the SNMP agent residing in the switch, at least one VLAN must have an IP address assigned to it.

Any network manager running SNMP can manage the switch (for v1/v2c), provided the MIB is installed correctly on the management station. Each network manager provides its own user interface to the management facilities.

For SNMPv3, additional security keys are used to control access, so an SNMPv3 manager is required for this type of access.

This command enables both v1/v2c and v3 access, so the switch can be accessed with either method. Use the following commands to allow only v3 access:

```
enable snmp access
disable snmp access snmp-v1v2c
```

Use the following command to prevent any SNMP access:

```
disable snmp access
```

There is no way to disable v3 access and allow v1/v2c access

Example

The following command enables all SNMP access for the switch:

```
enable snmp access
```

History

Support for SNMPv3 was added in ExtremeWare 7.1.0.

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable snmp dot1dTpFdbTable

```
enable snmp dot1dTpFdbTable
```

Description

Enables SNMP GetNext responses for the dot1dTpFdbTable in the BRIDGE-MIB.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

SNMP Get responses are not affected by this command.

To view the configuration of the dot1dTpFdb table on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable / disable state the dot1dTpFdb table.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `enable snmp dot1dTpFdbTable` command, use the `unconfigure management` command.

Example

The following command enables the dot1dTPFdb table:

```
enable snmp dot1dTpFdbTable
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable snmp traps

```
enable snmp traps
```

Description

Turns on SNMP trap support.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

An authorized trap receiver can be one or more network management stations on your network. The switch sends SNMP traps to all trap receivers.

Example

The following command enables SNMP trap support on the switch:

```
enable snmp trap
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable snmp traps port-up-down

```
enable snmp traps {port-up-down ports [all | mgmt | <portlist>]}
```

Description

Enables SNMP port up/down traps (also known as link up and link down traps) for the indicated ports.

Syntax Description

all	Specifies that link up/down traps should be sent for all ports. This does not include the management port which must be explicitly specified.
mgmt	Specifies that link up/down traps should be sent for the management port. This option will only appear on platforms that have a management port.
<portlist>	Specifies a list of ports.

Default

Enabled.

Usage Guidelines

This command is used to enable the sending of link up and link down traps for the specified ports. To see which ports have such traps enabled, use the *show management* command.

Example

The following command will enable link up or link down traps on all ports of the switch (except the management port if it has one).

```
enable snmp traps port-up-down all
```

History

This command was first available in ExtremeWare 6.2.2

This command was modified to include the management port in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable snmp traps mac-security

```
enable snmp traps mac-security
```

Description

Enables SNMP mac-security traps for all ports to be sent by the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command should be used in conjunction with the *configure ports <portlist> limit-learning* command. That command configures a limit on the number of MAC addresses that can be learned on a port(s). After that limit has been reached on a particular port, a trap will be sent by the switch, if a new MAC address appears on that port. In addition, a message will be generated in the syslog and the port will be blackholed.

Example

The following command allows SNMP mac-security traps to be sent from the switch.

```
enable snmp traps mac-security
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable sntp-client

```
enable sntp-client
```

Description

Enables the SNTP client.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. After the SNTP client has been enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean Time (GMT) offset and the use of Daylight Savings Time (DST).

Example

The following command enables the SNTP client:

```
enable sntp-client
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

enable system-watchdog

```
enable system-watchdog
```

Description

Enables the system watchdog timer.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

The watchdog timer reboots the switch if the CPU becomes trapped in a processing loop. If the watchdog timer is executed, the switch captures information on the cause of the reboot and posts it to the system log.

You must reboot to have this command take effect.

Example

The following command enables the watchdog timer:

```
enable system-watchdog
```

History

This command was first available in ExtremeWare 6.1.9.

Platform Availability

This command is available on all platforms.

enable telnet

```
enable telnet {access-profile [<access_profile> | none]} {port
<tcp_port_number>}
```

Description

Enables Telnet access to the switch.

Syntax Description

access profile	Specifies an access profile. (6.0, 6.1)
none	Cancels a previously configured access profile. (6.0, 6.1)
port	Specifies a TCP port number. (6.0, 6.1)

Default

Telnet is enabled with no access profile and uses TCP port number 23.

Usage Guidelines

You must be logged in as an administrator to enable Telnet.

If you are using IP without a BOOTP server, you must enter IP parameters for the switch for the Telnet software to communicate with the device. To assign IP parameters to the switch, you must:

- Log in to the switch with administrator privileges.
- Assign an IP address and subnet mask to a VLAN.

  The switch comes configured with a default VLAN named *default*. To use Telnet or an SNMP network manager, you must have at least one VLAN on the switch, and it must be assigned an IP address and subnet mask. IP addresses are always assigned to a VLAN. The switch can be assigned multiple IP addresses.

For version 6.0 and higher:

- Use an access profile to restrict Telnet access. An access profile permits or denies a named list of IP addresses and subnet masks. You must create and configure an access profile before you can use this option. You create an access profile using the `create access-profile` command. You configure an access profile using the `configure access-profile` command.
- Use the `none` option to cancel a previously configured access-profile.
- Use the `port` option to specify a TCP port number.

Example

The following command applies the access profile managers to Telnet:

```
enable telnet access-profile managers
```

History

This command was first available in ExtremeWare 2.0.

Support for the `access profile`, `none`, and `port` parameters was introduced in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable web

```
enable web {access-profile [<access_profile> | none]} {port
<tcp_port_number>}
```

Description

Enables ExtremeWare Vista web access to the switch.

Syntax Description

access profile	Specifies an access profile. (6.0, 6.1)
none	Cancels a previously configured access profile. (6.0, 6.1)
port	Specifies a TCP port number. (6.0, 6.1)

Default

Enabled, using TCP port 80.

Usage Guidelines

By default, web access is enabled on the switch.

For version 6.0 and higher:

- By default, web access has no access profile and uses TCP port number 80.
- Use an access profile to restrict ExtremeWare Vista web access. An access profile permits or denies a named list of IP addresses and subnet masks. You must create and configure an access profile before you can use this option. You create an access profile using the `create access-profile` command. You configure an access profile using the `configure access-profile` command. Apply an access profile only when ExtremeWare Vista is enabled.
- Use the none option to cancel a previously configured access-profile.
- Use the `port` option to specify a TCP port number.

Example

The following command applies the access profile administrators to the web:

```
enable web access-profile administrators
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.0 to include the access profile and port options.

Platform Availability

This command is available on all platforms.

exit

```
exit
```

Description

Logs out the session of a current user for CLI or Telnet.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to log out of a CLI or Telnet session.

Example

The following command logs out the session of a current user for CLI or Telnet:

```
exit
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on Summit switches.

logout

```
logout
```

Description

Logs out the session of a current user for CLI or Telnet.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to log out of a CLI or Telnet session.

Example

The following command logs out the session of a current user for CLI or Telnet:

```
logout
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

quit

```
quit
```

Description

Logs out the session of a current user for CLI or Telnet.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to log out of a CLI or Telnet session.

Example

The following command logs out the session of a current user for CLI or Telnet:

```
quit
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show snmpv3 context

```
show snmpv3 context
```

Description

Displays information about the SNMPv3 contexts on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines:

This command displays the entries in the View-based Access Control Model (VACM) context table (VACMContextTable).

Example

The following command displays information about the SNMPv3 contexts on the switch:

```
show snmpv3 context
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 engine-info

```
show snmpv3 engine-info
```

Description

Displays information about the SNMPv3 engine on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines:

The following show engine-info output is displayed:

- EngineID—Either the ID auto generated from MAC address of switch, or the ID manually configured.
- EngineBoots—Number of times the agent has been rebooted.
- EngineTime—Time since agent last rebooted, in centiseconds.
- Max. Message Size—Maximum SNMP Message size supported by the Engine (8192).

Example

The following command displays information about the SNMPv3 engine on the switch:

```
show snmpv3 engine-info
```

The following is output from this command:

```
SNMP Engine-ID         : 80:00:07:7c:03:00:01:30:23:c1:00 'H'
SNMP Engine Boots      : 4
SNMP Engine Time       : 1852673
SNMP Max. Message Size : 8192
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show management

```
show management
```

Description

Displays the SNMP settings configured on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines:

The following show management output is displayed:

- Enable/disable state for Telnet, SNMP, and web access
- SNMP community strings
- Authorized SNMP station list
- SNMP trap receiver list
- Login statistics

For ExtremeWare 4.0 and higher, the following show management output is also displayed:

- Enable/disable state for SSH2 and access profile information
- RMON polling configuration

For ExtremeWare 6.2.2 and higher, the enable/disable state of the port-up-down traps is also displayed.

For ExtremeWare 7.0.0 and higher, the enable/disable state of the mac-limit traps is also displayed.

For ExtremeWare 7.1.0 and higher, the SNMP access display item will show the additional states of v1, v2c disabled and v3 enabled. The flags field was enhanced to show the SNMP trap groups.

Example

The following command displays configured SNMP settings on the switch:

```
show management
```

Following is the output from this command:

```
CLI idle timeouts:              disabled
CLI Paging:                     enabled
CLI configuration logging:      enabled
Telnet access:                  enabled tcp port: 23
Web access:                     enabled tcp port: 80
Web access login timeout :     30 secs
SSH Access:                     key invalid, disabled tcp port: 22
UDP Echo Server:                disabled udp port: 7
SNMP Access:                    v1v2c disabled ; v3 enabled
SNMP Read Only Communities:     rykfcb
Total Read Only Communities:    1
SNMP Read Write Communities:    r~‘|kug
Total Read Write Communities:   1
SNMP dot1dTpFdbTable:           disabled
RMON polling:                   disabled
SNMP Traps:                     enabled
SNMP v1/v2c TrapReceivers:
    Destination           Community             Source IP Address   Flags
   10.255.254.22 /162     public                                    2EA
   111.111.111.111/162    ThisIsATestComm                           2SA

Flags:  Version: 1=v1 2=v2c
        Mode: S=Standard E=Enhanced
        Trap Groups:  s=STP b=BGP o=OSPF p=Ping/Traceroute v=VRRP y=System
                      e=Extreme m=Smart Traps a=Auth l=Link Up/Down r=RMON
                      c=Security
                      A=All
SNMP MAC Security traps:          disabled
Link Up/Link Down traps enabled on ports: All, including MgmtPort
SNMP stats:     inPkts 301      outPkts 302        errors 0        authErrors 0
                Gets 93         GetNexts 208       Sets 0
SNMP traps:     sent 10         authTraps enabled
Login stats:
        validLogins 3 badPasswords 0 unknownUSers 2(last bad user: admin1)
        Telnet: total 3 valid 1 invalid 2
        HTTP:   total 0 valid 0 invalid 0
Management access stats:
        Protocol   UDP/TCP    Port   Total packets  Rejected packets
        --         --         --     --             --
        Protocol   Soures IP Address UDP/TCP  Port  Time
        --         --                 --       --    --
```

History

This command was first available in ExtremeWare 2.0.

Support for the SSH2 state, access profile information and RMON polling configuration was introduced in ExtremeWare 4.0.

Additional information on traps configured per port port-up-down traps was added in ExtremeWare 6.2.2.

Additional information on mac-limit traps was added in ExtremeWare 7.0.0

Platform Availability

This command is available on all platforms.

show odometer

```
show odometer
```

Description

Displays a counter for each component of a switch that shows how long it has been functioning since it was manufactured.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The output from this command displays how long each individual component in the whole switch has been functioning since it is manufactured. This odometer counter will be kept in the EEPROM of each monitored component. This means that even when the component is plugged into different chassis, the odometer counter will be available in the new switch chassis. The following components are monitored by the odometer:

- For the Black Diamond—MSM and I/O modules
- For the Alpine—SMM, I/O slots, and power supplies
- For stackable switches—the CPU

Example

The following command displays how long each component of a switch has been functioning since it's manufacture date:

```
show odometer
```

Following is the output from this command:

```
* Alpine3804:4 # show odometers
                                Service   First Recorded
   Field Replaceable Units      Days      Start Date
------------------------------ ---------- -------------
Backplane:                        145      Jan-22-2003
SMM:                              145      Jan-22-2003
Slot 1:         Empty
Slot 2:         WM4T1             234      Oct-25-2002
Slot 3:         FM8V              145      Jan-22-2003
Slot 4:         GM4X              145      Jan-22-2003
Upper PS:       PSU-A             292      Apr-12-2002
Lower PS:       PSU-B             N/A    N/A
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

show session

```
show session
```

Description

Displays the currently active Telnet, console, and web sessions communicating with the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The `show session` command displays the username and IP address of the incoming Telnet session, whether a console session is currently active, and the login time.

The following table displays the `show session` command field definitions.

Table 8: Show Command Field Definitions

Field	Definition
#	Indicates session number.
Login Time	Indicates login time of session.
User	Indicates the user logged in for each session.
Type	Indicates the type of session.
Auth	Indicates how the user is logged in.
CLI Auth	Indicates the type of authentication (RADIUS and TACAS) if enabled.
Location	Indicates the location (IP address) from which the user logged in.

Example

The following command displays the active sessions on the switch:

```
show session
```

Following is the output from this command:

```
# Login Time                    User     Type     Auth     CLI Auth Location
================================================================================
     0 Tue Feb 19 18:08:42 2002 admin    console  local    disabled serial
     5 Thu Feb 21 19:09:48 2002 admin    http     local    disabled 10.0.4.76
* 1028 Thu Feb 21 18:56:40 2002 admin    telnet   local    disabled 10.0.4.19
```

History

This command was first available in ExtremeWare 2.0.

Support for the CLI Auth command field definition was introduced in ExtremeWare 6.0.

Support for the Auth command field definition was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show snmpv3 access

```
show snmpv3 access {{hex} <group name>}
```

Description

Displays SNMPv3 access rights.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
group name	Specifies the name of the group to display.

Default

N/A.

Usage Guidelines

The `show snmpv3 access` command displays the access rights of a group. If you do not specify a group name, the command will display details for all the groups.

This command displays the SNMPv3 VACMAccessTable entries.

Example

The following command displays all the access details.·

```
show  snmpv3 access
```

The following command displays the access rights for the group *group1*:

```
show snmpv3 access group1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 counters

```
show snmpv3 counters
```

Description

Displays SNMPv3 counters.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The `show snmpv3 counters` command displays the following SNMPv3 counters:

- snmpUnknownSecurityModels
- snmpInvalidMessages
- snmpUnknownPDUHandlers
- usmStatsUnsupportedSecLevels
- usmStatsNotInTimeWindows
- usmStatsUnknownUserNames
- usmStatsUnknownEngineIDs
- usmStatsWrongDigests
- usmStatsDecryptionErrors

Issuing the command `clear counters` will reset all counters to zero.

Example

The following command displays all the SNMPv3 counters.·

```
show snmpv3 counters
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 filter

```
show snmpv3 filter {{hex} <profile name> {{subtree} <object identifier>}
```

Description

Display the filters that belong a filter profile.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
profile name	Specifies the filter profile to display.
object identifier	Specifies a MIB subtree.

Default

N / A

Usage Guidelines

Use this command to display entries from the snmpNotifyFilterTable. If you specify a profile name and subtree, you will display only the entries with that profile name and subtree. If you specify only the profile name, you will display all entries for that profile name. If you do not specify a profile name, then all the entries are displayed.

Example

Use the following command to display the part of filter profile *prof1* that includes the MIB subtree *1.3.6.1.4.1*:

```
show snmpv3 filter prof1 subtree 1.3.6.1.4.1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 filter-profile

```
show snmpv3 filter-profile {{hex} <profile name>} {param {hex}
<param name>}
```

Description

Display the association between parameter names and filter profiles.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
profile name	Specifies the filter profile name.
param name	Specifies the parameter name.

Default

N / A.

Usage Guidelines

Use this command to display the snmpNotifyFilterProfileTable. This table associates a filter profile with a parameter name. The parameter name is associated with target addresses, and the filter profile is associated with a series of filters, so, in effect, you are associating a series of filters with a target address.

Example

Use the following command to display the entry with filter profile *prof1* with the parameter name *P1*:

```
show snmpv3 filter-profile prof1 param P1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 group

```
show snmpv3 group {{hex} <group name> {user {hex} <user name>}}
```

Description

Displays the user name (security name) and security model association with a group name.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
group name	Specifies the group name to display.
user name	Specifies the user name to display.

Default

N / A.

Usage Guidelines

The `show snmpv3 group` command displays the details of a group with the given group name. If you do not specify a group name, the command will display details for all the groups.

Example

The following command displays information about all groups for every security model and user name:

```
show snmpv3 group
```

The following command shows information about the group *testgroup* and user name *testuser*:

```
show snmpv3 group testgroup user testuser
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 mib-view

```
show snmpv3 mib-view {{hex} <view name> {subtree <object identifier>}}
```

Description

Displays a MIB view.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
view name	Specifies the name of the MIB view to display.
subtree	Specifies the object identifier of the view to display.

Default

N/A.

Usage Guidelines

The `show snmpv3 mib-view` command displays a MIB view. If you do not specify a view name, the command will display details for all the MIB views. If a subtree is not specified, then all subtrees belonging to the view name will be displayed.

This command displays the SNMPv3 VACMViewsTreeFamilyTable.

Example

The following command displays all the view details.·

```
show  snmpv3 mib-view
```

The following command displays a view with the view name *Roview* and subtree 1.3.6.1.2.1.1:

```
show snmpv3 mib-view Roview subtree 1.3.6.1.2.1.1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 notify

```
show snmpv3 notify {{hex} <notify name>}
```

Description

Display the notifications that are set. This command displays the snmpNotifyTable.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
param name	Specifies the parameter name associated with the target.

Default

- N/A

Usage Guidelines

Use this command to display entries from the SNMPv3 snmpNotifyTable. This table lists the notify tags that the agent will use to send notifications (traps).

If no notify name is specified, all the entries are displayed.

Example

The following command displays the notify table entry for *N1*:

```
show snmpv3 notify N1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 target-addr

```
show snmpv3 target-addr {{hex} <addr name>}
```

Description

Display information about SNMPv3 target addresses.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
addr name	Specifies a string identifier for the target address.

Default

- N/A

Usage Guidelines

Use this command to display entries in the SNMPv3 snmpTargetAddressTable. If no target address is specified, the entries for all the target addresses will be displayed.

Example

The following command displays the entry for the target address named *A1*:

```
show snmpv3 target-addr A1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 target-addr-ext

```
show snmpv3 target-addr-ext {hex} <addr name>
```

Description

Display information about SNMPv3 target addresses enhanced or standard mode.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
addr name	Specifies a string identifier for the target address.

Default

- N/A

Usage Guidelines

Use this command to display entries in the SNMPv3 extremeTargetAddressExtTable.

Example

The following command displays the entry for the target address named *A1*:

```
show snmpv3 target-addr-ext A1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 target-params

```
show snmpv3 target-params {{hex} <param name>}
```

Description

Display the information about the options associated with the parameter name.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
param name	Specifies the parameter name to display.

Default

- N/A

Usage Guidelines

Use this command to display entries from the SNMPv3 snmpTargetParamsTable. This table specifies the message processing model, security level, security model, and the storage parameters for messages to any target addresses associated with a particular parameter name.

If no parameter name is specified, all the entries are displayed.

Example

The following command displays the target parameter entry named *P1*:

```
show snmpv3 target-params P1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show snmpv3 user

```
show snmpv3 user {{hex} <user name>}
```

Description

Displays detailed information about the user.

Syntax Description

hex	Specifies that the value to follow is to be supplied as a colon separated string of hex octets.
user name	Specifies the user name to display.

Default

N/A.

Usage Guidelines

The `show snmpv3 user` command displays the details of a user. If you do not specify a user name, the command will display details for all the users. The authentication and privacy passwords and keys will not be displayed.

The user entries in SNMPv3 are stored in the USMUserTable, so the entries are indexed by EngineID and user name.

Example

The following command lists all user entries:

```
show snmpv3 user
```

The following command lists details for the specified user, *testuser*:

```
show snmpv3 user testuser
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show sntp-client

```
show sntp-client
```

Description

Displays the DNS configuration.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Displays configuration and statistics information of SNTP client.

Example

The following command displays the DNS configuration:

```
show sntp-client
```

Following is the output from this command:

```
SNTP client is enabled
SNTP time is valid
Primary server: 172.17.1.104
Secondary server: 172.17.1.104
Query interval: 64
Last valid SNTP update: From server 172.17.1.104, on Wed Oct 30 22:46:03 2002
SNTPC Statistics:
 Packets transmitted:
  to primary server:           1
  to secondary server:         0
 Packets received with valid time:
  from Primary server:         1
  from Secondary server:       0
  from Broadcast server:       0
 Packets received without valid time:
  from Primary server:         0
  from Secondary server:       0
  from Broadcast server:       0
 Replies not received to requests:
  from Primary server:         0
  from Secondary server:       0
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show vlan dhcp-address-allocation

```
show vlan <vlan name> dhcp-address-allocation
```

Description

Displays DHCP address allocation information about VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Summary information for all VLANs on the device.

Usage Guidelines

Display the IP address, MAC address, and time assigned to each end device.

Example

The following command displays DHCP address allocation information about VLAN *vlan1*:

```
show vlan vlan1 dhcp-address-allocation
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

show vlan dhcp-config

```
show vlan <vlan name> dhcp-config
```

Description

Displays DHCP configuration information about VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Summary information for all VLANs on the device.

Usage Guidelines

Displays the DHCP configuration, including the DHCP range, DHCP lease timer, network login lease timer, and DHCP-enabled ports.

Example

The following command displays DHCP configuration information about VLAN *vlan1*:

```
show vlan vlan1 dhcp-config
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

telnet

```
telnet [<ipaddress> | <hostname>] {<port_number>}
```

Description

Allows you to Telnet from the current command-line interface session to another host.

Syntax Description

ipaddress	Specifies the IP address of the host.
hostname	Specifies the name of the host. (4.x and higher)
port_number	Specifies a TCP port number. (4.x and higher)

Default

Enabled. If the TCP port number is not specified, the Telnet session defaults to port 23.

Usage Guidelines

Only VT100 emulation is supported.

Any workstation with a Telnet facility should be able to communicate with the switch over a TCP/IP network.

You need to configure the switch IP parameters.

Up to eight active Telnet sessions can access the switch concurrently. If `idletimeouts` are enabled, the Telnet connection will time out after 20 minutes of inactivity. If a connection to a Telnet session is lost inadvertently, the switch terminates the session within two hours.

Before you can start a Telnet session, you need to configure the switch IP parameters. To open a Telnet connection, you must specify the host IP address or the host name of the device you wish to manage. Check the user manual supplied with the Telnet facility if you are unsure of how to do this.

To view the status of Telnet on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for Telnet.

For version 4.x and higher:

- You must configure DNS in order to use the `hostname` option.

For version 2.0:

- The `hostname` parameter is not available.

Example

The following command configures Telnet communication with a host at IP address 123.45.67.8:

```
telnet 123.45.67.8
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.x to support the `hostname` and `port number` parameters.

Platform Availability

This command is available on all platforms.

unconfigure management

```
unconfigure management
```

Description

Restores default values to all SNMP-related entries.

Syntax Description

This command has no arguments or variables.

Default

N/A

Usage Guidelines

None.

Example

The following command restores default values to all SNMP-related entries on the switch:

```
unconfigure management
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

4 Commands for Configuring Slots and Ports on a Switch

This chapter describes:

- Commands related to enabling, disabling, and configuring individual ports
- Commands related to configuring port speed (Fast Ethernet ports only) and half- or full-duplex mode
- Commands related to creating load-sharing groups on multiple ports
- Commands related to displaying port statistics
- Commands related to enabling an disabling loopback detection

By default, all ports on the switch are enabled. After you configure the ports to your specific needs, you can select which ports are enabled or disabled.

Fast Ethernet ports can connect to either 10Base-T or 100Base-T networks. By default, the ports autonegotiate (automatically determine) the port speed. You can also configure each port for a particular speed (either 10 Mbps or 100 Mbps).

Gigabit Ethernet ports are statically set to 1 Gbps, and their speed cannot be modified.

The switch comes configured to use autonegotiation to determine the port speed and duplex setting for each port. You can select to manually configure the duplex setting and the speed of 10/100 Mbps ports, and you can manually configure the duplex setting on Gigabit Ethernet ports.

All ports on the switch can be configured for half-duplex or full-duplex operation. The ports are configured to autonegotiate the duplex setting, but you can manually configure the duplex setting for your specific needs.

Flow control is supported only on Gigabit Ethernet ports. It is enabled or disabled as part of autonegotiation. If autonegotiation is set to off, flow control is disabled. When autonegotiation is turned on, flow control is enabled.

Load sharing with Extreme Network switches allows you to increase bandwidth and resilience between switches by using a group of ports to carry traffic in parallel between switches. The sharing algorithm allows the switch to use multiple ports as a single logical port. For example, VLANs see the load-sharing group as a single logical port. The algorithm also guarantees packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.

Load sharing is most useful in cases where the traffic transmitted from the switch to the load-sharing group is sourced from an equal or greater number of ports on the switch. For example, traffic transmitted to a two-port load-sharing group should originate from a minimum of two other ports on the same switch.

You can view port status on the switch using the `show ports` commands. These commands, when used with specific keywords and parameters, allow you to view various issues such as real-time collision statistics, link speed, flow control, and packet size.

Commands that require you to enter one or more port numbers use the parameter `<portlist>` in the syntax. On a modular switch, a `<portlist>` can be a list of slots and ports. On a stand-alone switch, a `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Link Aggregation Control Protocol (LACP) is an extension to the existing sharing implementation. It provides several features:

- LACP protocol control of sets of links
- Loopback detection
- Configuration verification for systems connected using LACP

clear slot

```
clear slot <slot>
```

Description

Clears a slot of a previously assigned module type.

Syntax Description

slot	Specifies a modular switch slot number.

Default

N/A.

Usage Guidelines

All configuration information related to the slot and the ports on the module is erased. If a module is present when you issue this command, the module is reset to default settings.

If a slot is configured for one type of module, and a different type of module is inserted, the inserted module is put into a mismatch state (where the inserted module does not match the configured slot), and is not brought online. To use the new module type in a slot, the slot configuration must be cleared or configured for the new module type. Use the `configure slot` command to configure the slot.

For version 6.0 and later:

- This command is available on modular switches.

For version 4.0:

- This command is available on BlackDiamond switches only.

Example

The following command clears slot 2 of a previously assigned module type:

```
clear slot 2
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on modular switches only.

configure backplane-ls-policy

```
configure backplane-ls-policy [address-based | port-based | round-robin]
```

Description

Selects a load-sharing policy for the backplane on a BlackDiamond switch.

Syntax Description

address-based	Specifies address-based algorithm.
port-based	Specifies port-based algorithm.
round-robin	Specifies round-robin algorithm.

Default

Port-based.

Usage Guidelines

On BlackDiamond switches, you can specify the backplane load-sharing policy to use. There are multiple paths that a packet can travel from the MSM to an I/O module, so this command sets the algorithm used to choose the path for each packet crossing the backplane. Selecting a policy for a particular situation will depend on the type of traffic and network topology, however, for many situations an address-based policy will enhance performance over other policies. You must save for changes to be saved across reboots.

Example

The following command sets the backplane load-sharing policy to address-based:

```
configure backplane-ls-policy address-based
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on BlackDiamond switches.

configure ip-mtu vlan

```
configure ip-mtu <number> vlan <vlan name>
```

Description

Sets the maximum transmission unit (MTU) for the VLAN.

Syntax Description

number	Specifies the IP MTU value. Range is from 1500 to 9194.
vlan name	Specifies a VLAN name.

Default

The default IP MTU size is 1500.

Usage Guidelines

Use this command to enable jumbo frame support or for IP fragmentation with jumbo frames. Jumbo frames are Ethernet frames that are larger than 1522 bytes, including 4 bytes used for CRC. Both endstations involved in the transfer must be capable of supporting jumbo frames. The switch does not perform IP fragmentation or participate in MTU negotiation on behalf of devices that do not support jumbo frames.

When enabling jumbo frames and setting the MTU size for the VLAN, keep in mind that some network interface cards (NICs) have a configured maximum MTU size that does not include the additional 4 bytes of CRC included in a jumbo frame configuration. Ensure that the NIC maximum MTU is at or below the maximum MTU size configured on the switch. Frames that are larger than the MTU size configured on the switch are dropped at the ingress port.

If you use IP fragmentation with jumbo frames and you want to set the MTU size greater than 1500, all ports in the VLAN must have jumbo frames enabled.

For MPLS modules:

Fragmentation is based on either the minimum value of the configured MPLS IP MTU size or the configured IP MTU size for the egress VLAN.

Example

The following command sets the MTU size to 1500 for VLAN *sales*:

```
configure ip-mtu 1500 vlan sales
```

The following command increases the MTU size on the MPLS VLANs to accommodate the MPLS shim header:

```
configure ip-mtu 1550 vlan vlan1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure jumbo-frame size

```
configure jumbo-frame size <number>
```

Description

Sets the maximum jumbo frame size for the switch chassis.

Syntax Description

number	Specifies a maximum transmission unit (MTU) size for a jumbo frame.

Default

The default setting is 9216.

Usage Guidelines

Jumbo frames are used between endstations that support larger frame sizes for more efficient transfers of bulk data. Both endstations involved in the transfer must be capable of supporting jumbo frames.

The `number` keyword describes the maximum jumbo frame size "on the wire," and includes 4 bytes of cyclic redundancy check (CRC) plus another 4 bytes if 802.1Q tagging is being used.

To enable jumbo frame support, you must configure the maximum transmission unit (MTU) size of a jumbo frame that will be allowed by the switch.

Some network interface cards (NICs) have a configured maximum MTU size that does not include the additional 4 bytes of CRC. Ensure that the NIC maximum MTU size is at or below the maximum MTU size configured on the switch. Frames that are larger than the MTU size configured on the switch are dropped at the ingress port.

For MPLS modules:

You should enable jumbo frame support on the ports that are members of an MPLS VLAN. The jumbo frame size should be set to accommodate the addition of a maximally-sized label stack. For example, a jumbo frame size of at least 1530 bytes is needed to support a two-level label stack on a tagged Ethernet port and a jumbo frame size of at least 1548 bytes is needed to support a TLS encapsulated MPLS frame.

The MPLS module supports the MTU size configured using the `configure jumbo-frame size` command.

For version 6.1 and later:

- The jumbo_frame_mtu range is between 1523 through 9216.

For version 6.0:

- The jumbo_frame_mtu range is between 1522 through 9216.

Example

The following command configures the maximum MTU size of a jumbo frame size to 5500:

```
configure jumbo-frame size 5500
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure mirroring add

```
configure mirroring add [<mac_address> | vlan <vlan name> {ports <port
number>} | ports <portnumber> {vlan <vlan name>}]
```

Description

Adds a particular mirroring filter definition on the switch.

Syntax Description

mac_address	Specifies a MAC address. (Supported in versions 2.0 - 4x only)
vlan name	Specifies a VLAN name.
portnumber	Specifies a port or slot and port.

Default

N/A.

Usage Guidelines

On a modular switch, `<portnumber>` will be a slot and port in the form `<slot>:<port>`. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

You must enable port-mirroring using the `enable mirroring` command before you can configure the mirroring filter definitions.

Up to eight mirroring definitions can be added. You can mirror traffic from a VLAN, a physical port, or a specific VLAN/port combination.

Port-mirroring configures the switch to copy all traffic associated with one or more ports to a monitor port on the switch. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. The switch uses a traffic filter that copies a group of traffic to the monitor port. The traffic filter can be defined based on one of the following criteria:

- **Physical port**—All data that traverses the port, regardless of VLAN configuration, is copied to the monitor port.
- **VLAN**—All data to and from a particular VLAN, regardless of the physical port configuration, is copied to the monitor port.
- **Virtual port**—All data specific to a VLAN on a specific port is copied to the monitor port.

Up to eight mirroring filters and one monitor port can be configured on the switch. Once a port is specified as a monitor port, it cannot be used for any other function. Frames that contain errors are not mirrored.

For version 2.0 and 4.0:

In addition to the physical port, VLAN, and virtual port, the traffic filter can be defined based on the following criteria:

- **MAC source address/destination address**—All data sent to or received from a particular source or destination MAC address is copied to the monitor port.

For MAC mirroring to work correctly, the MAC address must already be present in the forwarding database (FDB). You need to enable and configure FDB for MAC mirroring to work correctly. See “FDB Commands” for more details.

Example

The following example sends all traffic coming into or out of a stand-alone switch on port 1 and the VLAN *default* to the mirror port:

```
configure mirroring add ports 1 vlan default
```

The following example sends all traffic coming into or out of a modular switch on slot 3, port 2 and the VLAN *default* to the mirror port:

```
configure mirroring add ports 3:2 vlan default
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.0 to discontinue support for the MAC address parameter.

Platform Availability

This command is available on all platforms.

configure mirroring delete

```
configure mirroring delete [<mac_address> | vlan <vlan name> {ports
<portnumber>} | ports <portnumber> {vlan <vlan name>}]
```

Description

Deletes a particular mirroring filter definition on the switch.

Syntax Description

mac_address	Specifies a MAC address. (Supported in versions 4.0 and 6.0 only)
vlan name	Specifies a VLAN name.
portnumber	Specifies a port or slot and port.

Default

N / A.

Usage Guidelines

On a modular switch, `<portnumber>` must be a slot and port in the form `<slot>:<port>`. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

For version 6.0:

- No longer supports using a MAC address to specify mirroring.

Example

The following example deletes the mirroring filter on a stand-alone switch defined for port 1 on VLAN *default*:

```
configure mirroring delete ports 1 vlan default
```

The following example deletes the mirroring filter on a modular switch defined for slot 3, port 2 on VLAN default:

```
configure mirroring add ports 3:2 vlan default
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.0 to discontinue support for the MAC address parameters.

Platform Availability

This command is available on all platforms.

configure msm-failover link-action

```
configure msm-failover link-action [keep-links-up | take-links-down]
```

Description

Configures external port response when MSM failover occurs.

Syntax Description

keep-links-up	Configures the external ports to not be reset when MSM failover occurs. This option is available on the "*i*" series switches only.
take-links-down	Configures the external ports to be reset when MSM failover occurs. This option is available on the "*i*" series switches only.

Default

Take-links-down.

Usage Guidelines

When MSM failover occurs, external ports will not be reset if the `keep-links-up` option is configured. When the `keep-links-up` option is configured, peer connections will not notice a link-down indication.

The `keep-links-up` and `take-links-down` options are available on the "*i*" series switches only.

Example

The following command prevents external ports from being reset when an MSM failover occurs:

```
configure msm-failover link-action keep-links-up
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ports

```
configure ports [<portlist> vlan <vlan name> | all] [limit-learning
<number> | lock-learning | unlimited-learning | unlock-learning]
```

Description

Configures virtual ports for limited or locked MAC address learning.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies that all virtual ports should be configured as indicated.
vlan name	Specifies the name of the VLAN.
limit-learning <number>	Specifies a limit on the number of MAC addresses that can be dynamically learned on the specified ports.
lock-learning	Specifies that the current FDB entries for the specified ports should be made permanent static, and no additional learning should be allowed.
unlimited-learning	Specifies that there should not be a limit on MAC addresses that can be learned.
unlock-learning	Specifies that the port should be unlocked (allow unlimited, dynamic learning).

Default

Unlimited, unlocked learning.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Limited learning. The limited learning feature allows you to limit the number of dynamically-learned MAC addresses per VLAN. When the learned limit is reached, all new source MAC addresses are blackholed at both the ingress and egress points. This prevent these MAC addresses from learning and responding to Internet control message protocol (ICMP) and address resolution protocol (ARP) packets.

If the limit you configure is greater than the current number of learned entries, all the current learned entries are purged.

Dynamically learned entries still get aged, and can be cleared. If entries are cleared or aged out after the learning limit has been reached, new entries will then be able to be learned until the limit is reached again.

Permanent static and permanent dynamic entries can still be added and deleted using the `create fdbentry` and `delete fdbentry` commands. These override any dynamically learned entries.

For ports that have a learning limit in place, the following traffic will still flow to the port:

- Packets destined for permanent MACs and other non-blackholed MACs

- Broadcast traffic
- EDP traffic

Traffic from the permanent MAC and any other non-blackholed MACs will still flow from the virtual port.

If you configure a MAC address limit on VLANS that have ESRP enabled, you should add an additional back-to-back link (that has no MAC address limit on these ports) between the ESRP-enabled switches. Doing so prevents ESRP PDU from being dropped due to MAC address limit settings.

Port lockdown. The port lockdown feature allows you to prevent any additional learning on the virtual port, keeping existing learned entries intact. This is equivalent to making the dynamically-learned entries permanent static, and setting the learning limit to zero. All new source MAC addresses are blackholed.

Locked entries do not get aged, but can be deleted like any other permanent FDB entries. The maximum number of permanent lockdown entries is 1024. Any FDB entries above will be flushed and blackholed during lockdown.

For ports that have lockdown in effect, the following traffic will still flow to the port:

- Packets destined for the permanent MAC and other non-blackholed MACs
- Broadcast traffic
- EDP traffic

Traffic from the permanent MAC will still flow from the virtual port.

Once the port is locked down, all the entries become permanent and will be saved across reboot. When you remove the lockdown using the unlock-learning option, the learning-limit is reset to unlimited, and all associated entries in the FDB are flushed.

To verify the MAC security configuration for the specified VLAN or ports, use the following commands:

```
show vlan <vlan name> security
show ports <portlist> info detail
```

Example

The following command limits the number of MAC addresses that can be learned on ports 1, 2, 3, and 6 in a VLAN named *accounting*, to 128 addresses:

```
configure ports 1, 2, 3, 6 vlan accounting learning-limit 128
```

The following command locks ports 4 and 5 of VLAN *accounting*, converting any FDB entries to static entries, and prevents any additional address learning on these ports:

```
configure ports 4,5 vlan accounting lock-learning
```

The following command removes the learning limit from the specified ports:

```
configure ports 1, 2, vlan accounting unlimited-learning
```

The following command unlocks the FDB entries for the specified ports:

```
configure ports 4,5 vlan accounting unlock-learning
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure ports auto off

```
configure ports [<portlist> | all | mgmt] auto off {speed [10 | 100 |
1000]} duplex [half | full]
```

Description

Manually configures port speed and duplex setting configuration on one or more ports on a switch.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all configured ports on the switch. (6.1 and later) See “Usage Guidelines” for more information.
mgmt	Specifies the management port. Supported only for switches that provide a management port.
speed [10]	Specifies 10 Mbps ports.
speed [100]	Specifies 100 Mbps ports.
speed [1000]	Specifies 1000 Mbps ports. (6.1 and later)
duplex [half]	Specifies half duplex; transmitting and receiving data one direction at a time.
duplex [full]	Specifies full duplex; transmitting and receiving data at the same time.

Default

Auto on.

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

You can manually configure the duplex setting and the speed of 10/100 Mbps ports, and you can manually configure the duplex setting on Gigabit Ethernet ports.

Fast Ethernet ports can connect to either 10BASE-T or 100BASE-T networks. By default, the ports autonegotiate port speed. You can also configure each port for a particular speed (either 10 Mbps or 100 Mbps).

Gigabit Ethernet ports are statically set to 1 Gbps, and their speed cannot be modified.

All ports on a stand-alone switch can be configured for half-duplex or full-duplex operation. By default, the ports autonegotiate the duplex setting.

In certain interoperability situations, it is necessary to turn autonegotiation off on a Gigabit Ethernet port. Even though a Gigabit Ethernet port runs only at full duplex and gigabit speeds, the command that turns off autonegotiation must still include the duplex setting.

Gigabit Ethernet ports support flow control only when autonegotiation is turned on. When autonegotiation is turned off, flow control is not supported.

For version 6.1:

- The `all` parameter specifies all ports on the switch.
- The `1000` parameter specifies 1000 Mbps ports.

Example

The following example turns autonegotiation off for port 4 (a Gigabit Ethernet port) on a stand-alone switch:

```
configure ports 4 auto off duplex full
```

The following example turns autonegotiation off for slot 2, port 1 on a modular switch:

```
configure ports 2:1 auto off duplex full
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.1 to support the `all` parameter.

Platform Availability

This command is available on all platforms.

configure ports auto on

```
configure ports [<portlist> | mgmt | all] auto on
```

Description

Enables autonegotiation for the particular port type.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
mgmt	Specifies the management port. Supported only for switches that provide a management port.
all	Specifies all configured ports on the switch. (6.1 and later) See “Usage Guidelines” for more information.

Default

Auto on.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The type of ports enabled for autonegotiation are 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.

Flow control is supported on Gigabit Ethernet ports only. It is enabled or disabled as part of autonegotiation. If autonegotiation is set to off, flow control is disabled. When autonegotiation is turned on, flow control is enabled.

For version 6.1:

- The `all` parameter specifies all ports on the switch.

Example

The following command configures the switch to autonegotiate for ports 4 and 6 on a stand-alone switch:

```
configure ports 4,6 auto on
```

The following command configures the switch to autonegotiate for slot 1, ports 2 and 4 on a modular switch:

```
configure ports 1:2, 1:4 auto on
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support the `all` parameter.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

configure ports auto-polarity

```
configure ports [<portlist> | all] auto-polarity [off | on]
```

Description

Configures the autopolarity detection feature on the specified Ethernet ports.

Syntax Description

portlist	Specifies one or more ports on the switch. May be in the form 1, 2, 3-5.
all	Specifies all of the ports on the switch.
off	Disables the autopolarity detection feature on the specified ports.
on	Enables the autopolarity detection feature on the specified ports.

Default

The autopolarity detection feature is on.

Usage Guidelines

Use the `all` keyword to enable or disable the autopolarity detection feature on all of the Ethernet ports on the Summit48si switch.

When autopolarity is disabled on one or more Ethernet ports, you can verify that status by using the command:

```
show configuration
```

This command will list the ports for which the feature has been disabled.

To verify the current autopolarity status, use the `show ports {<portlist> | all} info detail` command.

Example

The following command disables the autopolarity detection feature on ports 3-5 on the Summit48si switch:

```
configure ports 3-5 auto-polarity off
```

The following command enables the autopolarity detection feature on ports 3-5 on the Summit48si switch:

```
configure ports 3-5 auto-polarity on
```

History

This command was first available in ExtremeWare 6.2.2b108.

Platform Availability

This command is available on the Summit48si switch only.

configure ports display-string

```
configure ports [<portlist> | mgmt] display-string <alphanumeric string>
```

Description

Configures a user-defined string for a port or group of ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
mgmt	Specifies the management port. Supported only for switches that provide a management port.
alphanumeric string	Specifies a user-defined display string.

Default

N/A.

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

The display string can be up to 16 characters. Display strings do not need to be unique for each port—you can assign the same string to multiple ports. For example, you could give all the ports that connected to a particular department a common display string.

The string is displayed in certain commands such as the `show ports info` command.

NOTE

Do not use a port number as a display string. For example, do not assign the display string "2" to port 2.

Example

The following command configures the user-defined string *corporate* for port 1 on a stand-alone switch:

```
configure ports 1 display-string corporate
```

The following command configures the user-defined string *corporate* for ports 3, 4, and 5 on slot 1 on a modular switch:

```
configure ports 1:3-5 display-string corporate
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure port interpacket-gap

```
configure port <slot:port> interpacket-gap <byte_time>
```

Description

Configures the Interpacket Gap for a 10 Gigabit port.

Syntax Description

byte_time	Specifies the Interpacket Gap byte time.

Default

The default value of the byte time is 12.

Usage Guidelines

The standard compliant Interpacket Gap for 10 Gigabit Ethernet interfaces is 12. Some vendors' 10 Gigabit Ethernet interfaces drop packets when packets are transmitted using a value of 12. Thus, by increasing the Interpacket Gap, packet transmission is slowed and packet loss can be minimized or prevented. The Interpacket Gap value need not be modified when interconnecting Extreme Networks switches over 10 Gigabit Ethernet links.

The allowable range for the byte time is 12-1023.

Example

The following command configures Interpacket Gap to 48:

```
configure port 2:1 interpacket-gap 48
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms that support 10 Gigabit ports.

configure ports link-detection-level

```
configure ports <portlist> link-detection-level <link-detection-level>
```

Description

Configures the link detection level.

Syntax Description

portlist	Specifies one or more primary ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
link-detection-level	Specifies a link detection level.

Default

The default link detection level is 2.

Usage Guidelines

The range is 1 - 4. Table 9 lists the behavior of the switch at each level.

Table 9: Link detection level behavior

Level	ISR	Middle Layer Filter
1	off	off
2	on	off
3	off	on
4	on	on

Example

The following command configures the link detection level for port 3 to 4:

```
configure ports 3 link-detection-level 4
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure ports redundant

```
configure ports [<portlist> | <portid> | mgmt] redundant [<portlist> |
<portid>]
```

Description

Configures a software-controlled redundant port.

Syntax Description

portlist	Specifies one or more primary ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
portid	Specifies a primary port using the display string configured for the port. If this option is used to identify the port, the redundant port must also be specified using a port id (display string).
mgmt	Specifies the management port as the primary port. Supported only for switches that provide a management port.
portlist	Specifies one or more redundant ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
portid	Specifies a redundant port using the display string configured for the port. This option may be used to identify the redundant port of the primary port was specified using the port id (display string).

Default

N / A.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

The first port list specifies the primary ports. The second port list specifies the redundant ports.

A software-controlled redundant port is configured to backup a specified primary port. The redundant port tracks the link state of the associated primary port, and if the link on the primary port fails, the redundant port establishes a link and becomes active. You can back up a specified Ethernet port with a redundant, dedicated Ethernet port. You can also back up a load-shared group of Ethernet ports with a set of load-shared redundant Ethernet ports. If a link in the active load-shared group fails, the entire group fails over to the redundant group.

The following criteria must be considered when configuring a software-controlled redundant port:

- You must manually configure the primary and redundant ports identically in terms of VLANs, QoS settings, access lists, and so on.
- Auto-negotiation must be enabled on both the primary and redundant port.
- You cannot configure hardware redundant ports (such as ports 49 and 50 on a Summit48i) as software controlled redundant ports.
- Software redundant ports are supported on products that use the *"i"* chipset.

- Only one side of the link should be configured as redundant. For example, if ports 1 and 2 are connected between switches A and B, only switch A should be configured with redundant ports.
- Software redundant ports are not supported on 1000BASE-T ports.

Software redundant port only cover failures where both the TX and RX paths fail. If a single strand of fiber is pulled, the software redundant port cannot correctly recover from the failure.

Example

The following command configures a software-controlled redundant port on a stand-alone switch:

```
configure ports 3 redundant 4
```

The following command configures a software-controlled redundant port on a modular switch:

```
configure ports 1:3 redundant 2:3
```

The following command configures a software-controlled redundant port using the port display strings corp1 and corp5 to identify the ports:

```
configure ports corp1 redundant corp5
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure ports vdsl

```
configure ports <portlist> vdsl [5meg | 10meg | etsi]
```

Description

Configures VDSL ports.

Syntax Description

portlist	Specifies one or more slots and ports. Can specify a list of slots and ports, and may be in the form 2:*, 2:5, 2:6-2:8.
5meg	Specifies 5 Mbps.
10meg	Specifies 10 Mbps
etsi	Specifies ETSI Plan 997

Default

The default configuration for VDSL ports is 10 Mbps.

Usage Guidelines

Select the configuration that interoperates with the associated VDSL customer premises equipment (CPE). A lower rate may support a longer cable distance, depending on the installation.

Example

The following command configures all the VDSL ports on slot 2 to 5 Mbps:

```
configure ports 2:* vdsl 5meg
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms that support VDSL ports.

configure sharing address-based

```
configure sharing address-based [L2 | L2_L3 | L2_L3_L4]
```

Description

Configures the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data.

Syntax Description

L2	Indicates that the switch should examine the MAC source and destination address.
L2-L3	Indicates that the switch should examine the IP source and destination address.
L2-L3-L4	Indicates that the switch should examine the UDP or TCP well-know port number.

Default

N / A.

Usage Guidelines

This feature is available using the address-based load-sharing algorithm only. The address-based load-sharing algorithm uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:

- IP packets—Uses the source and destination MAC and IP address, and the TCP port number.
- IPX packets—Uses the source and destination MAC address and IPX identifiers.
- All other packets—Uses the source and destination MAC address.

To verify your configuration, use the `show sharing address-based` command. The show sharing address-based output displays the addressed-based configurations on the switch.

Example

The following example configures the switch to examine the MAC source and destination address:

```
configure sharing address-based l2
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on the "*i*" series platform.

configure slot

```
configure slot <slot> module <module name>
```

Description

Configures a slot for a particular I/O module card in a modular switch.

Syntax Description

slot	Specifies the slot number.
module name	Specifies the type of module for which the slot should be configured. The list of modules you can enter will vary depending on the type of switch and version of ExtremeWare you are running. Certain modules are supported only with specific ExtremeWare Technology Releases. The following are some of the modules you may specify for a BlackDiamond switch: 10giglr—Specifies a 10 Gigabit Ethernet, 1-port, long-range, fiber module. f32fi—Specifies a Fast Ethernet, 32-port, fiber module, “i” chipset. f48t—Specifies a Fast Ethernet, 48-port, copper module. f96t —Specifies a Fast Ethernet, 96-port, copper module. g8t—Specifies a Gigabit Ethernet, 8-port, copper module. g8x—Specifies a Gigabit Ethernet, 8-port, copper module. g12sx—Specifies a Gigabit Ethernet, 12-port, fiber module. g12tx—Specifies a Gigabit Ethernet, 12-port, copper module. g16x—Specifies a Gigabit Ethernet, 16-mini-GBIC port, oversubscribed, fiber module g24t—Specifies a Gigabit Ethernet, 24-port, oversubscribed, copper module. WDMi—Specifies a Gigabit Ethernet, WAN module. arm—Specifies an Accounting and Routing Module (ARM). a3c—Specifies an Asynchronous Transfer Mode (ATM) module. mpls—Specifies a MultiProtocol Label Switching (MPLS) module. p3c—Specifies an OC-3 PoS module. p12c—Specifies an OC-12 PoS module. The following are some of the modules you can specify for an Alpine switch: fm8v—Specifies a VDSL module. fm24t—Specifies a Fast Ethernet, 24-port, copper module. fm24mf—Specifies a Fast Ethernet, 24-port, multi-mode, fiber module. fm24sf—Specifies a Fast Ethernet, 24-port, single mode, fiber module. fm32t—Specifies a Fast Ethernet, 32-port, copper module. gm4s—Specifies Gigabit Ethernet, 4-port, fiber module. gm4t—Specifies a Gigabit Ethernet, 4-port, copper module. gm4x—Specifies a Gigabit Ethernet, 4-port, GBIC module. gm16x—Specifies a Gigabit Ethernet, 16-mini-GBIC port, oversubscribed, fiber module gm16t—Specifies a Gigabit Ethernet, 16-port, oversubscribed, copper module. wdmi—Specifies a Gigabit Ethernet WAN module. (6.1 or later)

	wm4t1—Specifies a T1 WAN module. (6.1 or later) wm4e1—Specifies an E1 WAN module. wm1t3—Specifies a T3 WAN module.

Default

If a slot has not been configured for a particular type of I/O module, then any type of module is accepted in that slot, and a default port and VLAN configuration is automatically generated.

Usage Guidelines

The `configure slot` command displays different module parameters depending on the type of modular switch you are configuring and the version of ExtremeWare running on the switch.

You can also preconfigure the slot before inserting the module card. This allows you to begin configuring the module and ports before installing the card in the chassis.

If a slot has not been configured for a particular type of I/O module, then any type of module is accepted in that slot, and a default port and VLAN configuration is automatically generated. If a slot is configured for one type of module, and a different type of module is inserted, the inserted module is put into a mismatch state, and is not brought online. To use the new module type in a slot, the slot configuration must be cleared or configured for the new module type.

Upon powering up the chassis, or when an I/O module is hot-swapped, ExtremeWare automatically determines the system power budget and protects the BlackDiamond switch from any potential overpower configurations. If power is available, ExtremeWare powers on and initializes the module. When ExtremeWare detects that a module will cause an overpower condition, the module remains powered down, and is not initialized. An entry is made to the system log indicating the condition.

For version 4.0:

- This command is available on BlackDiamond switches only.

Example

The following command configures the slot for a Fast Ethernet, 32-port, copper module:

```
configure slot 2 module F32T
```

History

This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 7.0.1 to support the oversubscribed Alpine and BlackDiamond I/O modules.

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.8b12 to support MPLS modules.

This command was modified in ExtremeWare 6.1 to support the PoS modules and additional Alpine I/O modules.

This command was modified in ExtremeWare 6.0 to support the Alpine and additional BlackDiamond F48T, G8X, and G12X I/O modules.

Platform Availability

This command is available on modular switches only.

disable edp ports

```
disable edp ports [<portlist> | all]
```

Description

Disables the Extreme Discovery Protocol (EDP) on one or more ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports on the switch. See “Usage Guidelines” for more information.

Default

Enabled.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

You can use the `disable edp ports` command to disable EDP on one or more ports when you no longer need to locate neighbor Extreme Networks switches.

For version 6.1:

- The `all` parameter specifies all ports on the switch.

For Version 6.0 and later:

- SummitLink is not supported.

For version 2.0 and 4.0:

- EDP cannot be disabled on a port that has SummitLink enabled, nor on ports that are connected to a Summit Virtual Chassis.

Example

The following command disables EDP on port 4 and port 6 on a stand-alone switch:

```
disable edp ports 4,6
```

The following command disables EDP on slot 1, ports 2 and 4 on a modular switch:

```
disable edp ports 1:2, 1:4
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.1 to support the `all` parameter.

Platform Availability

This command is available on all platforms.

disable flooding ports

```
disable flooding ports <portlist>
```

Description

Disables packet flooding on one or more ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Enabled.

Usage Guidelines

Flooding configures the specified ports to act like a hub. Disabling flooding means that only broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number, are forwarded.

Disabling flooding does not automatically enable learning on the port: use the `enable learning ports` command to re-enable learning on the specified ports.

Learning and flooding are mutually exclusive. To enable learning, you must disable flooding.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command disables flooding on ports 6, 7, and 8 on a stand-alone switch:

```
disable flooding ports 6,7,8
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on "*i*"-series platforms.

disable jumbo-frame ports

```
disable jumbo-frame ports [<portlist> | all]
```

Description

Disables jumbo frame support on a port.

For PoS modules, this command applies to PoS ports when disabling jumbo-frame support changes the negotiated maximum receive unit (MRU) size.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports on the switch.

Default

Disabled.

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Use the `disable jumbo-frame ports` command when you no longer need jumbo frame support.

Example

The following command disables jumbo frame support on port 4 on a stand-alone switch:

```
disable jumbo-frame ports 4
```

The following command disables jumbo frame support on slot 1, port 2 on a BlackDiamond switch:

```
disable jumbo-frame 1:2
```

History

This command was first available in ExtremeWare 6.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

Platform Availability

This command is available on all platforms.

disable lbdetect port

```
disable lbdetect port <portlist>
```

Description

Disables the detection of loops between ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports to be grouped to the master port. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

Each port may enable loop detection. This optional feature detects that a port has been looped back to the local system. If a loopback is detected, the port is disabled. Note that loopbacks may exist between different ports. The feature will disable any port that both has the feature enabled, and receives an LACP message that was sent from the local system.

Example

The following example disables loopback detection on ports 9 through 12:

```
disable lbdetect port 9-12
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable learning ports

```
disable learning ports <portlist>
```

Description

Disables MAC address learning on one or more ports for security purposes.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Enabled.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers.For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

If MAC address learning is disabled, only broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number, are forwarded.

Use this command in a secure environment where access is granted via permanent forwarding databases (FDBs) per port.

Learning must be disabled to allow port flooding. See the `enable flooding` command for information on enabling port flooding.

Example

The following command disables MAC address learning on port 4 on a stand-alone switch:

```
disable learning ports 4
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

Platform Availability

This command is available on all platforms.

disable mirroring

```
disable mirroring
```

Description

Disables port-mirroring.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Use the `disable mirroring` command to stop configured copied traffic associated with one or more ports.

Example

The following command disables port-mirroring:

```
disable mirroring
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable ports

```
disable ports [<portlist> | all]
```

Description

Disables one or more ports on the switch.

For PoS modules, brings down the PPP link on the specified port and changes the port status LED to blinking green.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports on the switch.

Default

Enabled.

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Use this command for security, administration, and troubleshooting purposes.

Even though a port is disabled, the link remains enabled for diagnostic purposes.

Example

The following command disables ports 3, 5, and 12 through 15 on a stand-alone switch:

```
disable ports 3,5,12-15
```

The following command disables slot 1, ports 3, 5, and 12 through 15 on a modular switch:

```
disable ports 1:3,1:5,1:12-1:15
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.1 to support PoS modules.

Platform Availability

This command is available on all platforms.

disable sharing

```
disable sharing [<port>]
```

Description

Disables a load-sharing group of ports.

Syntax Description

port	Specifies the master port of a load-sharing group. On a modular switch, is a combination of the slot and port number, in the format <slot>:<port>.

Default

Disabled.

Usage Guidelines

This command increases bandwidth tracking and resiliency.

On a modular switch, <port> is specified as <slot>:<port number>. On a stand-alone switch, <port> is the port configured as the load-sharing master port. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

When sharing is disabled, the master port retains all configuration including VLAN membership. Configuration for all other member ports is reset to default values. Member ports are removed from all VLANs to prevent loops.

Example

The following command disables sharing on master logical port 9, which contains ports 9-12 on a stand-alone switch:

```
disable sharing 9
```

The following command disables sharing on master logical port 9 in slot 3, which contains ports 9 through 12 on a modular switch:

```
disable sharing 3:9
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

disable slot

```
disable slot [<slot number> | all]
```

Description

Disables one or all slots on a BlackDiamond or Alpine switch, and leaves the blade in a power down state.

Syntax Description

slot number	Specifies the slot to be disabled.
all	Species that all slots in the device should be disabled.

Default

Enabled.

Usage Guidelines

This command allows the user to disable a slot. When the user types this command, the I/O card in that particular slot number is brought down, and the slot is powered down. The LEDs on the card go OFF.

A disabled slot can be re-enabled using the `enable slot` command.

The `show slot` command, if invoked after the user disables the slot, shows this slot state as "Disabled." The user can either disable a slot individually or use the `disable slot all` to disable all the slots.

If there is no I/O card present in a slot when the user disables the slot, the slot still goes to the "Disable" state. If a card is inserted in a slot that has been disabled, the card does not come up and stays in the "disabled" state until the slot is enabled by using the `enable slot` command. below.

If you do not save the configuration before you do a switch reboot, the slot will be re-enabled upon reboot. If you save the configuration after disabling a slot, the slot will remain disabled after a reboot.

Example

The following command disables slot 5 on the switch:

```
disable slot 5
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on BlackDiamond and Alpine switches only.

disable smartredundancy

```
disable smartredundancy [<portlist>]
```

Description

Disables the smart redundancy feature.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Use with Extreme Networks switches that support privacy and backup uplinks.

When smartredundancy is disabled, the switch changes the active link only when the current active link becomes inoperable.

Example

The following command disables the smart redundancy feature on ports 1-4:

```
disable smartredundancy 1-4
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms switches.

enable edp ports

```
enable edp ports [<portlist> | all]
```

Description

Enables the Extreme Discovery Protocol (EDP) on one or more ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports on the switch.

Default

Enabled.

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

EDP is useful when Extreme Networks switches are attached to a port.

The EDP is used to locate neighbor Extreme Networks switches and exchange information about switch configuration. When running on a normal switch port, EDP is used to by the switches to exchange topology information with each other. Information communicated using EDP includes the following:

- Switch MAC address (switch ID)
- Switch software version information
- Switch IP address
- Switch VLAN-IP information
- Switch port number

For version 2.0 and 4.0:

Information communicated using EDP also includes the following:

- Virtual chassis identifier and port number
- Listing of all virtual chassis identifiers

Example

The following command enables EDP on port 7 on a stand-alone switch:

```
enable edp ports 7
```

The following command enables EDP on slot 1, port 3 on a modular switch:

```
enable edp ports 1:3
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

enable flooding ports

```
enable flooding ports <portlist>
```

Description

Enables packet flooding on one or more ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Ports are enabled for learning, not flooding.

Usage Guidelines

This command configures the specified ports to act like a hub. When flooding is enabled on a particular port, *all* frames and packets are passed on to other member ports that have flooding enabled. This includes all broadcast, multicast, known unicast and unknown unicast packets (including EDP). To make effective use of this feature you should have flooding enabled on more than one port.

Learning and flooding are mutually exclusive. To enable flooding, you must first disable learning.

When ports are configured for flooding, the FDB will be flushed for the entire system, which means all the entries in the dynamic FDB must be relearned.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Example

The following command enables flooding on ports 6, 7, and 8 on a stand-alone switch:

```
enable flooding ports 6,7,8
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on “*i*”-series platforms.

enable jumbo-frame ports

```
enable jumbo-frame ports [<portlist> | all]
```

Description

Enables support on the physical ports that will carry jumbo frames.

For PoS modules, enables jumbo-frame support to specific PoS ports when jumbo-frame support changes the negotiated maximum receive unit (MRU) size.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports on the switch.

Default

Disabled.

Usage Guidelines

Increases performance to back-end servers or allows for VMAN 802.1q encapsulations.

You must configure the maximum MTU size of a jumbo frame before you can use the `enable jumbo-frame ports` command. Use the `configure jumbo-frame size` command to configure the MTU size.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command enables jumbo frame support on port 5 on a stand-alone switch:

```
enable jumbo-frame ports 5
```

The following command enables jumbo frame support on slot 3, port 5 on a modular switch:

```
enable jumbo-frame ports 3:5
```

History

This command was first available in ExtremeWare 6.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

Platform Availability

This command is available on all platforms.

enable lbdetect port

```
enable lbdetect port <portlist> [retry-timeout<seconds>]
```

Description

Enables the system to detect loops between ports. If a port is looped, it disables the port. Every N seconds, it re-enables the port and tries again, unless “none” is specified

Syntax Description

portlist	Specifies one or more ports or slots and ports to be grouped to the master port. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
retry-timeout	Specifies a time in seconds to check for loops on the ports.

Default

Disabled.

Usage Guidelines

Each port may enable loop detection. This optional feature detects that a port has been looped back to the local system. If a loopback is detected, the port is disabled. Note that loopbacks may exist between different ports. The feature will disable any port that both has the feature enabled, and receives an LACP message that was sent from the local system.

If no timeout is specified, the port is disabled permanently if there is a loop detected. Otherwise, the port is periodically re-enabled, and tested for loops every N seconds.

Example

The following example enables loopback detection on ports 9 through 12:

```
enable lbdetect port 9-12
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable learning ports

```
enable learning ports <portlist>
```

Description

Enables MAC address learning on one or more ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Enabled.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command enables MAC address learning on ports 7 and 8 on a stand-alone switch:

```
enable learning ports 7,8
```

The following command enables MAC address learning on slot 1, ports 7 and 8 on a modular switch:

```
enable learning ports 1:7-8
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

enable mirroring to port

```
enable mirroring to port [<portlist>] [tagged | untagged]
```

Description

Dedicates a port on the switch to be the mirror output port.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
tagged	Configures the ports as tagged.
untagged	Configures the ports as untagged.

Default

N/A.

Usage Guidelines

Port-mirroring configures the switch to copy all traffic associated with one or more ports to a monitor port on the switch. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. The switch uses a traffic filter that copies a group of traffic to the monitor port. The traffic filter can be defined based on one of the following criteria:

- **Physical port**—All data that traverses the port, regardless of VLAN configuration, is copied to the monitor port.
- **VLAN**—All data to and from a particular VLAN, regardless of the physical port configuration, is copied to the monitor port.
- **Virtual port**—All data specific to a VLAN on a specific port is copied to the monitor port.

Up to eight mirroring filters and one monitor port can be configured on the switch. After a port has been specified as a monitor port, it cannot be used for any other function. Frames that contain errors are not mirrored.

For version 6.0 and later:

- `tagged` and `untagged` are added to the command syntax.

For version 4.0 and later:

- `to` is added to the command syntax.
- Supports modular switches.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

For version 2.0 and 4.0:

- In addition to the physical port, VLAN, and virtual port, the traffic filter can be defined based on the following criteria:

— **MAC source address/destination address**—All data sent to or received from a particular source or destination MAC address is copied to the monitor port.

For MAC mirroring to work correctly, the MAC address must already be present in the forwarding database (FDB).

Example

The following example selects port 3 as a tagged mirror port on a stand-alone switch:

```
enable mirroring to port 3 tagged
```

The following example selects slot 1, port 3 as the mirror port on a modular switch:

```
enable mirroring to port 1:3
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support the `tag | untagged` keywords and modular switches.

Platform Availability

This command is available on all platforms.

enable ports

```
enable ports [<portlist> | all]
```

Description

Enables a port.

For PoS modules, enables the PPP link on the specified port, and changes the port status LED to solid green (if no other problems exist).

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports on the switch.

Default

All ports are enabled.

Usage Guidelines

Use this command to enable the port(s) if you disabled the port(s) for security, administration, or troubleshooting purposes.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command enables ports 3, 5, and 12 through 15 on the stand-alone switch:

```
enable ports 3,5,12-15
```

The following command enables slot 1, ports 3, 5, and 12 through 15 on the modular switch:

```
enable ports 1:3, 1:5, 1:12-1:15
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 4.0 to support the modular switches.

Platform Availability

This command is available on all platforms.

enable sharing grouping

```
enable sharing <port> grouping <portlist> {dynamic | algorithm {port-based
| address-based | round-robin}}
```

Description

This command enables the switch to configure static port load sharing or dynamic port load sharing. When configuring dynamic port load sharing, LACP will be used to detect and set up for the remote side's load sharing capabilities.

Syntax Description

port	Specifies the master port for a loadsharing group.
portlist	Specifies one or more ports or slots and ports to be grouped to the master port. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
dynamic	Specifies dynamic sharing by using LACP.
algorithm	Specifies sharing by port-based, address-based, or round-robin algorithms.

Default

Disabled

Usage Guidelines

On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Load sharing allows you to increase bandwidth and availability between switches by using a group of ports to carry traffic in parallel between switches. The sharing algorithm allows the switch to use multiple ports as a single logical port or a "master" port. For example, VLANs see the load-sharing group as a single logical port. The algorithm also guarantees packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.

Load sharing must be enabled on both ends of the link, or a network loop will result.

While LACP is based on industry standard, this feature is supported between Extreme Networks switches only. However, it may be compatible with third-party "trunking" or sharing algorithms. Check with an Extreme Networks technical representative for more information.

Modular switch load-sharing groups are defined according to the following rules:

- The first port in the load-sharing group is configured to be the "master" logical port. This is the reference port used in configuration commands. It can be thought of as the logical port representing the entire port group.
- A master port can be a member of a Spanning Tree Domain (STPD), but the other ports assigned to a load-sharing group cannot.

- When using load sharing, you should always reference the master logical port of the load-sharing group when configuring or viewing VLANs. VLANs configured to use other ports in the load-sharing group will have those ports deleted from the VLAN when load sharing becomes enabled.
- A load-sharing group can include a maximum of eight ports.
- The ports in a load-sharing group on a BlackDiamond 6816, and on a BlackDiamond 6804 and 6808 that do not use the MSM-3, must all be on the same I/O module. Groups can span multiple modules with other chassis.
- Dynamic load sharing (LACP) cannot be used for groups that span multiple modules.

There are two broad categories of load sharing supported on Extreme Network switches:

- **Dynamic load sharing**—A grouping of ports that will use IEEE 802.3ad load sharing to dynamically determine if load sharing is possible, and will automatically configure load sharing when possible. Uses Link Aggregation Control Protocol (LACP), part of the IEEE 802.3ad standard, to allow the switch to dynamically reconfigure the sharing groups. The group is only enabled when LACP detects that the other side is also using LACP, and wants these ports to be in a group
- **Static load sharing**—A grouping of ports specifically configured to load share. The switch ports at each end must be configured as part of a load-sharing group. Additionally, you can choose the load-sharing algorithm used by the group. This feature is supported between Extreme Networks switches only, but may be compatible with third-party trunking or link-aggregation algorithms. Check with an Extreme Networks technical representative for more information.

Load-sharing algorithms allow you to select the distribution technique used by the load-sharing group to determine the output port selection. Algorithm selection is not intended for use in predictive traffic engineering. You can only choose the algorithm used in static load sharing. There is no option to choose an algorithm when you use dynamic load sharing.

- **Port-based**—Uses the ingress port to determine which physical port in the load-sharing group is used to forward traffic out of the switch.
- **Address-based**—Uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:
  - IP packets—Uses the source and destination MAC and IP addresses, and the TCP port number.
  - IPX packets—Uses the source and destination MAC address, and IPX network identifiers.
  - All other packets—Uses the source and destination MAC address.
- **Round-robin**—When the switch receives a stream of packets, it forwards one packet out of each physical port in the load-sharing group using a round-robin scheme.

Using the round-robin algorithm, packet sequencing between clients is not guaranteed.

If you do not explicitly select an algorithm, the port-based scheme is used. However, the address-based algorithm has a more even distribution and is the recommended choice.

Example

The following example defines a load-sharing group that contains ports 9 through 12, and uses the first port in the group as the master logical port on a stand-alone switch:

```
enable sharing 9 grouping 9-12
```

The following example defines a load-sharing group that contains ports 9 through 12 on slot 3, ports 7 through 10 on slot 5, and uses the first port on slot 3 as the master logical port 9 on a modular switch:

```
enable sharing 3:9 grouping 3:9-3:12, 5:7-5:10
```

In this example, logical port 3:9 represents physical ports 3:9 through 3:12 and 5:7 through 5:10.

History

This command was first available in ExtremeWare 2.0.

The command was modified in ExtremeWare 4.0 to support modular switches.

The command was modified in ExtremeWare 6.0 to support the `algorithm` parameter.

The command was modified in ExtremeWare 7.0.0 to support the `dynamic` parameter.

The command was modified in ExtremeWare 7.1.1 to support cross-module trunking on BlackDiamond switches.

Platform Availability

This command is available on all platforms.

enable slot

```
enable slot [<slot number> | all]
```

Description

Enables one or all slots on a BlackDiamond or Alpine switch.

Syntax Description

slot number	Specifies the slot to be enabled.
all	Species that all slots in the device should be enabled.

Default

Enabled.

Usage Guidelines

This command allows the user to enable a slot that has been previously disabled using the `disable slot` command.

When the user enters the enable command, the disabled I/O card in the specified slot is brought up, and the slot is made operational, if possible, or goes to the appropriate state as determined by the card state machine. The LEDs on the card are brought ON as usual. The user can either enable a slot individually, or use the `enable slot all` command to enable all the slots.

After the user enables the slot, the `show slot` command shows the state as "Operational" or will display the appropriate state if the card could not be brought up successfully. Note that there is no card state named "Enable" and the card goes to the appropriate states as determined by the card state machine when the `enable slot` command is invoked.

Only slots that have their state as "disabled" can be enabled using this command. If this command is used on slots that are in states other than "disabled," the card state machine takes no action on these slots.

Example

The following command enables slot 5 on the switch:

```
enable slot 5
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on BlackDiamond and Alpine switches only.

enable smartredundancy

```
enable smartredundancy <portlist>
```

Description

Enables the Smart Redundancy feature on the redundant Gigabit Ethernet port.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Enabled.

Usage Guidelines

When the Smart Redundancy feature is enabled, the switch always uses the primary link when the primary link is available.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command enables the Smart Redundancy feature on port 4 on a switch:

```
enable smartredundancy 4
```

The following command enables the Smart Redundancy feature on slot 1, port 4 on a BlackDiamond switch:

```
enable smartredundancy 1:4
```

History

This command was first available in ExtremeWare 2.0.

Support for modular switches was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

restart ports

```
restart ports [<portlist>
```

Description

Resets autonegotiation for one or more ports by resetting the physical link.

For PoS modules, causes the PPP link to be renegotiated.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N / A.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command resets autonegotiation on port 4 on a stand-alone switch:

```
restart ports 4
```

The following command resets autonegotiation on slot 1, port 4 on a modular switch:

```
restart ports 1:4
```

History

This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified by removing the `mgmt` option in ExtremeWare 6.22.

Platform Availability

This command is available on all platforms.

run msm-failover

```
run msm-failover
```

Description

Causes a user-specified MSM failover.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command causes a user-specified MSM failover:

```
run msm-failover
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on the BlackDiamond switch only.

show edp

```
show edp {<portlist>}
```

Description

Displays connectivity and configuration information for neighboring Extreme Networks switches.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Use the show edp command to display neighboring switches and configurations. This is most effective with Extreme Networks switches.

Example

The following command displays the connectivity and configuration of neighboring Extreme Networks switches:

```
show edp
```

Following is the output from this command:

```
Port 1:  EDP is enabled
        Remote-system: Summit5i (Version 6.2.2)
                Remote-ID=00:00:00:01:30:e9:ef:00
                Remote-Port=1:1   Age=37
                Remote-Vlans:
                        Mgmt(4094, 10.45.208.223) test1(0) Default(1)
MacVlanDiscover(0)

Port 3:  EDP is enabled
        Remote-system: Summit7i (Version 6.2.2)
                Remote-ID=00:00:00:e0:2b:99:fe:00
                Remote-Port=1:3   Age=35
                Remote-Vlans:
                        Mgmt(4094) Default(1) MacVlanDiscover(0)
Port 5:  EDP is enabled
        Remote-system: Alpine3808 (Version 6.2.2)
                Remote-ID=00:00:00:01:30:31:55:00
                Remote-Port=1:1   Age=47
```

```
Remote-Vlans:
        Mgmt(4094, 10.45.208.226) Default(1) MacVlanDiscover(0)
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show mirroring

```
show mirroring
```

Description

Displays the port-mirroring configuration on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

You must configure mirroring on the switch to display mirroring statistics. Use the `show mirroring` command to configure mirroring.

You can use this command to display mirroring statistics and determine if mirroring is enabled or disabled on the switch.

To view the status of port-mirroring on the switch, use the `show mirroring` command. The `show mirroring` command displays information about the enable/disable state for port-mirroring.

Example

The following command displays switch mirroring statistics:

```
show mirroring
```

Following is the output from this command:

```
Mirror port: 5 is up
port number 1 in  all vlans
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ports collisions

```
show ports {mgmt | <portlist>} collisions
```

Description

Displays real-time collision statistics.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A

Usage Guidelines

If you do not specify a port number or range of ports, collision statistics are displayed for all ports.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

This status information may be useful for your technical support representative if you have a network problem.

Example

The following command displays real-time collision statistics on port 7 on a stand-alone switch:

```
show ports 7 collisions
```

The following command displays real-time collision statistics on slot 1, ports 1-16 on a modular switch:

```
show ports 1:1-1:16 collisions
```

Following is the output from this command:

```
Port Collision Monitor                                  Wed Oct 30 19:33:10 2002
Port    Link                Collision Histogram
        Status   1   2   3   4   5   6   7   8   9   10  11 12  13  14  15   16
================================================================================
1          A     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
2          R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
3          A     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
4          R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
5          A     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
6          R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
7          R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
8          R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
```

```
9          R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
10         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
11         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
12         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
13         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
14         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
15         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
16         R     0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
================================================================================
Link Status: A-Active R-Ready D-Disabled NP-Not Present LB-Loopback
           0->Clear Counters  U->page up  D->page down ESC->exit
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show ports configuration

```
show ports {mgmt | <portlist>} configuration
```

Description

Displays port configuration statistics.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

If you do not specify a port number or range of ports, configuration statistics are displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

This command displays port configuration, which includes:

- Port state
- Link state
- Link speed
- Duplex mode
- Flow control
- Load sharing information
- Link media information

For version 6.0 and later:

- Auto on/off

Example

The following command displays the port configuration statistics for all ports on a switch:

```
show ports config
```

Following is the output from this command:

```
Port Configuration Monitor                              Thu Oct 24 16:22:08 2002
Port          Port    Link  Auto    Speed       Duplex    Flow  Ld Share Media
              State  Status Neg   Cfg Actual  Cfg Actual  Ctrl   Master Pri  Red
1:1           ENABLED R     ON    AUTO 1000  AUTO  FULL   NONE         UTP
1:2           ENABLED R     ON    AUTO       AUTO                      UTP
1:3           ENABLED R     ON    AUTO       AUTO                      UTP
1:4           ENABLED R     ON    AUTO       AUTO                      UTP
1:5           ENABLED R     ON    AUTO       AUTO                      UTP
1:6           ENABLED R     ON    AUTO       AUTO                      UTP
1:7           ENABLED R     ON    AUTO       AUTO                      UTP
1:8           ENABLED R     ON    AUTO       AUTO                      UTP
2:1           ENABLED R     ON    1000       AUTO                       SX
2:2           ENABLED R     ON    1000       AUTO
2:3           ENABLED R     ON    1000       AUTO
2:4           ENABLED R     ON    1000       AUTO
2:5           ENABLED R     ON    1000       AUTO
2:6           ENABLED R     ON    1000       AUTO
2:7           ENABLED R     ON    1000       AUTO
2:8           ENABLED R     ON    1000       AUTO
3:1           ENABLED R     ON    1000       AUTO                       SX
3:1           ENABLED R     ON    1000       AUTO                       SX
3:2           ENABLED R     ON    1000       AUTO                       SX
3:3           ENABLED R     ON    1000       AUTO                       SX
3:4           ENABLED R     ON    1000       AUTO                       SX
3:5           ENABLED R     ON    1000       AUTO                       SX
3:6           ENABLED R     ON    1000       AUTO                       SX
3:7           ENABLED R     ON    1000       AUTO                       SX
3:8           ENABLED R     ON    1000       AUTO                       SX
3:9           ENABLED R     ON    1000       AUTO                       SX
3:10          ENABLED R     ON    1000       AUTO                       SX
3:11          ENABLED R     ON    1000       AUTO                       SX
3:12          ENABLED R     ON    1000       AUTO                       SX
4:1           ENABLED R     ON    622        AUTO                      SMF
4:2           ENABLED R     ON    622        AUTO                      SMF
5:1           ENABLED R     ON    AUTO       AUTO                      UTP
5:2           ENABLED R     ON    AUTO       AUTO                      UTP
5:3           ENABLED R     ON    AUTO       AUTO                      UTP
5:4           ENABLED R     ON    AUTO       AUTO                      UTP
================================================================================
     Link Status: A-Active R-Ready D-Disabled NP-Not Present LB-Loopback
                    U->page up  D->page down ESC->exit
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show ports info

```
show ports {mgmt | <portlist>} info {detail}
```

Description

Displays detailed system-related information.

For PoS modules, displays port information that includes new DiffServ and RED configuration parameters.

For "3" series modules, if you specify the `detail` keyword, the output displays the flow control state and the ingress QoS profile, ingress IPTOS replacement, and egress rate limiting configurations.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
detail	Specifies detailed port information. (6.0 and later)

Default

N/A.

Usage Guidelines

This command displays the following:

- Port number
- Diagnostics
- Port configuration
  - RED state
  - Admin state
  - Link state
  - Link counter
  - VLAN configuration
  - STP configuration
  - Trunking
  - EDP
  - DLCS
  - Load balancing
  - Learning
  - Flooding
  - QoS profiles

If you do not specify a port number or range of ports, detailed system-related information is displayed for all ports. The data is displayed in a table format.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

This status information may be useful for your technical support representative if you have a network problem.

For version 6.0 and later:

- The detail parameter is used to provided more specific port information. The data is called out with written explanations versus displayed in a table format.

For version 6.2.2 and later:

- The detailed output displays a link filter counter. The link filter counter is calculated at the middle layer on receiving an event. The link filter up indicates the number of link transitions from down to up at the middle layer filter. The link filter down indicates the number of link transitions from up to down at the middle layer filter.

Example

The following command displays port system-related information:

```
show ports info
```

Following is sample output from this command:

```
Port         Diag  Flags    Link       Link Num Num  Num   Jumbo QOS     Load
                            State      UPs  STP VLAN Proto Size  Profile Mast
 2:1           P e--m-------D ready      0    0   0    0     9216
 2:2           P e--m-------D ready      0    0   0    0     9216
 2:3           P e--m-------D ready      0    0   0    0     9216
 2:4           P e--m-------D ready      0    0   0    0     9216
 2:5           P e--m-------E ready      0    1   1    1     9216
 2:6           P e--m-------E ready      0    1   1    1     9216
iL2_7          P e--m-------D ready      0    0   0    0     9216
iL2_8          P e--m-------D ready      0    0   0    0     9216
iL2_9          P e--m-------D ready      0    0   0    0     9216
iL2_10         P e--m-------D ready      0    0   0    0     9216
iL2_11         P e--m-------D ready      0    0   0    0     9216
iL2_12         P e--m-------D ready      0    0   0    0     9216
iL2_13         P e--m-------D ready      0    0   0    0     9216
iL2_14         P e--m-------D ready      0    0   0    0     9216
 3:1           P e--m-------E ready      0    1   1    1     9216
 3:2           P e--m-------E ready      0    1   1    1     9216
 3:3           P e--m-------E ready      0    1   1    1     9216
 3:4           P e--m-------E ready      0    1   1    1     9216

Flags: (a) Load Sharing Algorithm address-based, (d) DLCS Enabled
       (D) Port Disabled, (dy) Dynamic Load Sharing
       (e) Extreme Discovery Protocol Enabled, (E) Port Enabled
       (f) Flooding Enabled, (g) Egress TOS Enabled, (G) SLB GoGo Mode
       (h) Hardware Redundant Phy, (j) Jumbo Frame Enabled
       (l) Load Sharing Enabled, (m) MAC Learning Enabled
       (n) Ingress TOS Enabled, (o) Dot1p Vlan Priority Replacement Enabled
```

```
       (p) Load Sharing Algorithm port-based, (P) Software Primary Port
       (q) Background QOS Monitoring Enabled
       (r) Load Sharing Algorithm round-robin, (R) Software Redundant Port

Diag: (P) Passed, (F) Failed

Port: (iL) Internal Loopback
```

The following command displays more specific information for slot 2, port 6 in a modular switch:

```
show ports 2:6 info detail
```

Following is sample output from this command:

```
Port 2:6:
        Type:           UTP
        Diagnostic:     passed
        Random Early Drop: Disabled
        Admin state:    Enabled, with auto-duplex auto-speed sensing
        Link state:     Ready
        Link counter:   Up 0 time(s), Down 0 times(s)
        VLAN cfg:
        Default [Internal Tag=0001,Mac-Limit:Cfg=No-limit,LRN=0,BlkHole=0]

        STP cfg:
                s0(disable), Tag=(none), Mode=802.1D, State=FORWARDING

        Trunking:       Load sharing is not enabled
        Protocol:       VLAN=Default  Vpri=0   Protocol=ANY [EtherType:ffff]
        EDP:            enabled
        DLCS:           disabled
        lbdetect:       disabled
        Learning:       enabled
        Flooding:       disabled
        Jumbo:          Disabled
        BG QoS monitor: disabled
        Ingress Rate Shaping:
        QoS profile:    None configured
        Queue:  Q0 using QP1  MinBw=0%  MaxBw=100%  Pri=0.
                Q1 using QP2  MinBw=0%  MaxBw=100%  Pri=1.
                Q2 using QP3  MinBw=0%  MaxBw=100%  Pri=2.
                Q3 using QP4  MinBw=0%  MaxBw=100%  Pri=3.
                Q4 using QP5  MinBw=0%  MaxBw=100%  Pri=4.
                Q5 using QP6  MinBw=0%  MaxBw=100%  Pri=5.
                Q6 using QP7  MinBw=0%  MaxBw=100%  Pri=6.
                Q7 using QP8  MinBw=0%  MaxBw=100%  Pri=7.
        Ingress IPTOS:  Examination is disabled
                IPTOS->QOSProfile mapping:
                00->QP1 01->QP1 02->QP1 03->QP1 04->QP1 05->QP1 06->QP1 07->QP1
                08->QP2 09->QP2 10->QP2 11->QP2 12->QP2 13->QP2 14->QP2 15->QP2
                16->QP3 17->QP3 18->QP3 19->QP3 20->QP3 21->QP3 22->QP3 23->QP3
                24->QP4 25->QP4 26->QP4 27->QP4 28->QP4 29->QP4 30->QP4 31->QP4
                32->QP5 33->QP5 34->QP5 35->QP5 36->QP5 37->QP5 38->QP5 39->QP5
                40->QP6 41->QP6 42->QP6 43->QP6 44->QP6 45->QP6 46->QP6 47->QP6
                48->QP7 49->QP7 50->QP7 51->QP7 52->QP7 53->QP7 54->QP7 55->QP7
                56->QP8 57->QP8 58->QP8 59->QP8 60->QP8 61->QP8 62->QP8 63->QP8
        Egress IPTOS:   Replacement is disabled
```

```
        802.1p Pri->IPTOS mapping:
        0->00 1->08 2->16 3->24 4->32 5->40 6->48 7->56
802.1p: Disabled marking of priority field based on queue number
Smart Redundancy:       Enabled

VLANs monitored for stats:
Software redundant port:  disabled
jitter-tolerance:  enabled
link filtering:  isr filter = yes, middle layer filter = no
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.0 to support the `detail` keyword.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 6.2.2 to indicate disabled or enabled status.

This command was modified in Extreme Ware 7.0.1 to support the "3" series modules.

Platform Availability

This command is available on all platforms.

show ports packet

```
show ports {mgmt | <portlist>} packet
```

Description

Displays a histogram of packet statistics.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, a histogram is displayed for all ports.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

This status information may be useful for your technical support representative if you have a network problem.

The following packet statistics are displayed:

- port number
- link status
- packet size

Example

The following command displays packet statistics for ports 1 through 3 on a stand-alone switch:

```
show ports 1-3 packet
```

The following command displays packet statistics for slot 1, ports 1 through 8, slot 2, ports 1 through 8, and slot 3, port 1 on a modular switch:

```
show ports 1:1-1:8, 2:1-2:8, 3:1 packet
```

Following is the output from this command:

```
Receive Packet Statistics                              Thu Oct 24 16:25:30 2002
Port        Link                    Packet Sizes
            Status    0-64   65-127  128-255  256-511 512-1023 1024-1518   Jumbo
================================================================================
 1:1          R        0         0        0        0        0         0        0
```

```
1:2          R        0          0          0          0          0          0          0
1:3          R        0          0          0          0          0          0          0
1:4          R        0          0          0          0          0          0          0
1:5          R        0          0          0          0          0          0          0
1:6          R        0          0          0          0          0          0          0
1:7          R        0          0          0          0          0          0          0
1:8          R        0          0          0          0          0          0          0
2:1          R        0          0          0          0          0          0          0
2:2          R        0          0          0          0          0          0          0
2:3          R        0          0          0          0          0          0          0
2:4          R        0          0          0          0          0          0          0
2:5          R        0          0          0          0          0          0          0
2:6          R        0          0          0          0          0          0          0
2:7          R        0          0          0          0          0          0          0
2:8          R        0          0          0          0          0          0          0
3:1          R        0          0          0          0          0          0          0
================================================================================
    Link Status: A-Active R-Ready D-Disabled NP-Not Present LB-Loopback
          0->Clear Counters  U->page up  D->page down ESC->exit
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show ports sharing

```
show ports {mgmt | <portlist>} sharing
```

Description

Displays port loadsharing groups.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A

Usage Guidelines

None.

Example

The following command displays the port loadsharing group configured for port 5:4; the current master has shifted to port 7:4 since both ports 5:4 and 5:5 of the group are not active links:

```
show ports 5:4 sharing
```

The following is the output from this command:

```
* admin:3 # sh port 5:4 sharing
Load Sharing Monitor
Config    Current    Ld Share    Ld Share   Link     Link
Master    Master     Type        Group      Status   Ups
=========================================================
5:4       7:4        r           5:4        NP       1
                     r           5:5        NP       1
                     r           7:4        A        2
                     r           7:5        A        1

Link Status: (A) Active, (D) Disabled, (ND) Not Distributing
             (NP) Not Present, (R) Ready

Ld Share Type: (a) address based, (p) port based, (r) round robin
               (dy) dynamic
```

History

This command was first available in ExtremeWare 6.2.2.

This command was modified in ExtremeWare 7.0.0 to support the `dynamic` algorithm.

Platform Availability

This command is available on all platforms.

show ports utilization

```
show ports {mgmt | <portlist>} utilization
```

Description

Displays real-time port utilization information.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

Use the [Spacebar] to toggle between packet, byte, and bandwidth utilization information.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

If you do not specify a port number or range of ports, port utilization information is displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

Example

The following command displays utilization statistics for port 1 on a stand-alone switch:

```
show ports 1 utilization
```

The following command displays utilization statistics for slot 3, port 1 on a modular switch:

```
show ports 3:1 utilization
```

The following examples show the output from the show ports utilization command for all ports on the switch. The three displays show the information presented when you use the spacebar to toggle through the display types. The first display shows utilization in terms of packets:

```
Link Utilization Averages                          Wed Jan 23 21:29:45 2002
Port         Link    Receive       Peak Rx       Transmit       Peak Transmit
             Status  packet/sec    pkt/sec       pkt/sec        pkt/sec
================================================================================
   1           A       43          255             4             14
   2           R        0            0             0              0
   3           R        0            0             0              0
   4           R        0            0             0              0
   5           R        0            0             0              0
   6           R        0            0             0              0
   7           R        0            0             0              0
   8           R        0            0             0              0

================================================================================
           Link Status: A-Active R-Ready D-Disabled NP-Not Present
        spacebar->toggle screen U->page up  D->page down ESC->exit
```

The second display shows utilization in terms of bytes:

```
Link Utilization Averages                          Wed Jan 23 21:30:03 2002
Port    Link    Receive      Peak Rx       Transmit       Peak Transmit
        Status  bytes/sec     bytes/sec     bytes/sec      bytes/sec
================================================================================
   1      A      1102       69555            536           2671
   2      R         0           0              0              0
   3      R         0           0              0              0
   4      R         0           0              0              0
   5      R         0           0              0              0
   6      R         0           0              0              0
   7      R         0           0              0              0
   8      R         0           0              0              0

================================================================================
           Link Status: A-Active R-Ready D-Disabled NP-Not Present
```

The third display shows bandwidth utilization:

```
Link Utilization Averages                          Wed Jan 23 21:30:19 2002
Port     Link     Link   Receive       Peak Rx      Transmit     Peak Transmit
         Status   Speed  % bandwidth   % bandwidth  % bandwidth  % bandwidth
================================================================================
   1      A       100    0.00          0.60         0.00         0.02
   2      R              0.00          0.00         0.00         0.00
   3      R              0.00          0.00         0.00         0.00
   4      R              0.00          0.00         0.00         0.00
   5      R              0.00          0.00         0.00         0.00
   6      R              0.00          0.00         0.00         0.00
   7      R              0.00          0.00         0.00         0.00
   8      R              0.00          0.00         0.00         0.00


================================================================================
           Link Status: A-Active R-Ready D-Disabled NP-Not Present
        spacebar->toggle screen U->page up  D->page down ESC->exit
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show sharing address-based

```
show sharing address-based
```

Description

Displays the address-based load sharing configuration.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This feature is available using the address-based load-sharing algorithm only. The address-based load-sharing algorithm uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:

- IP packets—Uses the source and destination MAC and IP address, and the TCP port number.
- IPX packets—Uses the source and destination MAC address and IPX identifiers.
- All other packets—Uses the source and destination MAC address.

To verify your configuration, use the `show sharing address-based` command. The show sharing address-based output displays the addressed-based configurations on the switch.

Example

The following example displays the address-based load sharing configuration on the switch:

```
show sharing address-based
```

Following is the output from this command:

```
Sharing address-based = L2_L3_L4
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on the "*i*" series platform and the Alpine 3800 series switch modules.

show slot

```
show slot <slot number>
```

Description

Displays the slot-specific information.

For ARM, ATM, MPLS, PoS, and WAN modules, displays information that includes data about the software images loaded on the module, as well as status information on the module's processors.

Syntax Description

slot number	Specifies a slot on a modular switch.

Default

N/A.

Usage Guidelines

The `show slot` command displays the following information:

- The name of the module installed in the slot
- The serial number of the module
- The part number of the module
- The state of the module, whether the power is down, if the module is operational, if a diagnostic being run, if there is a mismatch between the slot configuration and the module in the slot
- The status of the ports on the module

If you do not specify a slot number, information for all slots is displayed.

For ARM, ATM, MPLS, PoS and WAN (E1, T1, and T3) modules:

The ExtremeWare technology release that supports these modules includes multiple software packages. One software package runs on the MSM or SMMi module while another package runs on each ARM, ATM, MPLS, PoS, or WAN module. You must download the software packages independently using the ExtremeWare `download image` command. Each software package has an associated version number that you can display using the `show version` command. It is recommended (not required), that the ExtremeWare software package and the ARM, ATM, MPLS, PoS, or WAN module software package be the same version.

For ARM, ATM, MPLS and PoS modules:

To ensure compatibility, the MSM performs an automatic compatibility check before a ARM, ATM, MPLS or PoS module is activated. If the versions of the software packages are incompatible, the ARM, ATM, MPLS or PoS ports on the module will not come up and the `show slot` command will indicate that the software on the ARM, ATM, MPLS or PoS module is incompatible with ExtremeWare.

Assuming the ARM, ATM, MPLS or PoS module has no problems, the command `show slot <slot>` (where "*<slot>*" is the number of the slot where you installed the module) displays that ExtremeWare has detected the module and set it to the OPERATIONAL state.

As the module progresses through its initialization, the `show slot <slot>` command displays the general purpose processor (GPP) subsystem change state to OPERATIONAL, and then each of the network processors will change state to OPERATIONAL.

When the GPP subsystem completes its initialization cycle and the subsystem state is OPERATIONAL, use the `show diagnostics {<slot>}` *command to check the results of the module power-on self test (POST).*

If the STATUS LED on the ARM, ATM, MPLS or PoS module turns amber and blinks, use the `show slot <slot>` command to display the slot status information. The `show slot <slot>` command also displays operational information related to the ARM, ATM, MPLS or PoS module. Information displayed includes the BlackDiamond switch fabric card state, Network Processor status, General Purpose Processor status, hardware serial number and type, and image version and boot settings.

For the ARM, ATM, MPLS, PoS, and WAN modules, the information displayed by this command includes data about the software images loaded on the module and information about the operational status and backplane connections of the module.

Example

The following example displays module information for all slots:

```
show slot
```

Following is the output from this command:

```
Slot 1 information:
    State:              Operational
    Serial number:      701028-06-0026F38445
    HW Module Type:     G8Ti

    Configured Type:    Not configured
    UTP ports available:
        Link Active:
        Link Down:      01 02 03 04 05 06 07 08


Slot 2 information:
    State:              Operational
    Serial number:      701024-19-0125F06190
    HW Module Type:     G8Xi

    Configured Type:    Not configured
    Gigabit ports available:
        Link Active:
        Link Down:      01
        GBIC missing:   02 03 04 05 06 07 08


Slot 3 information:
    State:              Operational
    Serial number:      701020-11-0032F51006
    HW Module Type:     G12SXi

    Configured Type:    Not configured
    Gigabit ports available:
```

```
        Link Active:
        Link Down:      01 02 03 04 05 06 07 08
                        09 10 11 12


Slot 4 information:
    State:              Operational
        Network Processor 1 : Operational
        Network Processor 2 : Operational
        General Purpose Proc: Operational
    Serial number:      701039-04-0128F07843
    HW Module Type:     P12ci
        Optics: Single-mode Fiber
        NP 1:   Rev C0
        NP 2:   Rev C0

    Configured Type:    Not configured
    Bootrom Version: 1.18
    Software image booted:   secondary
    Software image configured:   secondary
    Primary software version:
        7.0.0 (Build 44) (oc12) by Beta_Master on Sat 10/12/2002 06:16p

    Secondary software version:
        7.0.0 (Build 44) (oc12) by Beta_Master on Sat 10/12/2002 06:16p

    POS ports available:
        Link Up:
        Link Down:      01 02


Slot 5 information:
    State:              Operational
    Serial number:      701026-10-0142F70250
    HW Module Type:     F48Ti

    Configured Type:    Not configured
    UTP ports available:
        Link Active:
        Link Down:      01 02 03 04 05 06 07 08
                        09 10 11 12 13 14 15 16
                        17 18 19 20 21 22 23 24
                        25 26 27 28 29 30 31 32
                        33 34 35 36 37 38 39 40
                        41 42 43 44 45 46 47 48


Slot 6 information:
    State:              Empty
    HW Module Type:     Empty
    Configured Type:    Not configured


Slot 7 information:
    State:              Empty
    HW Module Type:     Empty
```

```
    Configured Type:    Not configured


Slot 8 information:
    State:              Empty
    HW Module Type:     Empty
    Configured Type:    Not configured
```

History

This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 7.0.0 to support WAN modules.

Platform Availability

This command is available on modular switches only.

unconfigure ports display string

```
unconfigure ports <portlist> display-string
```

Description

Clears the user-defined display string from one or more ports.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

This command removes the display string that you configured using the `configure ports display-string` command.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command clears the user-defined display from port 4 on a stand-alone switch:

```
unconfigure ports 4 display-string
```

The following command clears the user-defined display string from slot 2, port 4 on a modular switch:

```
unconfigure ports 2:4 display-string
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

unconfigure ports redundant

```
unconfigure ports [<portlist> | <port id> | mgmt] redundant
```

Description

Clears a previously configured software-controlled redundant port.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
portid	Specifies a port using the display string configured for the port. Only one port can be specified using this method.
mgmt	Specifies the management port. Supported only for switches that provide a management port.

Default

N/A.

Usage Guidelines

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

The `<port id>` is the display string configured for the port. Use the `configure ports <portnumber> display-string <string>` command to configure a display string for the port.

The list of port numbers or the port display string specifies the redundant port(s).

Example

The following command unconfigures a software-controlled redundant port on a stand-alone switch:

```
unconfigure ports 4 redundant
```

The following command unconfigures a software-controlled redundant port on a modular switch:

```
unconfigure ports 2:3 redundant
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

unconfigure slot

```
unconfigure slot <slot number>
```

Description

Clears a slot of a previously assigned module type.

Syntax Description

slot number	Specifies a slot on a modular switch.

Default

N/A.

Usage Guidelines

None.

Example

The following command clears slot 4 of a previously assigned module type:

```
unconfigure slots 4
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on modular switches only.

5 VLAN Commands

This chapter describes the following commands:

- Commands for creating and deleting VLANs and performing basic VLAN configuration
- Commands for defining protocol filters for use with VLANs
- Commands for enabling or disabling the use of Generic VLAN Registration Protocol (GVRP) information on a switch and its ports

VLANs can be created according to the following criteria:

- **Physical port**—A port-based VLAN consists of a group of one or more ports on the switch. A port can be a member of only one port-based VLAN, and is by default a member of the VLAN named "Default."
- **802.1Q tag**—Tagging is most commonly used to create VLANs that span switches.
- **Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol type**—Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols.
- A combination of these criteria.

The Generic VLAN Registration Protocol (GVRP) allows switches to learn some VLAN information automatically instead of requiring manual configuration in each switch. A VLAN can provide GVRP information about its VLANs and accept information about VLANs from other GVRP-enabled switches. Depending on the circumstances, information learned in this manner may cause ports to be added to VLANs already existing on the switch, or may cause new tagged VLANs to be created automatically.

NOTE

GVRP is not supported in ExtremeWare versions 6.1 or later.

configure dot1q ethertype

```
configure dot1q ethertype <ethertype>
```

Description

Configures an IEEE 802.1Q Ethertype.

Syntax Description

ethertype	Specifies an Ethertype value.

Default

Ethertype value of 8100.

Usage Guidelines

Use this command if you need to communicate with a switch that supports 802.1Q, but uses an Ethertype value other than 8100. This feature is useful for VMAN tunneling. Extreme Networks recommends the use of IEEE registered ethertype 0x88a8 for deploying vMANs.

Extreme switches assume an Ethertype value of 8100.

You must reboot the switch for this command to take effect.

Example

The following command, followed by a switch reboot, changes the Ethertype value to 9100:

```
configure dot1q ethertype 88a8
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure gvrp

```
configure gvrp {listen | send | both | none} port <portlist>
```

Description

Configures the sending and receiving of Generic VLAN Registration Protocol (GVRP) information on a port.

Syntax Description

listen	Enables the receipt of GVRP packets on the specified port(s).
send	Enables sending of GVRP packets on the specified port(s).
both	Enables both sending and receiving of GVRP packets.
none	Disables the port from participating in GVRP operation.
portlist	Specifies one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

Both sending and receiving.

Usage Guidelines

GVRP must be enabled on the switch as a whole before GVRP data can be sent or received on individual ports.

If GVRP is enabled, `send` causes information (GVRP packets) about tagged VLANS on the switch to be sent on the specified ports, to neighboring GVRP-enabled switches.

If GVRP is enabled, `listen` means that the switch will receive and act on GVRP information it receives on the specified ports, from neighboring GVRP-enabled switches.

Example

The following commands configure port 3 to receive GVRP information only (by default it can send and listen) and then enables GVRP:

```
configure gvrp listen port 3
enable gvrp
```

If the switch receives GVRP information on this port, it will do one of the following:

- If a tagged VLAN already exists with a VLANid that matches the VLANid in the GVRP data, and port 3 is not already a member of that VLAN, add it as a tagged port.
- If no VLAN exists with a VLANid that matches the VLANid in the GVRP data, create a VLAN with the VLANid specified in the GVRP data, and add port 3 as a tagged member port.

History

This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 and later.

Platform Availability

This command is available on all platforms.

configure mac-vlan add mac-address

```
configure mac-vlan add mac-address [any | <mac_address>] mac-group [any |
<group_number>] vlan <vlan name>
```

Description

Adds a MAC address as a potential member of a MAC-based VLAN.

Syntax Description

mac_address	The MAC address to be added to the specified VLAN. Specified in the form nn:nn:nn:nn:nn:nn.
	any indicates that any MAC-address associated with the specified MAC group may be a member.
group_number	The group number that should be associated with the specified MAC address. Specified as an integer
	any indicates that this MAC address can be associated with any MAC group.
vlan name	The name of the VLAN with which this MAC address should associated.

Default

N/A.

Usage Guidelines

The specified MAC address must be associated with an end station/host only, not a layer-2 repeater device.

Adding a MAC address means that when the specified address is detected on a member port, as specified by its group membership, it can participate in the VLAN.

At least one port must be enabled to use the MAC-based VLAN algorithm before any MAC addresses can be added.

Example

Given ports enabled for MAC-based VLANs as follows:

```
enable mac-vlan mac-group any ports 16,17
enable mac-vlan mac-group 10 ports 11,12
```

The following command sets up the end-station with MAC address 00:00:00:00:00:01 to participate in VLAN engineering via the MAC-enabled ports 16 or 17:

```
configure mac-vlan add mac-address 00:00:00:00:00:01 mac-group any vlan engineering
```

MAC address 00:00:00:00:00:01 cannot get access via ports 11 or 12 because it is not configured for mac-group 10.

The following command sets up the endstation 00:00:00:00:00:02 to participate in VLAN engineering through the ports in group 10 (ports 11 or 12) or through ports 16 or 17 (enabled for any mac-group):

```
configure mac-vlan add mac-address 00:00:00:00:00:02 mac-group 10 vlan engineering
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure mac-vlan delete

```
configure mac-vlan delete [all | mac-address [<mac_address> | any]]
```

Description

Removes a MAC address from any MAC-based VLANs with which it was associated.

Syntax Description

all	Indicates that all MAC addresses should be removed from all VLANs.
mac_address	The MAC address to be removed. Specified in the form nn:nn:nn:nn:nn:nn. any indicates that all MAC-addresses should be removed from all VLANs.

Default

NA.

Usage Guidelines

None.

Example

The following command removes the endstation with MAC address 00:00:00:00:00:02 from participating in any MAC-based VLANs.

```
configure mac-vlan delete mac-address 00:00:00:00:00:02
```

The following commands remove the all MAC addresses from participating in any VLANs:

```
configure mac-vlan delete all
configure mac-vlan delete mac-address any
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure ports monitor vlan

```
configure ports <portlist> monitor vlan <vlan name>
```

Description

Configures VLAN statistic monitoring on a per-port basis.

Syntax Description

portlist	Specifies one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command configures per port monitoring for a set of ports on slot 8 for the VLAN named *accounting*:

```
configure ports 8:1-8:6 monitor vlan accounting
```

You can monitor up to four VLANs on the same port by issuing the command four times. For example, if you want to monitor VLANs dog1, dog2, dog3, and dog4 on slot 1, use the following commands:

```
configure ports 1:* monitor vlan dog1
configure ports 1:* monitor vlan dog2
configure ports 1:* monitor vlan dog3
configure ports 1:* monitor vlan dog4
```

After you have configured the ports for monitoring, you can use the show ports vlan statistics command to display information for the configured ports:

```
show ports 1:* vlan statistics
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure protocol add

```
configure protocol <protocol_name> add <protocol_type> <hex_value>
{<protocol_type> <hex_value>} ...
```

Description

Configures a user-defined protocol filter.

Syntax Description

protocol_name	Specifies a protocol filter name.
protocol_type	Specifies a protocol type. Supported protocol types include: • `etype` – IEEE Ethertype. • `llc` – LLC Service Advertising Protocol. • `snap` – Ethertype inside an IEEE SNAP packet encapsulation.
hex_value	Specifies a four-digit hexadecimal number between 0 and FFFF that represents: • The Ethernet protocol type taken from a list maintained by the IEEE. • The DSAP/SSAP combination created by concatenating a two-digit LLC Destination SAP (DSAP) and a two-digit LLC Source SAP (SSAP). • The SNAP-encoded Ethernet protocol type.

Default

N / A.

Usage Guidelines

A maximum of 15 protocol filters, each containing a maximum of six protocols, can be defined.

The protocol filter must already exist before you can use this command: use the `create protocol` command to create the protocol filter.

On the "*i*" series platform, all fifteen protocol filters can be active and configured for use. On all other platforms, no more than seven protocols can be active and configured for use.

Example

The following command configures a protocol named Fred by adding protocol type LLC SAP with a value of FFEF:

```
configure protocol fred add llc feff
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure protocol delete

```
configure protocol <protocol_name> delete <protocol_type> <hex_value>
{<protocol_type> <hex_value>} ...
```

Description

Deletes the specified protocol type from a protocol filter.

Syntax Description

protocol_name	Specifies a protocol filter name.
protocol_type	Specifies a protocol type. Supported protocol types include: • `etype` – IEEE Ethertype. • `llc` – LLC Service Advertising Protocol. • `snap` – Ethertype inside an IEEE SNAP packet encapsulation.
hex_value	Specifies a four-digit hexadecimal number between 0 and FFFF that represents: • The Ethernet protocol type taken from a list maintained by the IEEE. • The DSAP/SSAP combination created by concatenating a two-digit LLC Destination SAP (DSAP) and a two-digit LLC Source SAP (SSAP). • The SNAP-encoded Ethernet protocol type.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes protocol type LLC SAP with a value of FFEF from protocol *Fred*:

```
configure protocol fred delete llc feff
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure vlan add member-vlan

```
configure vlan <translation vlan name> add member-vlan <vlan name>
```

Description

Adds a member VLAN to a translation VLAN.

Syntax Description

translation vlan name	Specifies a translation VLAN.
vlan name	Specifies a VLAN to add to the translation VLAN.

Default

N/A.

Usage Guidelines

This command adds a member VLAN to a translation VLAN. The 802.1Q tags for member VLANs are translated to the single tag of the translation VLAN, so the layer 2 traffic from the member VLANs is carried by a single VLAN, improving VLAN scaling.

Traffic is switched locally between client devices on the same member VLANs as on normal VLANs. Traffic cannot be switched between clients on separate member VLANs. Traffic cannot be switched between clients on separate member VLANs. Traffic from any member VLAN destined to the translation VLAN is switched and the VLAN tag is translated appropriately. Traffic from the translation VLAN destined to any member VLAN is switched and the VLAN tag is translated.

The added VLAN cannot have an IP address configured, already be a member or a translation VLAN, and must contain only "*i*"-series module Ethernet ports. Additionally, ESRP, EAPS, Network Login, or DHCP cannot be enabled on any ports belonging to either of these VLANs.

Example

The following command adds the member VLAN named *v101* to the translation VLAN named *v1000*:

```
configure vlan v1000 add member-vlan v101
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan add ports

```
configure vlan <vlan name> add ports <portlist> {tagged | untagged}
{nobroadcast} {soft-rate-limit}
```

Description

Adds one or more ports in a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
tagged	Specifies the ports should be configured as tagged.
untagged	Specifies the ports should be configured as untagged.
nobroadcast	Prevents broadcasts, multicasts, and unknowns from being transmitted on these ports.
soft-rate-limit	Specifies that these ports should be added as rate-shaped ports. (ExtremeWare 6.0)

Default

Untagged.

Usage Guidelines

The VLAN must already exists before you can add (or delete) ports: use the `create vlan` command to create the VLAN.

If the VLAN uses 802.1Q tagging, you can specify tagged or untagged port(s). If the VLAN is untagged, the ports cannot be tagged.

Untagged ports can only be a member of a single VLAN. By default, they are members of the default VLAN (named *Default*). In order to add untagged ports to a different VLAN, you must first remove them from the default VLAN. You do not need to do this to add them to another VLAN as tagged ports.

You must configure a loopback port with a unique loopback VLAN tag ID before adding rate-shaped ports.

This command is not supported on SONET modules.

Example

The following command assigns tagged ports 1, 2, 3, and 6 to a VLAN named *accounting*:

```
configure vlan accounting add ports 1, 2, 3, 6 tagged
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure vlan add ports loopback-vid

```
configure vlan <vlan name> add ports <portlist> loopback-vid <vlan-id>
```

Description

Adds a loopback port to a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
port	Specifies a loopback port for the VLAN.
vlan-id	Specifies a unique loopback VLAN tag.

Default

Untagged.

Usage Guidelines

The VLAN must already exists before you can add (or delete) ports: use the `create vlan` command to create the VLAN.

You must configure a loopback port with a unique loopback VLAN tag ID before adding rate-shaped ports.

This command is not supported on SONET modules.

Example

The following example sets up bi-directional rate shaping using a loopback port and a rate-shaped port.

First, create the VLAN that will have rate-shaped ports as members:

```
create vlan ratelimit
```

Create the loopback port to rate-shape ingress traffic:

```
configure vlan ratelimit add ports 1 loopback-vid 100
```

Configure the user port that will be rate-shaped:

```
configure vlan ratelimit add ports 2 soft-rate-limit
```

Configure rate-shaping to be at 5% maximum bandwidth for ingress and egress traffic:

```
configure qosprofile QP1 minbw 0 % maxbw 5 % priority low 1,2
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan delete member-vlan

```
configure vlan <translation vlan name> delete member-vlan [<vlan name> |
all]
```

Description

Deletes a member VLAN from a translation VLAN.

Syntax Description

translation vlan name	Specifies a translation VLAN.
vlan name	Specifies a VLAN to add to the translation VLAN.

Default

N / A.

Usage Guidelines

This command deletes a member VLAN to a translation VLAN. Use the `all` keyword to delete all the member VLANs from the specified translation VLAN.

Example

The following command deletes the member VLAN named *v101* from the translation VLAN named *v1000*:

```
configure vlan v1000 delete member-vlan v101
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan delete port

```
configure vlan <vlan name> delete port <portlist>
```

Description

Deletes one or more ports in a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	A list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes ports 1, 2, 3, and 6 from a VLAN named *accounting*:

```
configure accounting delete port 1, 2, 3, 6
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure vlan ipaddress

```
configure vlan <vlan name> ipaddress <ipaddress> {<netmask> | <mask
length>}
```

Description

Assigns an IP address and an optional subnet mask to the VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
ipaddress	Specifies an IP address.
netmask	Specifies a subnet mask in dotted-quad notation (e.g. 255.255.255.0).
mask length	Specifies a subnet mask as the number of bits (e.g. /24).

Default

N/A.

Usage Guidelines

The VLAN must already exists before you can assign an IP address: use the `create vlan` command to create the VLAN.

NOTE

If you plan to use the VLAN as a control VLAN for an EAPS domain, do NOT configure the VLAN with an IP address.

Example

The following commands are equivalent; both assign an IP address of 10.12.123.1 to a VLAN named *accounting*:

```
configure vlan accounting ipaddress 10.12.123.1/24
configure vlan accounting ipaddress 10.12.123.1 255.255.255.0
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure vlan name

```
configure vlan <old_name> name <new_name>
```

Description

Renames a previously configured VLAN.

Syntax Description

old_name	Specifies the current (old) VLAN name.
new_name	Specifies a new name for the VLAN.

Default

N/A.

Usage Guidelines

You cannot change the name of the default VLAN “Default”

Example

The following command renames VLAN *vlan1* to *engineering*:

```
configure vlan vlan1 name engineering
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure vlan protocol

```
configure vlan <vlan name> protocol [<protocol_name> | any]
```

Description

Configures a VLAN to use a specific protocol filter.

Syntax Description

vlan name	Specifies a VLAN name.
protocol_name	Specifies a protocol filter name. This can be the name of a predefined protocol filter, or one you have defined. The following protocol filters are predefined: • IP • IPX • NetBIOS • DECNet • IPX_8022 • IPX_SNAP • AppleTalk any indicates that this VLAN should act as the default VLAN for its member ports.

Default

Protocol Any.

Usage Guidelines

If the keyword any is specified, all packets that cannot be classified into another protocol-based VLAN are assigned to this VLAN as the default for its member ports.

Use the `configure protocol` command to define your own protocol filter.

Example

The following command configures a VLAN named accounting as an IP protocol-based VLAN:

```
configure accounting protocol ip
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

configure vlan tag

```
configure vlan <vlan name> tag <vlan tag>
```

Description

Assigns a unique 802.1Q tag to the VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
vlan tag	Specifies a value to use as an 802.1Q tag. The valid range is from 2 to 4,095.

Default

The default VLAN uses an 802.1Q tag (and an internal VLANid) of 1.

Usage Guidelines

If any of the ports in the VLAN will use an 802.1Q tag, a tag must be assigned to the VLAN. The valid range is from 2 to 4,095 (tag 1 is assigned to the default VLAN).

The 802.1Q tag will also be used as the internal VLANid by the switch.

You can specify a value that is currently used as an internal VLANid on another VLAN; it will become the VLANid for the VLAN you specify, and a new VLANid will be automatically assigned to the other untagged VLAN.

Example

The following command assigns a tag (and internal VLANid) of 120 to a VLAN named *accounting*:

```
configure accounting tag 120
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

create protocol

```
create protocol <protocol_name>
```

Description

Creates a user-defined protocol filter.

Syntax Description

protocol_name	Specifies a protocol filter name. The protocol filter name can have a maximum of 31 characters.

Usage Guidelines

Protocol-based VLANs enable you to define packet filters that the switch can use as the matching criteria to determine if a particular packet belongs to a particular VLAN.

After you create the protocol, you must configure it using the `configure protocol` command. To assign it to a VLAN, use the `configure vlan <vlan name> protocol` command.

Example

The following command creates a protocol named *fred*:

```
create protocol fred
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

create vlan

```
create vlan <vlan name>
```

Description

Creates a named VLAN.

Syntax Description

vlan name	Specifies a VLAN name (up to 32 characters).

Default

A VLAN named *Default* exists on all new or initialized Extreme switches:

- It initially contains all ports on a new or initialized switch, except for the management port(s), if there are any.
- It has an 802.1Q tag of 1.
- The default VLAN is untagged on all ports.
- It uses protocol filter any.

An untagged VLAN named *MacVlanDiscover* exists on all new or initialized "*i*" series switches:

- It initially contains no ports.
- It does not initially use an 802.1Q tag, and is assigned the next available internal VLANid starting with 4095.

A VLAN named *Mgmt* exists on switches that have management modules or management ports.

- It initially contains the management port(s) the switch.
- It is assigned the next available internal VLANid as an 802.1Q tag.

Usage Guidelines

A newly-created VLAN has no member ports, is untagged, and uses protocol filter "any" until you configure it otherwise. Use the various `configure vlan` commands to configure the VLAN to your needs.

Internal VLANids are assigned automatically using the next available VLANid starting from the high end (4095) of the range.

By default the switch supports 1024 VLANs. The switch can support a maximum of 3000 VLANs if the `CPU-transmit-priority` is set to `normal`, rather than `high` (the default). Use the `configure cpu-transmit-priority` command to change the CPU transmit priority (v6.2 or later).

Each VLAN name can be up to 32 standard alphanumeric characters, but must begin with an alphabetical letter. Quotation marks can be used to enclose a VLAN name that does not begin with an alphabetical character, or that contains a space, comma, or other special character.

VLAN names are locally significant. That is, VLAN names used on one switch are only meaningful to that switch. If another switch is connected to it, the VLAN names have no significance to the other switch.

Example

The following command creates a VLAN named *accounting*:

```
create vlan accounting
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

delete protocol

```
delete protocol <protocol_name>
```

Description

Deletes a user-defined protocol.

Syntax Description

protocol_name	Specifies a protocol name.

Default

N/A.

Usage Guidelines

If you delete a protocol that is in use by a VLAN, the protocol associated with than VLAN will become "None."

Example

The following command deletes a protocol named *fred*:

```
delete protocol fred
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

delete vlan

```
delete vlan <vlan name>
```

Description

Deletes a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

If you delete a VLAN that has untagged port members, and you want those ports to be returned to the default VLAN, you must add them back explicitly using the `configure vlan add port` command.

NOTE

The default VLAN cannot be deleted.

Example

The following command deletes the VLAN *accounting*:

```
delete accounting
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

disable gvrp

```
disable gvrp
```

Description

Disables the Generic VLAN Registration Protocol (GVRP).

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command globally disables GVRP functionality on the switch. It does not change the GVRP configuration of individual ports, but GVRP will no longer function on these ports.

GVRP is not supported in ExtremeWare version 6.1 or later.

Example

The following command disables GVRP functionality:

```
disable gvrp
```

History

This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 or later.

Platform Availability

This command is available on all platforms.

disable mac-vlan port

```
disable mac-vlan port <portlist>
```

Description

Disables a port from using the MAC-based VLAN algorithm.

Syntax Description

portlist	A list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

Disabling a port removes it from the MacVlanDiscover VLAN. But does not automatically return it to the default VLAN. If you need this port to be a member of the default VLAN, you must explicitly add it back.

Example

The following command disables ports 16 and 17 from using the MAC-based VLAN algorithm:

```
disable mac-vlan port 16,17
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable gvrp

```
enable gvrp
```

Description

Enables the Generic VLAN Registration Protocol (GVRP).

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

The GVRP protocol allows switches to automatically discover some of the VLAN information that would otherwise have to be manually configured in each switch.

GVRP must be enabled on individual ports before GVRP information will be sent or received.

By default, GVRP is enabled for both sending and receiving on all ports, so executing this command will normally “turn on” GVRP functionality.

GVRP is not supported in ExtremeWare version 6.1 or later.

Example

The following command enables GVRP functionality:

```
enable gvrp
```

History

This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 or later.

Platform Availability

This command is available on all platforms.

enable mac-vlan mac-group port

```
enable mac-vlan mac-group [any | <group_number>] port <portlist>
```

Description

Enables a port to use the MAC-based VLAN algorithm.

Syntax Description

group_number	A group number that should be associated with a specific set of ports. Specified as an integer.
	any indicates that these ports can be considered members of any MAC group.
portlist	A list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

Enabling ports for MAC-based VLAN usage automatically adds them to the VLAN *MacVlanDiscover* as untagged ports.

In order to enable ports as part of a MAC group, they cannot be untagged members of any other VLAN. Before you can enable them, you must ensure that they have been removed from the default VLAN (named *Default*).

Example

The following set of commands removes ports 16 and 17 from the default VLAN, and then enables them for use with the MAC-based VLAN, associated with any MAC group:

```
configure default delete port 16, 17
enable mac-vlan mac-group any port 16,17
```

The following commands enable ports 11 and 12 for use with a MAC-based VLAN, associated with MAC group 10:

```
configure default delete port 11, 12
enable mac-vlan mac-group 10 port 11,12
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show gvrp

```
show gvrp
```

Description

Displays the current configuration and status of GVRP.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

GVRP is not supported in ExtremeWare version 6.1 or later.

Example

The following shows results of this command:

```
GVRP running (866422):   JoinTime 20  LeaveTime 200  LeaveAllTime 1000 cs
GVRP transmit 0  receive 0  tx errors 0  rx errors 0  int errors 0
Enabled for Tx/Rx on ports:     123456789
                10111213141516171819
                20212223242526272829
                303132
VLAN/Ports (t=static tagged, u=static untag, G=GVRP tagged, g=GVRP untag)
 Default (Tag 1)
uuuuuuuuuu..uuu..uuuuuuuuuuuuuuu
 Mgmt (Tag 4094)
.............................
 nat (Tag 4093)
.............................
```

History

This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 or later.

Platform Availability

This command is available on all platforms.

show mac-vlan

```
show mac-vlan {configuration | database}
```

Description

Displays the MAC-based VLAN configuration and MAC address database content.

Syntax Description

configuration	Specifies display of the MAC-based VLAN configuration only.
database	Specifies display of the MAC address database content only.

Default

Shows both configuration and database information.

Usage Guidelines

Use the keyword `configuration` to display only the top section of this information. Use the database keyword to display only the lower section.

Example

The following is an example of the `show mac-vlan` command:

```
Port    Vlan            Group   State
11      MacVlanDiscover 10      Discover
12      MacVlanDiscover 10      Discover
16      MacVlanDiscover any     Discover
17      MacVlanDiscover any     Discover

Total Entries in Database:2
Mac                     Vlan       Group
00:00:00:00:00:AA    anntest1     any
        any          anntest1     10
2 matching entries
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show protocol

```
show protocol {<protocol>}
```

Description

Displays protocol filter definitions.

Syntax Description

protocol	Specifies a protocol filter name.

Default

Displays all protocol filters.

Usage Guidelines

Displays the defined protocol filter(s) with the types and values of its component protocols.

Example

The following is an example of the `show protocol` command:

```
Protocol Name         Type  Value
----------------      ----- ------
IP                    etype 0x0800
                      etype 0x0806
ipx                   etype 0x8137
netbios                 llc 0xf0f0
                        llc 0xf0f1
decnet                etype 0x6003
                      etype 0x6004
appletalk              snap 0x809b
                       snap 0x80f3
ipx_8022                llc 0xe0e0
ipx_snap               snap 0x8137
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

show vlan

```
show vlan {<vlan name> | detail | stats {vlan} <vlan name>}
```

Description

Displays information about VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
detail	Specifies that detailed information should be displayed for each VLAN.
stats	Specifies a real-time display of utilization statistics (packets transmitted and received) for a specific VLAN.

Default

Summary information for all VLANs on the device.

Usage Guidelines

Unlike many other vlan-related commands, the keyword “vlan” is required in all forms of this command except when requesting information for a specific vlan.

Use the command `show vlan` to display summary information for all VLANs. It shows various configuration options as a series of “flags” (see the example below). VLAN and protocol names may be abbreviated in this display.

Use the command `show vlan detail` to display detailed information for all VLANs. This displays the same information as for an individual VLAN, but shows every VLAN, one-by-one. After each VLAN display you can elect to continue or quit.

Protocol None indicates that this VLAN was configured with a user-defined protocol that has subsequently been deleted.

Use the command `show vlan stats <vlan name>` to show real-time statistics on the number of packets transmitted and received for the named VLAN. This command will continue to run until you cancel it using the [Esc] key.

Example

The following is an example of the `show vlan` command:

```
MSM64:1 # show vlan
Name               VID  Protocol Addr        Flags        Proto   Ports
Default            1    0.0.0.0        /BP -----T-------- ANY     0/7
MacVlanDiscover    4095 ------------------- ------         ANY     0/0
Mgmt               4094 10.5.4.80      /24 -------------- ANY     1/1
pv1                4093 192.168.11.1   /24 ------f------- ANY     0/1
pv2                4092 192.168.12.1   /24 ------f------- ANY     0/1
pv3                4091 ------------------- ------         ANY     0/0
pv4                4090 ------------------- ------         ANY     0/0

Flags:  (C) Domain-masterVlan, (c) Domain-memberVlan, (d) DVMRP Enabled
        (E) ESRP Slave, (f) IP Forwarding Enabled, (G) GVRP Enabled
        (i) ISIS Enabled, (I) IP Forwarding lpm-routing Enabled
        (L) Loopback Enabled, (M) ESRP Master, (m) IPmc Forwarding Enabled
        (N) GNS Reply Enabled, (o) OSPF Enabled, (P) IPX SAP Enabled
        (p) PIM Enabled, (R) SubVLAN IP Range Configured, (r) RIP Enabled
        (S) SuperVlan, (s) SubVlan, (T) Member of STP Domain
        (v) VRRP Enabled, (X) IPX RIP Enabled
        (2) IPX Type 20 Forwarding Enabled

Total number of Vlan(s) : 7
```

The following is an example of the `show vlan Default` command:

```
VLAN Interface[0-200] with name "Default" created by user
     Tagging:   802.1Q Tag 1
     Priority:  802.1P Priority 7
     IP:        Waiting for bootp reply.
     STPD:      s0(Disabled,Auto-bind)
     Protocol:  Match all unfiltered protocols.
     Loopback:  Disable
     RateShape: Disable
     QosProfile:QP1
     QosIngress:None
     Ports:     72.     (Number of active ports=1)
        Flags:  (*) Active, (!) Disabled
                (B) BcastDisabled, (R) RateLimited, (L) Loopback
                (g) Load Share Group
        Untag:  *3:1     3:2     3:3     3:4     3:5     3:6     3:7     3:8
                 3:9     3:10    3:11    3:12    3:13    3:14    3:15    3:16
                 3:17    3:18    3:19    3:20    3:21    3:22    3:23    3:24
                 3:25    3:26    3:27    3:28    3:29    3:30    3:31    3:32
                 3:33    3:34    3:35    3:36    3:37    3:38    3:39    3:40
                 3:41    3:42    3:43    3:44    3:45    3:46    3:47    3:48
                 4:1     4:2     4:3     4:4     4:5     4:6     4:7     4:8
                 4:9     4:10    4:11    4:12    4:13    4:14    4:15    4:16
                 4:17    4:18    4:19    4:20    4:21    4:22    4:23    4:24
```

The following is an example of using the command to show a specific VLAN, *v2*, that contains a port for a load-sharing group that spans multiple modules:

```
VLAN Interface[3-201] with name "v2" created by user
      Tagging:    802.1Q Tag 2
      Priority:   802.1P Priority 7
```

```
IP:         10.222.0.2/255.255.255.0
STPD:       s0(Disabled,Auto-bind)
Protocol:   Match all unfiltered protocols.
Loopback:   Disable
RateShape:  Disable
QosProfile:QP1
QosIngress:IQP1
 Ports:      5.      (Number of active ports=4)
   Flags:   * - Active, ! - Disabled
             B - BcastDisabled, R - RateLimited, L - Loopback
            (g) Load Share Group, (c) Cross Module Trunk
   Untag:   *1:25     5:10     5:25     7:25
   Tagged:  *5:4c
```

History

This command was first available in ExtremeWare 1.0.

This command was modified to support longer VLAN names in ExtremeWare 6.2.2.

This command was modified to include the Member of STP Domain flag in ExtremeWare 7.0.

This command was modified to support the "3" series modules in ExtremeWare 7.0.1.

This command was modified to include the cross-module trunk flag in ExtremeWare 7.1.1

Platform Availability

This command is available on all platforms.

unconfigure ports monitor vlan

```
unconfigure ports <portlist> monitor vlan <vlan name>
```

Description

Removes port-based VLAN monitoring.

Syntax Description

portlist	Specifies one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes monitoring for ports on VLAN *accounting*:

```
unconfigure ports 8:1-8:6 monitor vlan accounting
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

unconfigure vlan ipaddress

```
unconfigure vlan <vlan name> ipaddress
```

Description

Removes the IP address of the VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
ipaddress	Specifies that the ipaddress association with this VLAN should be cleared.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes the IP address from the VLAN *accounting*:

```
unconfigure vlan accounting ipaddress
```

History

This command was first available in ExtremeWare 1.0.

Platform Availability

This command is available on all platforms.

6 FDB Commands

This chapter describes commands for:

- Configuring FDB entries
- Displaying FDB entries
- Configuring and enabling FDB scanning

The switch maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered.

Each FDB entry consists of the MAC address of the device, an identifier for the port on which it was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not in the FDB are flooded to all members of the VLAN.

The FDB has four types of entries:

- **Dynamic entries**—Initially, all entries in the database are dynamic. Entries in the database are removed (aged-out) if, after a period of time (aging time), the device has not transmitted. This prevents the database from becoming full of obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Dynamic entries are deleted from the database if the switch is reset or a power off/on cycle occurs.
- **Nonaging entries**—If the aging time is set to zero, all aging entries in the database are defined as static, nonaging entries. This means that they do not age, but they are still deleted if the switch is reset.
- **Permanent entries**—Permanent entries are retained in the database if the switch is reset or a power off/on cycle occurs. The system administrator must create permanent entries. A permanent entry can either be a unicast or multicast MAC address. All entries entered through the command line interface (CLI) are stored as permanent.
- **Blackhole entries**—A blackhole entry configures the switch to discard packets with a specified MAC destination address. Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged out of the database.

Entries are added into the FDB in the following two ways:

- The switch can learn entries. The system updates its FDB with the source MAC address from a packet, the VLAN, and the port identifier on which the source packet is received.
- You can enter and update entries using a MIB browser, an SNMP network manager, or the CLI.

A QoS profile can be associated with a MAC address (and VLAN) of a device that will be dynamically learned. The FDB treats the entry like a dynamic entry (it is learned, it can be aged out of the database, and so on). The switch applies the QoS profile as soon as the FDB entry is learned.

clear fdb

```
clear fdb {<mac_address> | blackhole | ports <portlist> | remap | vlan
<vlan name>}
```

Description

Clears dynamic FDB entries that match the filter.

Syntax Description

mac_address	Specifies a MAC address, using colon-separated bytes.
blackhole	Specifies the blackhole entries.
portlist	Specifies one or more ports. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
remap	Clears the remapped and questionable FDB entries.
vlan name	Specifies a VLAN name.

Default

Clears all dynamic FDB entries.

Usage Guidelines

This command clears FDB entries based on the specified criteria. When no options are specified, the command clears all dynamic FDB entries.

The system health checker also checks the integrity of the FDB. If you enable the system health checker, a section of the FDB memory on each module's switching fabric is non-intrusively compared to the software copy of the FDB. The switch takes one of the following actions if it detects a bad entry:

- If the entry is not in use—remaps around the entry location
- If the entry is in use, but is safely removable (most MAC and IP-DA entries)—removes the questionable entry, allows the table to be rebuilt naturally, and remaps around the entry location
- If the entry is in use and is *not* safely removable (MAC_NH, IPSA, IPMCDA, IPDP, IPSP, IPXSN)—sends a warning message to the log

If the switch detects more than eight questionable entries, it executes the configured failure action and stops remapping on the switch fabric. To see the questionable and remapped entries, use the `show fdb` command. The following information is displayed:

- Questionable entries are marked with a "Q" flag
- Remapped entries are marked with an "R" flag
- Total FDB count

You can also display FDB scan statistics using the following command:

```
show diagnostics sys-health-check
```

Example

The following command clears any FDB entries associated with ports 3-5:

```
clear fdb ports 3-5
```

The following command clears any FDB entries associated with VLAN *corporate*:

```
clear fdb vlan corporate
```

The following command clears all questionable and remapped entries from the FDB:

```
clear fdb remap
```

History

This command was available in ExtremeWare 2.0.

The command was modified in ExtremeWare 6.2.1 to support the broadcast-mac keyword and to support clearing locked-static entries.

This command was modified in ExtremeWare 6.2.2b108 to support the `remap` keyword, and questionable entries (known as suspect entries) are marked with an “S” flag.

The `remap` keyword was not supported in ExtremeWare 7.0.

The `remap` keyword is supported in ExtremeWare 7.1.0, and questionable entries are marked with a “Q” flag.

Platform Availability

This command is available on all platforms.

configure fdb agingtime

```
configure fdb agingtime <seconds>
```

Description

Configures the FDB aging time for dynamic entries.

Syntax Description

seconds	Specifies the aging time in seconds. Range is 15 through 1,000,000. A value of 0 indicates that the entry should never be aged out.

Default

300 seconds.

Usage Guidelines

The range is 15 through 1,000,000 seconds.

If the aging time is set to zero, all aging entries in the database are defined as static, nonaging entries. This means that they do not age out, but non-permanent static entries can be deleted if the switch is reset.

Example

The following command sets the FDB aging time to 3,000 seconds:

```
configure fdb agingtime 3000
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure fdb-scan failure-action

```
configure fdb-scan failure-action [log | sys-health-check]
```

Description

Configures the action the switch takes if too many failures are detected within the specified FDB scan period.

Syntax Description

log	Specifies that messages are sent to the syslog.
sys-health-check	Specifies the configured system health check action is taken.

Default

log.

Usage Guidelines

If you use the default `log`, only one instance of an error message is logged at this level.

If you select `sys-health-check`, and the switch detects too many failures, the switch takes the configured system health check action. To configure the system health check, use the `configure sys-health-check [alarm-level [card-down | default | log | system-down | traps] | auto-recovery <number of tries>]` command.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the `show switch` command. The following is sample FDB scanning output:

```
Fdb-Scan Diag:    Enabled.    Failure action:  log only
```

For ExtremeWare 6.2.2b108:

The default is `sys-health-check`, and the switch takes the configured system health check action.

Example

The following command configures the switch to perform the configured system health check action if too many failures are detected:

```
configure fdb-scan failure-action sys-health-check
```

History

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to `log` in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure fdb-scan period

```
configure fdb-scan period <period <1-60>>
```

Description

Configures the amount of time between FDB scans.

Syntax Description

period <1-60>	Specifies the timer interval, in seconds, between FDB scans. The range is 1 to 60 seconds.

Default

30 seconds.

Usage Guidelines

If you configure a timer interval of less than 15 seconds, the following warning message is displayed and you are asked to confirm the change:

```
Setting period below (15) may starve other tasks.
Do you wish to do this? (yes, no, cancel) 06/19/2003 10:29.28 <INFO:SYST> serial
admin: configure fdb-scan period 1
n
```

Extreme Networks recommends an interval period of at least 15 seconds.

This setting is independent of and does not affect the system health check configurations.

Example

The following command configures a timer interval of 20 seconds between FDB scans:

```
configure fdb-scan period 20
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

create fdbentry vlan blackhole

```
create fdbentry <mac_address> vlan <vlan name> blackhole {source-mac |
dest-mac | both}
```

Description

Creates a blackhole FDB entry.

Syntax Description

mac_address	Specifies a device MAC address, using colon-separated bytes.
vlan name	Specifies a VLAN name associated with a MAC address.
blackhole	Configures the MAC address as a blackhole entry.
source-mac	Specifies that the blackhole MAC address matches the ingress source MAC address. Support for this parameter was added in ExtremeWare 6.2.
dest-mac	Specifies that the blackhole MAC address matches the egress destination MAC address. Support for this parameter was added in ExtremeWare 6.2.
both	Specifies that the blackhole MAC address matches the ingress source MAC address or the egress destination MAC address. Support for this parameter was added in ExtremeWare 6.2.

Default

N/A.

Usage Guidelines

Blackhole entries are useful as a security measure or in special circumstances where packets with a specific source or destination address must be discarded.

A blackhole entry configures the switch to discard packets with the specified MAC address. You can specify whether the MAC address should match the source (ingress) MAC address, or the destination (egress) MAC address, or both.

Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged-out of the database. In the output from a `show fdb` command, entries will have “p” flag (permanent) set, as well as the “b” (for ingress blackhole) and/or “B” (for egress blackhole) flags set.

Example

The following example adds a blackhole entry to the FDB for MAC address is 00 E0 2B 12 34 56, in VLAN *marketing* on port 4:

```
create fdbentry 00:E0:2B:12:34:56 vlan marketing both
```

History

This command was available in ExtremeWare 2.0.

Support for specifying source or destination MAC address was added in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

create fdbentry vlan dynamic

```
create fdbentry [<mac_address> | broadcast-mac | any-mac] vlan <vlan name>
dynamic [qosprofile <qosprofile> {ingress-qosprofile <inqosprofile>} |
ingress-qosprofile <inqosprofile> {qosprofile <qosprofile>}]
```

Description

Creates a permanent dynamic FDB entry, and associates it with an ingress and/or egress QoS profile.

Syntax Description

mac_address	Specifies a device MAC address, using colon separated bytes.
broadcast-mac	Specifies the broadcast MAC address. May be used as an alternate to the colon-separated byte form of the address ff:ff:ff:ff:ff:ff.
any-mac	Specifies the wildcard, permanent FDB entry used to give higher priority to an 802.1p packet.
vlan name	Specifies a VLAN name associated with a MAC address.
dynamic	Specifies that the entry will be learned dynamically.
qosprofile	QoS profile associated with the destination MAC address of the egress port.
inqosprofile	QoS profile associated with the source MAC address of the ingress port. Support for this parameter was added in ExtremeWare 6.2.

Default

N/A.

Usage Guidelines

This command is used to associate QoS profiles with packets received from or destined for the specified MAC address, while still allowing the FDB entry to be dynamically learned. If you specify only the ingress QoS profile, the egress QoS profile defaults to none, and vice-versa. If both profiles are specified, the source MAC address of an ingress packet and the destination MAC address of an egress packet are examined for QoS profile assignment.

The FDB entry is not actually created until the MAC address is encountered as the source MAC address in a packet. Thus, initially the entry may not appear in the `show fdb` output. Once the entry has been learned, it is created as a permanent dynamic entry, designated by “dpm” in the flags field of the `show fdb` output.

A dynamic entry is flushed and relearned (updated) when any of the following take place:

- A VLAN is deleted.
- A VLAN identifier (VLANid) is changed.
- A port mode is changed (tagged/untagged).
- A port is deleted from a VLAN.
- A port is disabled.
- A port enters blocking state.
- A port QoS setting is changed.

- A port goes down (link down).

Using the `any-mac` keyword, you can enable traffic from a QoS VLAN to have higher priority than 802.1p traffic. Normally, an 802.1p packet has a higher priority over the VLAN classification. To use this feature, you must create a wildcard permanent FDB entry named `any-mac` and apply the QoS profile to the individual MAC entry.

You can use the `show fdb permanent` command to display permanent FDB entries, including their QoS profile associations.

Example

The following example associates the QoS profile qp2 with a dynamic entry for MAC address 00:A0:23:12:34:56 on VLAN net34 that will be learned by the FDB:

```
create fdbentry 00:A0:23:12:34:56 vlan net34 dynamic qosprofile qp2
```

QoS profile *qp2* will be applied when the entry is learned.

The following example associates the QoS profile qp5 with the wildcard permanent FDB entry any-mac on VLAN v110:

```
create fdbentry any-mac vlan v110 dynamic ingress-qosprofile qp5
```

History

This command was available in ExtremeWare 2.0.

Support for associating separate QoS profiles with ingress and egress ports was added in ExtremeWare 6.2.

This command was modified in ExtremeWare 6.2.1 to support the `broadcast-mac` option.

Platform Availability

This command is available on all platforms.

create fdbentry vlan ports

```
create fdbentry <mac_address> vlan <vlan name> ports [<portlist> | all]
{qosprofile <qosprofile>} {ingress-qosprofile <inqosprofile>}
```

Description

Creates a permanent static FDB entry, and optionally associates it with an ingress and/or egress QoS profile.

Syntax Description

mac_address	Specifies a device MAC address, using colon-separated bytes.
vlan name	Specifies a VLAN name associated with a MAC address.
portlist	Specifies one or more ports associated with the MAC address. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
qosprofile	QoS profile associated with the destination MAC address of the egress port
inqosprofile	QoS profile associated with the source MAC address of the ingress port. Support for this parameter was added in ExtremeWare 6.2.

Default

N/A.

Usage Guidelines

If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.

Permanent entries are retained in the database if the switch is reset or a power off/on cycle occurs. A permanent static entry can either be a unicast or multicast MAC address. The stand-alone switches can support a maximum of 64 permanent entries, and the modular switches support a maximum of 254 permanent entries.

After they have been created, permanent static entries stay the same as when they were created. If the same MAC address is encountered on another virtual port that is not included in the permanent MAC entry, it is handled as a blackhole entry. The static entry is not updated when any of the following take place:

- A VLAN is deleted.
- A VLAN identifier (VLANid) is changed.
- A port mode is changed (tagged/untagged).
- A port is deleted from a VLAN.
- A port is disabled.
- A port enters blocking state.
- A port QoS setting is changed.
- A port goes down (link down).

Permanent static entries are designated by "spm" in the flags field of the `show fdb` output. You can use the `show fdb permanent` command to display permanent FDB entries, including their QoS profile associations.

Example

The following example adds a permanent, static entry to the FDB for MAC address is 00 E0 2B 12 34 56, in VLAN *marketing* on port 4:

```
create fdbentry 00:E0:2B:12:34:56 vlan marketing port 4
```

History

This command was available in ExtremeWare 2.0.

Support for associating separate QoS profiles with ingress and egress ports was added in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

delete fdbentry

```
delete fdbentry [[<mac_address> | broadcast-mac] vlan <vlan name> | all]
```

Description

Deletes one or all permanent FDB entries.

Syntax Description

mac_address	Specifies a device MAC address, using colon-separated bytes.
broadcast-mac	Specifies the broadcast MAC address. May be used as an alternate to the colon-separated byte form of the address ff:ff:ff:ff:ff:ff.
vlan name	Specifies a VLAN name.
all	Specifies that all FDB entries should be deleted.

Default

N/A.

Usage Guidelines

None.

Example

The following example deletes a permanent entry from the FDB:

```
delete fdbentry 00:E0:2B:12:34:56 vlan marketing
```

The following example deletes all permanent entry from the FDB:

```
delete fdbentry all
```

History

This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.0 to support the `all` option.

This command was modified in ExtremeWare 6.2.1 to support the `broadcast-mac` option.

Platform Availability

This command is available on all platforms.

disable fdb-scan

```
disable fdb-scan [all | slot {{backplane} | <slot number> | msm-a | msm-b}]
```

Description

Disables FDB scanning on a stand-alone switch or on a per slot or backplane basis on a modular switch.

Syntax Description

all	Specifies all of the slots in the chassis. This is available on modular switches only.
backplane	Specifies the backplane of the chassis. This is available on Alpine switches only.
slot number	Specifies the slot number of the module to scan. This is available on BlackDiamond switches only.
msm-a	Specifies the MSM in slot A. This is available on BlackDiamond switches only
msm-b	Specifies the MSM in slot B. This is available on BlackDiamond switches only.

Default

Disabled.

Usage Guidelines

This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the `show switch` command. The following is sample FDB scanning output:

```
Fdb-Scan Diag:    Enabled.    Failure action:  log only
```

For ExtremeWare 6.2.2b108:

The default for the FDB scan is enabled.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the FDB scan is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, FDB scanning is enabled. You must manually disable FDB scanning if you want the feature disabled.

Example

The following command disables FDB scanning on a stand-alone switch:

```
disable fdb-scan
```

The following command disables FDB scanning on all of the slots of a modular switch:

```
disable fdb-scan all
```

History

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

enable fdb-scan

```
enable fdb-scan [all | slot {{backplane} | <slot number> | msm-a | msm-b}]
```

Description

Enables FDB scanning on a stand-alone switch or on a per slot or backplane basis on a modular switch.

Syntax Description

all	Specifies all of the slots in the chassis. This is available on modular switches only.
backplane	Specifies the backplane of the chassis. This is available on Alpine switches only.
slot number	Specifies the slot number of the module to scan. This is available on BlackDiamond switches only.
msm-a	Specifies the MSM in slot A. This is available on BlackDiamond switches only
msm-b	Specifies the MSM in slot B. This is available on BlackDiamond switches only.

Default

Disabled.

Usage Guidelines

In addition to the system health checker, you can scan the FDB on a stand-alone switch, or on a per slot or backplane basis on a modular switch. This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the `show switch` command. The following is sample FDB scanning output:

```
Fdb-Scan Diag:    Enabled.    Failure action:  log only
```

For ExtremeWare 6.2.2b108:

The default for the FDB scan is enabled.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the FDB scan is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, FDB scanning is enabled. You must manually disable FDB scanning if you want the feature disabled.

Example

The following command enables FDB scanning on a stand-alone switch:

```
enable fdb-scan
```

The following command enables FDB scanning on all of the slots of a modular switch:

```
enable fdb-scan all
```

History

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

run fdb-check

```
run fdb-check [index <bucket> <entry> | [<mac_address> | broadcast-mac]
{<vlan name>}] {extended} {detail}
```

Description

Checks MAC FDB entries for consistency.

Syntax Description

bucket	Specifies the bucket portion of the FDB hash index.
entry	Specifies the entry portion of the FDB hash index.
mac-address	Specifies a MAC address (hex octet). FDB entries with this MAC address will be checked.
broadcast-mac	Specifies the broadcast MAC address. May be used as an alternate to the hex octet form, ff:ff:ff:ff:ff:ff. (6.2.1 and higher)
vlan name	Specifies a VLAN name. FDB entries for this VLAN with the specified MAC address will be checked.
extended	Enables OTP index checking in the MAC entry and VPST of the egress port.
detail	Specifies that more detailed debug information should be logged.

Default

N / A.

Usage Guidelines

The FDB error checking function logs the error count into the system log. Use the `detail` option to log more detailed debug information.

If you do not enter a VLAN name, ExtremeWare check all FDB entries with the specified MAC address.

Example

Given the following FDB entry on an MSM 64:

```
Index              Mac              Vlan       Age  Use  Flags Port List

-------------------------------------------------------------------------------
  cf3c0-006 00:00:00:00:00:01         v1(4093)  0540 0000 d m      3:4
```

All the following commands will do consistency checking on this entry:

```
run fdb-check 00:00:00:00:00:01
run fdb-check 00:00:00:00:00:01 detail
run fdb-check 00:00:00:00:00:01 extended detail
run fdb-check 00:00:00:00:00:01 vlan v1
run fdb-check index cf3c 0 extended detail
```

History

This command was first available in ExtremeWare 6.1.9

This command was modified in ExtremeWare 6.2.1 to support the `broadcast-mac` keyword.

Platform Availability

This command is available on all platforms.

The `extended` option is available on the Black Diamond 6800 chassis-based system only.

show fdb

```
show fdb {<mac_address> | broadcast-mac | permanent | ports <portlist> |
remap | vlan <vlan name>}
```

Description

Displays FDB entries.

Syntax Description

mac_address	Specifies a MAC address, using colon-separated bytes, for which FDB entries should be displayed.
broadcast-mac	Specifies the broadcast MAC address. May be used as an alternate to the colon-separated byte form of the address ff:ff:ff:ff:ff:ff.
permanent	Displays all permanent entries, including the ingress and egress QoS profiles.
portlist	Displays the entries for one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
remap	Displays the remapped FDB entries.
vlan name	Displays the entries for a specific VLAN.

Default

All.

Usage Guidelines

Displays FDB entries as specified, or displays all FDB entries.

The show output displays the following information:

EQP	The Ingress QoS profile assigned to the entry (appears only if the keyword permanent is specified).
IQP	The Egress QoS profile assigned to the entry (appears only if the keyword permanent is specified).
Index	The FDB hash index, in the format <bucket>-<entry>.
Mac	The MAC address that defines the entry.
Vlan	The VLAN for the entry.
Age	The age of the entry, in seconds (does not appear if the keyword permanent is specified).
Use	The number of IP FDB entries that use this MAC address as a next hop or last hop (does not appear if the keyword permanent is specified).

Flags	Flags that define the type of entry: • B - Egress Blackhole • b - Ingress Blackhole • d - Dynamic • s - Static • p - Permanent • m - MAC • S - secure MAC • l - lockdown MAC • M - Mirror • i - an entry also exists in the IP FDB • x - an entry also exists in the IPX FDB • z - translation MAC • Q - Questionable • R - Remapped
Port List	The ports on which the MAC address has been learned

Example

The following command displays information about all the entries in the FDB:

```
show fdb
```

It produces output similar to the following:

```
Index              Mac               Vlan      Age  Use  Flags  Port List
-------------------------------------------------------------------------
0a0e0-100 00:01:30:EC:D3:00        lab(4000)  0000 0001 d i      1
2b560-ffb 01:00:0C:CC:CC:CD           (0000)  0000 0000 s m      CPU
30040-ffb 00:E0:2B:00:00:00        zzz(0652)  0000 0000 s m      CPU
332890-ffb 00:E0:2B:00:00:00   Default(0001)  0000 0000 s m      CPU
3d760-ffb 00:E0:2B:00:00:00       Mgmt(4094)  0000 0000 s m      CPU
3d770-ffb 00:E0:2B:00:00:00 MacVlanDis(4095)  0000 0000 s m      CPU
42560-ff0 00:01:30:6C:0D:00        lab(4000)  0000 0000 s m      CPU
46460-100 00:10:E3:1D:00:1E        lab(4000)  0000 0001 d i      1
4d060-100 00:10:E3:1D:00:05        lab(4000)  0000 0001 d i      1
4df70-ff0 00:01:30:6C:0D:00    Default(0001)  0000 0000 s m      CPU
4f7a0-ff0 00:01:30:6C:0D:00        zzz(0652)  0000 0000 s m      CPU
51f50-100 00:01:30:CA:F6:00        lab(4000)  0000 0001 d i      1
         ...
67b20-100 00:30:D3:01:5A:E0        lab(4000)  0000 0001 d i      1
80a10-204 FF:FF:FF:FF:FF:FF        lab(4000)  0000 0000 s m      CPU, 2, 1
80fe0-208 FF:FF:FF:FF:FF:FF MacVlanDis(4095)  0000 0000 s m      CPU
80ff0-202 FF:FF:FF:FF:FF:FF       Mgmt(4094)  0000 0000 s m      CPU
8d8d0-20a FF:FF:FF:FF:FF:FF        zzz(0652)  0000 0000 s m      CPU, 2
8f000-200 FF:FF:FF:FF:FF:FF    Default(0001)  0000 0000 s m      CPU
98670-100 00:01:30:E7:F2:00        lab(4000)  0000 0001 d i      1
fcf70-202 00:E0:2B:00:00:02       Mgmt(4094)  0000 0000 s m      CPU

Flags: (B) Egress Blackhole, (b) Ingress Blackhole, (d) Dynamic, (s) Static
       (p) Permanent, (m) MAC, (S) secure MAC, (l) lockdown MAC, (M) Mirror
       (i) IP, (x) IPX, (z) translation MAC, (Q) Questionable, (R) Remapped
```

```
Total: 33 Static: 16 Perm: 0 Locked: 0 Secure: 0 Dynamic: 17 Dropped: 0
Questionable: 0 Remapped: 0
FDB Aging time: 300 seconds
```

The following command displays information about the permanent entries in the FDB:

```
show fdb permanent
```

It produces output similar to the following:

```
EQP IQP Index              Mac              Vlan   Flags Port List
-------------------------------------------------------------------------------
QP3 QP2 ----- --- 00:10:E3:1D:00:05   anntest1(4094) pm     ---
QP3 QP2 4e610-206 00:01:03:2F:38:EE   anntest1(4094) spm     ---
QP3 QP2 ----- --- 00:60:B0:F9:58:9D    Default(0001) pm     ---

Flags: (B) Egress Blackhole, (b) Ingress Blackhole, (d) Dynamic, (s) Static
       (p) Permanent, (m) MAC, (S) secure MAC, (l) lockdown MAC, (M) Mirror
       (i) IP, (x) IPX, (z) translation MAC, (Q) Questionable, (R) Remapped
       [ ] : authorize port list
Total: 3 Secure: 0
```

History

This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.1 to support the `broadcast-mac` option.

This command was modified in ExtremeWare 6.2.2b108 to support the `remap` option.

The `remap` option was not supported in ExtremeWare 7.0.

This `remap` option is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

unconfigure fdb-scan failure-action

```
unconfigure fdb-scan failure-action
```

Description

Returns the switch to its default of sending FDB scan messages to the syslog if too many failures are detected within the specified scan period.

Syntax Description

The command has no arguments or variables.

Default

N/A.

Usage Guidelines

This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the `show switch` command.

For ExtremeWare 6.2.2b108:

The failure action default is `sys-health-check`. If you use the `unconfigure fdb-scan failure-action` command, the switch returns to its default of performing the configured system health check action.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The failure action default is `log`. If you use the `unconfigure fdb-scan failure-action` command, the switch sends one instance of an error message to the syslog.

Example

The following command returns the switch to its default of sending one instance of an error message to the syslog:

```
unconfigure fdb-scan failure-action
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

unconfigure fdb-scan period

```
unconfigure fdb-scan period
```

Description

Returns the FDB scan interval to the factory default of 30 seconds.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This setting is independent of and does not affect the system health check configurations.

Example

The following command returns the FDB scan interval to 30 seconds:

```
unconfigure fdb-scan period
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

7 QoS Commands

This chapter describes the following commands:

- Commands for configuring Quality of Service (QoS) profiles
- Commands creating traffic groupings and assigning the groups to QoS profiles
- Commands for configuring, enabling and disabling explicit class-of-service traffic groupings (802.1p and Diffserv)
- Commands for configuring, enabling and disabling Random Early Detection (RED)
- Commands for configuring traffic grouping priorities
- Commands for verifying configuration and performance
- Commands for enabling and disabling the Dynamic Link Context System (DLCS)

This chapter does not describe the additional ingress and egress QoS capabilities available on the High Density Gigabit Ethernet "3" series I/O modules. For more information and a full description of the "3" series I/O module command set, see Chapter 26.

Qualify of Service (QoS) is a feature of ExtremeWare that allows you to specify different service levels for outbound and inbound traffic. QoS is an effective control mechanism for networks that have heterogeneous traffic patterns. Using QoS, you can specify the service that a traffic type receives.

Policy-based QoS allows you to protect bandwidth for important categories of applications or specifically limit the bandwidth associated with less critical traffic. The switch contains separate hardware queues on every physical port. Each hardware queue is programmed by ExtremeWare with bandwidth management and prioritization parameters, defined as a QoS profile. The bandwidth management and prioritization parameters that modify the forwarding behavior of the switch affect how the switch transmits traffic for a given hardware queue on a physical port. Up to eight physical queues per port are available.

Policy-based QoS can be configured to perform per-port Random Early Detection (RED). Using this capability, the switch detects when traffic is filling up in any of the eight hardware queues, and performs a random discard on subsequent packets, based on the configured RED drop-probability. Instead of dropping sessions during times when the queue depth is exceeded, RED causes the switch to lower session throughput.

To configure QoS, you define how your switch responds to different categories of traffic by creating and configuring QoS profiles. The service that a particular type of traffic receives is determined by assigning a QoS profile to a traffic grouping or classification. The building blocks are defined as follows:

- **QoS profile**—Defines bandwidth and prioritization parameters.

- **Traffic grouping**—A method of classifying or grouping traffic that has one or more attributes in common.
- **QoS policy**—The combination that results from assigning a QoS profile to a traffic grouping.

QoS profiles are assigned to traffic groupings to modify switch-forwarding behavior. When assigned to a traffic grouping, the combination of the traffic grouping and the QoS profile comprise an example of a single policy that is part of Policy-Based QoS.

Extreme switch products support explicit Class of Service traffic groupings. This category of traffic groupings describes what is sometimes referred to as *explicit packet marking*, and includes:

- IP DiffServ code points, formerly known as IP TOS bits
- Prioritization bits used in IEEE 802.1p packets

All Extreme switches support the standard 802.1p priority bits that are part of a tagged Ethernet packet.

DLCS

The Dynamic Link Context System (DLCS) is a feature of ExtremeWare and Extreme switches that snoops Windows Internet Naming Service (WINS) NetBIOS packets and creates a mapping between a user name, the IP address or MAC address of the workstation, and a port on the switch. Based on the information in the packet, DLCS can detect when an workstation boots up or a user logs in or out, and dynamically maps the user or workstation name to the current IP address and switch port. For DLCS to operate within ExtremeWare, the user or workstation must allow for automatic DLCS updates.

Information obtained through DLCS is used by the EPICenter Policy Manager software, and enables the configuration of policies that apply to named users or workstations. Enabling the DLCS feature is only useful if you plan to use the EPICenter software. Currently, there are no other features that can make use of the information that the DLCS feature provides.

clear dlcs

```
clear dlcs
```

Description

Clears all learned DLCS data.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

If the IP address of an end-station changes, and the end-station is not immediately rebooted, the old host-to-IP mapping is not deleted. You must delete the mapping through the ExtremeWare Enterprise Manager Policy System.

Example

The following command clears all learned DLCS data from the switch:

```
clear dlcs
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure diffserv examination code-point qosprofile ports

```
configure diffserv examination code-point <code_point> qosprofile
<qosprofile> ports [<portlist> | all] {low-drop-probability |
high-drop-probability}
```

Description

Configures the default ingress Diffserv code points (DSCP) to QoS profile mapping.

Syntax Description

code_point	Specifies a DiffServ code point (a 6-bit value in the IP-TOS byte in the IP header).
qosprofile	Specifies the QoS profile to which the Diffserv code point is mapped.
portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that this applies to all ports on the device.
low-drop-probability	Specifies that the DSCP has a low drop-probability level. Supported only for SONET ports on a PoS module.
high-drop-probability	Specifies that the DSCP has a high drop-probability level. Supported only for SONET ports on a PoS module.

Default

See Table 10.

Usage Guidelines

You can specify up to 64 different code points for each port. Code point values are grouped and assigned to the default QoS profiles as follows:

Table 10: Default Code Point-to-QoS Profile Mapping

Code Point	QoS Profile
0-7	Qp1
8-15	Qp2
16-23	Qp3
24-31	Qp4
32-39	Qp5
40-47	Qp6
48-55	Qp7
56-63	Qp8

The mapping is applied in the ingress direction.

The `low-drop-probability` and `high-drop-probability` keywords are applicable only to SONET ports. The `low-drop-probability` and `high-drop-probability` keywords are useful in conjunction

with the weighted RED (WRED) implementation provided by SONET ports. This implementation supports two different drop probabilities; one for DSCPs designated as having low drop-probability and another for DSCPs designated as having high drop-probability. These keywords enable complete flexibility in assigning DSCPs to the two different drop-probability levels.

Example

The following command specifies that packets arriving on ports 5-8 that use code point 25 be assigned to qp2:

```
configure diffserv examination code-point 25 qosprofile qp2 ports 5-8
```

The following command sets up the mapping for the EF PHB (PoS module only):

```
configure diffserv examination code-point 46 qosprofile qp8 ports 2:1-2:2
```

History

This command was first available in ExtremeWare 6.0.

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

Platform Availability

This command is available on all platforms. The PoS module extensions are supported on the BlackDiamond switch only.

configure diffserv replacement priority

```
configure diffserv replacement priority <value> code-point <code_point>
ports [<portlist> | all]
```

Description

Configures the default egress Diffserv replacement mapping.

Syntax Description

value	Specifies the 802.1p priority value.
code_point	Specifies a 6-bit value to be used as the replacement code point in the IP-TOS byte in the IP header.
portlist	Specifies a list of egress ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N / A.

Usage Guidelines

To replace DiffServ code points you must enable both 802.1p replacement and DiffServ replacement using the `enable dot1p replacement ports` and `enable diffserv replacement ports` commands.

The default 802.1p priority value to code point mappings are described as follows:

Table 11: Default 802.1p Priority Value-to-Code Point Mapping

Hardware Queue "*i*" Chipset	802.1p Priority value	Code Point
Q0	0	0
Q1	1	8
Q2	2	16
Q3	3	24
Q4	4	32
Q5	5	40
Q6	6	48
Q7	7	56

Example

The following command specifies that a code point value of 25 should be used to replace the TOS bits in packets with an 802.1p priority of 2 for ports 5-9:

```
configure diffserv replacement priority 2 code-point 25 ports 5-9
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure dot1p type

```
configure dot1p type <dot1p_priority> qosprofile <qosprofile>
```

Description

Configures the default QoS profile to 802.1p priority mapping.

Syntax Description

dot1p_priority	Specifies the 802.1p priority value. The value is an integer between 0 and 7.
qosprofile	Specifies a QoS profile.

Default

N / A.

Usage Guidelines

An 802.1p priority value seen on ingress can be mapped to a particular QoS profile and with specific bandwidth management and priority behavior.

The default mapping of each 802.1p priority value to QoS profile is as follows:

Table 12: 802.1p Priority Value-to-QoS Profile Default Mapping

Priority Value	QoS Profile Summit Chipset	QoS Profile *"i"* Chipset
0	Qp1	Qp1
1	Qp1	Qp2
2	Qp2	Qp3
3	Qp2	Qp4
4	Qp3	Qp5
5	Qp3	Qp6
6	Qp4	Qp7
7	Qp4	Qp8

Example

The following commands swap the QoS profiles associated with 802.1p priority values 1 and 2 on an "*i*" series device:

```
configure dot1p type 2 qosprofile qp2
configure dot1p type 1 qosprofile qp3
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure ports qosprofile

```
configure ports <portlist> qosprofile <qosprofile>
```

Description

Configures one or more ports to use a particular QoS profile.

Syntax Description

portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
qosprofile	Specifies a QoS profile.

Default

N/A.

Usage Guidelines

Extreme switches support eight QoS profiles (QP1 - QP8).

Example

The following command configures port five to use QoS profile QP3:

```
configure ports 5 qosprofile QP3
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure qosprofile

```
configure qosprofile <qosprofile> minbw <min_percent> maxbw <max_percent>
priority <level> {[minbuf <percent> maxbuf <number> [K | M] | maxbuff
<number> [K | M] | <portlist>]}
```

Description

Modifies the default QoS profile parameters.

Syntax Description

qosprofile	Specifies a QoS profile name.
min_percent	Specifies a minimum bandwidth percentage for this queue. The default setting is 0.
max_percent	Specifies the maximum bandwidth percentage this queue is permitted to use. The default setting is 100.
level	Specifies a service priority setting. Settings include low, lowHi, normal, normalHi, medium, mediumHi, high, and highHi. The default setting is low. Available in egress mode only.
percent	Specifies the minimum percentage of the buffer set aside for the queue. Cumulative % of the queues should not exceed 100%.
number	Specifies the maximum buffer size in either M or K bytes. The range is 0 to 16384. The default is 256 K. You must reboot for changes to take effect. • K indicates the value is in K bytes. • M indicates the value is in M bytes.
portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

- Minimum bandwidth—0%
- Maximum bandwidth—100%
- Priority—low
- Minimum buffer percent—0%
- Maximum buffer size—256K

Usage Guidelines

On Summit chipset-based switches in ingress mode, any changes to parameters of the four predefined QoS profiles have the corresponding effect on the ports to which they are mapped.

The `minbuf` parameter reserves buffer memory for use exclusively by a QoS profile across all affected ports. The default value for buffer settings is 0%. The sum of all QoS profile buffer parameters should not exceed 100%. The `maxbuf` parameter allows you to set a maximum buffer for each queue, so that a single queue will not consume all of the unallocated buffer space. You should not modify the buffer parameter unless specific situations and application behavior indicate. You must reboot the switch for changes to this parameter to take effect.

For ExtremeWare 4.0:

- Only four priority levels are available (low, normal, medium, and high).

Example

The following command configures the QoS profile parameters of QoS profile *qp5* for specific ports on an "*i*" series switch:

```
configure qosprofile qp5 minbw 10% maxbw 80% priority highHi ports 5-7
```

The following command configures the buffer size for QoS profile *qp5* on an "*i*" series switch:

```
configure qosprofile qp5 minbw 10% maxbw 80% priority highhi minbuf 3% maxbuff 1024K
```

History

This command was available in ExtremeWare 2.0.

The minbuff, maxbuff, and ports arguments were available in ExtremeWare 6.0.

Platform Availability

The basic command is available on all platforms.

The minbuff, maxbuff, and ports arguments are available on "*i*" series platforms.

configure qostype priority

```
configure qostype priority [source-mac | dest-mac | access-list | vlan |
diffserv | dot1p] <priority>
```

Description

Configures the priority of the specified QoS traffic grouping.

Syntax Description

source-mac	Specifies the priority of traffic groupings based on FDB source MAC addresses. Default is 7.
dest-mac	Specifies the priority of traffic groupings based on FDB destination MAC addresses. Default is 8.
access-list	Specifies the priority of access-list based traffic groupings. Default is 11.
vlan	Specifies the priority of VLAN-based traffic groupings. Default is 1.
diffserv	Specifies the priority of traffic groupings based on DiffServ information. Default is 3.
dot1p	Specifies the priority of traffic groupings based on dot1p information. Default is 2.
priority	Specifies a priority value in the range of 0-15.

Default

access-list = 11
dest-mac = 8
source-mac = 7
diffserv = 3
dot1p = 2
vlan = 1

Usage Guidelines

QoS types with a greater value take higher precedence.

Port-based QoS traffic groupings are always the lowest priority. The priority of port-based traffic cannot be changed.

Example

The following command forces FDB source-mac QoS to take a higher precedence over FDB dest-mac QoS (with a default priority of 8):

```
configure qostype priority source-mac 9
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure red drop-probability

```
configure red drop-probability <percent>
```

Description

Configures the Random Early Detect (RED) drop-probability.

Syntax Description

percent	Specifies the RED drop probability as a percentage. Range is 0 -100.

Default

N/A.

Usage Guidelines

When the switch detects that traffic is filling up in any of the eight hardware queues, it performs a random discard on subsequent packets, based on the configured RED drop-probability. The destination node detects the dropped packet, and, using standard TCP windowing mechanisms, slows the transmission from the source node. RED drop-probability is configured on a system-wide basis.

The percentage range is 0 - 100%.

Example

The following command configures the RED drop-probability as 80%:

```
configure red drop-probability 80
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan priority

```
configure vlan <vlan name> priority <priority>
```

Description

Configures the 802.1p priority value for traffic generated on the switch.

Syntax Description

vlan name	Specifies a VLAN name.
priority	Specifies the 802.1p priority value. The value is an integer between 0 and 7.

Default

N/A.

Usage Guidelines

The 802.1p priority field is placed in the 802.1Q tag when a packet is generated by the switch. The switch CPU generates traffic, for example, when ping packets are sent out by a user on the switch console.

To configure which queue to use for traffic traveling across a VLAN, use the following command:

```
configure vlan <vlan name> qosprofile <qosprofile>
```

Example

The following command configures VLAN *accounting* to use priority 6 in its generated traffic:

```
configure vlan accounting priority 6
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan qosprofile

```
configure vlan <vlan name> qosprofile <qosprofile>
```

Description

Configures a VLAN to use a particular QoS profile.

Syntax Description

vlan name	Specifies a VLAN name.
qosprofile	Specifies a QoS profile.

Default

N/A.

Usage Guidelines

Extreme switches support eight QoS profiles (QP1 - QP8).

Example

The following command configures VLAN *accounting* to use QoS profile QP3:

```
configure vlan accounting qosprofile QP3
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable diffserv examination ports

```
disable diffserv examination ports [<portlist> | all]
```

Description

Disables the examination of the Diffserv field in an IP packet.

Syntax Description

portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that Diffserv examination should be disabled for all ports.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables Diffserv examination on selected ports:

```
disable diffserv examination ports 3,5,6
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable diffserv replacement ports

```
disable diffserv replacement ports [<portlist> | all]
```

Description

Disables the replacement of diffserv code points in packets transmitted by the switch.

Syntax Description

portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that Diffserv replacement should be disabled for all ports.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables Diffserv replacement on selected ports:

```
disable diffserv replacement ports 3,5,6
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable dlcs

```
disable dlcs {fast-ethernet-ports | ports [all | <port_number>]}
```

Description

This command disables WINS snooping for ports on this switch.

Syntax Description

fast-ethernet-ports	Specifies that WINS packet snooping should be disabled on all Fast Ethernet ports.
all	All specifies that WINS packet snooping should be disabled on all ports.
port_number	Specifies a port on which WINS packet snooping should be disabled.

Default

Disabled.

Usage Guidelines

Disabling DLCS means that DLCS information for this switch will no longer be available to the ExtremeWare Enterprise Manager Policy System.

Used with no parameters, this command disables WINS packet snooping on all ports on which it was enabled.

Using the port parameter disabled WINS packet snooping only on the specified port.

Example

The following command disables all WINS packet snooping on the switch:

```
disable dlcs
```

History

This command was available in ExtremeWare 6.0.

The command was modified in ExtremeWare 6.1 to support the `fast-ethernet-ports` parameter.

Platform Availability

This command is available on all platforms.

disable dot1p replacement ports

```
disable dot1p replacement ports [<portlist> | all]
```

Description

Disables the ability to overwrite 802.1p priority values for a given set of ports.

Syntax Description

portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that 892.1p replacement should be disabled for all ports.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables Diffserv replacement on all ports:

```
disable dot1p replacement ports all
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable qosmonitor

```
disable qosmonitor
```

Description

Disables the QoS monitoring capability.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command disables QoS monitoring:

```
disable qosmonitor
```

History

This command was available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

disable red ports

```
disable red ports <portlist>
```

Description

Disables Random Early Detection (RED) on the specified ports.

Syntax Description

portlist	Specifies the port number(s). May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

None.

Example

The following command disables RED on ports 5-7:

```
disable red ports 5-7
```

History

This command was first available in ExtremeWare 6.0.10.

Platform Availability

This command is available on all platforms.

enable diffserv examination ports

```
enable diffserv examination ports [<portlist> | all]
```

Description

Enables the Diffserv field of an ingress IP packet to be examined in order to select a QoS profile.

Syntax Description

portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that Diffserv examination should be enabled for all ports.

Default

Disabled.

Usage Guidelines

None.

Example

The following command enables Diffserv examination on selected ports:

```
enable diffserv examination ports 3,5,6
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable diffserv replacement ports

```
enable diffserv replacement ports [<portlist> | all]
```

Description

Enables the diffserv code point to be overwritten in packets transmitted by the switch.

Syntax Description

portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that Diffserv replacement should be enabled for all ports.

Default

Disabled.

Usage Guidelines

Eight user-defined code points can be configured on each port. The 802.1P priority bits (3-bits) are used to select one of the eight code points.

Example

The following command enables Diffserv replacement on selected ports:

```
enable diffserv replacement ports 3,5,6
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable dlcs

```
enable dlcs {fast-ethernet-ports | ports [all | <port_number>]}
```

Description

This command enables WINS snooping for ports on the switch.

Syntax Description

fast-ethernet-ports	Specifies that WINS packets should be snooped on all Fast Ethernet ports.
all	Specifies that WINS packets should be snooped on all ports.
port_number	Specifies a port on which WINS packets are to be snooped.

Default

Enables snooping on all ports.

Usage Guidelines

DLCS must be enabled to allow usage of DLCS information by the ExtremeWare Enterprise Manager Policy System.

`enable dlcs` used with no parameters is the same as `enable dlcs ports all`.

The `fast-ethernet-ports` parameter is a shortcut to enable DLCS on all gigabit Ethernet ports, rather than having to enter each port individually.

Example

The following command enables DLCS snooping on port 4:

```
enable dlcs ports 4
```

Either of the following commands enable DLCS snooping on all ports:

```
enable dlcs
enable dlcs ports all
```

History

This command was available in ExtremeWare 6.0.

The command was modified in ExtremeWare 6.1 to support the `fast-ethernet-ports` parameter.

Platform Availability

This command is available on all platforms.

enable dot1p replacement ports

```
enable dot1p replacement ports [<portlist> | all]
```

Description

Allows the 802.1p priority field to be overwritten on egress according to the QoS profile to 802.1p priority mapping for a given set of ports.

Syntax Description

portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that dot1p replacement should be enabled for all ports.

Default

Disabled.

Usage Guidelines

By default, 802.1p priority information is not replaced or manipulated, and the information observed on ingress is preserved when transmitting the packet.

If 802.1p replacement is enabled, the 802.1p priority information that is transmitted is determined by the hardware queue that is used when transmitting the packet. The mapping is described in Table 13. This mapping cannot be changed.

Table 13: Queue to 802.1p Priority Replacement Value

Hardware Queue	802.1p Priority Replacement Value
Q0	0
Q1	1
Q2	2
Q3	3
Q4	4
Q5	5
Q6	6
Q7	7

Example

The following command enables dot1p replacement on all ports:

```
enable dot1p replacement ports all
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable qosmonitor

```
enable qosmonitor {port <port>}
```

Description

Enables the QoS monitoring capability on the switch.

Syntax Description

port	Specifies a port.

Default

Disabled.

Usage Guidelines

When no port is specified, the QoS monitor automatically samples all the ports and records the sampled results. Error messages are logged to the syslog if the traffic exceeds the parameters of the QoS profile(s).

The QOS monitor is a utility that monitors the hardware queues associated with any port(s). The QOS monitor keeps track of the number of frames and the frames per second that a specific queue is responsible for transmitting on a physical port. Two options are available: a real-time display and a separate option for retrieving information in the background and writing it to the log.

The real-time display scrolls through the given portlist to provide statistics. The particular port being monitored at that time is indicated by an asterisk (*) appearing after the port number in the display.

Monitoring QoS in the background places transmit counter and any “overflow” information into the switch log. The log notification appears if one of the queues experiences an overflow condition since the last time it was sampled. An overflow entry indicates that a queue was over-subscribed at least temporarily, and is useful for determining correct QoS settings and potential over-subscription issues.

Example

The following command enables the QoS monitoring capability on port 4:

```
enable qosmonitor port 4
```

History

This command was available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

enable red ports

```
enable red ports [mgmt | <portlist>]
```

Description

Enables Random Early Detection (RED) on a port.

Syntax Description

mgmt	Specifies the management port.
portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

Policy-based QoS can be configured to perform per-port Random Early Detection (RED) and drop-probability. Using this capability, the switch detects when traffic is filling up in any of the eight hardware queues, and performs a random discard on subsequent packets, based on the configured RED drop-probability.

Instead of dropping sessions during times when the queue depth is exceeded, RED causes the switch to lower session throughput. The destination node detects the dropped packet, and, using standard TCP windowing mechanisms, slows the transmission from the source node. RED drop-probability is configured on a system-wide basis, and has a valid range from 0% to 100%.

Example

The following command enables RED on ports 5-7:

```
enable red ports 5-7
```

History

This command was first available in ExtremeWare 6.0.10.

Platform Availability

This command is available on all platforms.

show dlcs

```
show dlcs
```

Description

Displays the status of DLCS (enabled or disabled) and the status of ports that are snooping WINS packets.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays DLCS status and data from the switch:

```
show dlcs
```

It produces output such as the following:

```
DLCS:         Enabled
Ports:        4
```

History

This command was available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show dot1p

```
show dot1p
```

Description

Displays the 802.1p-to-QoS profile mappings.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the current 802.1p-to-QoS mappings on the switch:

```
show dot1p
```

Following is the output from this command:

```
802.1p Priority Value     QOS Profile
           0                QP1
           1                QP2
           2                QP3
           3                QP4
           4                QP5
           5                QP6
           6                QP7
           7                QP8
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show ports qosmonitor

```
show ports {mgmt | <portlist>} qosmonitor {egress | ingress} {discards}
```

Description

Displays real-time QoS statistics for egress packets on one or more ports.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
egress	Specifies to display statistics in egress. Default.
ingress	Specifies to display statistics in ingress.
discards	Specifies to display packets discarded.

Default

Shows QoS statistics for all ports in egress.

Usage Guidelines

The real-time display scrolls through the given portlist to provide statistics. You can choose screens for packet count and packets per second. The specific port being monitored is indicated by an asterisk (*) appearing after the port number in the display.

QoS monitor sampling is configured as follows:

- The port is monitored for 20 seconds before the switch moves on to the next port in the list.
- A port is sampled for five seconds before the packets per second (pps) value is displayed on the screen.

Example

The following command shows the real-time QoS statistics related to the specified ports:

```
show ports 1-2, 49 qosmonitor
```

Following is sample output from this command:

```
Qos Monitor Egress Queue Summary                    Mon Oct 21 20:35:21 2002
Port          Q0       Q1       Q2       Q3       Q4       Q5       Q6       Q7
             Xmts     Xmts     Xmts     Xmts     Xmts     Xmts     Xmts     Xmts
================================================================================
   1            7        0        0        0        0        0        0        4
   2*           0        0        0        0        0        0        0        6
  49            5        0      134      133        0        0        0        7


================================================================================
```

```
0->Clear Counters  U->page up  D->page down  R->rate screen  ESC->exit
```

History

This command was available in ExtremeWare 2.0.

This command was updated to support PoS in Extreme 6.2.

Platform Availability

This command is available on all platforms.

show qosprofile

```
show qosprofile {<qosprofile>} {port <portlist>}
```

Description

Displays QoS information on the switch.

Syntax Description

<qosprofile>	Specifies a QoS profile name.
portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

Displays QoS information for all profiles.

Usage Guidelines

Information displayed includes:

- QoS profile name
- Minimum bandwidth
- Maximum bandwidth
- Priority
- A list of all traffic groups to which the QoS profile is applied

Example

The following command shows the QoS information for the specified port:

```
show qosprofile 2:1
```

Following is sample output from this command:

```
2:1:
        Queue:  Q0 using QP1  MinBw=0%  MaxBw=100%  Pri=2.
                Q1 using QP2  MinBw=0%  MaxBw=100%  Pri=1.
                Q2 using QP3  MinBw=0%  MaxBw=100%  Pri=4.
                Q3 using QP4  MinBw=0%  MaxBw=100%  Pri=3.
                Q4 using QP5  MinBw=0%  MaxBw=100%  Pri=4.
                Q5 using QP6  MinBw=0%  MaxBw=100%  Pri=5.
                Q6 using QP7  MinBw=0%  MaxBw=100%  Pri=6.
                Q7 using QP8  MinBw=0%  MaxBw=100%  Pri=7.
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show qostype priority

```
show qostype priority
```

Description

Displays QoS traffic grouping priority settings.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the QoS traffic grouping priority settings for this switch:

```
show qostype priority
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

unconfigure diffserv examination ports

```
unconfigure diffserv examination ports [<portlist> | all]
```

Description

Removes the Diffserv examination code point from a port.

Syntax Description

portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that Diffserv examination code points should be removed from all ports.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes Diffserv code-point examination from ports 5-8:

```
unconfigure diffserv examination ports 5-8
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

unconfigure diffserv replacement ports

```
unconfigure diffserv replacement ports [<portlist> | all]
```

Description

Removes the diffserv replacement mapping from a port.

Syntax Description

portlist	Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that Diffserv replacement mapping should be removed from all ports.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes Diffserv replacement from ports 5-8:

```
unconfigure diffserv replacement ports 5-8
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

unconfigure qostype priority

```
unconfigure qostype priority
```

Description

Resets all traffic grouping priority values to their defaults.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Resets the traffic grouping priorities to the following:

access-list = 11
dest-mac = 8
source-mac = 7
diffserv = 3
dot1p = 2
vlan = 1

Example

The following command resets the QoS traffic grouping priorities:

```
unconfigure qostype priority
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

8 NAT Commands

This chapter covers the following topics:

- Configuring VLANs for Network Address Translation (NAT)
- Configuring NAT translation rules
- Displaying NAT settings

NAT is a feature that allows one set of IP addresses, typically private IP addresses, to be converted to another set of IP addresses, typically public Internet IP addresses. This conversion is done transparently by having a NAT device (any Extreme Networks switch using the "*i*" chipset) rewrite the source IP address and layer 4 port of the packets.

You can configure NAT to conserve IP address space by mapping a large number of inside (private) addresses to a much smaller number of outside (public) addresses.

In implementing NAT, you must configure at least two separate VLANs involved. One VLAN is configured as inside, and corresponds to the private IP addresses you would like to translate into other IP addresses. The other type of VLAN is configured as outside, which corresponds to the public (probably Internet) IP addresses you want the inside addresses translated to. The mappings between inside and outside IP addresses are done using rules that specify the IP subnets involved and the algorithms used to translate the addresses.

NOTE

The NAT modes in ExtremeWare only support translating traffic that initiates from inside addresses.

NAT rules are associated with a single outside VLAN. Multiple rules per outside VLAN are allowed. The rules take effect in the order they are displayed using the `show` command. Any number of inside VLANs can use a single outside VLAN, assuming that you have created proper rules. Similarly, a single inside VLAN can use any number of different outside VLANs, assuming that the rules and routing are set up properly.

TCP and UDP layer 4 ports, in combination with the IP addresses, form a unique identifier which allows hosts (as well as the NAT switch) to distinguish between separate conversations. NAT operates by replacing the inside IP packet's source IP and layer 4 port with an outside IP and layer 4 port. The NAT switch maintains a connection table to map the return packets on the outside VLAN back into their corresponding inside sessions.

clear nat

```
clear nat [connections | stats}
```

Description

Clears NAT connections or statistics.

Syntax Description

connections	Specifies the current NAT connections table.
stats	Specifies the statistics counter.

Default

N/A.

Usage Guidelines

None.

Example

The following command clears NAT connections:

```
clear nat connections
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat add vlan map

```
configure nat add vlan <vlan name> map source [any |
<source_ipaddress>/<mask>]
{l4-port [any | <port> {- <port>}]}
{destination <dest_ipaddress>/<mask> {l4-port [any | <port> {- <port>}]}}
to <ip address> [/<mask> | - <ip address>]
[tcp | udp | both] [portmap {<min> - <max>} | auto-constrain]
```

Description

Adds a NAT translation rule that translates private IP addresses to public IP addresses on the outside VLAN.

Syntax Description

vlan name	Specifies the name of the outside VLAN to which this rule applies.
source_ipaddress/mask	Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) that defines the source of the traffic to be mapped.
l4-port	Specifies a layer 4 port or port range. When used with a source IP address, indicates that the rule applies only to traffic from the specified layer 4 port(s). When used with a destination IP address, indicates that the rule applies only to packets with the specified layer 4 port(s) as their destination.
port	Specifies a port number in the range 1 to 65535. any indicates that the rule should be applied to traffic to/from any layer 4 port.
dest_ipaddress/mask	Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) used to determine the packets to which this rule applies.
nat_ipaddress	Specifies an IP address for the outside VLAN to which the source IP addresses will be mapped. This can be specified as a subnet (IP address and mask) or as an address range.
tcp	Specifies only TCP traffic should be translated.
udp	Specifies only UDP traffic should be translated.
both	Specifies that both TCP and UDP traffic should be translated.
portmap	Specifies that port-mapping mode should be used.
min	Specifies a port number in the range 1 to 65535.The default setting is 1024.
max	Specifies a port number in the range 1 to 65535. The default setting is 65535.
auto-constrain	Specifies that each inside IP address should be restricted in the number of simultaneous connections.

Default

N/A.

Usage Guidelines

Four different modes are used to determine how the outside IP addresses and layer 4 ports are assigned:

- Static mapping
- Dynamic mapping
- Port-mapping
- Auto-constraining

When static mapping is used, each inside IP address uses a single outside IP address. The layer 4 ports are not changed, and only the IP address is rewritten.

With dynamic mapping, the number of inside hosts can be greater than the number of outside hosts. The outside IP addresses are allocated on a first-come, first-serve basis to the inside IP addresses. The layer 4 ports are not changed. When the last session for a specific inside IP address closes, that outside IP address can be used by other hosts.

The `source` IP address specifies private side IP addresses and the `to` IP address (the NAT address) specifies the public side IP address. The addition of the `destination` optional keyword after the source IP address and mask species that the NAT rule to be applied to only packets with a specific destination IP address.

If the netmask for both the source and NAT addresses is /32, the switch will use static NAT translation. If the netmask for both the source and NAT addresses are not both /32, the switch will use dynamic NAT translation.

With static or dynamic translation rules, which do not rely on layer 4 ports, ICMP traffic is translated and allowed to pass.

The addition of a layer 4 protocol name and the `portmap` keyword tells the switch to use portmap mode. As each new connection is initiated from the inside, the NAT device picks the next available source layer 4 port on the first available outside IP address. When all ports on a given IP address are in use, the NAT device uses ports off of the next outside IP address.

Optionally, you may specify the range of layer 4 ports the switch chooses on the translated IP addresses. The default setting for `min` is 1024. The default setting for `max` is 65535. There is a performance penalty associated with specifying a specific port range other than the default.

ICMP traffic is not translated in portmap mode. You must add a dynamic NAT rule for the same IP address range to allow for ICMP traffic.

The auto-constraining algorithm for port-mapping limits the number of outside layer 4 ports a single inside host can use simultaneously. The limitation is based on the ratio of inside to outside IP addresses. The outside IP address and layer 4 port space is evenly distributed to all possible inside hosts. This guarantees that no single inside host can prevent other traffic from flowing through the NAT device.

Because of the large number of simultaneous requests that can be made from a web browser, it is not recommended that this mode be used when a large number of inside hosts are being translated to a small number of outside IP addresses.

ICMP traffic is not translated in auto-constrain mode. You must add a dynamic NAT rule for the same IP address range to allow for ICMP traffic.

The addition of the `l4-port` optional keyword allows the NAT rule to be applied to only packets with a specific layer 4 source or destination port. If you use the layer 4-port command after the source

IP/mask, the rule will only match if the port(s) specified are the source layer 4-ports. If you use the `l4-port` command after the destination IP/mask, the rule will only match if the port(s) specified are the destination layer 4 ports. Both options may be used together to further limit the rule. If you specify layer 4 ports, ICMP traffic will not translated and allowed to pass.

Rules are processed in order, usually in the order in which they were added. When a single rule is matched, no other rules are processed. You can view the rule order using the `show nat rules` command.

Example

The following command defines a static translation rule that specifies that traffic coming from 192.168.1.12 be mapped to 216.52.8.32 on outside VLAN `out_vlan_1`:

```
configure nat add out_vlan_1 map source 192.168.1.12/32 to 216.52.8.32/32
```

The following command defines a dynamic translation rule that specifies that traffic coming from subnet 192.168.1.0 should be mapped to IP addresses in the range of 216.52.8.1 to 216.52.8.31 on outside VLAN `out_vlan_1`:

```
configure nat add out_vlan_1 map source 192.168.1.0/24 to 216.52.8.1 - 216.52.8.31
```

The following command defines a translation rule that specifies that TCP/UDP packets coming from 192.168.1.12 and destined for 192.168.5.20 be mapped to 216.52.8.32 on outside VLAN `out_vlan_1`:

```
configure nat add out_vlan_1 map source 192.168.1.12/32 destination 192.168.5.20 to
216.52.8.32/32
```

The following command defines a portmap translation rule that specifies that both TCP and UDP traffic from subnet 102.168.2.0/25 be mapped to available layer 4 ports on the IP addresses in the subnet 216.52.8.32/28:

```
configure nat add out_vlan_2 map source 192.168.2.0/25 to 216.52.8.32 /28 both portmap
```

The following command defines a portmap translation rule that specifies that only TCP traffic from subnet 102.168.2.0/25 be mapped to layer 4 ports in the range of 1024-8192 on the IP addresses in the subnet 216.52.8.32/28:

```
configure nat add out_vlan_2 map source 192.168.2.128/25 to 216.52.8.64/28 tcp portmap
1024 - 8192
```

The following command specifies an autoconstrain NAT translation rule that applies to both TCP and UDP traffic:

```
configure nat add out_vlan_3 map source 192.168.3.0/24 to 216.52.8.64/32 both
auto-constrain
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat delete

```
configure nat delete [all |
vlan <vlan name> map source [any | <ip address>/<mask>]
  {l4-port [any | <port> {- <port>}]}
{destination <ip address>/<mask> {l4-port [any | <port> {- <port>}]}}
to <ip address> [/<mask> | - <ip address>]
[tcp | udp | both] [portmap {<min> - <max>} | auto-constrain]
```

Description

Deletes a NAT translation rule.

Syntax Description

all	Specifies that all NAT rules should be deleted.
vlan name	Specifies the name of the outside VLAN to which this rule applies.
source_ipaddress/mask	Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) that defines the source of the traffic to be mapped.
l4-port	Specifies a layer 4 port or port range. When used with a source IP address, indicates that the rule applies only to traffic from the specified layer 4 port(s).
	When used with a destination IP address, indicates that the rule applies only to packets with the specified layer 4 port(s) as their destination.
port	Specifies a port number in the range 1 to 65535.
	any indicates that the rule should be applied to traffic to/from any layer 4 port.
dest_ipaddress/mask	Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) used to determine the packets to which this rule applies.
nat_ipaddress	Specifies an IP address for the outside VLAN to which the source IP addresses will be mapped. This can be specified as a subnet (IP address and mask) or as an address range.
tcp	Specifies only TCP traffic should be translated.
udp	Specifies only UDP traffic should be translated.
both	Specifies that both TCP and UDP traffic should be translated.
min	Specifies a port number in the range 1 to 65535. The default setting is 1024.
max	Specifies a port number in the range 1 to 65535. The default setting is 65535.
autoconstrain	Specifies that each inside IP address should be restricted in the number of simultaneous connections.

Default

N/A.

Usage Guidelines

To delete all NAT rules, use the `all` keyword. To delete a specific NAT rule, you must use exactly the same parameters that you used to create the rule.

Example

The following command deletes a portmap translation rule:

```
configure nat delete out_vlan_2 map source 192.168.2.128/25 to 216.52.8.64/28 tcp
portmap 1024 - 8192
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat finrst-timeout

```
configure nat finrst-timeout <seconds>
```

Description

Configures the timeout for a TCP session that has been torn down or reset.

Syntax Description

seconds	Specifies the number of seconds to wait before the session table entry times out.

Default

Default timeout is 60 seconds.

Usage Guidelines

Setting the timeout to zero specifies that session table entries should not be timed-out. This is not normally recommended as NAT resources will get used up.

Example

The following command configures the timeout for a reset or torn-down TCP session to 120 seconds:

```
configure nat finrst-timeout 120
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat icmp-timeout

```
configure nat icmp-timeout <seconds>
```

Description

Configures the timeout for an ICMP packet.

Syntax Description

seconds	Specifies the number of seconds to wait before the session table entry times out.

Default

Default timeout is 3 seconds.

Usage Guidelines

Setting the timeout to zero specifies that session table entries should not be timed-out. This is not normally recommended as NAT resources will get used up.

Example

The following command configures the timeout for an ICMP packet to 5 seconds:

```
configure nat icmp-timeout 5
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat syn-timeout

```
configure nat syn-timeout <seconds>
```

Description

Configures the timeout for an entry with an unacknowledged TCP SYN state.

Syntax Description

seconds	Specifies the number of seconds to wait before the session table entry times out.

Default

Default timeout is 60 seconds.

Usage Guidelines

Setting the timeout to zero specifies that session table entries should not be timed-out. This is not normally recommended as NAT resources will get used up.

Example

The following command configures the timeout for a session with an unacknowledged SYN packet to 120 seconds:

```
configure nat syn-timeout 120
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat tcp-timeout

```
configure nat tcp-timeout <seconds>
```

Description

Configures the timeout for a fully setup TCP SYN session.

Syntax Description

seconds	Specifies the number of seconds to wait before the session table entry times out.

Default

Default timeout is 120 seconds.

Usage Guidelines

Setting the timeout to zero specifies that session table entries should not be timed-out. This is not normally recommended as NAT resources will get used up.

Example

The following command configures the timeout for a TCP session to 90 seconds:

```
configure nat tcp-timeout 90
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat timeout

```
configure nat timeout <seconds>
```

Description

Configures the timeout for any IP packet that is not TCP, UDP, or ICMP.

Syntax Description

seconds	Specifies the number of seconds to wait before the session table entry times out.

Default

Default timeout is 600 seconds.

Usage Guidelines

Setting the timeout to zero specifies that session table entries should not be timed-out. This is not normally recommended as NAT resources will get used up.

Example

The following command configures the timeout for packets other than TCP, UDP, or ICMP to 240 seconds:

```
configure nat timeout 240
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat udp-timeout

```
configure nat udp-timeout <seconds>
```

Description

Configures the timeout for a UDP session.

Syntax Description

seconds	Specifies the number of seconds to wait before the session table entry times out.

Default

Default timeout is 120 seconds.

Usage Guidelines

Setting the timeout to zero specifies that session table entries should not be timed-out. This is not normally recommended as NAT resources will get used up.

Example

The following command configures the timeout for a UDP session to 90 seconds:

```
configure nat udp-timeout 90
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure nat vlan

```
configure nat vlan <vlan name> [inside | outside | none]
```

Description

Configures a VLAN to participate in NAT.

Syntax Description

vlan name	Specifies a VLAN name.
inside	Specifies that the VLAN is an inside VLAN.
outside	Specifies that the VLAN is an outside VLAN.
none	Disables NAT functions on this VLAN.

Default

N/A.

Usage Guidelines

When a VLAN is configured to be `inside`, traffic from that VLAN is translated only if it has a matching NAT rule. Any unmatched traffic will be routed normally and not be translated. When a VLAN is configured to be `outside`, it routes all traffic.

Because all traffic runs through the central processing unit (CPU), it cannot run at line-rate.

Normally, outside traffic will be able to initiate connections to the internal private IP addresses. If you want to prevent this, you can create IP and ICMP access-lists on the outside VLAN ports to deny traffic destined for the inside IP addresses. There is a NAT performance penalty when you do this.

When a VLAN is configured to be none, all NAT functions are disabled and the VLAN operates normally.

Example

The following command configures the VLAN out_vlan_1 as an outside VLAN for use with NAT:

```
configure nat vlan out_vlan_1 outside
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable nat

```
disable nat
```

Description

Disables network address translation on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command disables NAT functionality on the switch:

```
disable nat
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable nat

```
enable nat
```

Description

Enables network address translation on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command enables NAT functionality on the switch:

```
enable nat
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show nat

```
show nat {timeout | stats | connections | rules {vlan <outside_vlan>}}
```

Description

Displays NAT settings.

Syntax Description

timeout	Specifies the display of NAT timeout settings.
stats	Specifies the display of statistics for NAT traffic.
connections	Specifies the display of the current NAT connection table.
rules	Specifies the display of NAT rules, optionally for a specific VLAN.
outside_vlan	Specifies the outside VLAN for which NAT rules should be displayed.

Default

Displays all NAT settings.

Usage Guidelines

Use the keyword `stats` to display statistics for the NAT traffic, including:

- The number of rules
- The number of current connections
- The number of translated packets on the inside and outside VLANs
- Information on missed translations

Use the keyword `connections` to display the current NAT connection table, including source IP/layer 4 port mappings from inside to outside.

Use the keyword `rules` to display the NAT translation rules for the outside VLANs configured on the switch. Rules are displayed in the order they are processed, starting with the first one. To display the NAT rules for a specific VLAN, add the VLAN name.

Use the keyword `timeout` to display the NAT timeout settings configured on the switch.

Example

The following command shows the NAT translation rules configured for VLAN *out_vlan_1*:

```
show nat rules vlan out_vlan_1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

9 SLB Commands

This chapter discusses server load balancing (SLB) and flow redirect commands.

SLB transparently distributes client requests among several servers. The main use for SLB is for web hosting (using redundant servers to increase the performance and reliability of busy websites).

You can use SLB to manage and balance traffic for client equipment such as web servers, cache servers, routers, and proxy servers. SLB is especially useful for e-commerce sites, Internet service providers, and managers of large intranets.

SLB also provides health checking. Health checking allows you to actively poll nodes to determine their health. The switch makes new connections only if the virtual server and node are both enabled and passing health checks. The switch considers a virtual server or node active unless a health check fails. If a health check fails, the switch considers the virtual server or node inactive. A virtual server or node is also considered inactive if it is disabled and has zero active connections.

Flow redirect overrides routing decisions to transparently redirect client requests to a target device (or group of devices). Unlike SLB, you do not duplicate content on the target device(s).

The switch can only redirect traffic that crosses a VLAN boundary, because flow redirect operates at layer 3. Flow redirection examines traffic and redirects it based on the following criteria, in order of priority:

1 Destination IP address and mask

2 Layer 4 port

3 Source IP address and mask

You can use flow redirect for the following:

- Web cache redirection
- Policy-based routing

clear slb connections

```
clear slb connections {ipaddress <ip address> : <port> | vip <vip name>}
```

Description

Clears all existing SLB connections.

Syntax Description

ip address	Specifies an IP address.
port	Specifies a port.
vip name	Specifies a virtual server.

Default

N / A.

Usage Guidelines

If you do not specify an IP address or a virtual server, all connections are cleared.

This interrupts all current connections, but does not prevent new connections from being established. To prevent new connections from being established, disable SLB to each virtual server using the following command:

```
disable slb vip <vip name> all
```

To prevent new connections from being established to a specific virtual server and simultaneously close all current connections, use the following command:

```
disable slb vip <vip name> all close-connections-now
```

Example

The following command clears the connections to the virtual server “content”:

```
clear slb connections content
```

History

This command was available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

clear slb persistence vip

```
clear slb persistence vip <vip name>
```

Description

Clears the connection information in the persistence table.

Syntax Description

vip name	Specifies a virtual server.

Default

N/A.

Usage Guidelines

Use this command only during testing. Clearing persistence disables applications, such as shopping carts, that require persistence.

Example

The following command clears all information in the persistence table:

```
clear slb vip all persistence
```

History

This command was available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure flow-redirect add next-hop

```
configure flow-redirect <flow redirect> add next-hop <ip address>
```

Description

Adds the next hop host (gateway) that is to receive the packets that match the flow redirect policy.

Syntax Description

flow redirect	Specifies a flow redirect policy.
ip address	Specifies an IP address.

Default

N/A.

Usage Guidelines

This command also automatically enables ping-based health checking.

Example

The following command adds the next hop of 10.2.1.20 to the flow redirect policy named “http_flow”:

```
configure flow-redirect http_flow add next-hop 10.2.1.20
```

History

This command was available in ExtremeWare 6.1.4.

Platform Availability

This command is available on all platforms.

configure flow-redirect delete next-hop

```
configure flow-redirect <flow redirect> delete next-hop <ip address>
```

Description

Deletes the next hop host (gateway).

Syntax Description

flow redirect	Specifies a flow redirect policy.
ip address	Specifies an IP address.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the next hop of 10.2.1.20 from the flow redirect policy named "http_flow":

```
configure flow-redirect http_flow delete next-hop 10.2.1.20
```

History

This command was available in ExtremeWare 6.1.4.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check ftp

```
configure flow-redirect <flow redirect> service-check ftp user <user name>
<password>
```

Description

Configures the flow redirect FTP check.

Syntax Description

flow redirect	Specifies a flow redirect policy.
user name	Specifies the user name for logging in to the FTP service.
password	Specifies the password for logging in to the FTP service.

Default

N / A.

Usage Guidelines

This command automatically enables FTP check. The FTP check logs in to each next hop specified in the flow redirect policy with the user name and password specified.

For ExtremeWare 6.2.0 and prior, the frequency of the FTP check is 60 seconds, the timeout of the FTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example

The following command configures (and enables) FTP check for the flow redirect policy named “ftp_flow” and logs in with the user name “test” and password “extreme”:

```
configure flow-redirect ftp_flow service-check ftp user test extreme
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check http

```
configure flow-redirect <flow redirect> service-check http url <url>
match-string <alphanumeric string>
```

Description

Configures the flow redirect HTTP check.

Syntax Description

flow redirect	Specifies a flow redirect policy.
url	Specifies the URL to be checked.
alphanumeric string	Specifies the text to search for.

Default

N/A.

Usage Guidelines

This command automatically enables HTTP check. The HTTP requests the designated URL from each next hop specified in the flow redirect policy and checks for the specified alphanumeric string in the first 5000 bytes. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include "http://" in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

For ExtremeWare 6.2.0 and prior, the frequency of the HTTP check is 60 seconds, the timeout of the HTTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example

The following command configures (and enables) HTTP check for the flow redirect policy named "http_flow" and checks http://www.checktest.com for the string "test":

```
configure flow-redirect http_flow service-check http url www.checktest.com
match-string test
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check L4-port

```
configure flow-redirect <flow redirect> service-check L4-port
```

Description

Configures the flow redirect layer 4 port check.

Syntax Description

flow redirect	Specifies a flow redirect policy.

Default

N/A.

Usage Guidelines

This command automatically enables layer 4 port check. The layer 4 port check opens and closes the layer 4 port specified in the flow redirect policy.

For ExtremeWare 6.2.0 and prior, the frequency of the layer 4 port check is 10 seconds, the timeout of the layer 4 port check is 30 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer tcp-port-check
```

Example

The following command configures (and enables) layer 4 port check for the flow redirect policy named “http_flow”:

```
configure flow-redirect http_flow service-check L4-port
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check nntp

```
configure flow-redirect <flow redirect> service-check nntp <newsgroup>
```

Description

Configures the flow redirect NNTP check.

Syntax Description

flow redirect	Specifies a flow redirect policy.
newsgroup	Specifies the news group to be checked.

Default

N/A.

Usage Guidelines

This command automatically enables NNTP check. The NNTP check checks the news server specified in the flow redirect policy.

For ExtremeWare 6.2.0 and prior, the frequency of the NNTP check is 60 seconds, the timeout of the NNTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example

The following command configures (and enables) NNTP check for the flow redirect policy named “nttp_flow” and checks the newsgroup “testgroup”:

```
configure flow-redirect nttp_flow service-check nntp testgroup
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check ping

```
configure flow-redirect <flow redirect> service-check ping
```

Description

Configures the flow redirect ping check.

Syntax Description

flow redirect	Specifies a flow redirect policy.

Default

N / A.

Usage Guidelines

This command automatically enables ping check.

Ping check is also automatically enabled when you add a next hop using the following command:

`configure flow-redirect add next-hop`

In ExtremeWare 6.2.0 and prior, the frequency of the ping check is 10 seconds, the timeout of the ping check is 30 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

`configure flow-redirect timer ping-check`

Example

The following command configures (and enables) ping check for the flow redirect policy named “http_flow”:

`configure flow-redirect http_flow service-check ping`

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check pop3

```
configure flow-redirect <flow redirect> service-check pop3 user <user name>
<password>
```

Description

Configures the flow redirect POP3 check.

Syntax Description

flow redirect	Specifies a flow redirect policy.
user name	Specifies the user name for logging in to the POP3 service.
password	Specifies the password for logging in to the POP3 service.

Default

N/A.

Usage Guidelines

This command automatically enables POP3 check. The POP3 check logs in to each next hop specified in the flow redirect policy with the user name and password specified.

For ExtremeWare 6.2.0 and prior, the frequency of the POP3 check is 60 seconds, the timeout of the POP3 check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example

The following command configures (and enables) POP3 check for the flow redirect policy named “pop3_flow” and logs in with the user name “test” and the password “extreme”:

```
configure flow-redirect pop3_flow service-check pop3 user test extreme
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check smtp

```
configure flow-redirect <flow redirect> service-check smtp <dns domain>
```

Description

Configures the flow redirect SMTP check.

Syntax Description

flow redirect	Specifies a flow redirect policy.
dns domain	Specifies the DNS domain of the mail server.

Default

N / A.

Usage Guidelines

This command automatically enables SMTP check. The SMTP ensures that the mail server specified in the flow redirect policy is able to send and receive mail.

For ExtremeWare 6.2.0 and prior, the frequency of the SMTP check is 60 seconds, the timeout of the SMTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example

The following command configures (and enables) SMTP check for the flow redirect policy named “smtp_flow”:

```
configure flow-redirect smtp_flow service-check smtp 10.4.1.40
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect service-check telnet

```
configure flow-redirect <flow redirect> service-check telnet user <user
name> <password>
```

Description

Configures the flow redirect Telnet check.

Syntax Description

flow redirect	Specifies a flow redirect policy.
user name	Specifies the user name for logging in to the telnet service.
password	Specifies the password for logging in to the telnet service.

Default

N/A.

Usage Guidelines

This command automatically enables Telnet check. The Telnet check logs in to each next hop specified in the flow redirect policy with the user name and password specified.

For ExtremeWare 6.2.0 and prior, the frequency of the Telnet check is 60 seconds, the timeout of the Telnet check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example

The following command configures (and enables) Telnet check for the flow redirect policy named “telnet_flow” and logs in with the user name “test” and the password “extreme”:

```
configure flow-redirect telnet_flow service-check telnet user test extreme
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure flow-redirect timer ping-check

```
configure flow-redirect timer ping-check frequency <seconds> timeout
<seconds>
```

Description

Configures the flow redirect ping-check frequency and timeout.

Syntax Description

frequency	Specifies the ping-check frequency. The range is 1 to 60.
timeout	Specifies the ping-check timeout. The range is 1 to 60.

Default

The default frequency is 10 seconds.

The default timeout is 30 seconds.

Usage Guidelines

The frequency must be less than the timeout.

Example

The following command configures a flow redirect ping-check frequency of 5 seconds and a timeout of 15 seconds:

```
configure flow-redirect timer ping-check frequency 5 timeout 15
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure flow-redirect timer service-check

```
configure flow-redirect timer service-check frequency <seconds> timeout
<seconds>
```

Description

Configures the flow redirect service-check frequency and timeout.

Syntax Description

frequency	Specifies the service-check frequency. The range is 15 to 300.
timeout	Specifies the service-check timeout. The range is 15 to 300.

Default

The default frequency is 60 seconds.

The default timeout is 180 seconds.

Usage Guidelines

The frequency must be less than the timeout.

This frequency and timeout apply to all layer 7 service checks.

Example

The following command configures a flow redirect service-check frequency of 100 seconds and a timeout of 300 seconds:

```
configure flow-redirect timer service-check frequency 100 timeout 300
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure flow-redirect timer tcp-port-check

```
configure flow-redirect timer tcp-port-check frequency <seconds> timeout
<seconds>
```

Description

Configures the flow redirect TCP port check frequency and timeout.

Syntax Description

frequency	Specifies the tcp-port-check frequency. The range is 5 to 120.
timeout	Specifies the tcp-port-check timeout. The range is 5 to 300.

Default

The default frequency is 10 seconds.

The default timeout is 30 seconds.

Usage Guidelines

The frequency must be less than the timeout.

Example

The following command configures a flow redirect tcp-port-check frequency of 15 seconds and a timeout of 45 seconds:

```
configure flow-redirect timer tcp-port-check frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure slb esrp vlan

```
configure slb esrp vlan <vlan name> [add | delete] unit [number]
```

Description

Configures all virtual servers with the specified unit number to match the state of the specified ESRP VLAN.

Syntax Description

vlan name	Specifies an ESRP VLAN.
unit	Specifies a unit identifier on a virtual server. The range is 1 to 16.

Default

The default is unit 1.

Usage Guidelines

You must configure ESRP for the VLAN that you specify.

Virtual servers added with a unit number that is already configured for ESRP failover automatically match the ESRP state configured for that unit number.

Use the unit number to associate a group of virual servers with an ESRP VLAN so that ESRP controls the failover state of the virtual servers. To set the unit number of a virtual server, use the following command:

```
configure slb vip
```

For simplicity, Extreme Networks recommends that you put client, server, and virtual server VLANs in the same ESRP group.

Example

The following command configures ESRP VLAN “servers” to control the failover state of all virtual servers configured with unit 3:

```
configure slb esrp vlan servers add unit 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb failover alive-frequency

```
configure slb failover alive-frequency <seconds> timeout <seconds>
```

Description

Configures the frequency at which the local SLB device polls the remote SLB device.

Syntax Description

alive-frequency	The frequency at which the local SLB device polls the remote SLB device. The range is 1 to 60.
timeout	The amount of time within which the local switch must receive a response from the remote switch. The range is 1 to 60.

Default

The default alive frequency is 1 second.

The default timeout is 3 seconds.

Usage Guidelines

The frequency must be less than the timeout. Extreme Networks recommends that you set the timout greater than an even multiple of the frequency.

To enable active-active operation, use the following command:

```
enable slb failover
```

Example

The following command sets the alive frequency to 5 seconds and the timeout to 10 seconds:

```
configure slb alive-frequency 5 timeout 10
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb failover dead-frequency

```
configure slb failover dead-frequency <seconds>
```

Description

Configures the frequency at which the local switch attempts to re-establish communication with the unresponsive remote switch.

Syntax Description

dead-frequency	The frequency at which the local switch attempts to re-establish communication with the unresponsive remote switch. The range is 1 to 60.

Default

The default dead frequency is 2 seconds.

Usage Guidelines

To enable active-active operation, use the following command:

```
enable slb failover
```

Example

The following command sets the dead frequency to 5 seconds:

```
configure slb dead-frequency 5
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb failover failback-now

```
configure slb failover failback-now
```

Description

Configures the local SLB to release the remote SLB resources if the remote SLB is alive.

Syntax Description

This command has no arguments or variables.

Default

N/A

Usage Guidelines

When an active SLB unit fails and recovers, and manual failback is enabled, use this command to force the recovered SLB unit to become the active unit. Executing this command does not affect the SLB configuration.

To enable manual failback, use the following command:

```
enable slb failover manual-failback
```

To disable manual failback, use the following command:

```
disable slb failover manual-failback
```

Example

The following command forces SLB to immediately failback to the backup unit:

```
configure slb failover failback-now
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb failover ping-check

```
configure slb failover ping-check <ip address> {frequency <seconds> timeout
<seconds>}
```

Description

Configures the SLB device to actively determine if a remote gateway is reachable by performing a ping.

Syntax Description

ip address	Specifies the IP address of the remote gateway.
frequency	Specifies the frequency of pings sent to the remote gateway. The range is 1 to 60.
timeout	Specifies the time before the local device declares the remote gateway down. The range is 1 to 60.

Default

The default frequency is 1 second.

The default timeout is 3 seconds.

Usage Guidelines

The frequency must be less than the timeout.

If the external gateway is not reachable, the virtual servers failover to the remote SLB device.

Do not configure ping-check to the remote SLB switch. If you configure ping-check to the remote SLB switch and the remote switch fails, the local switch also fails.

Example

The following command sets the IP address of the remote gateway to 10.10.10.21 with a ping frequency of 5 seconds and a timeout of 10 seconds:

```
configure slb failover ping-check 10.10.10.21 frequency 5 timeout 10
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb failover unit

```
configure slb failover unit <number> remote-ipaddress <ip address>
local-ipaddress <ip address> {L4-port <port number>}
```

Description

Configures the switch for active-active operation.

Syntax Description

unit	Specifies a unit identifier on a virtual server. The range is 1 to 16.
number	Specifies a number from 1 - 16.
remote-ipaddress	Specifies the remote peer IP address.
local-ipaddress	Specifies the local failover IP address.
ip address	Specifies an IP address.
L4-port	Specifies the TCP port used for keep alive packets between failover peers.
port number	Specifies a port.

Default

The default L4-port is 1028.

Usage Guidelines

You must configure both active switches. You must use the actual IP address of the switches for the `remote-ip` and `local-ip`; you cannot use the IP address of a virtual server.

To enable active-active operation, use the following command:

```
enable slb failover
```

Extreme Networks recommends that you use a dedicated layer 2 VLAN to connect the two active-active switches.

Example

The following command configures the local SLB switch (with an IP address of 10.10.10.22) to direct unit 2 virtual servers to failover to the SLB switch with an IP address of 10.10.10.21:

```
configure slb failover unit 2 remote-ipaddress 10.10.10.21 local-ipaddress 10.10.10.22
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global connection-block

```
configure slb global connection-block <number>
```

Description

Configures the number of SLB connections to allocate in memory, which improves performance.

Syntax Description

number	Specifies the number of connection blocks. The range is 100 to 20,000.

Default

The default is 10,000.

Usage Guidelines

Use this command when you are sure that you will have a minimum guaranteed number of connections. Additional connection blocks are allocated when necessary.

Do not use this command unless you are absolutely sure that you will use the memory allocated.

Example

The following command allocates memory for 500 connections:

```
configure slb global connection-block 500
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global connection-timeout

```
configure slb global connection-timeout <seconds>
```

Description

Configures the connection timeout for transparent and translation modes.

Syntax Description

seconds	Specifies the number of seconds. The range is 1 to 180.

Default

The default is one second.

Usage Guidelines

None.

Example

The following command configures the connection timeout for 50 seconds:

```
configure slb global connection-timeout 50
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global ftp

```
configure slb global ftp user <user name> {password {encrypted} <password>}
```

Description

Configures the default parameters for layer 7 FTP service checking.

Syntax Description

user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

The default value for user and password is anonymous.

Usage Guidelines

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The FTP service check provides a more thorough check than ping check, because the FTP service check logs into the service.

To enable service checking, use the following command:

```
enable slb vip <vip name> service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip <vip name> service-check ftp
```

Example

The following command configures service check to login using the user name “service” and the password “check”:

```
configure slb global ftp user service password check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global http

```
configure slb global http url <url> match-string [any-content |
alphanumeric string]
```

Description

Configures the default parameters for layer 7 HTTP service checking.

Syntax Description

url	Specifies a URL.
match string	Specifies the text to be matched at the specified URL.
any-content	Specifies that any content confirms check.
alphanumeric string	Specifies the text string to match.

Default

The default value for url is /.

The default match string is any content.

Usage Guidelines

The HTTP service check provides a more thorough check than ping check, because the HTTP service check connects to a specific URL and checks for a specific text string. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include “http://” in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

To enable service checking, use the following command:

```
enable slb vip <vip name> service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip <vip name> service-check ftp
```

Example

The following command configures service check to access http://www.checktest.com and look for the text “test”:

```
configure slb global http url www.checktest.com match-string test
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global nntp

```
configure slb global nntp <newsgroup>
```

Description

Configures the default parameters for layer 7 NNTP service checking.

Syntax Description

newsgroup	Specifies a newsgroup.

Default

The default newsgroup is ebusiness.

Usage Guidelines

The NNTP service check provides a more thorough check than ping check, because the NNTP service check logs into the service.

To enable service checking, use the following command:

```
enable slb vip <vip name> service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip <vip name> service-check ftp
```

Example

The following command configures the service check to log into the newsgroup “comp.dcom.lans.ethernet”:

```
configure slb global nntp comp.dcom.lans.ethernet
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global persistence-level

```
configure slb global persistence-level [any-vip | same-vip-any-port |
same-vip-same-port]
```

Description

Configures the persistence level globally.

Syntax Description

any-vip	Specifies that an entry can match any port on any virtual server.
same-vip-any-port	Specifies that an entry must match virtual server, and can be any port.
same-vip-same-port	Specifies that an entry must match both virtual server and port for persistence.

Default

The default level is `same-vip-same-port`.

Usage Guidelines

Use this command when different virtual servers do not require different persistence settings.

If you configure `any-vip` persistence, ensure that all virtual servers in all pools have the same services.

Example

The following command sets the global persistence level to `any-vip`:

```
configure slb global persistence-level any-vip
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global persistence-method

```
configure slb global persistence-method [per-packet | per-session]
```

Description

Configures the behavior of the persistence timer.

Syntax Description

per-packet	Resets the persistence timer at the receipt of each packet.
per-session	Resets the persistence timer at the beginning of the session. When the timer expires, persistence for the session ends.

Default

The default method is `per-session`.

Usage Guidelines

Using per-packet persistence requires more CPU processing.

To set the persistence timer, use the following command:

`configure slb vip <vip name> client-persistence-timeout`

Example

The following command sets the global persistence method to expire at the end of the session:

`configure slb global persistence-method per-session`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global ping-check

```
configure slb global ping-check frequency <seconds> timeout <seconds>
```

Description

Configures default health checking frequency and timeout period using layer 3-based pinging of the physical node.

Syntax Description

frequency	Specifies the frequency of the ping check. The range is 1 to 60 seconds.
timeout	Specifies the timeout of the ping check. The range is 1 to 60 seconds.

Default

The default frequency is 10 seconds.

The default timeout is 30 seconds.

Usage Guidelines

This command sets the global values for ping check. Use the global values if your servers are all equally reliable. You can configure a node to override the global values using the following command:

```
configure slb node <ip address> ping-check
```

The frequency must be less than the timeout.

If the pinged node does not respond within the specified timeout period (three ping intervals by default), the node is considered down.

Shorter ping intervals require more CPU processing.

Example

The following command sets the global ping-check frequency to 5 seconds and the timeout to 15 seconds:

```
configure slb global ping-check frequency 5 timeout 15
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global pop3

```
configure slb global pop3 user <user name> {password {encrypted}
<password>}
```

Description

Configures the default parameters for layer 7 POP3 service checking.

Syntax Description

user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

The default value for user and password is anonymous.

Usage Guidelines

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The POP3 service check provides a more thorough check than ping check, because the POP3 service check logs into the service.

To enable service checking, use the following command:

```
enable slb vip <vip name> service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip <vip name> service-check ftp
```

Example

The following command configures the service check to login using the user name “service” and the password “check”:

```
configure slb global pop3 user service password check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global service-check

```
configure slb global service-check frequency <seconds> timeout <seconds>
```

Description

Configures default health checking frequency and timeout period using layer 7-based application-dependent checking.

Syntax Description

frequency	Specifies the frequency of the service check. The range is 15 to 300 seconds.
timeout	Specifies the timeout of the service check. The range is 5 to 300 seconds.

Default

The default frequency is 60 seconds.

The default timeout is 180 seconds.

Usage Guidelines

The frequency must be less than the timeout.

If the health check frequency and timeout are not specified for a specific virtual server, the global values are used. To set specific frequency and timeout values for a virtual server, use the following command:

```
configure slb vip <vip name> service-check
```

Shorter intervals require more CPU processing.

Example

The following command sets the service check frequency to 90 seconds and the timeout to 270 seconds:

```
configure slb global service-check frequency 90 timeout 270
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global smtp

```
configure slb global smtp <dns domain>
```

Description

Configures the default parameters for layer 7 SMTP service checking.

Syntax Description

dns domain	Specifies the domain to check.

Default

The default value for `dns domain` is the switch's domain. If the switch does not have a DNS domain configured, the value is "mydomain.com".

Usage Guidelines

The SMTP service check provides a more thorough check than ping check, because the SMTP service check accesses the service.

To enable service checking, use the following command:

```
enable slb vip <vip name> service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip <vip name> service-check ftp
```

Example

The following command configures the service check to access the DNS domain servicecheck.domain.com:

```
configure slb global smtp servicecheck.domain.com
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global synguard

```
configure slb global synguard max-unacknowledged-SYNs <number>
```

Description

Configures the the SYN-guard feature.

Syntax Description

max-unacknowledged-SYNs	Specifies the number of half-open connections that the switch allows. The range is 10 to 4000.

Default

The default value is 50.

Usage Guidelines

If the number of half-open connections exceeds the number specified, the switch immediately ages out the half-open connections. This only applies to connections from the same source IP address.

SYN-guard is disabled by default. To enable SYN-guard, use the following command:

```
enable slb global synguard
```

SYN-guard is automatically enabled if you configure a `max-unacknowledged-SYNs` value greater than 0. A `max-unacknowledged-SYNs` value of 0 automatically disables SYN-guard.

Example

The following command configures the SYN-guard feature to age out half-open connections from the same source IP address when the number of connections exceeds 30:

```
configure slb global synguard max-unacknowledged-SYNs 30
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global tcp-port-check

```
configure slb global tcp-port-check frequency <seconds> timeout <seconds>
```

Description

Configures default health checking frequency and timeout period using layer 4-based TCP port testing.

Syntax Description

frequency	Specifies the frequency of the TCP port check. The range is 5 to 120 seconds.
timeout	Specifies the timeout of the TCP port check. The range is 5 to 300 seconds.

Default

The default frequency is 30 seconds.

The default timeout is 90 seconds.

Usage Guidelines

The frequency must be less than the timeout.

The TCP port check is the least intrusive health check, as it does not log into or access the server.

If the frequency and timeout are not specified for a specific node, the global values are used. You can configure a node to override the global values using the following command:

```
configure slb node <ip address> : <L4 port> tcp-port-check
```

To enable TCP port checking, use the following command:

```
enable slb node tcp-port-check
```

Example

The following command sets the global TCP-port-check frequency to 15 seconds and timeout to 45 seconds:

```
configure slb global tcp-port-check frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb global telnet

```
configure slb global telnet userid <userid> password {encrypted}
{<password>}
```

Description

Configures the default parameters for layer 7 telnet service checking.

Syntax Description

user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

The default value for user and password is anonymous.

Usage Guidelines

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The telnet service check provides a more thorough check than ping check, because the telnet service check logs into the service.

To enable service checking, use the following command:

```
enable slb vip <vip name> service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip <vip name> service-check ftp
```

Example

The following command configures the service check to login using the user name “service” and the password “check”:

```
configure slb global telnet user service password check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode health-check

```
configure slb gogo-mode <port number> health-check <ip address>
```

Description

Configures the health checker with the common IP addresses of the GoGo mode servers in this group.

Syntax Description

port number	Specifies the GoGo mode master port.
ip address	Specifies an IP address.

Default

N/A.

Usage Guidelines

Use this command to configure the IP address before configuring individual health checks.

Example

The following command configures the GoGo mode health check for the group with port 29 as the master port and an IP address of 192.168.200.2:

```
configure slb gogo-mode 29 health-check 192.168.200.2
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode ping-check

```
configure slb gogo-mode <port number> ping-check frequency <seconds>
timeout <seconds>
```

Description

Overrides the global default ping-check frequency and timeout values for this GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
frequency	Specifies the frequency of the ping check. The range is 1 to 60 seconds.
timeout	Specifies the timeout of the ping check. The range is 1 to 60 seconds.

Default

The default frequency is 10 seconds.

The default timeout is 30 seconds.

Usage Guidelines

The frequency must be less than the timeout.

To restore a configured frequency and timeout back to the global default, specify 0 for the frequency and timeout.

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```
configure slb gogo-mode health-check
```

To enable ping check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> ping-check
```

To disable ping check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> ping-check
```

Example

The following command configures a GoGo mode ping check frequency of 15 seconds and a timeout of 45 seconds for the group with port 29 as the master port:

```
configure slb gogo-mode 29 ping-check frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode service-check ftp

```
configure slb gogo-mode <port number> service-check ftp {L4-port <L4-port>}
{user <user> | password {encrypted} <password>}
```

Description

Configures the FTP service check parameters for a GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
L4-port	Specifies a layer 4 port.
user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

The default value for user and password is anonymous.

Usage Guidelines

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```
configure slb gogo-mode health-check
```

To enable service check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> service-check
```

To disable service check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> service-check
```

Example

The following command configures GoGo mode service check for the group with port 29 as the master port to login using the user name “service” and the password “check”:

```
configure slb gogo-mode 29 service-check ftp user service password check
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode service-check http

```
configure slb gogo-mode <port number> service-check http {L4-port
<L4-port>} {url <url> match-string [any-content | <alphanumeric string>]}
```

Description

Configures the HTTP service check parameters for a GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
L4-port	Specifies a layer 4 port.
url	Specifies a URL.
any-content	Specifies that any content confirms check.
alphanumeric string	Specifies the text string to match.

Default

The default value for url is /.

The default match string is any content.

Usage Guidelines

This command accesses the specified URL and checks for the specified alphanumeric string in the first 1000 bytes. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include "http://" in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```
configure slb gogo-mode health-check
```

To enable service check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> service-check
```

To disable service check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> service-check
```

Example

The following command configures GoGo mode service check for the group with port 29 as the master port to access http://www.checktest.com and look for the text "test":

```
configure slb gogo-mode 29 service-check http url www.checktest.com match-string test
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode service-check pop3

```
configure slb gogo-mode <port number> service-check pop3 {L4-port
<L4-port>} {userid <userid> | password {encrypted} <password>}
```

Description

Configures the service check parameters for a GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
L4-port	Specifies a layer 4 port.
user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

The default value for user and password is anonymous.

Usage Guidelines

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```
configure slb gogo-mode health-check
```

To enable service check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> service-check
```

To disable service check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> service-check
```

Example

The following command configures GoGo mode service check for the group with port 29 as the master port to login using the user name “service” and the password “check”:

```
configure slb gogo-mode 29 service-check pop3 user service password check
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode service-check smtp

```
configure slb gogo-mode <port number> service-check smtp {L4-port
<L4-port>} {<dns domain>}
```

Description

Configures the service check parameters for a GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
L4-port	Specifies a layer 4 port.
dns domain	Specifies the domain to check.

Default

The default value for `dns domain` is the switch's domain. If the switch does not have a DNS domain configured, the value is "mydomain.com".

Usage Guidelines

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```
configure slb gogo-mode health-check
```

To enable service check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> service-check
```

To disable service check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> service-check
```

Example

The following command configures the GoGo mode service check for the group with port 29 as the master port to access the DNS domain servicecheck.domain.com:

```
configure slb gogo-mode 29 service-check smtp servicecheck.domain.com
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode service-check telnet

```
configure slb gogo-mode <port number> service-check telnet {L4-port
<L4-port>} {user <user name> | password {encrypted} <password>}
```

Description

Configures the service check parameters for a GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
L4-port	Specifies a layer 4 port.
user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

The default value for user and password is anonymous.

Usage Guidelines

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

`configure slb gogo-mode health-check`

To enable service check for a GoGo mode group, use the following command:

`enable slb gogo-mode <port number> service-check`

To disable service check for a GoGo mode group, use the following command:

`disable slb gogo-mode <port number> service-check`

Example

The following command configures GoGo mode service check for the group with port 29 as the master port to login using the user name “service” and the password “check”:

`configure slb gogo-mode 29 service-check telnet user service password check`

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode service-check timer

```
configure slb gogo-mode <port number> service-check timer [all | ftp | http
| telnet | smtp | nntp | pop3 | <TCP port number>] frequency <seconds>
timeout <seconds>
```

Description

Overrides the global service-check frequency and timeout values.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Specifies all service checks.
ftp	Specifies the FTP service check.
http	Specifies the HTTP service check.
telnet	Specifies the telnet service check.
smtp	Specifies the SMTP service check.
nntp	Specifies the NNTP service check.
pop3	Specifies the POP3 service check.
TCP port number	Specifies a TCP port, instead of a service, for the service check.
frequency	Specifies the frequency of the service check. The range is 15 to 300 seconds.
timeout	Specifies the timeout of the service check. The range is 15 to 300 seconds.

Default

The default frequency is 60 seconds.

The default timeout is 180 seconds.

Usage Guidelines

You can use this command at any time. This command affects the frequency and timeout for the specified service-check in the specified GoGo mode group.

The frequency must be less than the timeout.

Example

The following command configures GoGo mode FTP service check for the group with port 29 as the master port with a frequency of 15 seconds and a timeout of 45 seconds:

```
configure slb gogo-mode 29 service-check timer ftp frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode tcp-port-check add

```
configure slb gogo-mode <port number> tcp-port-check add [ftp | http |
https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web |
www | <TCP port number>]
```

Description

Adds the specified layer 4 port.

Syntax Description

port number	Specifies the GoGo mode master port.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
www	Specifies the www TCP-port-check.
TCP port number	Specifies a TCP port for the TCP-port-check.

Default

N/A.

Usage Guidelines

This command adds the port to the specified TCP-port-check in the specified GoGo mode group. You can only add a single port with each command; to add multiple ports, you must enter multiple commands.

Example

The following command adds FTP as a GoGo mode TCP-port-check for the group with port 29 as the master port:

```
configure slb gogo-mode 29 tcp-port-check add ftp
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode tcp-port-check delete

```
configure slb gogo-mode <port number> tcp-port-check delete [ftp | http |
https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web |
www | <TCP port number>]
```

Description

Deletes the specified layer 4 port.

Syntax Description

port number	Specifies the GoGo mode master port.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
www	Specifies the www TCP-port-check.
TCP port number	Specifies a TCP port for the TCP-port-check.

Default

N/A.

Usage Guidelines

This command deletes the port from the specified TCP-port-check in the specified GoGo mode group. You can only delete a single port with each command; to delete multiple ports, you must enter multiple commands.

Example

The following command deletes FTP from the GoGo mode TCP-port-check for the group with port 29 as the master port:

```
configure slb gogo-mode 29 tcp-port-check delete ftp
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb gogo-mode tcp-port-check timer

```
configure slb gogo-mode <port number> tcp-port-check timer [ftp | http |
https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web |
www | <TCP port number>] frequency <seconds> timeout <seconds>
```

Description

Overrides the global TCP-port-check frequency and timeout values.

Syntax Description

port number	Specifies the GoGo mode master port.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
www	Specifies the www TCP-port-check.
TCP port number	Specifies a TCP port for the TCP-port-check.
frequency	Specifies the frequency of the TCP port check. The range is 5 to 120 seconds.
timeout	Specifies the timeout of the TCP port check. The range is 5 to 300 seconds.

Default

The default frequency is 30 seconds.

The default timeout is 90 seconds.

Usage Guidelines

This command affects only the specified GoGo mode group.

To set the global TCP-port-check frequency and timeout, use the following command:

```
configure slb global tcp-port-check
```

The frequency must be less than the timeout.

Example

The following command configures GoGo mode FTP TCP-port-check for the group with port 29 as the master port with a frequency of 15 seconds and a timeout of 45 seconds:

```
configure slb gogo-mode 29 tcp-port-check timer ftp frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure slb L4-port

```
configure slb L4-port [ftp | http | https | imap4 | ldap | nntp | pop3 |
smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port
number>] [treaper-timeout <seconds> } udp-idle-timeout <seconds>]
```

Description

Configures the inactive period for TCP or UDP before the connection is aged out.

Syntax Description

ftp	Specifies the FTP service.
http	Specifies the HTTP service.
https	Specifies the HTTPS service.
imap4	Specifies the IMAP4 service.
ldap	Specifies the LDAP service.
nntp	Specifies the NNTP service.
pop3	Specifies the POP3 service.
smtp	Specifies the SMTP service.
socks	Specifies the SOCKS service.
telnet	Specifies the Telnet service.
tftp	Specifies the TFTP service.
web	Specifies the Web service.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies the WWW service.
TCP or UDP port number	Specifies a TCP or UDP port for the service.
treaper-timeout	Specifies the timeout for TCP.
udp-idle-timeout	Specifies the timeout for UDP.

Default

The default treaper-timeout is 600 seconds.

The default udp-idle-timeout is 600 seconds.

Usage Guidelines

You must configure the port and add it to a pool before you use this command. The timeout value affects all connections to the specified service on all virtual servers.

To set the timeout values for a wildcard virtual server, use a TCP or UDP port number of 0.

Example

The following command configures the ftp nodes with a TCP idle period of 30 seconds:

```
configure slb l4-port ftp treaper-timeout 30
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb node max-connections

```
configure slb node <ip address>:[ftp | http | https | imap4 | ldap | nntp |
pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP
port number>] max-connections <number>
```

Description

Configures the maximum number of simultaneous connections that can be established to a node.

Syntax Description

ip address	Specifies the IP address of the node.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies the www TCP-port-check.
TCP or UDP port number	Specifies a TCP or UDP port for the TCP-port-check.
max-connections	Specifies the maximum number of simultaneous connections. The range is 0 to 999999999.

Default

The default is 0.

Usage Guidelines

Use this command to limit the number of connections possible to a server with limited capabilities. Use `max-connections` of 0 to specify no limit.

Example

The following command configures the server with an IP address of 10.1.1.2:80 to accept a maximum of 10 connections:

```
configure slb node 10.1.1.2 : 80 max-connections 10
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb node ping-check

```
configure slb node <ip address> ping-check frequency <seconds> timeout
<seconds>
```

Description

Overrides the global default frequency and timeout values for this node.

Syntax Description

ip address	Specifies the IP address of the node.
frequency	Specifies the frequency of the ping check. The range is 1 to 60 seconds.
timeout	Specifies the timeout of the ping check. The range is 1 to 60 seconds.

Default

The default frequency is 10 seconds.

The default timeout is 30 seconds.

Usage Guidelines

The frequency must be less than the timeout.

To set the global ping-check frequency and timeout, use the following command:

`configure slb global ping-check`

Example

The following command sets the ping-check for the node with an IP address of 10.2.1.2 to a frequency of 30 seconds and a timeout of 90 seconds:

```
configure slb node 10.2.1.2 ping-check frequency 30 timeout 90
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb node tcp-port-check

```
configure slb node <ip address>:[ftp | http | https | imap4 | ldap | nntp |
pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP
port number>] tcp-port-check frequency <seconds> timeout <seconds>
```

Description

Overrides the global default frequency and timeout values for this node.

Syntax Description

ip address	Specifies the IP address of the node.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies the www TCP-port-check.
TCP or UDP port number	Specifies a TCP or UDP port for the TCP-port-check.
frequency	Specifies the frequency of the TCP port check. The range is 5 to 120 seconds.
timeout	Specifies the timeout of the TCP port check. The range is 5 to 300 seconds.

Default

The default frequency is 30 seconds.

The default timeout is 90 seconds.

Usage Guidelines

To set the global TCP-port-check frequency and timeout, use the following command:

`configure slb global tcp-port-check`

The frequency must be less than the timeout.

Example

The following command sets the FTP TCP-port-check for the node with an IP address of 10.2.1.2 to a frequency of 30 seconds and a timeout of 90 seconds:

```
configure slb node 10.2.1.2 : ftp tcp-port-check frequency 30 timeout 90
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb pool add

```
configure slb pool <pool name> add <ip address>:[ftp | http | https | imap4
| ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www
| <TCP or UDP port number>] {ratio <number> | priority <number>}
```

Description

Adds a node to a pool.

Syntax Description

pool name	Specifies a pool.
ip address	Specifies the IP address of the node.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.
ratio	Specifies the ratio for the ratio load balancing method. The range is 0 to 65,535.
priority	Specifies the priority for the priority load balancing method. The range is 1 to 65535.

Default

The default ratio is 1.

The default priority is 1.

Usage Guidelines

This command also configures the ratio or priority for the ratio and priority load balancing methods.

You must create the pool before you add nodes. When you add a new node, ping-check is automatically enabled.

A ratio of 2 results in twice as much traffic as a ratio of 1. If all nodes use the same ratio, connections are distributed equally among the nodes. A ratio of 0 results in no traffic to the node. When you

configure the ratio, use the smallest common denominator. For example, to configure a ratio of 25% and 75%, use ratios of 1 and 3, instead of 25 and 75.

To configure a pool to use the ratio load balancing method, use the following command:

```
configure slb pool <pool name> lb-method ratio
```

Higher priority numbers indicate higher priority. To configure a pool to use the priority load balancing method, use the following command:

```
configure slb pool <pool name> lb-method priority
```

To change the ratio or priority of a node that is already in a pool, use the following command:

```
configure slb pool <pool name> member
```

Example

The following command adds the FTP node with an IP address of 10.2.1.2 to the pool “ftp” and configures the node with a priority of 2:

```
configure slb pool ftp add 10.2.1.2 : ftp priority 2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb pool delete

```
configure slb pool <pool name> delete <ip address>:[ftp | http | https |
imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard
| www | <TCP or UDP port number>]
```

Description

Deletes a node from a pool.

Syntax Description

pool name	Specifies a pool.
ip address	Specifies the IP address of the node.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

N / A.

Usage Guidelines

Deleting a node from a pool does not delete the node from other pools. You can delete all nodes in a pool by deleting the pool. To delete a pool, use the following command:

```
delete slb pool
```

Example

The following command deletes the FTP node with an IP address of 10.2.1.2 from the pool “ftp”:

```
configure slb pool ftp delete 10.2.1.2 : ftp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb pool lb-method

```
configure slb pool <pool name> lb-method [least-connections | priority |
ratio | round-robin]
```

Description

Configures the SLB load balancing method.

Syntax Description

pool name	Specifies a pool.
least-connections	Specifies the least connections load balancing method.
priority	Specifies the priority load balancing method.
ratio	Specifies the ratio load balancing method.
round-robin	Specifies the round robin load balancing method.

Default

N/A.

Usage Guidelines

Use this command to change the load balancing method after you have already created a pool.

To set the ratio or priority of a node, use the following command:

```
configure slb pool <pool name> member
```

Example

The following command changes the load balancing method for the pool “ftp” to ratio:

```
configure slb pool ftp lb-method ratio
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb pool member

```
configure slb pool <pool name> member <ip address>:[ftp | http | https |
imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www |
<TCP or UDP port number>] [ratio <number> | priority <number>]
```

Description

Configures the ratio or priority of an existing pool member.

Syntax Description

pool name	Specifies a pool.
ip address	Specifies the IP address of the node.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.
ratio	Specifies the ratio for the ratio load balancing method. The range is 0 to 65,535.
priority	Specifies the priority for the priority load balancing method. The range is 1 to 65535.

Default

The default ratio is 1.

The default priority is 1.

Usage Guidelines

Use this command to change the ratio or priority of an existing node. To add a node to a pool (and set the ratio or priority), use the following command:

```
configure slb pool <pool name> add
```

Example

The following command changes the priority of the FTP node with an IP address of 10.2.1.2 in the pool “ftp” to 2:

```
configure slb pool ftp member 10.2.1.2 : ftp priority 2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb proxy-client-persistence

```
configure slb proxy-client-persistence [add | delete] <ip
address>/<netmask>
```

Description

Configures a client subnet that should be treated as one persistent entity.

Syntax Description

ip address/netmask	Specifies an IP address and netmask.

Default

N/A.

Usage Guidelines

Use this command to force all clients from the specified proxy array to connect to the same physical server.

Example

The following command specifies that the subnet 10.10.10.20/24 should be treated as a single, persistent entity:

```
configure slb proxy-client-persistence add 10.10.10.20/24
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip

```
configure slb vip <vip name> unit [number]
```

Description

Configures the unit number for active-active failover.

Syntax Description

vip name	Specifies a virtual server.
unit	Specifies a unit identifier on a virtual server. The range is 1 to 16.

Default

The default unit is 1.

Usage Guidelines

You must first create the virtual server before you use this command. To create a virtual server, use the following command:

```
creat slb vip
```

Example

The following command configures the virtual server “test” with a unit number of 3:

```
configure slb vip test unit 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip client-persistence-timeout

```
configure slb vip [<vip name> | all] client-persistence-timeout <seconds>
```

Description

Configures the client persistence timeout value.

Syntax Description

vip name	Specifies a virtual server.
all	Specifies all virtual servers.
client-persistence-timeout	Specifies the persistence timeout. The range is 1 to 999,999,999.

Default

The default `client-persistence-timeout` is 3600.

Usage Guidelines

Extreme Networks recommends that you specify a short client persistence timeout, because longer timeout values consume more memory.

Example

The following command configures the virtual server “ftp” with a client persistence timeout of 3000 seconds:

```
configure slb vip ftp client-persistence-timeout 3000
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip max-connections

```
configure slb vip <vip name> max-connections <number>
```

Description

Configures the maximum connections allowed to a particular virtual server.

Syntax Description

vip name	Specifies a virtual server.
max-connections	Specifies the maximum number of connections allowed to a virtual server. The range is 0 to 999,999,999.

Default

The default value is 0.

Usage Guidelines

A value of 0 indicates that no maximum is enforced. When the maximum number of connections is reached, the server stops responding to new requests; existing connections are maintained.

Example

The following command sets the maximum connections to the virtual server “ftp” to 10:

```
configure slb vip ftp max-connections 10
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check frequency

```
configure slb vip <vip name> service-check frequency <seconds> timeout
<seconds>
```

Description

Configures the layer 7 service check frequency and timeout for a particular virtual server.

Syntax Description

vip name	Specifies a virtual server.
frequency	Specifies the frequency of the service check. The range is 15 to 300 seconds.
timeout	Specifies the timeout of the service check. The range is 5 to 300 seconds.

Default

The default frequency is 60 seconds.

The default timeout is 180 seconds.

Usage Guidelines

The frequency must be less than the timeout.

To return to the global values, specify 0 for frequency and timeout. To set the global service check frequency and timeout, use the following command:

```
configure slb global service-check
```

Example

The following command sets the service check frequency to 15 and timeout to 45 for the virtual server “ftp”:

```
configure slb vip ftp service-check frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check ftp

```
configure slb vip <vip name> service-check ftp {user <user name> password
{encrypted} <password>}
```

Description

Configures layer 7 FTP service checking for a specific virtual server.

Syntax Description

vip name	Specifies a virtual server.
user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

N/A.

Usage Guidelines

This command automatically enables service checking.

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The FTP service check provides a more thorough check than ping check, because the FTP service check logs into the service.

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the global parameters, use the following command:

```
configure slb global ftp
```

Example

The following command configures service check to login using the user name “service” and the password “check” on the virtual server “ftpvip”:

```
configure slb vip ftpvip service-check ftp user service password check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check http

```
configure slb vip <vip name> service-check http {url <url> match-string
[any-content | <alphanumeric string>]}
```

Description

Configures layer 7 HTTP service checking for a specific virtual server.

Syntax Description

vip name	Specifies a virtual server.
url	Specifies a URL.
match string	Specifies the text to be matched at the specified URL.
any-content	Specifies that any content confirms check.
alphanumeric string	Specifies the text string to match.

Default

N/A.

Usage Guidelines

This command automatically enables service checking.

The HTTP service check provides a more thorough check than ping check, because the HTTP service check connects to a specific URL and checks for a specific text string. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include "http://" in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the global parameters, use the following command:

```
configure slb global http
```

Example

The following command configures service check to access http://www.checktest.com and look for the text "test" on the virtual server "httpvip":

```
configure slb vip httpvip service-check http url www.checktest.com match-string test
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check nntp

```
configure slb vip <vip name> service-check nntp <newsgroup>
```

Description

Configures layer 7 NNTP service checking for a specific virtual server.

Syntax Description

vip name	Specifies a virtual server.
newsgroup	Specifies a newsgroup.

Default

N/A.

Usage Guidelines

This command automatically enables service checking.

The NNTP service check provides a more thorough check than ping check, because the NNTP service check logs into the service.

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the global parameters, use the following command:

```
configure slb global nntp
```

Example

The following command configures the service check to log into the newsgroup "comp.dcom.lans.ethernet" on the virtual server "nntpvip":

```
configure slb vip nntpvip service-check nntp comp.dcom.lans.ethernet
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check pop3

```
configure slb vip <vip name> service-check pop3 user <user name> password
{encrypted} {password}
```

Description

Configures layer 7 POP3 service checking for a specific virtual server.

Syntax Description

vip name	Specifies a virtual server.
user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

N / A.

Usage Guidelines

This command automatically enables service checking.

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The POP3 service check provides a more thorough check than ping check, because the POP3 service check logs into the service.

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the global parameters, use the following command:

```
configure slb global pop3
```

Example

The following command configures the service check to login using the user name “service” and the password “check” to the virtual server “pop3vip”:

```
configure slb vip pop3vip service-check pop3 user service password check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check smtp

```
configure slb vip <vip name> service-check smtp {<dns domain>}
```

Description

Configures layer 7 SMTP service checking for a specific virtual server.

Syntax Description

vip name	Specifies a virtual server.
dns domain	Specifies the domain to check.

Default

N/A.

Usage Guidelines

This command automatically enables service checking.

The SMTP service check provides a more thorough check than ping check, because the SMTP service check accesses the service.

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the global parameters, use the following command:

```
configure slb global smtp
```

Example

The following command configures the service check to access the DNS domain servicecheck.domain.com on the virtual server “smtpvip”:

```
configure slb vip smtpvip service-check smtp servicecheck.domain.com
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure slb vip service-check telnet

```
configure slb vip <vip name> service-check telnet {user <user name>
password {encrypted} <password>}
```

Description

Configures layer 7 telnet service checking for a specific virtual server.

Syntax Description

vip name	Specifies a virtual server.
user	Specifies the user name that is checked.
password	Specifies the password for the user name.
encrypted	Encrypts the password stored in the configuration file.

Default

N / A.

Usage Guidelines

This command automatically enables service checking.

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The telnet service check provides a more thorough check than ping check, because the telnet service check logs into the service.

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the global parameters, use the following command:

```
configure slb global telnet
```

Example

The following command configures the service check to login using the user name “service” and the password “check” on the virtual server “telnetvip”:

```
configure slb vip telnetvip service-check telnet user service password check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure vlan slb-type

```
configure vlan <vlan name> slb-type [both | client | none | server]
```

Description

Marks a VLAN as either a server VLAN or a client VLAN.

Syntax Description

both	Configures the VLAN as both a server and a client VLAN.
client	Configures the VLAN as a client VLAN.
none	Disables SLB on the VLAN.
server	Configures the VLAN as a server VLAN.

Default

The default is none.

Usage Guidelines

Use the both option if a server originates or could possibly originate connections to other servers.

Example

The following command configures the VLAN “client_vlan” as a client VLAN:

```
configure vlan client_vlan slb-type client
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

create flow-redirect

```
create flow-redirect <flow redirect> [any | tcp | tup | udp] destination
[<ip address> / <mask> [ip-port <number> | src-ip-port <number>] | any]
source [<ip address> / <mask> | any]
```

Description

Creates a flow redirect policy.

Syntax Description

flow redirect	Specifies a flow redirect policy.
any	Forwards traffic using either TCP or UDP on any IP port.
tcp	Forwards TCP traffic on a single IP port.
tup	Forwards traffic using either TCP or UDP on a single IP port.
udp	Forwards traffic using only UDP on a single IP port.
ip address	Specifies an IP address.
ip-port	Specifies the destination TCP or UDP layer 4 port for traffic going to a destination range.
src-ip-port	Specifies the TCP or UDP layer 4 port for traffic coming from the source IP ranges to the destination IP ranges.
number	Specifies the port.

Default

N / A.

Usage Guidelines

Creating a flow redirect policy automatically enables flow redirect.

To delete a flow redirect policy, use the following command:

```
delete flow-redirect <flow redirect>
```

To rename or modify a flow redirect policy, you must delete and recreate the flow redirect policy.

Example

The following command creates a flow redirect policy named “http” that forwards TCP traffic to 10.1.1.10 port 80 from any source IP address:

```
create flow-redirect http tcp destination 10.1.1.10/29 ip-port 80 source any
```

History

This command was available in ExtremeWare 6.1.4. This command was modified in 6.2 to add the tup parameter.

Platform Availability

This command is available on all platforms.

create slb pool

```
create slb pool <pool name> {lb-method [least-connections | priority |
ratio | round-robin]}
```

Description

Creates a server pool and optionally assigns a load-balancing method to the pool.

Syntax Description

pool name	Specifies a pool.
lb-method	Specifies the load-balancing method.

Default

The default load-balancing method is round-robin.

Usage Guidelines

To change the load-balancing method of an existing pool, use the following command:

`configure slb pool <pool name> lb-method`

To add a node to the pool (and set the ratio or priority), use the following command:

`configure slb pool <pool name> add`

Example

The following command creates the pool “ftp_pool” and assigns the priority load-balancing method:

`configure slb pool ftp_pool lb-method priority`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

create slb vip

```
create slb vip <vip name> pool <pool name> mode [transparent | translation
| port-translation] <ip address> {- <upper range>} : <L4 port> {unit
<number>}
```

Description

Creates one or more new virtual servers.

Syntax Description

vip name	Specifies a virtual server.
pool name	Specifies a pool.
mode	Specifies the forwarding mode.
ip address	Specifies the IP address of the virtual server.
upper range	Specifies the upper IP address for a range of IP addresses.
L4 port	Specifies a port.
unit	Specifies a unit identifier on a virtual server. The range is 1 to 16.

Default

N/A.

Usage Guidelines

You must create the pool before assigning a virtual server to the pool. To create a pool, use the following command:

`create slb pool`

Example

The following command creates the virtual server “ftp_vip” with an IP address of 10.10.10.2 in the pool “ftp_pool” and assigns the port-translation forwarding mode:

```
configure slb vip ftp_vip pool ftp_pool mode port-translation 10.10.10.2 : ftp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

delete flow-redirect

```
delete flow-redirect <flow redirect>
```

Description

Deletes a flow redirect policy.

Syntax Description

flow redirect	Specifies a flow redirect policy.

Default

N/A.

Usage Guidelines

To rename or modify a flow redirect policy, you must delete and recreate the flow redirect policy.

Example

The following command deletes a flow redirect policy named “http”:

```
delete flow-redirect http
```

History

This command was available in ExtremeWare 6.1.4.

Platform Availability

This command is available on all platforms.

delete slb pool

```
delete slb pool [<pool name> | all]
```

Description

Deletes a server pool.

Syntax Description

pool name	Specifies a pool.
all	Specifies all pools.

Default

N/A.

Usage Guidelines

You must first delete all virtual servers before deleting the pool. To delete a virtual server, use the following command:

```
delete slb vip
```

Example

The following command the pool named “http_pool”:

```
delete slb pool http_pool
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

delete slb vip

```
delete slb vip [<vip name> | all]
```

Description

Deletes one or all virtual servers.

Syntax Description

vip name	Specifies a virtual server.
all	Specifies all virtual servers.

Default

N/A.

Usage Guidelines

You must use this command to delete all virtual servers from a pool before deleting the pool.

Example

The following command the virtual server named “http_vip”:

```
delete slb pool http_vip
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable flow-redirect

```
disable flow-redirect [all | <flow redirect>]
```

Description

Disables flow redirect.

Syntax Description

all	Specifies all flow policies.
flow redirect	Specifies a single flow redirect policy.

Default

The default parameter is all.

Flow redirect is disabled by default.

Usage Guidelines

When you create a new flow redirect policy, flow redirect is automatically enabled.

To enable flow redirect, use the following command:

```
enable flow-redirect
```

Example

The following command disables flow redirect for all flow policies:

```
disable flow-redirect all
```

History

This command was available in ExtremeWare 6.1.4.

Platform Availability

This command is available on all platforms.

disable slb

```
disable slb
```

Description

Disables SLB processing.

Syntax Description

This command has no arguments or variables.

Default

SLB is disabled by default.

Usage Guidelines

Disabling SLB causes the following to occur:

- Closes all connections.
- Withdraws virtual server routes or routes that do not respond with proxy ARP responses of virtual server addresses.
- Disconnects the switch from redundant SLB switches.

To enable SLB, use the following command:

```
enable slb
```

Example

The following command disables SLB:

```
disable slb
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb 3dns

```
disable slb 3dns iquery-client
```

Description

Disables 3DNS support.

Syntax Description

This command has no arguments or variables.

Default

3DNS is disabled by default.

Usage Guidelines

To enable 3DNS, use the following command:

`enable slb 3dns iquery-client`

Example

The following command disables 3DNS:

`disable slb 3dns iquery-client`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb failover

```
disable slb failover
```

Description

Disables the SLB failover mechanism.

Syntax Description

This command has no arguments or variables.

Default

SLB failover is disabled by default.

Usage Guidelines

To enable SLB failover, use the following command:

`enable slb failover`

Example

The following command disables SLB failover:

`disable slb failover`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb failover manual-failback

```
disable slb failover manual-failback
```

Description

Disables manual failback.

Syntax Description

This command has no arguments or variables.

Default

Manual failback is disabled by default.

Usage Guidelines

To enable manual failback, use the following command:

`enable slb failover manual-failback`

Example

The following command disables manual failback:

`disable slb failover manual-failback`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb failover ping-check

```
disable slb failover ping-check
```

Description

Disables ping-check to an external gateway.

Syntax Description

This command has no arguments or variables.

Default

Ping-check is disabled by default.

Usage Guidelines

To enable ping-check, use the following command:

`enable slb failover ping-check`

Example

The following command disables ping-check:

`disable slb failover ping-check`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb global synguard

```
disable slb global synguard
```

Description

Disables the TCP SYN-guard feature.

Syntax Description

This command has no arguments or variables.

Default

SYN-guard is disabled by default.

Usage Guidelines

To enable SYN-guard, use the following command:

`enable slb global synguard`

Example

The following command disables SYN-guard:

`disable slb global synguard`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb gogo-mode

```
disable slb gogo-mode <port number> {all}
```

Description

Disables GoGo mode processing.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Disables all health checking.

Default

GoGo mode is disabled by default.

Usage Guidelines

Before you disable GoGo mode, disconnect the servers, as they all have identical MAC and IP addresses, which can cause VLAN conflicts.

To enable GoGo mode, use the following command:

```
enable slb gogo-mode
```

Example

The following command disables GoGo mode for the group with port 29 as the master port:

```
disable slb gogo-mode 29
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb gogo-mode ping-check

```
disable slb gogo-mode <port number> ping-check
```

Description

Disables layer-3 ping-check to this GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.

Default

GoGo mode ping check is disabled by default.

Usage Guidelines

To enable ping-check for a GoGo mode group, use the following command:

`enable slb gogo-mode <port number> ping-check`

Example

The following command disables GoGo mode ping-check for the group with port 29 as the master port:

```
disable slb gogo-mode 29 ping-check
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

disable slb gogo-mode service-check

```
disable slb gogo-mode <port number> service-check [all | ftp | http | nntp
| pop3 | smtp | telnet | <TCP port number>]
```

Description

Disables layer 7 service check to this GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Specifies all service checks.
ftp	Specifies the FTP service check.
http	Specifies the HTTP service check.
nntp	Specifies the NNTP service check.
pop3	Specifies the POP3 service check.
smtp	Specifies the SMTP service check.
telnet	Specifies the telnet service check.
TCP port number	Specifies the TCP port, instead of the service.

Default

GoGo mode service check is disabled by default.

Usage Guidelines

To enable service-check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> service-check
```

Example

The following command disables GoGo mode FTP service-check for the group with port 29 as the master port:

```
disable slb gogo-mode 29 service-check ftp
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

disable slb gogo-mode tcp-port-check

```
disable slb gogo-mode <port number> tcp-port-check [all | ftp | http |
https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web |
www | <TCP port number>]
```

Description

Disables layer 4 TCP-port-check to this GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Specifies all TCP-port-checks.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
www	Specifies the www TCP-port-check.
TCP port number	Specifies the TCP port of the TCP-port-check.

Default

GoGo mode TCP-port-check is disabled by default.

Usage Guidelines

To enable TCP-port-check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> tcp-port-check
```

Example

The following command disables all GoGo mode TCP-port-checks for the group with port 29 as the master port:

```
disable slb gogo-mode 29 tcp-port-check all
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

disable slb L4-port

```
disable slb L4-port [all | ftp | http | https | imap4 | ldap | nntp | pop3
| smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port
number>]
```

Description

Disables one or all SLB ports.

Syntax Description

all	Specifies all nodes.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

N/A.

Usage Guidelines

To enable an SLB port, use the following command:

`enable slb L4-port`

Example

The following command disables SLB for FTP ports:

`disable slb L4-port ftp`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb node

```
disable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap |
nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or
UDP port number>]] {close-connections-now}
```

Description

Disables one or all nodes.

Syntax Description

all	Specifies all nodes.
ip address	Specifies an IP address.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.
close-connections-now	Immediately closes all open connections.

Default

N / A.

Usage Guidelines

This command stops nodes from accepting new connections; existing connections are not closed unless you specify `close-connections-now`. SLB continues to function with other nodes.

If you disable all nodes in a pool, all virtual servers associated with that pool are effectively disabled.

To enable a node, use the following command:

`enable slb node`

Example

The following command disables all nodes and immediately closes all open connections:

```
disable slb node all close-connections-now
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb node ping-check

```
disable slb node [all | <ip address>] ping-check
```

Description

Disables layer 3 ping-check.

Syntax Description

all	Specifies all nodes.
ip address	Specifies the IP address of the node.

Default

Ping-check is disabled by default.

Usage Guidelines

Ping-check is automatically enabled when a node is added to a pool.

To enable ping-check on a node, use the following command:

`enable slb node ping-check`

Example

The following command disables all ping-checks:

`disable slb node all ping-check`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb node tcp-port-check

```
disable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap |
nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or
UDP port number>]] tcp-port-check
```

Description

Disables layer 4 TCP-port-checking.

Syntax Description

all	Specifies all nodes.
ip address	Specifies an IP address.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

TCP-port-check is disabled by default.

Usage Guidelines

To enable TCP-port-check, use the following command:

```
enable slb node tcp-port-check
```

Example

The following command disables all TCP-port-checks:

```
disable slb node all tcp-port-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb proxy-client-persistence

```
disable slb proxy-client-persistence
```

Description

Disables proxy client persistence.

Syntax Description

This command has no arguments or variables.

Default

Proxy client persistence is disabled by default.

Usage Guidelines

To enable proxy client persistence, use the following command:

`enable slb proxy-client-persistence`

Example

The following command disables proxy client persistence:

`disable slb proxy-client-persistence`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb vip

```
disable slb vip [all | <vip name> | ipaddress <ip address> : [ftp | http |
https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web |
wildcard | www | <TCP or UDP port number>]] {close-connections-now}
```

Description

Disables one or all virtual servers.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.
ip address	Specifies an IP address.
ftp	Specifies an FTP virtual server.
http	Specifies an HTTP virtual server.
https	Specifies an HTTPS virtual server.
imap4	Specifies an IMAP4 virtual server.
ldap	Specifies an LDAP virtual server.
nntp	Specifies an NNTP virtual server.
pop3	Specifies a POP3 virtual server.
smtp	Specifies an SMTP virtual server.
socks	Specifies a SOCKS virtual server.
telnet	Specifies a telnet virtual server.
tftp	Specifies a TFTP virtual server.
web	Specifies a Web virtual server.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www virtual server
TCP or UDP port number	Specifies a TCP or UDP port for the virtual server.
close-connections-now	Immediately closes all open connections.

Default

SLB is disabled by default.

Usage Guidelines

When disabled, no new connections are allowed to the real servers. If `close-connections-now` is specified, all existing connections are immediately closed.

To enable a virtual server, use the following command:

`enable slb vip`

Example

The following command disables the virtual server “ftp_vip” and closes all open connections:

```
disable slb vip ftp_vip close-connections-now
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb vip client-persistence

```
disable slb vip [all | <vip name>] client-persistence
```

Description

Disables client persistence.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

Client persistence is disabled by default.

Usage Guidelines

To enable client persistence, use the following command:

```
enable slb vip client-persistence
```

Example

The following command disables client persistence for the virtual server “ftp_vip”:

```
disable slb vip ftp_vip client-persistence
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb vip service-check

```
disable slb vip [all | <vip name>] service-check
```

Description

Disables layer 7 service-check.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

Service-check is disabled by default.

Usage Guidelines

To enable service-check, use the following command:

`enable slb vip service-check`

Example

The following command disables service-check for the virtual server “ftp_vip”:

```
disable slb vip ftp_vip service-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb vip sticky-persistence

```
disable slb vip [all | <vip name>] sticky-persistence
```

Description

Disables sticky persistence.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

Sticky persistence is disabled by default.

Usage Guidelines

To enable sticky persistence, use the following command:

```
enable slb vip sticky-persistence
```

Example

The following command disables sticky persistence for the virtual server “ftp_vip”:

```
disable slb vip ftp_vip sticky-persistence
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable slb vip svcdown-reset

```
disable slb vip [all | <vip name>] svcdown-reset
```

Description

Disables svcdown-reset.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

The svcdown-reset feature is disabled by default.

Usage Guidelines

To enable svcdown-reset, use the following command:

```
enable slb vip svcdown-reset
```

Example

The following command disables svcdown-reset for the virtual server “ftp_vip”:

```
disable slb vip ftp_vip svcdown-reset
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable flow-redirect

```
enable flow-redirect [all | <flow redirect>]
```

Description

Enables flow redirect.

Syntax Description

all	Specifies all flow policies.
flow redirect	Specifies a single flow redirect policy.

Default

The default parameter is all.

Flow redirection is disabled by default.

Usage Guidelines

When you create a new flow redirect policy, flow redirect is automatically enabled.

To disable flow redirect, use the following command:

```
disable flow-redirect
```

Example

The following command enables flow redirect for all flow policies:

```
enable flow-redirect all
```

History

This command was available in ExtremeWare 6.1.4.

Platform Availability

This command is available on all platforms.

enable slb

```
enable slb
```

Description

Enables SLB processing.

Syntax Description

This command has no arguments or variables.

Default

SLB is disabled by default.

Usage Guidelines

This command activates the following functions for transparent, translational, and port translation modes:

- Exporting of VIP routes or proxy ARP for VIP addresses.
- Processing of VIP lookup and connection setup.
- Establishing communication with redundant SLB switches.
- Positively responding to MIB, 3DNS, and SeeIT requests.

Before you enable SLB, enable IP forwarding on the associated VLANs.

NOTE

SLB cannot be enabled when MPLS or Destination-sensitive accounting is enabled or SLPM is active.

Example

The following command enables SLB:

```
enable slb
```

History

This command was first available in ExtremeWare 6.1.

This command was updated in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was modified in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable slb 3dns

```
enable slb 3dns iquery-client
```

Description

Enables 3DNS support.

Syntax Description

This command has no arguments or variables.

Default

3DNS is disabled by default.

Usage Guidelines

The following 3DNS global balance modes are supported:

- completion
- rate
- global_availability
- leastcon
- null
- packet_rate
- random
- ration
- rr
- return_to_dns

To disable 3DNS, use the following command:

```
disable slb 3dns iquery-client
```

Example

The following command enables 3DNS:

```
enable slb 3dns iquery-client
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb failover

```
enable slb failover
```

Description

Enables SLB failover.

Syntax Description

This command has no arguments or variables.

Default

Failover is disabled by default.

Usage Guidelines

When SLB failover is enabled, the primary SLB switch automatically resumes primary status when it becomes active.

Before you enable SLB failover, configure your switches using the following command:

```
configure slb failover unit
```

To disable SLB failover, use the following command:

```
disable slb failover
```

Example

The following command enables SLB failover:

```
enable slb failover
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb failover manual-failback

```
enable slb failover manual-failback
```

Description

Enables manual failback.

Syntax Description

This command has no arguments or variables.

Default

Manual failback is disabled by default.

Usage Guidelines

When manual failback is enabled, the primary SLB switch does not automatically resume primary status until you use the following command:

```
configure slb failover failback-now
```

To disable manual failback, use the following command:

```
disable slb failover manual-failback
```

Example

The following command enables manual failback:

```
enable slb failover manual-failback
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb failover ping-check

```
enable slb failover ping-check
```

Description

Enables ping-check.

Syntax Description

This command has no arguments or variables.

Default

Ping-check is disabled by default.

Usage Guidelines

To disable ping-check, use the following command:

```
disable slb failover ping-check
```

Example

The following command enables ping-check:

```
enable slb failover ping-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb global synguard

```
enable slb global synguard
```

Description

Enables the TCP SYN-guard feature.

Syntax Description

This command has no arguments or variables.

Default

SYN-guard is disabled by default.

Usage Guidelines

To disable SYN-guard, use the following command:

```
disable slb global synguard
```

Example

The following command enables SYN-guard:

```
enable slb global synguard
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb gogo-mode

```
enable slb gogo-mode <port number> grouping <port list>
```

Description

Enables GoGo mode processing for a group of ports.

Syntax Description

port number	Specifies the GoGo mode master port.
port list	Specifies a range or list of ports assigned to the group.

Default

GoGo mode is disabled by default.

Usage Guidelines

To disable GoGo mode, use the following command:

```
disable slb gogo-mode
```

Example

The following command enables GoGo mode for the group containing ports 15, 17, 19-23, and 25-30 with port 29 as the master port:

```
enable slb gogo-mode 29 grouping 15, 17, 19 - 23, 25 - 30
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb gogo-mode ping-check

```
enable slb gogo-mode <port number> ping-check <ip address>
```

Description

Enables layer-3 ping-check for the GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
ip address	Specifies an IP address to be pinged.

Default

GoGo mode ping check is disabled by default.

Usage Guidelines

GoGo mode ping-check sends a ping from each physical port in the GoGo mode grouping to the configured IP address.

If you do not specify an IP address, GoGo mode ping-check uses the previously configured IP address.

You must enable GoGo mode for the group before you enable ping-check. To enable GoGo mode, use the following command:

```
enable slb gogo-mode
```

To disable ping-check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> ping-check
```

Example

The following command enables GoGo mode ping-check for the group with port 29 as the master port to IP address 10.10.200.3:

```
enable slb gogo-mode 29 ping-check 10.10.200.3
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

enable slb gogo-mode service-check

```
enable slb gogo-mode <port number> service-check [all | ftp | http | nntp |
pop3 | smtp | telnet | <TCP port number>]
```

Description

Enables layer 7 service checking for the GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Specifies all service checks.
ftp	Specifies the FTP service check.
http	Specifies the HTTP service check.
nntp	Specifies the NNTP service check.
pop3	Specifies the POP3 service check.
smtp	Specifies the SMTP service check.
telnet	Specifies the telnet service check.
TCP port number	Specifies the TCP port, instead of the service.

Default

GoGo mode service check is disabled by default.

Usage Guidelines

To disable service-check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> service-check
```

Example

The following command enables GoGo mode FTP service-check for the group with port 29 as the master port:

```
enable slb gogo-mode 29 service-check ftp
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

enable slb gogo-mode tcp-port-check

```
enable slb gogo-mode <port number> tcp-port-check [all | ftp | http | https
| imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www |
<TCP port number>]
```

Description

Enables layer 4 TCP-port-check for the GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Specifies all TCP-port-checks.
ftp	Specifies the FTP TCP-port-check.
http	Specifies the HTTP TCP-port-check.
https	Specifies the HTTPS TCP-port-check.
imap4	Specifies the IMAP4 TCP-port-check.
ldap	Specifies the LDAP TCP-port-check.
nntp	Specifies the NNTP TCP-port-check.
pop3	Specifies the POP3 TCP-port-check.
smtp	Specifies the SMTP TCP-port-check.
socks	Specifies the SOCKS TCP-port-check.
telnet	Specifies the telnet TCP-port-check.
tftp	Specifies the TFTP TCP-port-check.
web	Specifies the Web TCP-port-check.
www	Specifies the www TCP-port-check.
TCP port number	Specifies the TCP port of the TCP-port-check.

Default

GoGo mode TCP-port-check is disabled by default.

Usage Guidelines

To disable TCP-port-check for a GoGo mode group, use the following command:

```
disable slb gogo-mode <port number> tcp-port-check
```

Example

The following command enables all GoGo mode TCP-port-checks for the group with port 29 as the master port:

```
enable slb gogo-mode 29 tcp-port-check all
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

enable slb L4-port

```
enable slb L4-port [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp
| socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]
```

Description

Enables an SLB port.

Syntax Description

ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

Layer 4 ports are enabled by default.

Usage Guidelines

To disable a layer 4 port, use the following command:

```
disable slb L4-port
```

Example

The following command enables SLB for FTP ports:

```
enable slb L4-port ftp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb node

```
enable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap |
nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or
UDP port number>]]
```

Description

Enables one or all nodes.

Syntax Description

all	Specifies all nodes.
ip address	Specifies an IP address.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

Nodes are enabled by default.

Usage Guidelines

This command allows nodes to accept new connections.

To disable a node, use the following command:

```
disable slb node
```

Example

The following command enables all nodes:

```
enable slb node all
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb node ping-check

```
enable slb node [all | <ip address>] ping-check
```

Description

Enables layer 3 ping-check.

Syntax Description

all	Specifies all nodes.
ip address	Specifies the IP address of the node.

Default

Ping-check is enabled by default.

Usage Guidelines

Ping-check is automatically enabled when a node is added to a pool.

To disable ping-check on a node, use the following command:

```
disable slb node ping-check
```

Example

The following command enables all ping-checks:

```
enable slb node all ping-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb node tcp-port-check

```
enable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap |
nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or
UDP port number>]] tcp-port-check
```

Description

Enables layer 4 TCP-port-check.

Syntax Description

all	Specifies all nodes.
ip address	Specifies an IP address.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

TCP-port-check is disabled by default.

Usage Guidelines

To disable TCP-port-check, use the following command:

```
disable slb node tcp-port-check
```

Example

The following command enables all TCP-port-checks:

```
enable slb node all tcp-port-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb proxy-client-persistence

```
enable slb proxy-client-persistence
```

Description

Enables proxy client persistence.

Syntax Description

This command has no arguments or variables.

Default

Proxy client persistence is disabled by default.

Usage Guidelines

To disable proxy client persistence, use the following command:

`disable slb proxy-client-persistence`

Example

The following command enables proxy client persistence:

`enable slb proxy-client-persistence`

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb vip

```
enable slb vip [all | <vip name> | ipaddress <ip address> : [ftp | http |
https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web |
wildcard | www | <TCP or UDP port number>]]
```

Description

Enables one or all virtual servers.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.
ip address	Specifies an IP address.
ftp	Specifies an FTP virtual server.
http	Specifies an HTTP virtual server.
https	Specifies an HTTPS virtual server.
imap4	Specifies an IMAP4 virtual server.
ldap	Specifies an LDAP virtual server.
nntp	Specifies an NNTP virtual server.
pop3	Specifies a POP3 virtual server.
smtp	Specifies an SMTP virtual server.
socks	Specifies a SOCKS virtual server.
telnet	Specifies a telnet virtual server.
tftp	Specifies a TFTP virtual server.
web	Specifies a Web virtual server.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www virtual server
TCP or UDP port number	Specifies a TCP or UDP port for the virtual server.

Default

SLB is disabled by default.

Usage Guidelines

To disable a virtual server, use the following command:

```
disable slb vip
```

Example

The following command enables the virtual server “ftp_vip”:

```
enable slb vip ftp_vip
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb vip client-persistence

```
enable slb vip [all | <vip name>] client-persistence {netmask <netmask>}
```

Description

Enables client persistence.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.
netmask	Specifies a netmask.

Default

The default is disabled.

Usage Guidelines

To disable client persistence, use the following command:

```
disable slb vip client-persistence
```

Example

The following command enables client persistence for the virtual server “ftp_vip”:

```
enable slb vip ftp_vip client-persistence
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb vip service-check

```
enable slb vip [all | <vip name>] service-check
```

Description

Enables layer 7 service check.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

Service-check is disabled by default.

Usage Guidelines

The service checks are based on the following information:

- If a service check is already configured, then it will use the configured service-checking information.
- If a service-check is configured for a TCP port number (instead of for a service), ExtremeWare assigns the service based on the port number (if the port number is well known) and uses the global default parameters.

To disable service-check, use the following command:

```
disable slb vip service-check
```

Example

The following command enables service-check for the virtual server “ftp_vip”:

```
enable slb vip ftp_vip service-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb vip sticky-persistence

```
enable slb vip [all | ipaddress <ip address> | <vip name>]
sticky-persistence {netmask <netmask>}
```

Description

Enables the sticky persistence feature and specifies the client address mask.

Syntax Description

all	Specifies all virtual servers.
ip address	Specifies an IP address.
vip name	Specifies a virtual server.
netmask	Specifies a netmask.

Default

Sticky persistence is disabled by default.

Usage Guidelines

To disable sticky persistence, use the following command:

```
disable slb vip sticky-persistence
```

Example

The following command enables sticky persistence for the virtual server “ftp_vip”:

```
enable slb vip ftp_vip sticky-persistence
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable slb vip svcdown-reset

```
enable slb vip [all | <vip name>] svcdown-reset
```

Description

Enables svcdown-reset.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

The svcdown-reset feature is disabled by default.

Usage Guidelines

The svcdown-reset feature configures the switch to send TCP RST packets to both the clients and the virtual server if the virtual server fails a health-check.

To disable svcdown-reset, use the following command:

```
disable slb vip svcdown-reset
```

Example

The following command enables svcdown-reset for the virtual server “ftp_vip”:

```
enable slb vip ftp_vip svcdown-reset
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show flow-redirect

```
show flow-redirect <flow redirect>
```

Description

Displays the current flow redirect configuration and statistics.

Syntax Description

flow redirect	Specifies a flow redirect policy.

Default

N/A.

Usage Guidelines

If you do not specify a flow redirect policy, configuration and statistics for all flow redirect policies are displayed.

Following are the fields displayed:

Service Check Timer Settings:	Displays the frequency and timeout settings for the flow-redirect ping-check, TCP-port-check, and service-check.
Flow IPSA Mode	Displays the IP source address mode: • Enumeration Mode—The default mode, used for network masks from /32 to /20. • Subnet Mode—Used for network masks from /19 to /1. The mode is selected automatically when you specify a network mask.
Proto:	Displays the flow type. • any—Forwards any traffic over any IP port. • tcp—Forwards TCP traffic over a single IP port. • tup—Forwards both TCP and UDP traffic over a single IP port. • udp—Forwards UDP traffic over a single IP port.
Dest:	Displays the desitnation IP address.
L4-src-port:	Displays the source port number.
Enabled:	Displays status of flow-redirect. • Yes—Flow redirect is enabled. • No—Flow redirect is not enabled.
Source:	• Displays the source IP address.
# Servers Up:	Displays the number of next hops up over the number of next hops configured.

Service Checking:	Displays the configured service check type. • ftp • http • L4-port • nntp • ping • pop3 • smtp • telnet
IP Address	Displays the IP address of the next hop.
State	Displays the status of the next hop, either up or down.
Flow Info	Displays hardware mapping information.

Example

The following command displays the current flow redirect configuration and statistics for the flow policy “flow1”:

```
show flow-redirect flow1
```

Following is the output from this command:

```
Service Check Timer Settings:
  Ping-check     Frequency:  10  Timeout:  30
  TCP-Port-check Frequency:  10  Timeout:  30
  Service-check  Frequency:  60  Timeout: 180

Flow IPSA Mode: Enumeration Mode

http1
        Proto:tcp  Dest:      0.0.0.0/ 0  L4-Port:    80   Enabled: yes
                   Source:    0.0.0.0/ 0              # Servers Up: 0/1
        Service Checking: ping
        IP Address      State   Flow Info
        24.3.89.145     Down    0000
```

History

This command was available in ExtremeWare 6.1.4.

Platform Availability

This command is available on all platforms.

show slb 3dns members

```
show slb 3dns members
```

Description

Displays the current connection information between the switch and the 3DNS querier.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the current 3DNS information:

```
show slb 3dns members
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb connections

```
show slb connections [ipaddress <ip address>: [ftp | http | https | imap4 |
ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www |
<TCP or UDP port number>] | vip <vip name>]
```

Description

Displays information on current connections.

Syntax Description

ip address	Specifies an IP address.
vip name	Specifies a virtual server.
ftp	Specifies an FTP port.
http	Specifies an HTTP port.
https	Specifies an HTTPS port.
imap4	Specifies an IMAP4 port.
ldap	Specifies an LDAP port.
nntp	Specifies an NNTP port.
pop3	Specifies a POP3 port.
smtp	Specifies an SMTP port.
socks	Specifies a SOCKS port.
telnet	Specifies a telnet port.
tftp	Specifies a TFTP port.
web	Specifies a Web port.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www port
TCP or UDP port number	Specifies a TCP or UDP port.

Default

N / A.

Usage Guidelines

You can specify a client, virtual server, or node. If you do not specify a virtual server or IP address, information on all connections is displayed. An IP address of 0.0.0.0:0 is a wildcard.

Example

The following command displays the current connection information for all connections:

```
show slb connections
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb esrp

```
show slb esrp
```

Description

Displays SLB configuration for ESRP.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the current ESRP configuration:

```
show slb esrp
```

Following is the output from this command:

```
VLAN Name  SLB Unit Status    SLB Unit(s)
servers    Standby            1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb failover

```
show slb failover
```

Description

Displays SLB failover configuration and status.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The `show slb global` command also displays SLB failover configuration and status.

Example

The following command displays the current SLB failover configuration and status:

```
show slb failover
```

Following is the output from this command:

```
SLB Failover Configuration:
 Failover: Enabled
 Local unit ID: 1
 Local IP address: 10.1.1.1
 Remote IP address: 10.1.1.2
 TCP port number: 1028
 Remote Alive frequency: 1
 Remote Dead frequency: 2
 Keepalive Timeout: 3
 Ping check: Disabled
 Ping check IP address: 0.0.0.0
 Ping frequency: 1
 Ping timeout: 3
 Manual failback: Disabled
#
#
SLB Failover Status: Running
 Units active in local SLB: 2
 Units active in or
  requested by remote SLB: None
 Send connection: Down
 Receive connection: Down
 Ping check: Not Running
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb global

```
show slb global
```

Description

Displays the current SLB global configuration information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Displays the following:

- Global enable/disable mode
- Global modes
- Default settings for health checker
- Failover configuration

Example

The following command displays the current SLB global configuration information:

```
show slb global
```

Following is the output from this command:

```
SLB: Enabled
SynGuard: Disabled
3DNS IQuery Support Status: Disabled
SLB persist-level: same-vip-same-port
SLB persistence-method: per-session
SLB pre-allocated connection-block size: 10000
SLB connection timeout: 1
SLB persistence on client proxies: Disabled
Proxy Client Persistence entries:
No. of Proxy Client Persistence entries: 0
#
#
Health Check Defaults:
  Ping-check    Frequency: 10  Timeout: 30
  Port-check    Frequency: 30  Timeout: 90
  Service-check Frequency: 60  Timeout: 180
  HTTPURL: "/"
     Match String: (any-content)
  FTP User: anonymous
     Password: (not shown)
  TelnetUser: anonymous
```

```
      Password: (not shown)
  SMTPDomain: "mydomain.com"
      NNTP Newsgroup: "ebusiness"
      User: anonymous
      Password: (not shown)
  POP3User: anonymous
      Password: (not shown)
#
#
SLB Failover Configuration:
Failover: Enabled
 Local unit ID: 1
 Local IP address: 10.1.1.1
 Remote IP address: 10.1.1.2
 TCP port number: 1028
 Remote Alive frequency: 1
 Remote Dead frequency: 2
 Keepalive Timeout: 3
 Ping check: Disabled
 Ping check IP address: 0.0.0.0
 Ping frequency: 1
 Ping timeout: 3
 Manual failback: Disabled
#
#
SLB Failover Status: Running
 Units active in local SLB: 2
 Units active in or
  requested by remote SLB: None
 Send connection: Down
 Receive connection: Down
 Ping check: Not Running
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb gogo-mode

```
show slb gogo-mode <port number> {configuration}
```

Description

Displays GoGo mode ping-check, TCP-port-check, and service-check status.

Syntax Description

port number	Specifies the GoGo mode master port.
configuration	Displays configuration instead of status.

Default

N/A.

Usage Guidelines

If you do not specify a master port, status for all GoGo mode groups with health checks configured is displayed.

Example

The following command displays the current GoGo mode health check configuration for the group with port 29 as the master port:

```
show slb gogo-mode 29 configuration
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

show slb L4-port

```
show slb L4-port [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp |
socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]
```

Description

Displays the SLB configuration for the active layer 4 ports.

Syntax Description

ftp	Specifies an FTP port.
http	Specifies an HTTP port.
https	Specifies an HTTPS port.
imap4	Specifies an IMAP4 port.
ldap	Specifies an LDAP port.
nntp	Specifies an NNTP port.
pop3	Specifies a POP3 port.
smtp	Specifies an SMTP port.
socks	Specifies a SOCKS port.
telnet	Specifies a telnet port.
tftp	Specifies a TFTP port.
web	Specifies a Web port.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www port
TCP or UDP port number	Specifies a TCP or UDP port.

Default

N/A.

Usage Guidelines

If you do not specify a port, configuration and status for all layer 4 ports is displayed.

Example

The following command displays the current layer 4 port configuration:

```
show slb L4-port
```

Following is the output from this command:

```
Port:    80  Enabled  TCP idle timeout (treaper): 600  UDP idle timeout: 600
```

History

This command was first available in ExtremeWare 6.1.

show slb node

```
show slb node {<ip address> [ftp | http | https | imap4 | ldap | nntp |
pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP
port number>]}
```

Description

Displays node configuration and status.

Syntax Description

ip address	Specifies an IP address.
ftp	Specifies an FTP node.
http	Specifies an HTTP node.
https	Specifies an HTTPS node.
imap4	Specifies an IMAP4 node.
ldap	Specifies an LDAP node.
nntp	Specifies an NNTP node.
pop3	Specifies a POP3 node.
smtp	Specifies an SMTP node.
socks	Specifies a SOCKS node.
telnet	Specifies a telnet node.
tftp	Specifies a TFTP node.
web	Specifies a Web node.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www node
TCP or UDP port number	Specifies a TCP or UDP port for the node.

Default

N/A.

Usage Guidelines

If you do not specify a node, status for all nodes is displayed.

Example

The following command displays the current node configuration and statistics for all nodes:

```
show slb node
```

Following is the output from this command:

```
                    IP     Freq/        TCP/UDP      Frequency/Max
Node IP Address    Flags   Timeout    Port    Flags   Timeout#PoolsConns
1.111.1.1          E--H--  10/30      80      E---    30/90 2(no limit)
1.111.1.2          E--H--  10/30      80      E---    30/90 2(no limit)
1.111.1.3          E--H--  10/30      80      E---    30/90 2(no limit)

Flags: E - Enable,   U - Up,   R - IP Route Up,   H - Health check enabled,
       P - Health check passed,   ! - VLAN not configured with "slb-type"
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb persistence

```
show slb persistence
```

Description

Displays persistence status of existing clients.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the current persistence status:

```
show slb persistence
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb pool

```
show slb pool <pool name>
```

Description

Displays the current SLB pool configuration and status.

Syntax Description

pool name	Specifies a pool.

Default

N/A.

Usage Guidelines

If you do not specify a pool, configuration and status for all pools is displayed.

Example

The following command displays the current pool configuration and statistics for all pools, currently "rr_pool" and "ratio_pool":

```
show slb pool
```

Following is the output from this command:

```
Name                        IP                  TCP/UDP    Ratio/
      IP                   Flags      Port      Flags      Priority
-------------------------------------------------------------------
rr_pool               # VIPs sharing: 1  Load Bal. Method: Round Robin
      1.111.1.1         E--H--     80      E---
      1.111.1.2         E--H--     80      E---
      1.111.1.3         E--H--     80      E---
ratio_pool            # VIPs sharing: 1  Load Bal. Method: Ratio
      1.111.1.3         E--H--     80      E---      3
      1.111.1.2         E--H--     80      E---      2
      1.111.1.1         E--H--     80      E---      1

Flags: E - Enable,   U - Up,   R - IP Route Up,   H - Health check enabled,
       P - Health check passed,   ! - VLAN not configured with "slb-type"
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb stats

```
show slb stats [pool <pool name> | vip <vip name>]
```

Description

Displays the current SLB pool connection status.

Syntax Description

pool name	Specifies a pool.
vip name	Specifies a virtual server.

Default

N/A.

Usage Guidelines

If you specify `pool` but do not specify a specific pool, status for all pools is displayed.

If you specify `vip` but do not specify a specifuc virtual server, status for all virtual servers is displayed.

If you do not specify a pool or virtual server, status for all pools and virtual servers is displayed.

Example

The following command displays the current pool connection status for all pools:

```
show slb stats pool
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show slb vip

```
show slb vip [<vip name> | ipaddress <ip address> : [ftp | http | https |
imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard
| www | <TCP or UDP port number>]] {detail}
```

Description

Displays the current virtual server configuration and statistics.

Syntax Description

vip name	Specifies a virtual server.
ip address	Specifies an IP address.
ftp	Specifies an FTP virtual server.
http	Specifies an HTTP virtual server.
https	Specifies an HTTPS virtual server.
imap4	Specifies an IMAP4 virtual server.
ldap	Specifies an LDAP virtual server.
nntp	Specifies an NNTP virtual server.
pop3	Specifies a POP3 virtual server.
smtp	Specifies an SMTP virtual server.
socks	Specifies a SOCKS virtual server.
telnet	Specifies a telnet virtual server.
tftp	Specifies a TFTP virtual server.
web	Specifies a Web virtual server.
wildcard	Specifies any port associated with a wildcard server.
www	Specifies a www virtual server
TCP or UDP port number	Specifies a TCP or UDP port for the virtual server.

Default

N/A.

Usage Guidelines

If you do not specify a virtual server or IP address, information on all virtual servers is displayed.

Example

The following command displays the current virtual server configuration and statistics for all virtual servers, currently “ratio_vip” and “rr_vip”:

```
show slb vip
```

Following is the output from this command:

```
                                        Unit   Export     # Servers
Name              IP Address         Port -- Mode --  FlagsPool     Up/Defined
ratio_vip         4.1.1.100          80    1  TL  SR  EUA-----ratio_po0/3
rr_vip            10.1.1.10          80    1  TP  PA  EUA----!rr_pool0/3

Modes: TP - Transparent,  TL - Translational,  PT - Port Translational
Automatically Exported via: PA - Proxy Arp, HR - Host Route, SR - Subnet Route
Flags: E - Enable,  U - Up,  A - Active Unit,  H - Health-Check Enabled,
       P - Persistence,  S - Sticky,  R - SvcDown-Reset,
       ! - VLAN has not been configured with "slb-type"
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

unconfigure slb all

```
unconfigure slb all
```

Description

Resets SLB global defaults and clears the SLB configuration.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command does not delete nodes, pools, or virtual servers. To delete all nodes and pools, use the following command:

```
delete slb pool all
```

To delete all virtual servers, use the following command:

```
delete slb vip all
```

Example

The following command resets SLB global defaults and clears the SLB configuration:

```
unconfigure slb all
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

unconfigure slb gogo-mode health-check

```
unconfigure slb gogo-mode <port number> health-check
```

Description

Disables and deletes all the ping-check, TCP-port-check, and service-check configurations for this GoGo mode group.

Syntax Description

port number	Specifies the GoGo mode master port.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes all health-check configurations for the GoGo mode group with port 29 as the master port:

```
unconfigure slb gogo-mode 29 health-check
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

unconfigure slb gogo-mode service-check

```
unconfigure slb gogo-mode <port number> service-check [all | ftp | http |
nntp | pop3 | smtp | telnet | <TCP port number>]
```

Description

Disables and deletes the GoGo mode service-check configuration.

Syntax Description

port number	Specifies the GoGo mode master port.
all	Specifies all service checks.
ftp	Specifies the FTP service check.
http	Specifies the HTTP service check.
nntp	Specifies the NNTP service check.
pop3	Specifies the POP3 service check.
smtp	Specifies the SMTP service check.
telnet	Specifies the telnet service check.
TCP port number	Specifies the TCP port, instead of the service.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables and deletes all the FTP service-check configuration for the GoGo mode group with port 29 as the master port:

```
unconfigure slb gogo-mode 29 service-check ftp
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

unconfigure slb vip service-check

```
unconfigure slb vip [all | <vip name>] service-check
```

Description

Disables and deletes the service check configuration.

Syntax Description

all	Specifies all virtual servers.
vip name	Specifies a virtual server.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables and deletes the FTP service-check configurations for the virtual server “ftp_vip:

```
unconfigure slb vip ftp_vip service-check
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

10 Commands for Status Monitoring and Statistics

This chapter describes:

- Commands for configuring and managing the Event Management System/Logging
- Commands for enabling and disabling NetFlow flow statistics collection
- Commands for configuring flow-collection port and filtering options
- Commands for configuring the flow-collector devices to which NetFlow datagrams are exported

When an event occurs on a switch, the Event Management System (EMS) allows you to send messages generated by these events to a specified log target. You can send messages to the memory buffer, NVRAM, the console display, the current session, or to a syslog host. The log messages contain configuration and fault information pertaining to the device. The log messages can be formatted to contain various items of information, but typically a message will consist of:

- Timestamp: The timestamp records when the event occurred.
- Severity level:
  - Critical: A desired switch function is inoperable. The switch may need to be reset.
  - Error: A problem is interfering with normal operation.
  - Warning: An abnormal condition exists that may lead to a function failure.
  - Notice: A normal but significant condition has been detected; the system is functioning as expected.
  - Info: Actions and events that are consistent with expected behavior.
  - Debug-Summary, Debug-Verbose, and Debug -Data: Information that is useful when performing detailed trouble shooting procedures.

  By default, log entries that are assigned a critical, error, or warning level are considered static entries and remain in the NVRAM log target after a switch reboot.
- Component: The component refers to the specific functional area to which the error refers.
- Message: The message contains the log information with text that is specific to the problem.

The switch maintains a configurable number of messages in its internal (memory-buffer) log (1000 by default). You can display a snapshot of the log at any time. In addition to viewing a snapshot of the log, you can configure the system to maintain a running real-time display of log messages on the console display or telnet session. In addition to maintaining an internal log, the switch supports remote logging by way of the UNIX syslog host facility.

NetFlow Statistics

NetFlow flow statistics provides a way for a switch to capture and export traffic classification or precedence information as data traverses, or flows, across portions of a network. A network flow is defined as a unidirectional sequence of packets between a particular source device and destination device that share the same protocol and transport-layer information. Flows are defined by the combination of their source IP address, destination IP address, source port, destination port, and protocol type.

NetFlow records are unidirectional in nature, which means that two flow records are maintained for a typical TCP connection: one record for flow in the ingress direction; a second for the flow in the egress direction. Records are maintained only for TCP and UDP flows. Flow records are grouped together into UDP datagrams for export to a flow-collector device. A NetFlow Version 1 export datagram can contain up to 25 flow records.

The IP addresses (or hostnames) and UDP port numbers of the available flow collectors can be configured on a per-switch basis. The ExtremeWare NetFlow implementation also enables a single port to distribute statistics across multiple groups of flow-collector devices. The NetFlow distribution feature is enabled by configuring export distribution groups that contain the addresses of multiple flow-collector devices. The feature uses a distribution algorithm that ensures all of the records for a given flow are exported to the same collector. The algorithm also ensures that the flow records of the ingress direction of a TCP or UDP connection are exported to the same collector. For Ethernet applications, only ingress traffic is monitored on Ethernet ports.

By default, each Ethernet port configured for flow switching maintains statistics for all the flows traversing the link in the ingress direction. Generalized filtering options exist that enable you to configure an Ethernet port to maintain statistics selectively for only those flows that match a specified filter. Up to eight filters are supported for each Ethernet port, with a total of 128 filters possible per each I/O module.

NOTE

Some of the NetFlow commands are implemented differently in the version of ExtremeWare that supports the PoS module, than in ExtremeWare 6.2 or later. Commands or options unique to the PoS module are indicated in the comments, or are documented separately in Chapter 22.

clear counters

```
clear counters
```

Description

Clears all switch statistics and port counters, including port packet statistics, bridging statistics, IP statistics, log event counters, and MPLS statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

You should view the switch statistics and port counters before you clear them. Use the `show port` command to view port statistics. Use the `show log counters` command to show event statistics.

Viewing and maintaining statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. By clearing the counters, you can see fresh statistics for the time period you are monitoring.

Example

The following command clears all switch statistics and port counters:

```
clear counters
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

clear log

```
clear log {diag-status | error-led | static | messages [memory-buffer |
nvram]}
```

Description

Clears the log database.

Syntax Description

diag-status	Clears the hardware error code.
error-led	Clears the ERR LED on the MSM.
static	Specifies that the messages in the NVRAM target are cleared, and the ERR LED on the MSM is cleared.
memory-buffer	Clears entries from the memory buffer..
nvram	Clears entries from NVRAM

Default

N/A.

Usage Guidelines

The switch log tracks configuration and fault information pertaining to the device.

By default, log entries that are sent to the NVRAM remain in the log after a switch reboot. The `clear log` and `clear log messages memory-buffer` commands remove entries in the memory buffer target; the `clear log static` and `clear log messages nvram` commands remove messages from the NVRAM target as well as the memory buffer target.

When there is a hardware failure, a hardware error code might be saved to the FLASH or NVRAM (depending on the switch configuration). Upon reboot, the switch will not try to bring up a card with an error code, so it will be shown in a failed state. Use the `clear log diag-status` command to clear the hardware error code, so the module can be brought up after the next reboot. This command clears the state for all the modules.

There are three ways to clear the ERR LED. Clear the log, reboot the switch, or use the `clear log error-led` command. To clear the ERR LED without rebooting the switch or clearing the log messages, use the `clear log error-led` command.

Example

The following command clears all log messages, from the NVRAM:

```
clear log static
```

History

This command was first available in ExtremeWare 2.0.

The `diag-status` option was added in ExtremeWare 7.0.0.

The `error-led` option was added in ExtremeWare 7.1.0

The `messages` option was added in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

clear log counters

```
clear log counters {<event condition> | [all | <event component>] {severity
<severity> {only}}}
```

Description

Clears the incident counters for events.

Syntax Description

event condition	Specifies the event condition counter to clear.
all	Specifies that all events counters are to be cleared.
event component	Specifies that all the event counters associated with a particular component should be cleared.
severity	Specifies the minimum severity level of event counters to clear (if the keyword only is omitted).
only	Specifies that only event counters of the specified severity level are to be cleared.

Default

If severity is not specified, then the event counters of any severity are cleared in the specified component.

Usage Guidelines

This command sets the incident counters to zero for each event specified. To display event counters, use the following command:

```
show log counters
```

See the command `show log` on page 666 for more information about severity levels.

To get a listing of the event conditions in the system, use the following command:

```
show log events {detail}
```

To get a listing of the components present in the system, use the following command:

```
show log components
```

Example

The following command clears the event counters for event conditions of severity error or greater in the component *BGP*:

```
clear log counters "BGP" severity error
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

clear transceiver-test

```
clear transceiver-test
```

Description

Clears (resets) the transceiver test statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

To display the transceiver test statistics, use the `show diagnostics sys-health-check` command. The following is sample output:

```
Transceiver system health diag result
Pass/Fail Counters Are in HEX
Slot    Cardtype Cardstate   Test        Pass     Fail Time_last_fail
----    -------- ---------   ----    -------- -------- --------------
slot 1  Unknown
slot 2  Unknown
slot 3  FM8V     Operational MAC        2b81b        0
slot 4  GM4X     Operational MAC        2b81b        0
BPLNE   SMMI     Operational UART       2b81a        0
BPLNE   SMMI     Operational FLASH      2b81a        0
BPLNE   SMMI     Operational SRAM       2b81a        0
BPLNE   SMMI     Operational NVRAM      2b81a        0
BPLNE   SMMI     Operational ENET       2b81a        0
BPLNE   Basbrd   Operational QUAKE      2b81a        0
BPLNE   Basbrd   Operational TWISTER    2b81a        0
```

Example

The following command clears (resets) all of the transceiver test statistics:

```
clear transceiver-test
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

configure flowstats export add port

```
configure flowstats export <group#> add [<ipaddress> | <hostname>]
<udp_port>
```

Description

Adds a flow-collector device to an export group to which NetFlow datagrams are exported.

Syntax Description

group#	Specifies the export group to which the specified flow-collector device should be added. The group number is an integer in the range of 1-32.
ipaddress	Specifies the IP address of a flow-collector destination.
hostname	Specifies the host name of a flow-collector destination.
udp_port	Specifies a UDP port for the destination flow-collector.

Default

N/A.

Usage Guidelines

You can configure up to 32 export distribution groups. Each group may contain up to eight flow-collection devices. At least one flow-collector destination must be configured for NetFlow datagrams to be exported to a group.

When multiple flow-collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations. This NetFlow-distribution feature enables a scalable collection architecture that is able to accommodate high volumes of exported data. The distribution algorithm ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that flow records for both the ingress and egress directions of a TCP or UDP connection are exported to the same collector (when both flows traverse the same link and both filters are configured to export to the same group).

Issuing this command also enables the collection of NetFlow statistics.

See Chapter 22 for information on a similar command for the PoS module (BlackDiamond switch only).

Example

The following command adds the flow-collector device with IP address 10.205.30.15 using UDP port 2025 to export group 5 for this switch:

```
configure flowstats export 5 add 10.205.30.15 2025
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.This command is available on all platforms.

configure flowstats export delete port

```
configure flowstats export <group#> delete [<ipaddress> | <hostname>]
<udp_port>
```

Description

Removes a flow-collector device from an export group to which NetFlow datagrams are exported.

Syntax Description

group#	Specifies the export group to which the specified flow-collector device belongs. The group number is an integer in the range of 1-32.
ipaddress	Specifies the IP address of the flow-collector destination.
hostname	Specifies the host name of the flow-collector destination.
udp_port	Specifies a UDP port of the destination flow-collector.

Default

N/A.

Usage Guidelines

See Chapter 22 for information on a similar command for the PoS module (BlackDiamond switch only).

Example

The following command removes the flow-collector device with IP address 10.205.30.15 using UDP port 2025 from export group 5 on this switch:

```
configure flowstats export 5 delete 10.205.30.15 2025
```

History

This command first available in ExtremeWare 6.2 for "*i*" series platforms.

Platform Availability

This command is available on all platforms.

configure flowstats filter ports

```
configure flowstats filter <filter#> {aggregation} {export <group#>} ports
<portlist> [ingress | egress] <filterspec>
```

Description

Configures a flow record filter for the specified ports.

Syntax Description

filter#	The `filter#` parameter is an integer in the range from 1 to 8 that identifies the filter being defined.
<group#>	Specifies the group number that identifies the set of flow collector devices to which records for flows matching the filter are to be exported. If Group is not specified, then group # 1 will be used as default export group.
aggregation	To reduce the volume of exported data, use this optional keyword to maintain a single set of statistics for all the flows that match the specified filter.
filterspec	Specifies a set of five parameters (four are value/mask pairs) that define the criteria by which a flow is evaluated to determine if it should be exported. The parameters are: `[{dest-ip <ipaddress_value/mask ipaddress_filtermask>} {source-ip <ipaddress_value/mask ipaddress_filtermask>} {dest-port <port_value/port_filtermask>} {source-port <port_value/port_filtermask>} {protocol <tcp/udp/ip/protocol_value/protocol_filtermask>} | match-all-flows |match-no-flows]` All five specifications must be included in the order specified. The range for port/port_mask is calculated using the following formula: (minport = port, maxport = 2^(32-port_mask)-1). Conceptually, the filters work by ANDing the contents of each of the five components of a forwarded flow with the associated masks from the first defined filter (filter #1). Statistics are maintained if the results of the AND operations match the configured filter values for all fields of the sequence. If there is no match, then the operation is repeated for filter #2, and so on. If there is no match for any of the filters, then statistics are not maintained for the flow. Filters for any or all of the sequence components can be configured with a single command.
match-all-flows	Specifies that the filter should match any flow.
match-no-flows	Specifies that the filter should discard all flow. This option is not valid for Ethernet blades.
egress	Specifies that the filter should capture only egress traffic. This option is not valid for Ethernet blades.
ingress	Specifies that the filter should capture only ingress traffic.

Default

N / A.

Usage Guidelines

Configuring a filter specification enables that filter for the specified ports. To specify all ports, you can use specify them as the range of all ports (such as 1-32 or 7:1-7:4) or in the form <slot>:* on a modular switch.

Each Ethernet port supports eight filters for ingress flows.

Conceptually, the filters work by ANDing the contents of each of the five components of a forwarded flow with the associated masks from the first defined filter (filter #1). Statistics are maintained if the results of the AND operations match the configured filter values for all fields of the sequence. If there is no match, then the operation is repeated for filter #2, and so on. If there is no match for any of the filters, then statistics are not maintained for the flow. Filters for any or all of the sequence components can be configured with a single command.

Example

The following command example configures filter 2 to collect aggregate statistics for all traffic flowing through ports 1-8 from the 192.170.0.0/16 subnet to the 192.171.132.0/24 subnet:

```
configure flowstats filter 2 aggregation export 1 ports 1-8 ingress dest-ip
192.171.132.0/24 source-ip 192.170.0.0/16 dest-port 0/0 source-port 0/0 protocol ip
```

The following command configures filter 3 to collect statistics on any flows for ports 4-32 that did not match the filters defined in filters 1 and 2:

```
configure flowstats filter 3 aggregation export 1 ports 4-32 ingress match-all-flows
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure flowstats source

```
configure flowstats source ipaddress <ipaddress>
```

Description

Configures the IP address that is to be used as the source IP address for NetFlow datagrams to be exported.

Syntax Description

ipaddress	Specifies the IP address of a VLAN to be used as the source address for the Net FL ow datagrams.

Default

Uses the IP address of the VLAN that has the default route to the flow-collector device.

Usage Guidelines

The IP address must have a route to the flow-collector device.

Example

The following command specifies that IP address 198.168.100.1 is the source:

```
configure flowstats source ipaddress 198.168.100.1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure flowstats timeout ports

```
configure flowstats timeout <minutes> ports [<portlist> | all]
```

Description

Configures the timeout value for flow records on the specified ports.

Syntax Description

minutes	Specifies the number of minutes to use in deciding when to export flow records. The default is five minutes.
portlist	Specifies the ports to which the timeout applies. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. `all` indicates that the timeout should be set for all ports on this switch. Note: The parameter `any` is not supported for the PoS module.

Default

Five minutes.

Usage Guidelines

The timeout is used to export flow records on an age basis. All flow records are examined at least once every 30 minutes. If the age of the flow record is greater than the configured timeout, the record is exported. If the flow is still active, a new flow record will be created when the next packet arrives.

For the PoS module, the `minutes` parameter is an integer in the range [1-1440].

Example

The following command configures a timeout value of 15 minutes for ports 1-8:

```
configure flowstats timeout 15 ports 1-8
```

This means that flow records for these ports will be exported after they have aged 15 minutes.

History

This command was first available in ExtremeWare 6.1.5b20 for the PoS module only

This command was first available in ExtremeWare 6.2 for all "*i*" series platforms.

Platform Availability

This command is available on all platforms.

configure log display

```
configure log display {<severity>}
```

Description

Configures the real-time log display.

Syntax Description

severity	Specifies a message severity. Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.

Default

If not specified, messages of all severities are displayed on the console display.

Usage Guidelines

You must enable the log display before messages are displayed on the log display. Use the `enable log display` command to enable the log display. This allows you to configure the system to maintain a running real-time display of log messages on the console.

Options for displaying the real-time log display include:

- severity—Filters the log to display messages with the selected severity or higher (more critical). Severities include critical, error, warning, info, notice, debug-summary, debug-verbose, and debug-data.

In ExtremeWare 7.1.0, the ability to control logging to different targets was introduced. The new command equivalent to `configure log display` is the following:

```
configure log target console-display severity <severity>
```

To display the current configuration of the log display, use the following command:

```
show log configuration target console-display
```

Example

The following command configures the system log to maintain a running real-time display of log messages of critical severity:

```
configure log display critical
```

History

This command was first available in ExtremeWare 2.0.

The severity levels alert and emergency were deprecated to critical, and the levels debug-summary, debug-verbose, and debug-data were added in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure log filter events

```
configure log filter <filter name> [add | delete] {exclude} events [<event
condition> | [all | <event component>] {severity <severity> {only}}]
```

Description

Configures a log filter by adding or deleting a specified set of events.

Syntax Description

filter name	Specifies the filter to configure.
add	Add the specified events to the filter
delete	Remove the specified events from the filter
exclude	Events matching the specified events will be excluded
event condition	Specifies an individual event.
all	Specifies all components and subcomponents.
event component	Specifies all the events associated with a particular component.
severity	Specifies the minimum severity level of events (if the keyword only is omitted).
only	Specifies only events of the specified severity level.

Default

If the `exclude` keyword is not used, the events will be included by the filter. If `severity` is not specified, then the filter will use the component default severity threshold (see the note on on page 587 when `delete` or `exclude` is specified).

Usage Guidelines

This command controls the incidents that pass a filter by adding, or deleting, a specified set of events. If you want to configure a filter to include or exclude incidents based on event parameter values (for example, MAC address or BGP Neighbor) see the command `configure log filter events match` on page 589.

When the `add` keyword is used, the specified event name, or set of events described by component and severity value, is added to the beginning of the filter item list maintained for this filter. The new filter item either includes the events specified, or if the `exclude` keyword is present, excludes the events specified.

The `delete` keyword is used to remove events from the filter item list that were previously added using the add command. All filter items currently in the filter item list that are identical to, or a subset of, the set of events specified in the delete command will be removed.

Event Filtering Process. From a logical standpoint, the filter associated with each enabled log target is examined to determine whether a message should be logged to that particular target. The determination is made for a given filter by comparing the incident with the most recently configured filter item first. If the incident matches this filter item, the incident is either included or excluded, depending on whether the `exclude` keyword was used. Subsequent filter items on the list are compared if necessary. If the list of filter items has been exhausted with no match, the incident is excluded.

Events, Components, and Subcomponents. As mentioned, a single event can be included or excluded by specifying the event's name. Multiple events can be added or removed by specifying an ExtremeWare component name plus an optional severity. Some components, such as *BGP*, contain subcomponents, such as *Keepalive*, which is specified as *BGP.Keepalive*. Either components or subcomponents can be specified. The keyword `all` in place of a component name can be used to indicate all ExtremeWare components.

Severity Levels. When an individual event name is specified following the events keyword, no severity value is needed since each event has pre-assigned severity. When a component, subcomponent, or the `all` keyword is specified following the `events` keyword, a severity value is optional. If no severity is specified, the severity used for each applicable subcomponent is obtained from the pre-assigned severity threshold levels for those subcomponents. For example, if *STP* were specified as the component, and no severity is specified for the add of an include item, then only messages with severity of `error` and greater would be passed, since the threshold severity for the *STP* component is `error`. If *STP.InBPDU* were specified as the component, and no severity is specified, then only messages with severity of `warning` and greater would be passed, since the threshold severity for the *STP.InPBDU* subcomponent is `warning`. Use the `show log components` command to see this information.

The severity keyword `all` can be used as a convenience when `delete` or `exclude` is specified. The use of `delete` (or `exclude`) with severity `all` deletes (or excludes) previously added events of the same component of all severity values.

NOTE

If no severity is specified when delete *or* exclude *is specified, severity* all *is used*

If the `only` keyword is present following the severity value, then only the events in the specified component at that exact severity are included. Without the `only` keyword, events in the specified component at that severity or more urgent are included. For example, using the option `severity warning` implies critical, error, or warning events, whereas the option `severity warning only` implies warning events only. Severity `all only` is not a valid choice.

Any EMS events with severity `debug-summary`, `debug-verbose`, or `debug-data` will not be logged unless debug mode is enabled

Filter Optimization. Each time a `configure log filter` command is issued for a given filter name, the events specified are compared against the current configuration of the filter to try to logically simplify the configuration.

For example, if the command:

```
configure log filter bgpFilter1 add events bgp.keepalive severity error only
```

were to be followed by the command:

```
configure log filter bgpFilter1 add events bgp severity info
```

the filter item in the first command is automatically deleted since all events in the *BGP.Keepalive* subcomponent at severity `error` would be also included as part of the second command, making the first command redundant.

As another example, a new exclude filter item may not need to be added if no current include filter items contain any of the events described in the exclude statement. To illustrate, suppose a new filter were created and configured as follows:

```
create log filter myFilter
```

```
configure log filter myFilter add events bgp.keepalive severity error only
```

then the following exclude item actually results in no change to the filter item list:

```
configure log filter myFilter add exclude events bgp.updatein severity all
```

Since the newly created filter, *myFilter*, only includes some items from the subcomponent *BGP.Keepalive*, there are no *BGP.UpdateIn* events that need to be excluded.

More Information. See the command `show log` on page 666 for more information about severity levels.

To get a listing of the components present in the system, use the following command:

```
show log components
```

To get a listing of event condition definitions, use the following command:

```
show log events
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

Example

The following command adds all events in the *STP.InBPDU* component at severity `info` to the filter *mySTPFilter*:

```
configure log filter myStpFilter add events stp.inbpdu severity info
```

The following command adds events in the *STP.OutBPDU* component, at the pre-defined severity level for that component, to the filter *myStpFilter*:

```
configure log filter myStpFilter add events stp.outbpdu
```

The following command excludes one particular event, *STP.InBPDU.Drop*, from the filter:

```
configure log filter myStpFilter add exclude events stp.inbpdu.drop
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure log filter events match

```
configure log filter <filter name> [add | delete] {exclude} events [<event
condition> | [all | <event component>] {severity <severity> {only}}] [match
| strict-match] <type> <value> {and <type> <value> ...}
```

Description

Configures a log filter by adding or deleting a specified set of events and specific set of match parameter values.

Syntax Description

filter name	Specifies the filter to configure.
add	Add the specified events to the filter
delete	Remove the specified events from the filter
exclude	Events matching the filter will be excluded
event condition	Specifies the event condition.
all	Specifies all events.
event component	Specifies all the events associated with a particular component.
severity	Specifies the minimum severity level of events (if the keyword only is omitted).
only	Specifies only events of the specified severity level.
match	Specifies events whose parameter values match the <type> <value> pair.
strict-match	Specifies events whose parameter values match the <type> <value> pair, and possess all the parameters specified.
type	Specifies the type of parameter to match
value	Specifies the value of the parameter to match
and	Specifies additional <type> <value> pairs that must be matched

Default

If the `exclude` keyword is not used, the events will be included by the filter. If `severity` is not specified, then the filter will use the component default severity threshold (see the note on on page 587 when `delete` or `exclude` is specified).

Usage Guidelines

This command controls the incidents that pass a filter by adding, or deleting, a specified set of events that match a list of <type> <value> pairs. This command is an extension of the command `configure log filter events`, and adds the ability to filter incidents based on matching specified event parameter values to the event.

See the `configure log filter events` command on page 586 for more information on specifying and using filters, on event conditions and components, on the details of the filtering process. The discussion here is about the concepts of matching <type> <value> pairs to more narrowly define filters.

Types and Values. Each event in ExtremeWare is defined with a message format and zero or more parameter types. The `show log events detail` command on page 679 can be used to display event

definitions (the event text and parameter types). The syntax for the parameter types (represented by <type> in the command syntax above) is:

```
[bgp [neighbor | routerid] <ip address>
| eaps <eaps domain name>
| {destination | source} [ipaddress <ip address> | L4-port | mac-address ]
| {egress | ingress} [slot <slot number> | ports <portlist>]
| netmask <netmask>
| number <number>
| string <match expression>
| vlan <vlan name>
| vlan tag <vlan tag>]
```

The <value> depends on the parameter type specified. As an example, an event may contain a physical port number, a source MAC address, and a destination MAC address. To allow only those incidents with a specific source MAC address, use the following in the command:

```
configure log filter myFilter add events bridge severity notice match source
mac-address 00:01:30:23:C1:00
```

The string type is used to match a specific string value of an event parameter, such as a user name. A string can be specified as a simple regular expression.

Match Versus Strict-Match. The `match` and `strict-match` keywords control the filter behavior for incidents whose event definition does not contain all the parameters specified in a `configure log filter events match` command. This is best explained with an example. Suppose an event in the *XYZ* component, named *XYZ.event5*, contains a physical port number, a source MAC address, but no destination MAC address. If you configure a filter to match a source MAC address and a destination MAC address, *XYZ.event5* will match the filter when the source MAC address matches regardless of the destination MAC address, since the event contains no destination MAC address. If you specify the `strict-match` keyword, then the filter will never match, since *XYZ.event5* does not contain the destination MAC address.

In other words, if the `match` keyword is specified, an incident will pass a filter so long as all parameter values in the incident match those in the match criteria, but all parameter types in the match criteria need not be present in the event definition.

And Keyword. Use the and keyword to specify multiple parameter type/value pairs that must match those in the incident. For example, to allow only those events with specific source and destination MAC addresses, use the following command:

```
configure log filter myFilter add events bridge severity notice match source
mac-address 00:01:30:23:C1:00 and destination mac-address 01:80:C2:00:00:02
```

Multiple Match Commands. Multiple configure log add events match commands are logically ORed together. For example, the following commands define a filter that allows layer 2 bridging incidents with a source MAC address of one of three possible values:

```
create log filter bridgeFilter

configure log bridgeFilter add events bridge severity notice match source mac-address
00:11:12:13:14:15

configure log bridgeFilter add events bridge severity notice match source mac-address
00:21:22:23:24:25
```

```
configure log bridgeFilter add events bridge severity notice match source mac-address
00:31:32:33:34:35
```

In order to exclude only incidents whose parameter values match the specified criteria, follow this two step process. First, include the applicable event(s) using either the `configure log filter events` command, or using the `configure log filter events match` command described here, with a superset of the match criteria. Second, use the `exclude` keyword in the `configure log filter events match` command to exclude incidents with the specified parameter values.

As an example, the following commands define a filter that allows incidents in the *BGP.Keepalive* component at severity `notice` or more severe, except those incidents containing a BGP neighbor in the 10.1.2.0/24 subnet:

```
create log filter bgpFilter

configure log bgpFilter add events bgp.keepalive severity notice

configure log bgpFilter add exclude events bgp.keepalive severity notice match bgp
neighbor 10.1.2.0/24
```

Filter Optimization. As explained in the `configure log filter events` command, each time a `configure log filter match` command is issued, an attempt is made to logically simplify the configuration. This simplification extends to cases where one set of match criteria is a superset of another. For example, if you issued the following commands:

```
create log filter bgpFilter1

configure log bgpFilter1 add events bgp.event severity notice match bgp neighbor
10.0.0.0/8

configure log bgpFilter1 add events bgp.event severity notice match bgp neighbor
10.1.2.0/24 and L4-port 80
```

then the third command is redundant and no filter item is actually added. The reason is that the IP subnet 10.1.2.0/24 is wholly contained within the IP subnet 10.0.0.0/8, which is already included in this filter, and with any value for the layer 4 port.

More Information. See the command `show log` on page 666 for more information about severity levels.

To get a listing of the components present in the system, use the following command:

```
show log components
```

To get a listing of event condition definitions, use the following command:

```
show log events
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

Example

By default, all log targets are associated with the built-in filter, *DefaultFilter*. Therefore, the most straightforward way to send additional messages to a log target is to modify *DefaultFilter*. In the following example, the command modifies the built-in filter to allow incidents in the *STP* component,

and all subcomponents of *STP*, of severity critical, error, warning, notice and info. For any of these events containing a physical port number as a match parameter, limit the incidents to only those occurring on physical ports 3, 4 and 5 on slot 1, and all ports on slot 2:

```
configure log DefaultFilter add events stp severity info match ports 1:3-1:5, 2:*
```

If desired, issue the `unconfigure log DefaultFilter` command to restore the *DefaultFilter* back to its original configuration.

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure log filter set severity

```
configure log filter <filter name> set severity <severity> events
[<event component> | all ]
```

Description

Sets the severity level of an existing filter item.

Syntax Description

filter name	Specifies the filter to configure.
severity	Specifies the severity level to send.
event component	Specifies all the events associated with a particular component.

Default

N/A.

Usage Guidelines

This command modifies the severity level of an existing filter item describing a particular set of events. Using this command is equivalent to deleting the filter item from the filter and then adding back a filter item describing the same set of events with a different severity level. The command can only be used to modify a filter item referring to a set of events with a severity level, as opposed to one that makes use of only a single severity. It can be used to modify either “exclude” or “include” filter items.

For example, to change the severity level of the filter item added with this command:

```
configure log filter bgpFilter2 add events bgp.keepalive severity notice
```

use the following command:

```
configure log filter bgpFilter2 set severity info events bgp.keepalive
```

Using this single command is preferred to using a `delete` command followed by an `add` command:

```
configure log filter bgpFilter2 delete events bgp.keepalive
configure log filter bgpFilter2 add events bgp.keepalive severity info
```

Using the single command eliminates the possibility of missing an event of interest between the separate `delete` and `add` commands.

Note that the severity of a filter item configured to include or exclude incidents based on event parameter values (for example slot number) can also be modified using the `configure log filter set severity match` command on page 595.

See the command `show log` on page 666 for a detailed description of severity levels.

To see the current configuration of a target, use the following command:

```
show log configuration target {console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]}
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

Example

To change the severity level of the filter item added with this command:

```
configure log filter bgpFilter2 add events bgp.keepalive severity notice
```

use the following command:

```
configure log filter bgpFilter2 set severity info events bgp.keepalive
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

configure log filter set severity match

```
configure log filter <filter name> set severity <severity> events
[<event condition> | [all | <event component>]] [match | strict-match]
<type> <value> {and <type> <value> ...}
```

Description

Sets the severity level of an existing filter item.

Syntax Description

filter name	Specifies the filter to configure.
severity	Specifies the severity level to send.
event component	Specifies all the events associated with a particular component.
only	Specifies only events of the specified severity level.
match	Specifies events whose parameter values match the <type> <value> pair.
strict-match	Specifies events whose parameter values match the <type> <value> pair, and possess all the parameters specified.
type	Specifies the type of parameter to match
value	Specifies the value of the parameter to match
and	Specifies additional <type> <value> pairs that must be matched

Default

N / A.

Usage Guidelines

This command modifies the severity level of an existing filter item describing a particular set of events and the parameter values of the desired events. Using this command is equivalent to deleting the filter item from the filter and then adding back a filter item describing the same set of events with a different severity level. The command can only be used to modify a filter item referring to a set of events with a severity level, as opposed to one that makes use of only a single severity. It can be used to modify either “exclude” or “include” filter items.

For example, to change the severity level of the filter item added with this command:

```
configure log slbFilter2 add exclude events slb.conn severity notice match
source ipaddress 10.1.2.0/24
```

use the following command:

```
configure log slbFilter2 set severity info events events slb.conn match
source ipaddress 10.1.2.0/24
```

Using this single command is preferred to using a `delete` command followed by an `add` command:

```
configure log slbFilter2 delete exclude events slb.conn severity notice match
source ipaddress 10.1.2.0/24
configure log slbFilter2 add exclude events slb.conn severity info match
```

```
source ipaddress 10.1.2.0/24
```

Using the single command eliminates the possibility of missing an event of interest between the separate `delete` and `add` commands.

See the command `show log` on page 666 for a detailed description of severity levels.

To see the current configuration of a target, use the following command:

```
show log configuration target {console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]}
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

Example

To change the severity level of the filter item added with this command:

```
configure log filter bgpFilter2 add events bgp.keepalive severity notice
```

use the following command:

```
configure log filter bgpFilter2 set severity info events bgp.keepalive
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

configure log target filter

```
configure log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]]
filter <filter name> {severity <severity> {only}}
```

Description

Associates a filter to a target.

Syntax Description

target	Specifies the device to send the log entries.
console-display	Specifies the console display.
memory-buffer	Specifies the switch memory buffer.
nvram	Specifies the switch NVRAM.
session	Specifies the current session (including console display).
syslog	Specifies a syslog remote server.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.
filter name	Specifies the filter to associate with the target.
severity	Specifies the minimum severity level to send (if the keyword only is omitted).
only	Specifies that only the specified severity level is to be sent.

Default

If severity is not specified, the severity level for the target is left unchanged.

Usage Guidelines

This command associates the specified filter and severity with the specified target. A filter limits messages sent to a target.

Although each target can be configured with its own filter, by default, all targets are associated with the built-in filter, *DefaultFilter*. Each target can also be configured with its own severity level. This provides the ability to associate multiple targets with the same filter, while having a configurable severity level for each target.

A message is sent to a target if the target has been enabled, the message passes the associated filter, the message is at least as severe as the configured severity level, and the message output matches the regular expression specified. By default, the memory buffer and the NVRAM targets are enabled. For other targets, use the command `enable log target` on page 650. Table 14 describes the default characteristics of each type of target.

Table 14: Default Target Log Characteristics

Target	Enabled	Severity Level	Pre-7.1.0 Command to Set Log Severity
console display	no	info	`configure log display {<severity>}`
memory buffer	yes	debug-data	N/A
NVRAM	yes	warning	N/A
session	no	info	N/A
syslog	no	debug-data	`configure syslog add <host name/ip> {: <udp-port>} [local0 ... local7] <severity>`

The built-in filter, *DefaultFilter*, and a severity level of `info` are used for each new telnet session. These values may be overridden on a per-session basis using the `configure log target filter` command and specify the target as `session`. Use the following form of the command for per-session configuration changes:

```
configure log target session filter <filter name> {severity <severity> {only}}
```

Configuration changes to the current session target are in effect only for the duration of the session, and are not saved in FLASH memory. The `session` option can also be used on the console display, if the changes are desired to be temporary. If changes to the console-display are to be permanent (saved to FLASH memory), use the following form of the command:

```
configure log target console-display filter <filter name> {severity <severity> {only}}
```

In versions prior to ExtremeWare 7.1.0, so-called `static` messages with a severity level of `warning` and above were stored in NVRAM so they would be available across a reboot. This remains the default behavior for ExtremeWare releases, but message filtering for the NVRAM target is now configurable.

Example

The following command sends log messages to the previously syslog host at 10.31.8.25, port 8993, and facility `local3`, that pass the filter *myFilter* and are of severity `warning` and above:

```
configure log target syslog 10.31.8.25:8993 local3 filter myFilter severity warning
```

The following command sends log messages to the current session, that pass the filter *myFilter* and are of severity `warning` and above:

```
configure log target session filter myFilter severity warning
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

configure log target format

```
configure log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]]
format [timestamp [seconds | hundredths | none]
| date [dd-mm-yyyy | dd-Mmm-yyyy | mm-dd-yyyy | Mmm-dd | yyyy-mm-dd | none]
| severity [on | off]
| event-name [component | condition | none | subcomponent]
| host-name [on | off]
| priority [on | off]
| tag-id [on | off]
| tag-name [on | off]
| sequence-number [on | off]
| process-name [on | off]
| process-id [on | off]
| source-function [on | off]
| source-line [on | off]]
```

Description

Configures the formats of the items that comprise a message, on a per-target basis.

Syntax Description

console-display	Specifies the console display.
memory-buffer	Specifies the switch memory buffer.
nvram	Specifies the switch NVRAM.
session	Specifies the current session (including console display).
syslog	Specifies a syslog target.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.
timestamp	Specifies a timestamp formatted to display seconds, hundredths, or none.
date	Specifies a date formatted as specified, or none.
severity	Specifies whether to include the severity.
event-name	Specifies how detailed the event description will be. Choose from none, component, subcomponent, or condition.
host-name	Specifies whether to include the host name.
priority	Specifies whether to include the priority
tag-id	Specifies whether to include the internal task identifier.
tag-name	Specifies whether to include the task name.
sequence-number	Specifies whether to include the event sequence number.
process-name	Specifies whether to include the internal process name.
process-id	Specifies whether to include the internal process identifier.
source-function	Specifies whether to include the source function name.
source-line	Specifies whether to include the source file name and line number.

Default

The following defaults apply to console display, memory buffer, NVRAM, and session targets:

- timestamp—hundredths
- date—mm-dd-yyyy
- severity—on
- event-name—condition
- host-name—off
- priority—off
- tag-id—off
- tag-name—off
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

The following defaults apply to syslog targets (per RFC 3164):

- timestamp—seconds
- date—mmm-dd
- severity—on
- event-name—none
- host-name—off
- priority—on
- tag-id—off
- tag-name—on
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

Usage Guidelines

This command configures the format of the items that make up log messages. You can choose to include or exclude items and set the format for those items, but you cannot vary the order in which the items are assembled.

When applied to the targets `console-display` or `session`, the format specified is used for the messages sent to the console display or telnet session. Configuration changes to the `session` target, be it either a telnet or console display target session, are in effect only for the duration of the session, and are not saved in FLASH.

When this command is applied to the target `memory-buffer`, the format specified is used in subsequent `show log` and `upload log` commands. The format configured for the internal memory buffer can be overridden by specifying a format on the `show log` and `upload log` commands.

When this command is applied to the target `syslog`, the format specified is used for the messages sent to the specified syslog host.

Timestamps. Timestamps refer to the time an event occurred, and can be output in either seconds as described in RFC 3164 (for example, "13:42:56"), hundredths of a second (for example, "13:42:56.98"), or suppressed altogether. To display timestamps as hh:mm:ss, use the `seconds` keyword, to display as hh:mm:ss.HH, use the `hundredths` keyword, or to suppress timestamps altogether, use the `none` keyword. Timestamps are displayed in hundredths by default.

Date. The date an event occurred can be output as described in RFC 3164. Dates are output in different formats, depending on the keyword chosen. The following lists the `date` keyword options, and how the date "March 26, 2003" would be output:

- `Mmm-dd`—Mar 26
- `mm-dd-yyyy`—03/26/2003
- `dd-mm-yyyy`—26-03-2003
- `yyyy-mm-dd`—2003-03-26
- `dd-Mmm-yyyy`—26-Mar-2003

Dates are suppressed altogether by specifying `none`. Dates are displayed as `mm-dd-yyyy` by default.

Severity. A four-letter abbreviation of the severity of the event can be output by specifying `severity on` or suppressed by specifying `severity off`. The default setting is `severity on`. The abbreviations are: Crit, Erro, Warn, Noti, Info, Summ, Verb, and Data. These correspond to: Critical, Error, Warning, Notice, Informational, Debug-Summary, Debug-Verbose, and Debug-Data.

Event Names. Event names can be output as the component name only by specifying `event-name component`, as component and subcomponent name by specifying `event-name subcomponent`, as component and subcomponent name with condition mnemonic by specifying `event-name condition`, or suppressed by specifying `event-name none`. The default setting is `event-name condition` to specify the complete name of the events.

Host Name. The configured SNMP name of the switch can be output as *HOSTNAME* described in RFC 3164 by specifying `host-name on` or suppressed by specifying `host-name off`. The default setting is `host-name off`.

Tag ID. The (internal) ExtremeWare task identifiers of the applications detecting the events can be output as the pid described in RFC 3164 by specifying `tag-id on` or suppressed by specifying `tag-id off`. The default setting is `tag-id off`.

Tag Name. The component name used by the application when detecting the events can be output as the TAG described in RFC 3164 by specifying `tag-name on` or suppressed by specifying `tag-name off`. The default setting is `tag-name off`.

Sequence Number. Sequence numbers refer to the specific ordering of events as they occur, and can be output as an ASCII decimal integer by specifying `sequence-number on` or suppressed by specifying `sequence-number off`. The default setting is `sequence-number off`.

Process Name. For providing detailed information to technical support, the (internal) ExtremeWare task names of the applications detecting the events can be displayed by specifying `process-name on` or suppressed by specifying `process-name off`. The default setting is `process-name off`.

Process ID. For providing detailed information to technical support, the (internal) ExtremeWare task identifiers of the applications detecting the events can be displayed by specifying `process-id on` or suppressed by specifying `process-id off`. The default setting is `process-id off`.

Source Function. For providing detailed information to technical support, the names of the application source functions detecting the events can be displayed by specifying `source-function on` or suppressed by specifying `source-function off`. The default setting is `source-function off`.

Source Line. For providing detailed information to technical support, the application source file names and line numbers detecting the events can be displayed by specifying `source-line on` or suppressed by specifying `source-line off`. The default setting is `source-line off`.

Example

In the following example, the switch generates the identical event from the component SNTP, using three different formats.

Using the default format for the session target, an example log message might appear as:

```
05/29/2003 12:15:25.00 <Warn:SNTP.RslvSrvrFail> The SNTP server parameter value
(TheWrongServer.example.com) can not be resolved.
```

If you set the current session format using the following command:

```
configure log target session format date mm-dd-yyy timestamp seconds event-name
component
```

The same example would appear as:

```
05/29/2003 12:16:36 <Warn:SNTP> The SNTP server parameter value
(TheWrongServer.example.com) can not be resolved.
```

In order to provide some detailed information to technical support, you set the current session format using the following command:

```
configure log target session format date mmm-dd timestamp hundredths event-name
condition source-line on process-name on
```

The same example would appear as:

```
May 29 12:17:20.11 SNTP: <Warn:SNTP.RslvSrvrFail> tSntpc: (sntpcLib.c:606) The SNTP
server parameter value (TheWrongServer.example.com) can not be resolved.
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

configure log target match

```
configure log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]] match [any
|<match-expression>]
```

Description

Associates a match expression to a target.

Syntax Description

console-display	Specifies the console display.
memory-buffer	Specifies the switch memory buffer.
nvram	Specifies the switch NVRAM.
session	Specifies the current session (including console display).
syslog	Specifies a syslog target.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.
any	Specifies that any messages will match. This effectively removes a previously configured match expression.
match-expression	Specifies a regular expression. Only messages that match the regular expression will be sent.

Default

By default, targets do not have a match expression.

Usage Guidelines

This command configures the specified target with a match expression. The filter associated with the target is not affected. A message is sent to a target if the target has been enabled, the message passes the associated filter, the message is at least as severe as the configured severity level, and the message output matches the regular expression specified.

See the command `show log` on page 666 for a detailed description of simple regular expressions. By default, targets do not have a match expression.

Specifying `any` instead of `match-expression` effectively removes a match expression that had been previously configured, causing any message to be sent that has satisfied all of the other requirements.

To seethe configuration of a target, use the following command:

```
show log configuration target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]]
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

Example

The following command sends log messages to the current session, that pass the current filter and severity level, and contain the string *user5*:

```
configure log target session match user5
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

configure log target severity

```
configure log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]] {severity
<severity> {only}}
```

Description

Sets the severity level of messages sent to the target.

Syntax Description

console-display	Specifies the console display.
memory-buffer	Specifies the switch memory buffer.
nvram	Specifies the switch NVRAM.
session	Specifies the current session (including console display).
syslog	Specifies a syslog target.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.
severity	Specifies the least severe level to send (if the keyword only is omitted).
only	Specifies that only the specified severity level is to be sent.

Default

By default, targets are sent messages of the following severity level and above:

- console display—info
- memory buffer—debug-data
- NVRAM—warning
- session—info
- syslog—debug-data

Usage Guidelines

This command configures the specified target with a severity level. The filter associated with the target is not affected. A message is sent to a target if the target has been enabled, the message passes the associated filter, the message is at least as severe as the configured severity level, and the message output matches the regular expression specified.

See the command `show log` on page 666 for a detailed description of severity levels.

To see the current configuration of a target, use the following command:

```
show log configuration target {console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]}
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

Example

The following command sends log messages to the current session, that pass the current filter at a severity level of info or greater, and contain the string *user5*:

```
configure log target session severity info
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

configure packet-mem-scan-recovery-mode

```
configure packet-mem-scan-recovery-mode [offline | online] [msm-a | msm-b |
<slot number>]
```

Description

Configures packet memory scanning and the recovery mode setting on a BlackDiamond module.

Syntax Description

offline	Specifies that a faulty BlackDiamond module is taken offline and kept offline if one of the following occurs: • More than eight defects are detected. • Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process. • After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.
online	Specifies that a faulty module is kept online, regardless of how many errors are detected.
msm-a	Specifies the MSM module installed in slot A.
msm-b	Specifies the MSM module installed in slot B.
slot number	Specifies a module installed in a slot.

Default

Disabled.

Usage Guidelines

Use this command to scan and check the health of an individual module rather than the overall system.

This command overrides the system health check auto-recovery setting. If you have the system health check alarm level configured, the individual packet memory scanning configuration is ignored.

This command is only effective if the system health check is configured for auto-recovery. If you have the system health check configured for auto-recovery, and you configure packet-mem-scan-recovery, you can define a specific slot's behavior if an error is discovered.

To configure the system health check for auto-recovery, use the `configure sys-health-check auto-recovery <number> [offline | online] | alarm-level [card-down | default | log | system-down | traps]` command.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

Example

The following command enables packet memory scanning on slot 1, and specifies that the module be taken offline:

```
configure packet-mem-scan-recovery mode offline slot 1
```

The following command enables packet memory scanning on the MSM module in slot B, and specifies that the module be kept online

```
configure packet-mem-scan-recovery mode online slot msm-b
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on BlackDiamond switches only.

configure sys-health-check alarm-level

```
configure sys-health-check alarm-level [log | system-down | traps | default
| auto-recovery <number of tries> [online | offline]]
```

Description

Configures the system health checker.

Syntax Description

log	Posts a CRIT message to the log.
system-down	Posts a CRIT message to the log, sends a trap, and turns off the system.
traps	Posts a CRIT message to the log and sends a trap.
default	Resets the alarm level to log.
auto-recovery	Specifies the number of times that the health checker attempts to auto-recover. The range is from 0 through 255 times. Default is 3 times.
offline	Specifies that a faulty Summit switch or Alpine module is taken offline and kept offline if one of the following occurs: • More than eight defects are detected. • Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process. • After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.
online	Specifies that a faulty module is kept online, regardless of how many errors are detected.

Default

The default alarm level is log.

Usage Guidelines

This command allows you to configure the switch's reaction to a failed health check.

The system health checker tests I/O modules, SMMi modules, and the backplane by forwarding packets every 4 seconds. Additional checking for the validity of these packets is completed by performing a checksum.

By isolating faults to a specific module, SMMi, or backplane connection, the system health checker prevents corrupted packets from being propagated to the CPU, upper layer modules, or the rest of your network. If you observe a failure, please contact Extreme Technical Support.

Depending on how you have configured the system health checker, failed system health checks may generate critical error messages in the syslog, and may also send a trap and/or shut down the system. The system health checker will continue to periodically forward test packets to failed components. If auto-recovery is configured, the system will attempt to automatically reset the faulty module and bring it back online.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

In ExtremeWare versions prior to 6.2, you cannot use both mirroring and the system health checker at the same time. If you configure mirroring with the system health checker enabled, the health checker will indicate that it has been disabled by sending a message to the syslog. In ExtremeWare 6.2 or later, this restriction does not apply.

The `auto-recovery` option configures the number of times the system health checker attempts to automatically reset a faulty module and bring it online. If the system health checker fails more than the configured number of attempts, it sets the module to card-down.

In ExtremeWare 6.2.1 or later, when auto-recovery is configured, the occurrence of three consecutive checksum errors will cause the packet memory (PM) defect detection program to be run against the I/O module. Checksum errors may include internal and external MAC port parity errors, EDP checksum errors, and CPU packet or diagnostic packet checksum errors. If defects are detected, the card is taken offline, the memory defect information is recorded in the card EEPROM, the defective buffer is mapped out of further use, and the card is returned to operational state. A maximum of 8 defects can be stored in the EEPROM.

After the PM defect detection and mapping process has been run, a card is considered failed and is taken offline in the following circumstances:

- More than eight defects are detected.
- Three consecutive checksum errors were detected by the health checker, but no new PM defects were found by the PM defect detection process.
- After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.

The auto-recovery repetition value is ignored in these cases. In any of these cases, please contact Extreme Technical Support.

If you specify the `online` option, the module is kept online, but the following error messages are recorded in the log:

```
<WARN:SYST> card_db.c 832: Although card 2 is back online, contact Tech. Supp. for
assistance.
<WARN:SYST> card_db.c 821: Card 2 has nonrecoverable packet memory defect.
```

To view the status of the system health checker, use the `show diag` command.

To enable the health checker, use the `enable sys-health-check` command.

To disable the health checker, use the `disable sys-health-check` command.

The alarm-level `system-down` option is especially useful in an ESRP configuration where the entire system is backed by an identical system. By powering down the faulty system, you ensure that erratic ESRP behavior in the faulty system does not affect ESRP performance and ensures full system failover to the redundant system.

If you are using ESRP with ESRP diagnostic tracking enabled in your configuration, the system health check failure will automatically reduce the ESRP priority of the system to the configured failover priority. This allows the healthy standby system to take over ESRP and become responsible for handling traffic.

I/O module faults are permanently recorded on the module's EEPROM. A module that has failed a system health check cannot be brought back online.

To view the failure messages, use the `show diag` command.

Example

The following command configures the system health checker to post a CRIT message to the log and send a trap:

```
configure sys-health-check alarm-level traps
```

History

This command was first available in ExtremeWare 6.1.9.

The system health check functionality was modified in ExtremeWare 6.2.1 to support packet memory defect detection and mapping on selected I/O modules.

This command was modified in ExtremeWare 6.2.2 to support system health check and checksum error checking and to add the `online` and `offline` parameters.

Platform Availability

This command is available only on Alpine and Summit switches.

configure sys-health-check auto-recovery

```
configure sys-health-check auto-recovery <number> [offline | online] |
alarm-level [card-down | default | log | system-down | traps]
```

Description

Configures the system health checker.

Syntax Description

number	Specifies the number of times that the health checker attempts to auto-recover a faulty module. The range is from 0 through 255 times. Default is 3 times.
offline	Specifies that a faulty module is taken offline and kept offline if one of the following occurs: • More than eight defects are detected. • Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process. • After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.
online	Specifies that a faulty module is kept online, regardless of memory scanning or memory mapping errors.
card-down	Posts a CRIT message to the log and brings the module down.
default	Resets the alarm level to log.
log	Posts a CRIT message to the log.
system-down	Posts a CRIT message to the log, sends a trap, and turns off the system.
traps	Posts a CRIT message to the log and sends a trap.

Default

Log.

Usage Guidelines

This command allows you to configure the switch's reaction to a failed health check.

The system health checker tests I/O modules, MSM64i modules, and the backplane by forwarding packets every 4 seconds. Additional checking for the validity of these packets is completed by performing a checksum.

By isolating faults to a specific module, MSM64i, or backplane connection, the system health checker prevents corrupted packets from being propagated to the CPU, upper layer modules, or the rest of your network. If you observe a failure, please contact Extreme Technical Support.

Depending on how you have configured the system health checker, failed system health checks may generate critical error messages in the syslog, and may also send a trap and/or shut down the system. The system health checker will continue to periodically forward test packets to failed components. If auto-recovery is configured, the system will attempt to automatically reset the faulty module and bring it back online.

In ExtremeWare versions prior to 6.2, you cannot use both mirroring and the system health checker at the same time. If you configure mirroring with the system health checker enabled, the health checker will indicate that it has been disabled by sending a message to the syslog. In ExtremeWare 6.2 or later, this restriction does not apply.

The `auto-recovery` option configures the number of times the system health checker attempts to automatically reset a faulty module and bring it online. If the system health checker fails more than the configured number of attempts, it sets the module to card-down.

In ExtremeWare 6.2.1 or later, when auto-recovery is configured, the occurrence of three consecutive checksum errors will cause the packet memory (PM) defect detection program to be run against the I/O module. Checksum errors may include internal and external MAC port parity errors, EDP checksum errors, and CPU packet or diagnostic packet checksum errors. If defects are detected, the card is taken offline, the memory defect information is recorded in the card EEPROM, the defective buffer is mapped out of further use, and the card is returned to operational state. A maximum of 8 defects can be stored in the EEPROM.

After the PM defect detection and mapping process has been run, a card is considered failed and is taken offline in the following circumstances:

- More than eight defects are detected.
- Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process.
- After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.

The auto-recovery repetition value is ignored in these cases. In any of these cases, please contact Extreme Technical Support.

Auto-recovery mode only affects an MSM64i if the system has no slave MSM64i. If the faulty module is the only MSM64i in the system, auto recovery automatically resets the MSM64i and brings it back online. Otherwise, auto-recovery has no effect on an MSM64i.

If you specify the `online` option, the module is kept online, but the following error messages are recorded in the log:

```
<WARN:SYST> card_db.c 832: Although card 2 is back online, contact Tech. Supp. for
assistance.
<WARN:SYST> card_db.c 821: Card 2 has nonrecoverable packet memory defect.
```

To view the status of the system health checker, use the `show diag` command.

To enable the health checker, use the `enable sys-health-check` command.

To disable the health checker, use the `disable sys-health-check` command.

The alarm-level `system-down` option is especially useful in an ESRP configuration where the entire system is backed by an identical system. By powering down the faulty system, you ensure that erratic ESRP behavior in the faulty system does not affect ESRP performance and ensures full system failover to the redundant system.

If you are using ESRP with ESRP diagnostic tracking enabled in your configuration, the system health check failure will automatically reduce the ESRP priority of the system to the configured failover priority. This allows the healthy standby system to take over ESRP and become responsible for handling traffic.

I/O module faults are permanently recorded on the module's EEPROM. A module that has failed a system health check cannot be brought back online.

If the faulty module is a master MSM64i, the slave MSM64i automatically becomes the master and sets the faulty MSM64i to `card-down`. The new master MSM64i re-initializes and brings up all the I/O modules.

If the faulty module is a master MSM64i and there is no slave MSM64i, the system continues operation in a "limited commands" mode. In the "limited commands" mode, the I/O slots are not initialized, and only commands that do no affect the switch hardware configuration are allowed.

If the faulty module is a slave MSM64i, the fault is recorded in the slave's MSM64i's NVRAM and the slave MSM64i is taken offline.

To view the failure messages, use the `show diag` command.

To clear the MSM64i failure messages posted to the log, use the `clear log diag-status` command. This command will clear the error messages from the MSM64i NVRAM. If the MSM64i failed a system health check, this command restores the MSM64i to full functionality. This command should only be used for additional testing purposes and reproduction efforts of the original fault.

Example

The following command configures the system health checker to try ten times to bring a faulty MSM64i back online:

```
configure sys-health-check auto-recovery 10
```

History

This command was first available in ExtremeWare 6.1.9.

The system health check functionality was modified in ExtremeWare 6.2.1 to support packet memory defect detection and mapping on selected I/O modules.

This command was modified in ExtremeWare 6.2.2 to support system health check and checksum error checking on the BlackDiamond 6804 switch and to add the `online` and `offline` parameters.

Platform Availability

This command is available on the BlackDiamond switch only.

The packet-memory defect detection and mapping feature is supported only on selected I/O modules. See the release note for your version of ExtremeWare for information on the supported modules.

configure sys-recovery-level

```
configure sys-recovery-level [none | [all | critical] [msm-failover |
reboot | shutdown | system-dump [maintenance-mode | msm-failover | reboot |
shutdown]]]
```

Description

Configures a recovery option for instances where an exception occurs in ExtremeWare.

Syntax Description

none	Configures the level to no recovery. No action is taken when a task exception occurs; there is no system shutdown or reboot.
all	Configures ExtremeWare to log an error into the syslog and either shutdown or reboot the system after any task exception occurs.
critical	Configures ExtremeWare to log an error into the syslog and either shutdown or reboot the system after a critical task exception.
msm-failover	Triggers the slave MSM64i to take over control of the switch if there is a software exception on the master MSM64i. BlackDiamond switches only.
reboot	Reboots the switch.
shutdown	Shuts down the switch.
system-dump	Triggers a dump transfer, followed by the specified completion action (reboot, shutdown, msm-failover, or maintenance-mode). Maintenance mode leaves the switch in whatever state the dump transfer puts it in. Some subsystems may no longer behave correctly or operate at all after a system dump. The system-dump option should only be used with assistance from TAC. Available on switches with Ethernet management ports only.

Default

None.

Usage Guidelines

This command is used for system troubleshooting. If the system fails before the switch is booted up, the switch will automatically start the console and allow access to the system to view the logs or debug the failure. You can also configure the system to respond to software failures automatically. You must specify one of the following parameters for the system to respond to software failures:

- none—No action is taken when a task exception occurs.
- `all`—The system will reboot or shut down if any task exception occurs.
- `critical`—The system will reboot or shutdown if a critical task exception occurs. Critical tasks include the tBGTask, tNetTask, tEdpTask, and tESRPTask.

For ExtremeWare 6.1, the system will always reboot after a task exception when the system recovery level is specified as `all` or `critical`.

For ExtremeWare 6.2 or later, you must specify whether the system should shut down or reboot upon a task exception if the recovery level is `all` or `critical`.

For ExtremeWare 6.2.2 or later, if `msm-failover` is specified on a BlackDiamond switch and there is a software exception on the master MSM64*i*, the interrupt handler triggers the slave MSM64*i* to take over control of the switch.

Example

The following command configures a switch to reboot after a critical task exception occurs:

```
configure sys-recovery-level critical reboot
```

The following command configures the Master MSM64*i* to failover to the Slave MSM64*i* if a software exception occurs:

```
configure sys-recovery-level critical msm-failover
```

History

This command was first available in ExtremeWare 6.1.

Modified in ExtremeWare 6.2 to support the `shutdown` and `reboot` options.

Modified in ExtremeWare 6.2.2 to support the `msm-failover` option.

Platform Availability

This command is available on all *i*-series switches. The `msm-failover` option is available on BlackDiamond switch only.

configure syslog add

```
configure syslog {add} <host name/ip> {: <udp-port>} [local0 ... local7]
{<severity>}
```

Description

Configures the remote syslog server host address, and filters messages to be sent to the remote syslog target.

Syntax Description

host name/ip	Specifies the remote syslog server host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.
severity	Specifies a message severity. Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.

Default

If a severity level is not specified, all messages are sent to the remote syslog server target. If UDP port is not specified, 514 is used.

Usage Guidelines

Options for configuring the remote syslog server include:

- host name/ip—The name or IP address of the remote syslog server host.
- udp-port—The UDP port
- facility—The syslog facility level for local use (local0– local7).
- severity—Filters the messages sent to the remote syslog server target to have the selected severity or higher (more critical). Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.

The switch log overwrites existing log messages in a wrap-around memory buffer, which may cause you to lose valuable information once the buffer becomes full. The remote syslog server does not overwrite log information, and can store messages in non-volatile files (disks, for example).

The `enable syslog` command must be issued in order for messages to be sent to the remote syslog server(s). Syslog is disabled by default. A total of four syslog servers can be configured at one time.

When a syslog server is added, it is associated with the filter *DefaultFilter*. Use the `configure log target filter` command to associate a different filter.

For version 4.0 and higher:

- The syslog facility level is defined as local0 – local7. The facility level is used to group syslog data.

Example

The following command configures the remote syslog server target with an critical severity:

```
configure syslog 123.45.67.78 local1 critical
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure syslog delete

```
configure syslog delete <host name/ip> {: <udp-port>} [local0 ... local7]
```

Description

Deletes a remote syslog server address.

Syntax Description

host name/ip	Specifies the remote syslog server host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.

Default

If a UDP port number is not specified, 514 is used.

Usage Guidelines

This command is used to delete a remote syslog server target.

Example

The following command deletes the remote syslog server with an IP address of 10.0.0.1:

```
configure syslog delete 10.0.0.1 local1
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure transceiver-test failure-action

```
configure transceiver-test failure-action [log | sys-health-check]
```

Description

Configures the action the switch takes if too many failures are detected within the specified window.

Syntax Description

log	Specifies that messages are sent to the syslog.
sys-health-check	Specifies the configured system health check action is taken.

Default

log.

Usage Guidelines

If you select `log`, only one instance of an error message is logged at this level.

If you select `sys-health-check`, and the switch detects too many failures, the switch takes the configured system health check action. To configure the system health check, use the `configure sys-health-check [alarm-level [card-down | default | log | system-down | traps] | auto-recovery <number of tries>]` command.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

By default, the switch checks for errors within the *last* eight 20-second windows. Use the `configure transceiver-test window` command to modify the number of windows.

To determine if you have the transceiver test enabled and the failure action the switch takes, use the `show switch` command. The following is sample transceiver test output:

```
Transceiver Diag: Enabled.    Failure action:  log only
```

For ExtremeWare 6.2.2b108:

The default is `sys-health-check`, and the switch takes the configured system health check action.

Example

The following command configures the switch to perform the configured system health check action if too many failures are detected:

```
configure transceiver-test failure-action sys-health-check
```

History

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to `log` in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

configure transceiver-test period

```
configure transceiver-test period <period <1-60>>
```

Description

Configures how often the switch runs the transceiver test.

Syntax Description

period <1-60>	Specifies, in seconds, how often the transceiver test runs. The range is 1 to 60.

Default

12 seconds.

Usage Guidelines

Use this feature when the switch can be brought off-line.

Configuring the transceiver test period to 11 seconds or less can affect system performance; therefore, Extreme Networks does not recommend changing the default transceiver test period. The default is adequate for most networks.

Example

The following command configures the transceiver test to run every 15 seconds:

```
configure transceiver-test period 15
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

configure transceiver-test threshold

```
configure transceiver-test threshold <1-8>
```

Description

Configures the number of errors the switch accepts before an action is taken.

Syntax Description

threshold	Specifies the number of errors. The range is 1 to 8 errors.

Default

3 errors.

Usage Guidelines

Use this feature when the switch can be brought off-line.

Extreme Networks does not recommend changing the default transceiver test threshold parameter. The default parameter is adequate for most networks.

Example

The following command configures the switch to accept 4 errors before an action is taken:

```
configure transceiver-test threshold 4
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

configure transceiver-test window

```
configure transceiver-test window <1-8>
```

Description

Configures the number of 20-second windows within which the configured number of errors can occur.

Syntax Description

window	Specifies the number of 20-second windows. The range is 1 to 8 20-second windows.

Default

8 windows.

Usage Guidelines

Use this feature when the switch can be brought off-line.

This configuration provides a sliding window. If you keep the window configuration at 8, the switch checks for errors within the *last* eight 20-second windows.

To determine the number of errors the switch accepts before it takes action, use the `configure transceiver-test threshold <1-8>` command.

Extreme Networks does not recommend changing the default transceiver test window parameter. The default parameter is adequate for most networks.

Example

The following command configures the switch to check for errors within the last seven 20-second windows:

```
configure transceiver-test window 7
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

create log filter

```
create log filter <name> {copy <filter name>}
```

Description

Create a log filter with the specified name.

Syntax Description

name	Specifies the name of the filter to create.
copy	Specifies that the new filter is to be copied from an existing one.
filter name	Specifies the existing filter to copy.

Default

N/A

Usage Guidelines

This command creates a filter with the name specified. A filter is a customizable list of events to include or exclude, and optional parameter values. The list of events can be configured by component or subcomponent with optional severity, or individual condition, each with optional parameter values. See the commands `configure log filter events` and `configure log filter events match` for details on how to add items to the filter.

The filter can be associated with one or more targets using the `configure log target filter` command to control the messages sent to those targets. The system has one built-in filter named *DefaultFilter*, which itself may be customized. Therefore, the `create log filter` command can be used if a filter other than *DefaultFilter* is desired. As its name implies, *DefaultFilter* initially contains the default level of logging in which every ExtremeWare component and subcomponent has a pre-assigned severity level.

If another filter needs to be created that will be similar to an existing filter, use the `copy` option to populate the new filter with the configuration of the existing filter. If the `copy` option is not specified, the new filter will have no events configured and therefore no incidents will pass through it.

The total number of supported filters, including *DefaultFilter*, is 20.

Example

The following command creates the filter named *fdb2*, copying its configuration from the filter *DefaultFilter*:

```
create log filter fdb2 copy DefaultFilter
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

delete log filter

```
delete log filter [<filter name> | all]
```

Description

Delete a log filter with the specified name.

Syntax Description

filter name	Specifies the filter to delete.
all	Specifies that all filters, except DefaultFilter, are to be deleted

Default

N / A

Usage Guidelines

This command deletes the specified filter, or all filters except for the filter *DefaultFilter*. The specified filter must not be associated with a target. To remove that association, associate the target with *DefaultFilter* instead of the filter to be deleted, using the following command:

```
configure log target <target> filter DefaultFilter
```

Example

The following command deletes the filter named *fdb2*:

```
delete log filter fdb2
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

disable cli-config-logging

```
disable cli-config-logging
```

Description

Disables the logging of CLI configuration commands to the switch Syslog.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

The `disable cli-config-logging` command discontinues the recording of all switch configuration changes and their sources that are made using the CLI via Telnet or the local console. After you disable configuration logging, no further changes are logged to the system log.

To view the status of configuration logging on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for configuration logging.

Example

The following command disables the logging of CLI configuration command to the Syslog:

```
disable cli-config-logging
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable flowstats

```
disable flowstats
```

Description

Disables the flow statistics feature on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

When this feature is disabled, no flow records are exported.

Example

The following command disables the NetFlow statistics feature on this switch:

```
disable flowstats
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable flowstats filter ports

```
disable flowstats filter <filter#> ports <portlist> {ingress | egress}
```

Description

Disables a specified flow record filter for the specified ports.

Syntax Description

filter#	Specifies the flow record filter that should be disabled.
portlist	Specifies a list of ports or slots and ports for which the filter should be disabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
ingress	Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to inbound flows. Supported on the PoS module only.
egress	Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to outbound flows. Supported on the PoS module only.

Default

For the PoS module, filter #1 is enabled on all SONET ports, and the remaining filters are disabled.

For other switches or modules, filters are enabled by default when they are configured.

Usage Guidelines

The `filter#` parameter is an integer in the range [1-8].

For each SONET port on a PoS module, sixteen filters are supported—eight filters for ingress flows and another eight filters for egress flows. The `filter#` parameter and either the `ingress` or `egress` keyword are used to identify the particular filter that is being disabled.

One of either the `ingress` or `egress` keywords are required for SONET ports.

Example

The following command disables filter 3 for ports 1-8 on an "*i*" series switch:

```
disable flowstats filter 3 ports 1-8
```

The following command example disables ingress filter #2 on port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
disable flowstats filter 2 ports 8:1 ingress
```

History

This command was first available in ExtremeWare 6.1.5b20 for the PoS module only.

This command was first available in ExtremeWare 6.2 for all "*i*" series platforms.

Platform Availability

This command is available on all platforms.

disable flowstats ping-check

```
disable flowstats ping-check {<group#> | all}
```

Description

Disables the flow statistics ping-check function for a specified group of collector devices.

Syntax Description

group#	Specifies the export group for which the ping-check function should be disabled.

Default

Disabled.

Usage Guidelines

On the PoS module, if you do not include a group number, ping-check is disabled for all export groups. The group number is not optional for other Extreme "*i*" series devices.

Example

The following command disables the ping-check function for all export groups.

```
disable flowstats ping-check
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable flowstats ports

```
disable flowstats ports <portlist>
```

Description

Disables the flow statistics function on the specified ports.

Syntax Description

portlist	Specifies a list of ports or slots and ports for which the flowstats function should be disabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

On the PoS module, flow statistics are only collected on SONET ports that are configured to use the IP control protocol, IPCP, (in other words, flow statistics are not collected on ports that are configured to use the bridging control protocol, BCP). Also, there are no configuration restrictions that prohibit enabling of the flow statistics function on ports that are not configured to use IPCP; statistics are not collected on those ports.

Example

The following command disables NetFlow statistics for ports 1-8 on this switch:

```
disable flowstats ports 1-8
```

History

This command was first available in ExtremeWare 6.1.5b20 for the PoS module

This command was made available in ExtremeWare 6.2 for all “i” series platforms.

Platform Availability

This command is available on all platforms.

disable log debug-mode

```
disable log debug-mode
```

Description

Disables debug mode. The switch stops logging events of severity debug-summary, debug-verbose, and debug-data.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command disables debug mode. Debug mode must be enabled prior to logging debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

Example

The following command disables debug mode:

```
disable log debug-mode
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

disable log display

```
disable log display
```

Description

Disables the sending of messages to the console display.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

If the log display is disabled, log information is no longer written to the serial console.

This command setting is saved to FLASH and determines the initial setting of the console display at boot up.

In ExtremeWare 7.1.0, the ability to control logging to different targets was introduced. The new command equivalent to `disable log display` is the following:

```
disable log target console-display
```

Example

The following command disables the log display:

```
disable log display
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable log target

```
disable log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]]
```

Description

Stop sending log messages to the specified target.

Syntax Description

console-display	Specifies the console display.
memory-buffer	Specifies the switch memory buffer.
nvram	Specifies the switch NVRAM.
session	Specifies the current session (including console display).
syslog	Specifies a syslog target.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.

Default

Enabled, for memory buffer and NVRAM; all other targets are disabled by default.

Usage Guidelines

This command stops sending messages to the specified target. By default, the memory buffer and the NVRAM targets are enabled. Other targets must be enabled before messages are sent to those targets.

Configuration changes to the `session` target are in effect only for the duration of the console display or telnet session, and are not saved in FLASH. Changes to the other targets are saved to FLASH.

In earlier versions of ExtremeWare, a similar command was used to disable displaying the log on the console. That command:

```
disable log display
```

is equivalent to:

```
disable log target console-display
```

Example

The following command disables log messages to the current session:

```
disable log target session
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

disable rmon

```
disable rmon
```

Description

Disables the collection of RMON statistics on the switch.

Syntax Description

This command has no arguments or variables.

Default

By default, RMON is disabled. However, even in the disabled state, the switch responds to RMON queries and sets for alarms and events.

Usage Guidelines

The switch supports four out of nine groups of Ethernet RMON statistics. In a disabled state, the switch continues to respond to the following two groups:

- Alarms—The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be auto calibrated or set manually.
- Events—The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

To view the status of RMON polling on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for RMON polling.

Example

The following command disables the collection of RMON statistics on the switch:

```
disable rmon
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

disable sys-health-check

```
disable sys-health-check
```

Description

Disables the BlackDiamond system health checker.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

If the system health checker is disabled, it does not test I/O modules, MSM64i modules, and the backplane for system faults.

Example

The following command disables the BlackDiamond system health checker:

```
disable sys-health-check
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on BlackDiamond switches only.

disable syslog

```
disable syslog
```

Description

Disables logging to all remote syslog server targets.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Disables logging to all remote syslog server targets, not to the switch targets. This setting is saved in FLASH, and will be in effect upon boot up.

Example

The following command disables logging to all remote syslog server targets:

```
disable syslog
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable temperature-logging

```
disable temperature-logging
```

Description

Stops recording the system temperature in celsius for the BlackDiamond and Alpine systems to the syslog.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Use this command to stop recording the system temperature to the syslog.

If you already enabled temperature logging, and you want to view the current temperature of the system, do the following:

1. Disable the temperature logging feature using the following command:

   `disable temperature-logging`
2. Re-enable the temperature logging feature using the following command:

   `enable temperature-logging`
3. Display the syslog using the following command:

   `show log`

Example

The following command stops recording the system temperature to the syslog:

`disable temperature-logging`

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This is supported and the command syntax changed from `disable log temperature` in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

disable transceiver-test

```
disable transceiver-test [all | slot <slot number> {backplane} | msm-a |
msm-b]
```

Description

Disable the integrity testing of the transceivers used for communication between the ASICs and the CPU on an MSM or an SMMi module.

Syntax Description

all	Specifies all of the slots in the chassis.
slot number	Specifies a single slot in the chassis.
backplane	Specifies the backplane of the chassis. This is available on Alpine switches only.
msm-a	Specifies the MSM module installed in slot A. This is available on BlackDiamond switches only.
msm-b	Specifies the MSM module installed in Slot B. This is available on BlackDiamond switches only.

Default

Disabled.

Usage Guidelines

To determine if you have the transceiver test enabled and the failure action the switch takes, use the `show switch` command. The following is sample transceiver test output:

```
Transceiver Diag: Enabled.    Failure action:  log only
```

To display the transceiver test statistics, use the `show diagnostics sys-health-check` command. The following is sample output:

```
Transceiver system health diag result
Pass/Fail Counters Are in HEX
Slot    Cardtype Cardstate   Test        Pass     Fail Time_last_fail
----    -------- ---------   ----    -------- -------- --------------
slot 1  Unknown
slot 2  Unknown
slot 3  FM8V     Operational MAC        2b81b        0
slot 4  GM4X     Operational MAC        2b81b        0
BPLNE   SMMI     Operational UART       2b81a        0
BPLNE   SMMI     Operational FLASH      2b81a        0
BPLNE   SMMI     Operational SRAM       2b81a        0
BPLNE   SMMI     Operational NVRAM      2b81a        0
BPLNE   SMMI     Operational ENET       2b81a        0
BPLNE   Basbrd   Operational QUAKE      2b81a        0
BPLNE   Basbrd   Operational TWISTER    2b81a        0
```

For ExtremeWare 6.2.2b108:

The default for the transceiver test is enabled. The test is enabled two minutes after the switch boots or immediately after you enable the test.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the transceiver test is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, the transceiver test is enabled. You must manually disable the transceiver test if you want the feature disabled.

Example

The following command disables the transceiver test on slot 4 of a modular switch:

```
disable transceiver-test slot 4
```

History

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

enable cli-config-logging

```
enable cli-config-logging
```

Description

Enables the logging of CLI configuration commands to the Syslog for auditing purposes.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

ExtremeWare allows you to record all configuration changes and their sources that are made using the CLI by way of Telnet or the local console. The changes are logged to the system log. Each log entry includes the user account name that performed the changes and the source IP address of the client (if Telnet was used). Configuration logging applies only to commands that result in a configuration change.

To view the status of configuration logging on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for configuration logging.

Example

The following command enables the logging of CLI configuration commands to the Syslog:

```
enable cli-config-logging
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable flowstats

```
enable flowstats
```

Description

Enables the flow statistics feature on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command enables NetFlow statistics feature on this switch:

```
enable flowstats
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable flowstats filter ports

```
enable flowstats filter <filter#> ports <portlist> {ingress | egress}
```

Description

Enables a specified flow record filter for the specified ports.

Syntax Description

filter#	Specifies the flow record filter that should be enabled.
portlist	Specifies the ports or slots and ports for which the filter should be enabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
ingress	Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to inbound flows on the SONET port(s). Supported on the PoS module only.
egress	Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to outbound flows on the SONET port(s). Supported on the PoS module only.

Default

For the PoS module, filter #1 is enabled on all SONET ports, and the remaining filters are disabled.

For other switches or modules, filters are enabled by default when they are configured.

Usage Guidelines

The `filter#` parameter is an integer in the range [1-8]. A filter must be enabled to match a flow. For "i" series devices other than the PoS module, these apply to outbound flows only.

For each SONET port on a PoS module, sixteen filters are supported—eight filters for ingress flows and another eight filters for egress flows. The `filter#` parameter and either the `ingress` or `egress` keyword are used to identify the particular filter that is being disabled.

One of either the `ingress` or `egress` keywords are required for SONET ports.

Example

The following command enables filter 3 for ports 1-8 on the switch:

```
enable flowstats filter 3 ports 1-8
```

History

This command was first available in ExtremeWare 6.1.5b20 for the PoS module only.

This command was first available in ExtremeWare 6.2 for all "*i*" series platforms.

Platform Availability

This command is available on all platforms.

enable flowstats ping-check

```
enable flowstats ping-check {<group#>}
```

Description

Enables the flow statistics ping-check function for a specified group of collector devices.

Syntax Description

group#	Specifies the export group for which the ping-check function should be enabled.

Default

Enabled.

Usage Guidelines

If a flow-collector device is repeatedly unresponsive to ping requests, it is temporarily removed from the distribution list for any export groups of which it is a member. The device will be returned to the distribution list automatically when subsequent ping-checks are successful.

On the PoS module, if you do not include a group number, ping-check is enabled for all export groups.

Example

The following command enables the ping-check function for export group 3.

```
enable flowstats ping-check 3
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable flowstats ports

```
enable flowstats ports <portlist>
```

Description

Enables the flow statistics function on the specified ports.

Syntax Description

portlist	Specifies a list of ports or slots and ports for which the flowstats function should be enabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

On the PoS module, flow statistics are only collected on SONET ports that are configured to use the IP control protocol, IPCP, (in other words, flow statistics are not collected on ports that are configured to use the bridging control protocol, BCP). Also, there are no configuration restrictions that prohibit enabling of the flow statistics function on ports that are not configured to use IPCP; statistics are not collected on those ports.

Example

The following command enables the ping-check function for all export groups.

```
enable flowstats ping-check
```

History

This command was first available in ExtremeWare 6.1.5b20 for the PoS module

This command was made available in ExtremeWare 6.2 for all “i” series platforms.

Platform Availability

This command is available on all platforms.

enable log debug-mode

```
enable log debug-mode
```

Description

Enables debug mode. The switch allows debug events included in log filters to be logged.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command enables debug mode. Debug mode must be enabled prior to logging debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

Example

The following command enables debug mode:

```
enable log debug-mode
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

enable log display

```
enable log display
```

Description

Enables a running real-time display of log messages on the console display.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

If you enable the log display on a terminal connected to the console port, your settings will remain in effect even after your console session is ended (unless you explicitly disable the log display).

You configure the messages displayed in the log using the `configure log display`, or `configure log target console-display` commands.

In ExtremeWare 7.1.0, the ability to control logging to different targets was introduced. The new command equivalent to `enable log display` is the following:

```
enable log target console-display
```

To change the log filter association, severity threshold, or match expression for messages sent to the console display, use the `configure log target console-display` command

Example

The following command enables a real-time display of log messages:

```
enable log display
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable log target

```
enable log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]]
```

Description

Start sending log messages to the specified target.

Syntax Description

console-display	Specifies the console display.
memory-buffer	Specifies the switch memory buffer.
nvram	Specifies the switch NVRAM.
session	Specifies the current session (including console display).
syslog	Specifies a syslog target.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.

Default

Enabled, for memory buffer and NVRAM; all other targets are disabled by default.

Usage Guidelines

This command starts sending messages to the specified target. By default, the memory-buffer and the NVRAM targets are enabled. Other targets must be enabled before messages are sent to those targets.

Configuration changes to the `session` target are in effect only for the duration of the console display or telnet session, and are not saved in FLASH. Others are saved in FLASH.

In earlier versions of ExtremeWare, a similar command was used to enable displaying the log on the console. That command:

```
enable log display
```

is equivalent to:

```
enable log target console-display
```

Example

The following command enables log messages on the current session:

```
enable log target session
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

enable rmon

```
enable rmon
```

Description

Enables the collection of RMON statistics on the switch.

Syntax Description

This command has no arguments or variables.

Default

By default, RMON is disabled. However, even in the disabled state, the switch responds to RMON queries and sets for alarms and events. By enabling RMON, the switch begins the processes necessary for collecting switch statistics.

Usage Guidelines

The switch supports four out of nine groups of Ethernet RMON statistics. In an enabled state, the switch responds to the following four groups:

- Statistics—The RMON Ethernet Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts, and errors on a LAN segment or VLAN.
- History—The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.
- Alarms—The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be auto calibrated or set manually.
- Events—The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

NOTE

You can only use the RMON features of the system if you have an RMON management application and have enabled RMON on the switch.

RMON requires one probe per LAN segment, and standalone RMON probes have traditionally been expensive. Therefore, Extreme's approach has been to build an inexpensive RMON probe into the agent of each system. This allows RMON to be widely deployed around the network without costing more than traditional network management. The switch accurately maintains RMON statistics at the maximum line rate of all of its ports.

For example, statistics can be related to individual ports. Also, because a probe must be able to see all traffic, a stand-alone probe must be attached to a nonsecure port. Implementing RMON in the switch means that all ports can have security features enabled.

To view the status of RMON polling on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for RMON polling.

Example

The following command enables the collection of RMON statistics on the switch:

```
enable rmon
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

enable sys-health-check

```
enable sys-health-check
```

Description

Enables the BlackDiamond system health checker.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

The system health checker tests I/O modules, MSM64i modules, and the backplane by forwarding packets every 4 seconds. Additional checking for the validity of these packets is completed by performing a checksum.

By isolating faults to a specific module, MSM64i, or backplane connection, the system health checker prevents corrupted packets from being propagated to the CPU, upper layer modules, or the rest of your network. If you observe a failure, please contact Extreme Technical Support.

Depending on how you have configured the system health checker, failed system health checks may generate critical error messages in the syslog, and may also send a trap and/or shut down the system. The system health checker will continue to periodically forward test packets to failed components. If auto-recovery is configured, the system will attempt to automatically reset the faulty module and bring it back online.

In ExtremeWare versions prior to 6.2, you cannot use both mirroring and the system health checker at the same time. If you configure mirroring with the system health checker enabled, the health checker will indicate that it has been disabled by sending a message to the syslog. In version 6.2 or later, this restriction does not apply.

To configure the health checker, use the following command:

```
configure sys-health-check [alarm-level [card-down | default | log | system-down |
traps] | auto-recovery <number of tries>]
```

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

Example

The following command enables the BlackDiamond system health checker:

```
enable sys-health-check
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on BlackDiamond switches only.

enable syslog

```
enable syslog
```

Description

Enables logging to all remote syslog host targets.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

In order to enable remote logging, you must do the following:

- Configure the syslog host to accept and log messages.
- Enable remote logging by using the `enable syslog` command.
- Configure remote logging by using the `configure syslog` command.

When you use the `enable syslog` command, the exporting process of the syslog begins. This command also determines the initial state of an added remote syslog target.

Example

The following command enables logging to all remote syslog hosts:

```
enable syslog
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable temperature-logging

```
enable temperature-logging
```

Description

Records the system temperature in celsius for the BlackDiamond and Alpine systems to the syslog.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

When you enable temperature logging, the temperature is recorded every hour.

To view the temperature of the system, use the `show log` command. The following is sample temperature output from the `show log` command:

```
06/12/2003 19:50:59.00 <Info:ELRP> Current temperature reading [197] is 49C.
06/12/2003 18:50:59.00 <Info:ELRP> Current temperature reading [196] is 48C.
06/12/2003 17:50:59.00 <Info:ELRP> Current temperature reading [195] is 48C.
```

To clear all of the log statistics, including the system temperature output, use the `clear log` command. Since the temperature is recorded based on the time you enabled temperature logging, it may take up to one hour for a new temperature to be recorded to the syslog.

If you already enabled temperature logging, and you want to view the current temperature of the system, do the following:

1. Disable the temperature logging feature using the following command:

   ```
   disable temperature-logging
   ```

2. Re-enable the temperature logging feature using the following command:

   ```
   enable temperature-logging
   ```

3. Display the syslog using the following command:

   ```
   show log
   ```

Example

The following command records the system temperature to the syslog:

```
enable temperature-logging
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

The command was supported and the syntax changed from `enable log temperature` in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

enable transceiver-test

```
enable transceiver-test [all | slot <slot number> {backplane} | msm-a |
msm-b]
```

Description

Enables an integrity test of the transceivers used for communication between the ASICs and the CPU on an MSM or an SMMi module.

Syntax Description

all	Specifies all of the slots in the chassis.
slot number	Specifies a single slot in the chassis.
backplane	Specifies the backplane of the chassis. This is available on Alpine switches only.
msm-a	Specifies the MSM module installed in slot A. This is available on BlackDiamond switches only.
msm-b	Specifies the MSM module installed in Slot B. This is available on BlackDiamond switches only.

Default

Disabled.

Usage Guidelines

The `enable transceiver-test` command is a useful diagnostic tool. Use this command if you suspect a problem with the system and to test the integrity of the transceivers.

To determine if you have the transceiver test enabled and the failure action the switch takes, use the `show switch` command. The following is sample transceiver test output:

```
Transceiver Diag: Enabled.    Failure action:  log only
```

To display the transceiver test statistics, use the `show diagnostics sys-health-check` command. The following is sample output:

```
Transceiver system health diag result
Pass/Fail Counters Are in HEX
Slot    Cardtype Cardstate   Test        Pass     Fail Time_last_fail
----    -------- ---------   ----    -------- -------- --------------
slot 1  Unknown
slot 2  Unknown
slot 3  FM8V     Operational MAC        2b81b        0
slot 4  GM4X     Operational MAC        2b81b        0
BPLNE   SMMI     Operational UART       2b81a        0
BPLNE   SMMI     Operational FLASH      2b81a        0
BPLNE   SMMI     Operational SRAM       2b81a        0
BPLNE   SMMI     Operational NVRAM      2b81a        0
BPLNE   SMMI     Operational ENET       2b81a        0
BPLNE   Basbrd   Operational QUAKE      2b81a        0
BPLNE   Basbrd   Operational TWISTER    2b81a        0
```

For ExtremeWare 6.2.2b108:

The default for the transceiver test is enabled. The test is enabled two minutes after the switch boots or immediately after you enable the test.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the transceiver test is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, the transceiver test is enabled. You must manually disable the transceiver test if you want the feature disabled.

Example

The following command enables the transceiver test on slot 4 of a modular switch:

```
enable transceiver-test slot 4
```

History

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

show flowstats

```
show flowstats {<portlist> | export {<group#>}}
```

Description

Displays status information for the flow statistics function.

Syntax Description

portlist	Use this optional parameter to specify one or more ports or slots and ports for which status information is to be displayed.
group#	Use this optional parameter with the `group` keyword to display status information for a specific export group.

Default

Displays summary statistics information for all ports.

Usage Guidelines

The command with no arguments displays flowstats configuration information for all ports. The information is displayed in a format similar to the flowstats command syntax. For the statistics that apply to individual ports, the port number is presented without a "port" keyword. For example, in the `NetFlow Enable/Disable per port` and `NetFlow TimeOut Config` sections of the example below, the port number immediately follows the `flowstats` keyword. The following information is displayed:

- Whether the flowstats feature is enabled or disabled
- Whether flowstats is enabled or disabled for individual ports
- The configuration of flow-collector devices (`NetFlow Server Config`)
- NetFlow Timeout configurations
- Whether NetFlow Filters are enable or disabled
- NetFlow filter specifications
- NetFlow ping-check configuration

When the `detail` keyword is included, the NetFlow Servers Config section is replaced by detailed configuration information that includes counts of the number of times each flow-collector device has been removed from the distribution list due to ping-check failures.

For each export group, the following information is displayed:

- Whether ping-check is enabled
- The source IP address
- An entry for each flow-collector device in the export group, displaying the following:
  - The IP address of the device
  - The UPD port number for the device
  - Whether the device is up or down (based on the ping-check response)
  - The number of times the device has been unreachable based on the ping-check response

Example

The `show flowstats` command with no options, for a switch with NetFlow statistics enabled on ports 1, 40, and 43, displays output similar to the following:

```
Summit48i: show flowstats

Flowstats enabled

Port      Filter     proto   timeout     group    OverflowPkts     flags
-------------------------------------------------------------------------------
-------
1         1        IP           5        3         N/A           EIA
   DestIP:      10.203.0.1/255.255.255.255         DestPort: any
   SrcIP:  any                                     SrcPort: any

40         8         -           5         1       N/A           EIA
   Dest/Src Info: match-all-flows

43         3       TCP        5       32           N/A         EIA
   DestIP:        10.0.1.1/255.255.255.254         DestPort: any
   SrcIP:     10.201.32.1/255.255.255.255          SrcPort: any

Flags:  E - Enable, D - Disable; I - Ingress, S - Egress; A - Aggregation
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show flowstats export

```
show flowstats export [ detail |{<group number> detail} ]
```

Description

Displays configuration information an export group.

Syntax Description

group number	Specifies a group number for which configuration information should be displayed.

Default

N/A.

Usage Guidelines

The information displayed by this command is displayed in a format similar to the `configure flowstats export` command. The following information is displayed:

- Whether the flowstats feature is enabled or disabled
- The configuration of flow-collector devices for the export group (`NetFlow Server Config`)
- NetFlow ping-check configuration

Example

The following command displays detailed configuration information for export group 1:

```
show flowstats export 1 detail
Group: 1  ping-check: enable  Source ip_address: 10.201.26.217
ip_address 10.201.31.237   udp_port  9995 status   up    0 times, outpkts   256
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show flowstats

```
show flowstats <portlist>
```

Description

Displays status information for the flow statistics function.

Syntax Description

portlist	Specifies a list of ports or slots and ports for which flow statistics should be displayed. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

This command displays flowstats configuration information for an individual port. The information is displayed in a format similar to the flowstats command syntax. The following information is displayed:

- Whether the flowstats feature is enabled or disabled
- Whether flowstats is enabled or disabled for the specified port
- NetFlow Timeout configuration for the port
- Whether NetFlow Filters are enable or disabled for the port
- NetFlow filter specifications for the port

Example

The following command displays statistics for ports 1, 40, and 48:

```
Summit48i: show flowstats 1, 40, 48
Flowstats enabled

Port      Filter     proto   timeout     group    OverflowPkts     flags
--------------------------------------------------------------------------------
1         3        IP           5         3         N/A           EIA
   DestIP:      10.203.0.1/255.255.255.255         DestPort: any
   SrcIP:  any                                     SrcPort: any

40         8         -           5         1       N/A           EIA
   Dest/Src Info: match-all-flows

48         1       TCP          20         1       N/A           EIA
   DestIP:     10.201.26.0/  255.255.255.0         DestPort: any
   SrcIP:     10.201.31.0/  255.255.255.0          SrcPort: any

48         2       UDP          20         1         N/A           EIA
   DestIP:     10.201.26.0/  255.255.255.0         DestPort: any
   SrcIP:     10.201.31.0/  255.255.255.0          SrcPort: any
Flags:  E - Enable, D - Disable; I - Ingress, S - Egress; A - Aggregation
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show log

```
show log {messages [memory-buffer | nvram]} {severity <severity> {only}}
{starting [date <date> time <time> | date <date> | time <time>]} {ending
[date <date> time <time> | date <date> | time <time>]} {match
<match-expression>} {format <format>} {chronological}
```

Description

Displays the current log messages.

Syntax Description

messages	Specifies the target location from which to display the log messages.
memory-buffer	Show messages stored in volatile memory (default).
nvram	Show messages stored in NVRAM.
severity	Specifies the minimum severity level to display (if the keyword only is omitted).
only	Specifies that only the specified severity level is to be displayed
starting	Show messages with timestamps equal to or greater than that specified
date	Specifies the date, where date is <month (1-12)> / <day> {/ <year (yyyy)>}.
time	Specifies the time, where time is <hour (0-23)> {: <minute (0-59)> {: <seconds> {. <hundredths>}}}
ending	Show messages with timestamps equal to or less than that specified.
match-expression	Specifies a regular expression. Only messages that match the regular expression will be displayed.
format	Specifies a format to use to override the format configured for the memory buffer.
chronological	Specifies displaying log messages in ascending chronological order (oldest to newest).

Default

The following defaults apply:

- messages—memory buffer
- severity—none (displays everything stored in the target)
- starting, ending—if not specified, no timestamp restriction
- match—no restriction
- format—the format configured with the `configure log target format` command
- chronological—if not specified, show messages in order from newest to oldest

Usage Guidelines

Switch configuration and fault information is filtered and saved to target logs, in a memory buffer, and in NVRAM. Each entry in the log contains the following information:

- Timestamp—records the month and day of the event, along with the time (hours, minutes, seconds, and hundredths).

- Severity Level—indicates the urgency of a condition reported in the log. Table 15 describes the severity levels assigned to events.
- Component, Subcomponent, and Condition Name—describes the subsystem in the software that generates the event. This provides a good indication of where a fault might lie.
- Message—a description of the event occurrence. If the event was caused by a user, the user name is also provided.

This command displays the messages stored in either the internal memory buffer or in NVRAM. The messages shown can be limited by specifying a severity level, a time range, or a match expression. Messages stored in the target have already been filtered as events occurred, and specifying a severity or match expression on the `show log` command can only further limit the messages shown.

If the `messages` keyword is not present, the messages stored in the memory-buffer target are displayed. Otherwise, the messages stored in the specified target are displayed.

If the `only` keyword is present following the severity value, then only the events at that exact severity are included. Without the `only` keyword, events at that severity or more urgent are displayed. For example, severity `warning` implies critical, error, or warning, whereas severity `warning only` implies only warning.

Messages whose timestamps are equal or later than the starting time and are equal or earlier than the specified ending time will be shown if they also pass the severity requirements and match expression, if specified.

If the format phrase is specified, this format overrides the format already configured for the specified log. See the command `configure log target format` on page 599 for more information on specifying a format.

If a `match` phrase is specified, the formatted message must match the simple regular expression specified by `match-expression` for it to be shown.

A simple regular expression is a string of single characters including the dot character (.), which are optionally combined with quantifiers and constraints. A dot matches any single character while other characters match only themselves (case is significant). Quantifiers include the star character (*) that matches zero or more occurrences of the immediately preceding character or dot. Constraints include the caret character (^) that matches at the beginning of a message, and the currency character ($) that matches at the end of a message. Bracket expressions are not supported. There are a number of sources available on the Internet and in various language references describing the operation of regular expressions.

If the `chronological` keyword is specified, messages are shown from oldest to newest; otherwise, messages are displayed newest to oldest.

Severity Level. The severity levels are `critical`, `error`, `warning`, `notice`, and `info`, plus three severity levels for extended debugging, `debug-summary`, `debug-verbose`, and `debug-data`. In log messages, the severity levels are shown by four letter abbreviations. The abbreviated forms are:

- Critical—Crit
- Error—Erro
- Warning—Warn
- Notice—Noti
- Info—Info
- Debug-Summary—Summ
- Debug-Verbose—Verb

- Debug-Data—Data

The three severity levels for extended debugging, `debug-summary`, `debug-verbose`, and `debug-data`, require that debug mode be enabled (which may cause a performance degradation). See the command `enable log debug-mode` on page 648.

Table 15: Severity Levels Assigned by the Switch[1]

Level	Description
Critical	A serious problem has been detected which is compromising the operation of the system and that the system can not function as expected unless the situation is remedied. The switch may need to be reset.
Error	A problem has been detected which is interfering with the normal operation of the system and that the system is not functioning as expected.
Warning	An abnormal condition, not interfering with the normal operation of the system, has been detected which may indicate that the system or the network in general may not be functioning as expected.
Notice	A normal but significant condition has been detected, which signals that the system is functioning as expected.
Info (Informational)	A normal but potentially interesting condition has been detected, which signals that the system is functioning as expected and simply provides information or confirmation about the condition.
Debug-Summary	A condition has been detected that may interest a developer determining the reason underlying some system behavior.
Debug-Verbose	A condition has been detected that may interest a developer analyzing some system behavior at a more verbose level than provided by the debug summary information.
Debug-Data	A condition has been detected that may interest a developer inspecting the data underlying some system behavior.

1. In ExtremeWare version 7.1.0, the levels alert and emergency were deprecated. The equivalent level is critical.

Log entries remain in the NVRAM log after a switch reboot. Issuing a `clear log` command does not remove these static entries. To remove log entries from NVRAM, use the following command:

```
clear log messages nvram
```

Example

The following command displays messages with a critical severity:

```
show log critical
```

The following command displays messages with warning, error, or critical severity:

```
show log warning
```

The following command displays messages containing the string “slot 2”:

```
show log match "slot 2"
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.2 to include the `chronological` option.

This command was modified in ExtremeWare 7.1.0 to include the `messages`, `severity`, `only`, `starting`, `ending`, `match`, and `format` options.

Platform Availability

This command is available on all platforms.

show log components

```
show log components {<event component> | all}
```

Description

Display the name, description and default severity for all components.

Syntax Description

event component	Specifies component to display.
all	Displays all components.

Default

N/A.

Usage Guidelines

This command displays the name, description, and default severity defined for the specified components and subcomponents.

Example

The following command displays the log components:

```
show log components
```

The output produced by the `show log components` command is similar to the following:

```
show log components
                                                                  Severity
Component           Title                                         Threshold
------------------- --------------------------------------------- -------------
BGP                 Border Gateway Protocol                       Error
        Dampening   BGP Route Flap Dampening                      Error
        Event       BGP Finite State Machine                      Error
        Keepalive   BGP Keepalive Messages                        Error
        Message     BGP Messages (Open, Update, Notification)     Error
        Misc        BGP Miscellaneous (Import, Aggregate, NextHop) Error
        UpdateIn    BGP Incoming Update Messages                  Error
        UpdateOut   BGP Outgoing Update Messages                  Error
Bridge              Layer 2 Bridging                              Error
        Learning    Layer 2 Bridge Learning                       Error
EAPS                Ethernet Automatic Protection Switching (EAPS) Error
        MSMFailover EAPS MSM Failover                             Error
        SharedPort  EAPS SharedPort Domain                        Error
EDP                 Extreme Discovery Protocol (EDP)              Error
ELRP                Extreme Loop Recovery Protocol (ELRP)         Error
ESRP                Extreme Standby Router Protocol (ESRP)        Notice
        Aware       ESRP Aware Processing                         Notice
        Message     ESRP PDU Tx/Rx                                Error
        MSMFailover ESRP MSM Failover                             Error
        State       ESRP State Transitions                        Notice
```

```
        Tracking    ESRP Tracking                                Error
FDB                 Forwarding Data Base                         Error
        IP          IP FDB                                       Error
        IPMC        IP Multicast FDB                             Error
        Replacement FDB Replacement                              Error
IGMP                Internet Group Management Protocol           Error
        Snooping    IGMP Snooping                                Error
IP                                                               N/A
        AccessList  IP Access List                               Error
        Forwarding  IP Forwarding                                Error
Log                 Event Management System (EMS)                Error
OSPF                Open Shortest Path First                     Error
        Event       OSPF Events                                  Error
        Hello       OSPF Hello                                   Error
        LSA         OSPF Link-State Advertisement                Error
        Neighbor    OSPF Neighbor                                Error
        SPF         OSPF Shortest Path First                     Error
SNTP                Simple Network Time Protocol                 Warning
STP                 Spanning-Tree Protocol (STP)                 Error
        InBPDU      STP In BPDU subcomponent                     Warning
        OutBPDU     STP Out BPDU subcomponent                    Warning
        System      STP System subcomponent                      Error
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show log configuration

```
show log configuration
```

Description

Displays the log configuration for switch log settings, and for certain targets.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command displays the log configuration for all targets. The state of the target, enabled or disabled is displayed. For the enabled targets, the associated filter, severity, match expression, and format is displayed. The debug mode state of the switch is also displayed.

Example

The following command displays the configuration of all the log targets:

```
show log configuration
```

The output produced by the command is similar to the following:

```
Severities: Critical, Error, Warning, Notice, Info, Debug-Summary, Debug-Verbose,
 Debug-Data

Log Target      : session 1028 (10.38.0.42)
    Enabled     : no
    Filter Name : DefaultFilter
    Severity    : info (through critical)
    Match       : (none)
    Format      : MM/DD/YYYY HH:MM:SS.hh <Severity:Component.SubComponent.Conditi
on>

Log Target      : console-display
    Enabled     : no
    Filter Name : DefaultFilter
    Severity    : info (through critical)
    Match       : (none)
    Format      : MM/DD/YYYY HH:MM:SS.hh <Severity:Component.SubComponent.Conditi
on>

Remote syslog targets are disabled by default.
Debug-Mode is disabled.
```

History

This command was first available in ExtremeWare 2.0.

The additional EMS information was added in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

show log configuration filter

```
show log configuration filter {<filter name>}
```

Description

Displays the log configuration for the specified filter.

Syntax Description

filter name	Specifies the filter to display.

Default

If no options are specified, the command displays the configuration for all filters.

Usage Guidelines

This command displays the configuration for filters.

Example

The following command displays the configuration for the filter, *myFilter*:

```
show log configuration filter myFilter
```

The output of this command is similar to the following:

```
Log Filter Name : myFilter
I/                                    Severity  Parameter(s)           Even If
E  Comp.   Sub-comp.   Condition       CEWNISVD  Type   Value           Missing
-  ------- ----------- --------------- --------  ------ --------------------- -
I  BGP     Event       *               CEWN----  B-Nbr  10.1.2.0 / 24         N
                                                   L4   80
E  STP     OutBPDU     *               CEWNISVD                                N
I  STP     *           *               --------                                N

Include/Exclude: I - Include,  E - Exclude
Component Unreg: * - Component/Subcomponent is not currently registered
Severity Values: C - Critical,  E - Error,  W - Warning,  N - Notice,  I - Info
Debug Severity : S - Debug-Summary,  V - Debug-Verbose,  D - Debug-Data
                 (Caution: Debug Severities require "enable log debug-mode")
Parameter Flags: S - Source,  D - Destination  (as applicable)
                 I - Ingress,  E - Egress,  B - BGP
Parameter Types: Port - Physical Port list,  Slot - Physical Slot #
                 MAC  - MAC address,  IP - IP Address/netmask,  Mask - Netmask
                 VID  - Virtual LAN ID (tag),  VLAN - Virtual LAN name
                 L4   - Layer-4 Port #,  Num  - Number,  Str  - String
                 Nbr  - Neighbor, Rtr  - Routerid, EAPS - EAPS Domain
Even If Parameters Missing: Y - Yes,  N - No, or no parameters specified
```

The above output shows three filter items. The first item includes events from the *BGP.Event* subcomponent of severity `notify` and greater where the BGP neighbor matches the 10.1.2.0/24 subnet and the L4 port value is 80. The second item excludes all events from the *STP.OutBPDU* component.

The third item includes the remaining events from the *STP* component. The severity value is show as "-", indicating that the component's default severity threshold controls which messages are passed.

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

show log configuration target

```
show log configuration target {console-display | memory-buffer | nvram |
session | syslog <host name/ip> {: <udp-port>}[local0 ... local7]}
```

Description

Displays the log configuration for the specified target.

Syntax Description

console-display	Show the log configuration for the console display.
memory-buffer	Show the log configuration for volatile memory.
nvram	Show the log configuration for NVRAM.
session	Show the log configuration for the current session (including console display).
syslog	Show the configuration for the specified syslog target.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.

Default

If no options are specified, the command displays the configuration for the current session and console display.

Usage Guidelines

This command displays the log configuration for the specified target. The associated filter, severity, match expression, and format is displayed.

Example

The following command displays the log configuration:

```
show log configuration target
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show log counters

```
show log counters {<event condition> | [all | <event component>] {severity
<severity> {only}}}
```

Description

Displays the incident counters for events.

Syntax Description

event condition	Specifies the event condition to display.
all	Specifies that all events are to be displayed.
event component	Specifies that all the events associated with a particular component or subcomponent should be displayed.
severity	Specifies the minimum severity level of events to display (if the keyword only is omitted).
only	Specifies that only events of the specified severity level are to be displayed

Default

If severity is not specified, then events of all severity are displayed. If detail is not specified, then summary only information is displayed.

Usage Guidelines

This command displays the incident counters for each event specified. Two incident counters are displayed. One counter displays the number of times an event has occurred, and the other displays the number of times that notification for the event was made to the system (an incident record was injected into the system for further processing). Both incident counters reflect totals accumulated since reboot or since the counters were cleared using the `clear log counters` or `clear counters` command, regardless of whether it was filtered or not.

This command also displays a reference count (the column titled `Rf` in the output). The reference count is the number of enabled targets receiving notifications of this event.

See the command `show log` on page 666 for more information about severity levels.

To get a listing of the event conditions in the system, use the following command:

```
show log events
```

To get a listing of the components present in the system, use the following command:

```
show log components
```

Example

The following command displays the event counters for event conditions of severity debug-summary or greater in the component *STP.InBPDU*:

```
show log counters stp.inbpdu severity debug-summary
```

The output produced by the above command is similar to the following:

```
Comp    SubComp     Condition               Severity      Rf Notified Occurred
------- ----------- ----------------------- ------------- -- -------- --------
STP     InBPDU
                    PDUDrop                 Error          1        0        0
                    PDUIgn                  Debug-Summary  0        0        0
                    PDUTrace                Info           0        0        0
```

The following command displays the event counters for the event condition *PDUDrop* in the component *STP.InBPDU*:

```
show log counters "STP.InBPDU.PDUDrop"
```

The output produced by the above command is similar to the following:

```
Comp    SubComp     Condition               Severity      Rf Notified Occurred
------- ----------- ----------------------- ------------- -- -------- --------
STP     InBPDU
                    PDUDrop                 Error          1        0        0
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show log events

```
show log events {<event condition> | [all | <event component>] {severity
<severity> {only}}} {detail}
```

Description

Displays information about the individual events (conditions) that can be logged.

Syntax Description

event condition	Specifies the event condition to display.
all	Specifies that all events are to be displayed.
event component	Specifies that all the events associated with a particular component should be displayed.
severity	Specifies the minimum severity level of events to display (if the keyword only is omitted).
only	Specifies that only events of the specified severity level are to be displayed
detail	Specifies that detailed information, including the message format and parameter types, be displayed.

Default

If severity is not specified, then events of all severity are displayed. If detail is not specified, then summary only information is displayed.

Usage Guidelines

This command displays the mnemonic, message format, severity, and parameter types defined for each condition in the event set specified.

See the command `show log` on page 666 for more information about severity levels.

When the `detail` option is specified, the message format is displayed for the event conditions specified. The message format parameters are replaced by the value of the parameters when the message is generated.

To get a listing of the components present in the system, use the following command:

```
show log components
```

Example

The following command displays the event conditions of severity debug-summary or greater in the component *STP.InBPDU*:

```
show log events stp.inbpdu severity debug-summary
```

The output produced by the above command is similar to the following:

```
Comp    SubComp     Condition               Severity      Parameters
------- ----------- ----------------------- ------------- ----------
STP     InBPDU
                    PDUDrop                 Error          3
                    PDUIgn                  Debug-Summary  2
                    PDUTrace                Info           2
```

The following command displays the details of the event condition *PDUTrace* in the component *STP.InBPDU*:

```
show log events stp.inbpdu.pdutrace detail
```

The output produced by the above command is similar to the following:

```
Comp    SubComp     Condition               Severity      Parameters
------- ----------- ----------------------- ------------- ----------
STP     InBPDU      PDUTrace                Info           2 Total
                                                           0 - string
                                                           1 - ports
                    "Port=%1%: %0%"
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show memory

```
show memory {detail}
```

Description

Displays the current system memory information.

Syntax Description

detail	Specifies task-specific memory usage.

Default

N/A.

Usage Guidelines

Your BlackDiamond or Summit switch must have 32MB of DRAM to support the features in ExtremeWare version 4.0 and above.

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

The `show memory` command displays the following information in a tabular format:

- System memory information including the total DRAM size of your system.
- Current memory (both free and allocated memory) used by the system and the users.
- Cumulative memory (both free and allocated memory) used by the users.
- Software packet memory statistics including the type of packet, the number of allocated and free packets, the number of packet failures, and data and other blocks.
- Memory utilization statistics including the total blocks of memory available and the memory being used on your system. You can review how your memory is being utilized For example you can view memory utilization for the system, management, ESRP, IP, and other system functions.

This information may be useful for your technical support representative if you experience a problem.

For version 2.0 and 4.0:

- The `detail` parameter is not available.

Depending on the software version running on your switch, additional or different memory information may be displayed.

Example

The following command displays current system memory information:

```
show memory
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show packet-mem-scan-recovery-mode

```
show packet-mem-scan-recovery-mode
```

Description

Displays the recovery mode setting for slot's that have packet memory scanning enabled.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The `show packet-mem-scan-recovery-mode` command displays the following information:

- Global settings for the system health check
- Auto-recovery settings for slots that have packet memory scanning enabled

Example

The following command displays the settings for each slot that has packet memory scanning enabled:

```
show packet-mem-scan-recovery-mode
```

The following is sample output from this command:

```
Global sys-health-check 'online' setting  is ONLINE
slot 3: AUTORECOVERY MODE is OFFLINE
MSM-B: AUTORECOVERY MODE is ONLINE

# NOTE Global setting is always online for sys-health-check alarm-level
configurations.
       It is only offline when "sys-health-check auto-recovery <#> offline" is
configured.
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on BlackDiamond switches only.

show ports rxerrors

```
show ports {mgmt | <portlist>} rxerrors
```

Description

Displays real-time receive error statistics.

For PoS modules, displays the `rxerror` information for the PoS ports. Only a subset of the statistics displayed by this command are applicable to PoS ports. The fields that do not apply to PoS ports are displayed with values of all zeroes.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, receive error statistics are displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

The following port receive error information is collected by the switch:

- Port Number
- Link Status—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- Receive Bad CRC Frames (RX CRC)—The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- Receive Oversize Frames (RX Over)—The total number of good frames received by the port greater than the supported maximum length of 1,522 bytes. For products that use the “i” chipset, ports with jumbo frames enabled do not increment this counter.
- Receive Undersize Frames (RX Under)—The total number of frames received by the port that were less than 64 bytes long.
- Receive Fragmented Frames (RX Frag)—The total number of frames received by the port were of incorrect length and contained a bad FCS value.

- Receive Jabber Frames (RX Jabber)—The total number of frames received by the port that was of greater than the support maximum length and had a Cyclic Redundancy Check (CRC) error.
- Receive Alignment Errors (RX Align)—The total number of frames received by the port that occurs if a frame has a CRC error and does not contain an integral number of octets.
- Receive Frames Lost (RX Lost)—The total number of frames received by the port that were lost because of buffer overflow in the switch.

For version 2.0 and 4.0

- Disabled and Not Present are not available as link status indicators.

Example

The following command displays receive error statistics for ports 1 through 3 on a stand-alone switch:

```
show ports 1-3 rxerrors
```

The following command displays receive error statistics for slot 1, ports 1 through 3 on a modular switch:

```
show ports 1:1-1:3 rxerrors
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 6.0 to support the Disabled and Not Present link status indicators.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show ports stats

```
show ports {mgmt | <portlist>} stats
```

Description

Displays real-time port statistics.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, statistics are displayed for all ports.

Jumbo frame statistics are displayed for *"i"* series switches only that are configured for jumbo frame support.

This status information may be useful for your technical support representative if you have a network problem.

The following port statistic information is collected by the switch:

- Port Number
- Link Status—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- Transmitted Packet Count (Tx Pkt Count)—The number of packets that have been successfully transmitted by the port.
- Transmitted Byte Count (Tx Byte Count)—The total number of data bytes successfully transmitted by the port.
- Received Packet Count (Rx Pkt Count)—The total number of good packets that have been received by the port.
- Received Byte Count (RX Byte Count)—The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- Received Broadcast (RX Bcast)—The total number of frames received by the port that are addressed to a broadcast address.

- Received Multicast (RX Mcast)—The total number of frames received by the port that are addressed to a multicast address.

For version 2.0 and 4.0

- Disabled and Not Present are not available as link status indicators.
- Chassis is available as a link status indicator. If chassis is listed, the link is connected to a Summit Virtual Chassis.

Example

The following command displays port statistics for ports 1 through 3 on a stand-alone switch:

```
show ports 1-3 stats
```

The following command displays port statistics for slot 1, ports 1 through 3 on a modular switch:

```
show ports 1:1-1:3 stats
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in Extreme 4.1 to discontinue support for the chassis link status indicator.

Platform Availability

This command is available on all platforms.

show ports txerrors

```
show ports {mgmt | <portlist>} txerrors
```

Description

Displays real-time transmit error statistics.

For PoS modules, displays the `txerror` information for the PoS ports.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, error statistics are displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

For PoS modules, displays the `txerror` information for the PoS ports. Only a subset of the statistics displayed by this command are applicable to PoS ports. The fields that do not apply to PoS ports are displayed with values of all zeroes.

The following port transmit error information is collected by the switch:

- Port Number
- Link Status—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- Transmit Collisions (TX Coll)—The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- Transmit Late Collisions (TX Late Coll)—The total number of collisions that have occurred after the port's transmit window has expired.
- Transmit Deferred Frames (TX Deferred)—The total number of frames that were transmitted by the port after the first transmission attempt was deferred by other network traffic.
- Transmit Errored Frames (TX Error)—The total number of frames that were not completely transmitted by the port because of network errors (such as late collisions or excessive collisions).

- Transmit Lost Frames (TX Lost)—The total number of frames transmitted by the port that were lost.
- Transmit Parity Frames (TX Parity)—The bit summation has a parity mismatch.

For version 2.0 and 4.0

- Disabled and Not Present are not available as link status indicators.

Example

The following command displays transmit error statistics for ports 1 through 3 on a stand-alone switch:

```
show ports 1-3 txerrors
```

The following command displays transmit error statistics for slot 1, ports 1 through 3 on a modular switch:

```
show ports 1:1-1:3 txerrors
```

The output produced by the `show ports txerrors` command is similar to the following:

```
Port Tx Error Monitor                       Thu Dec 27 19:19:07 2001
Port         Link    Tx    Tx       Tx       Tx    Tx    Tx
            Status   Coll  Late Coll Deferred  Error  Lost  Parity
================================================================================
  1         A       0      0       0       0      0      0
  2         R       0      0       0       0      0      0
  3         R       0      0       0       0      0      0
  4         R       0      0       0       0      0      0
  5         R       0      0       0       0      0      0
  6         R       0      0       0       0      0      0
  7         R       0      0       0       0      0      0
  8         R       0      0       0       0      0      0


================================================================================
         Link Status: A-Active R-Ready D-Disabled NP-Not Present
           0->Clear Counters  U->page up  D->page down ESC->exit
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 6.0 to support the Disabled and Not Present link status indicators.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

show version

```
show version {detail}
```

Description

Displays the hardware serial numbers and versions, and software versions currently running on the switch, and (if applicable) the modules.

Syntax Description

detail	Specifies display of slot board name and chassis or platform name.

Default

N/A.

Usage Guidelines

On chassis-based switches, displays the switch serial number and version numbers of MSM modules (BlackDiamond switch) and I/O modules (BlackDiamond and Alpine switches).

For ARM, ATM, MPLS or PoS modules, displays information that includes data about the ARM, ATM, MPLS or PoS module and the BootROM version of the ARM, ATM, MPLS or PoS module.

The following is an example of the type of information displayed when you execute the `show version` command:

- System Serial Number—A collection of numbers and letters that make up the serial number of the switch.
- CPU Serial Number—A collection of numbers and letters that make up the serial number of the CPU running in the switch. A rev number may also be listed.
- Image—The ExtremeWare software version currently running on the switch. If you have two software images downloaded on the switch, only the currently running ExtremeWare version information is displayed. The information displayed includes the version number, build number, and the software build date.
- BootROM—The BootROM version currently running on the switch.

If you use the `detail` option (supported in ExtremeWare version 6.2.1 or later) you may also see the following:

- Board/Chassis/Platform Name—The name of the system or module, inserted before the Serial Number in the display.

Depending on the model of your switch, the software running on your switch, and whether you have a stackable or modular switch, different version information may be displayed.

For ARM, ATM, MPLS or PoS modules, the command also shows the software version running on the module.

Example

The following command displays the hardware and software versions currently running on the switch:

```
show version
```

On a stackable switch, this command produces output similar to the following:

```
System Serial Number: 800078-11-0035M02442
CPU Serial Number: 700027-11  0034M-01445 CPLD Rev 04
Daughtercard Serial Number: 703015-02  0029M-02701 CPLD Rev ÿ
Image  :  Extremeware Version 6.2.0 (Build 60)  by Release_Master 09/21/0120:53:17
```

On a BlackDiamond switch, this command produces output similar to the following:

```
Chassis:  801000-07-9946F00987
MSM A  :
MSM B  :  701021-08-0023F25758
SLOT 1 :  701026-03-0003Y00043
SLOT 2 :  701024-04-9949Y00055
SLOT 3 :  701005-09-9946F25172
SLOT 4 :
SLOT 5 :
SLOT 6 :  701028-01-0004Y00038
SLOT 7 :
SLOT 8 :

Image  :  Extremeware Version 6.2.0 (Build 60)  by Release_Master 09/21/0120:53:17

BootROM : 7.2
```

Using the `detail` option in the `show version` command produces output similar to the following on a BlackDiamond switch:

```
Chassis  :      MSM64  801000-07-9946F00987
MSM    A :     MSM64i
MSM    B :     MSM64i  701021-08-0023F25758
SLOT   1 :      F48Ti  701026-03-0003Y00043
SLOT   2 :       G8Xi  701024-04-9949Y00055
SLOT   3 :       F32T  701005-09-9946F25172
SLOT   4 :      Empty
SLOT   5 :      Empty
SLOT   6 :       G8Ti  701028-01-0004Y00038
SLOT   7 :      Empty
SLOT   8 :      Empty


Image : Extremeware Version 6.2.1 (Build 18)  by Release_Master 02/14/02 15:04:26

BootROM : 7.2
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.1 to support the `detail` option.

Platform Availability

This command is available on all platforms.

unconfigure flowstats filter ports

```
unconfigure flowstats filter <filter#> ports <portlist>
```

Description

Removes the filter specification for the specified ports.

Syntax Description

filter#	Specifies the filter specification that should be removed.
portlist	Specifies a set of ports or slots and ports from which the filter specification is removed. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8

Default

N/A.

Usage Guidelines

By unconfiguring the filter specification, this effectively disables this filter on all ports for which it was configured.

Example

The following command resets the values for filter 4 on slot 1, port s 2 and 3:

```
unconfigure flowstats filter 4 ports 1:2-1:3
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

unconfigure flowstats ports

```
unconfigure flowstats ports [<portlist> | all]
```

Description

Resets the flow statistics configuration parameters for the specified ports to their default values.

Syntax Description

portlist	Specifies a set of ports or slots and ports that should be reset. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
all	Specifies that all ports or slots and ports should be reset.

Default

N / A.

Usage Guidelines

This command does not affect the enabled or disabled status of flow collection on these ports, nor does it affect the configured export destinations.

Example

The following command resets the flow statistics configuration parameters for port 1 of slot 8 to their default values:

```
unconfigure flowstats ports 8:1
```

History

This command was first available in ExtremeWare 6.1.5b20 for the PoS module

This command was made available in ExtremeWare 6.2 for all “i” series platforms.

Platform Availability

This command is available on all platforms.

unconfigure log filter

```
unconfigure log filter <filter name>
```

Description

Resets the log filter to its default values; removes all filter items.

Syntax Description

filter name	Specifies the log filter to unconfigure.

Default

N/A.

Usage Guidelines

If the filter name specified is *DefaultFilter*, this command restores the configuration of *DefaultFilter* back to its original settings.

If the filter name specified is not *DefaultFilter*, this command sets the filter to have no events configured and therefore, no incidents will pass. This is the configuration of a newly created filter that was not copied from an existing one.

See the `delete log filter` command for information about deleting a filter.

Example

The following command sets the log filter myFilter to stop passing any events:

```
unconfigure log filter myFilter
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available all platforms.

unconfigure log target format

```
unconfigure log target [console-display | memory-buffer | nvram | session |
syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]] format
```

Description

Resets the log target format to its default values.

Syntax Description

console-display	Specifies the console display format.
memory-buffer	Specifies the switch memory buffer format.
nvram	Specifies the switch NVRAM format.
session	Specifies the current session (including console display) format.
syslog	Specifies a syslog target format.
host name/ip	Specifies the syslog host name or IP address.
udp-port	Specifies the UDP port number for the syslog target.
local0 ... local7	Specifies the local syslog facility.
format	Specifies that the format for the target will be reset to the default value.

Default

When a target format is unconfigured, it is reset to the default values.

The following defaults apply to console display, memory buffer, NVRAM, and session targets:

- timestamp—hundredths
- date—mm-dd-yyyy
- severity—on
- event-name—condition
- host-name—off
- priority—off
- tag-id—off
- tag-name—off
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

The following defaults apply to syslog targets (per RFC 3164):

- timestamp—seconds
- date—mmm-dd

- severity—on
- event-name—none
- host-name—off
- priority—on
- tag-id—off
- tag-name—on
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

Usage Guidelines

Use this command to reset the target format to the default format.

Example

The following command sets the log format for the target `session` (the current session) to the default:

```
unconfigure log target session format
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available all platforms.

unconfigure packet-mem-scan-recovery-mode

```
unconfigure packet-mem-scan-recovery-mode slot [msm-a | msm-b | <slot
number>]
```

Description

Disables packet memory scanning and the recovery mode on a BlackDiamond module, and returns the system to the configured system health check behavior.

Syntax Description

msm-a	Specifies the MSM module installed in slot A. This is available on the BlackDiamond chassis only.
msm-b	Specifies the MSM module installed in slot B. This is available on the BlackDiamond chassis only.
slot number	Specifies a module installed in a slot.

Default

N/A.

Usage Guidelines

If you disable packet memory scanning on a BlackDiamond module, the system health check system resumes. However, if you have the system health check alarm level configured, individual packet memory scanning is ignored.

Example

The following command disables packet memory scanning on a module installed in slot 1:

```
unconfigure packet-mem-scan-recovery mode slot 1
```

The following command disables packet memory scanning on the MSM module installed in slot B:

```
unconfigure packet-mem-scan-recovery mode slot msm-b
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on BlackDiamond switches only.

unconfigure transceiver-test failure-action

```
unconfigure transceiver-test failure-action
```

Description

Returns the switch to its default of sending transceiver test messages to the syslog if too many failures are detected within the specified window.

Syntax Description

The command has no arguments or variables.

Default

N/A.

Usage Guidelines

By default, the switch checks for errors within the *last* eight 20-second windows and sends messages to the syslog

To configure the number of windows the switch waits to check for errors, use the `configure transceiver-test window` command. To modify how the switch responds if too many failures are detected, use the `configure transceiver-test failure-action` command.

Example

The following command returns the switch to its default of sending error messages to the syslog:

```
unconfigure transceiver-test failure-action
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

unconfigure transceiver-test period

```
unconfigure transceiver-test period
```

Description

Returns the transceiver test period to the factory default of 12 seconds.

Syntax Description

The command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this feature when the switch can be brought off-line.

Configuring the transceiver test period to 11 seconds or less can affect system performance; therefore, Extreme Networks does not recommend changing the default transceiver test period. The default is adequate for most networks.

Example

The following command returns the transceiver test period to 12 seconds:

```
unconfigure transceiver-test period
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

unconfigure transceiver-test threshold

```
unconfigure transceiver-test threshold
```

Description

Returns the transceiver test threshold to the factory default of 3 errors.

Syntax Description

The command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this feature when the switch can be brought off-line.

Extreme Networks does not recommend changing the default transceiver test period. The default is adequate for most networks.

Example

The following command returns the transceiver test threshold to 3 errors:

```
unconfigure transceiver-test threshold
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

unconfigure transceiver-test window

```
unconfigure transceiver-test window
```

Description

Returns the transceiver test window to the factory default of eight 20-second windows.

Syntax Description

The command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this feature when the switch can be brought off-line.

This configuration provides a sliding window. When you return to the default window, the switch checks for errors within the *last* eight 20-second windows.

Extreme Networks does not recommend changing the default transceiver test window. The default is adequate for most networks.

Example

The following command returns the transceiver test window to eight 20-second windows:

```
configure transceiver-test window
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

upload log

```
upload log <host name/ip> <filename> {messages [memory-buffer | nvram]}
{severity <severity> {only}} {starting [date <date> time <time> | date
<date> | time <time>]} {ending [date <date> time <time> | date <date> |
time <time>]} {match <match-expression>} {format <format>} {chronological}
```

Description

Uploads the current log messages to a TFTP server.

Syntax Description

host name/ip	Specifies the TFTP server.
filename	Specifies the file name for the log stored on the TFTP server.
messages	Specifies the location from which to display the log messages.
memory-buffer	Show messages stored in volatile memory.
nvram	Show messages stored in NVRAM
severity	Specifies the minimum severity level to display (if the keyword only is omitted).
only	Specifies that only the specified severity level is to be displayed
starting	Show messages with timestamps equal to or greater than that specified
date	Specifies the date, where date is <month (1-12)> / <day> {/ <year (yyyy)>}.
time	Specifies the time, where time is <hour (0-23)> {: <minute (0-59)> {: <seconds> {. <hundredths>}}}
ending	Show messages with timestamps equal to or less than that specified.
match-expression	Specifies a regular expression. Only messages that match the regular expression will be displayed.
format	Specifies a format to use to override the format configured for the memory buffer.
chronological	Specifies uploading log messages in ascending chronological order (oldest to newest).

Default

The following defaults apply:

- messages—memory buffer
- severity—none (displays everything stored in the target)
- starting, ending—if not specified, no timestamp restriction
- match—no restriction
- format—the format configured with the `configure log target format` command
- chronological—if not specified, show messages in order from newest to oldest

Usage Guidelines

This command is similar to the `show log` command, but instead of displaying the log contents on the command line, this command saves the log to a file on the TFTP server you specify. For more details on

most of the options of this command, see the command `show log` on page 666, and for the `format` option see the command `configure log target format` on page 599.

Example

The following command uploads messages with a critical severity to the filename *switch4critical.log* on TFTP server at 10.31.8.25:

```
upload log 10.31.8.25 switch4critical.log critical
```

The following command uploads messages with warning, error, or critical severity to the filename *switch4warn.log* on TFTP server at 10.31.8.25:

```
upload log 10.31.8.25 switch4warn.log warning
```

The following command uploads messages starting August 1, ending August 31, containing the string "slot 2" in order of oldest to newest to the filename *switch4aug03.log* on TFTP server at 10.31.8.25:

```
upload log 10.31.8.25 switch4aug03.log starting date 8/1 ending date 8/31 match "slot
2"
```

History

This command was first available in ExtremeWare 7.1.0

Platform Availability

This command is available on all platforms.

11 Security Commands

This chapter describes:

- Commands for creating and configuring routing access policies
- Commands for creating and configuring IP access lists
- Commands for creating and configuring route maps
- Commands for managing the switch using SSH2
- Commands related to switch user authentication through a RADIUS client
- Commands related to switch user authentication through TACACS+
- Commands for protecting the switch from Denial of Service attacks
- Commands for Network Login configuration

Access policies are a generalized category of features that impact forwarding and route forwarding decisions. Access policies are used primarily for security and quality of service (QoS) purposes.

IP access lists (also referred to as Access Lists or ACLs) consist of IP access rules and are used to perform packet filtering and forwarding decisions on incoming traffic. Each packet arriving on an ingress port is compared to the access list in sequential order and is either forwarded to a specified QoS profile or dropped. Using access lists has no impact on switch performance.

Access lists are typically applied to traffic that crosses layer 3 router boundaries, but it is possible to use access lists within a layer 2 VLAN. Extreme products are capable of performing this function with no additional configuration.

Routing access policies are used to control the advertisement or recognition of routing protocols, such as RIP, OSPF, IS-IS, or BGP. Routing access policies can be used to 'hide' entire networks or to trust only specific sources for routes or ranges of routes. The capabilities of routing access policies are specific to the type of routing protocol involved, but are sometimes more efficient and easier to implement than access lists.

To use routing access policies, follow these steps:

1. Create an access profile.
2. Configure the access profile mode to be of type *permit*, *deny*, or *none (which allows per-entry configuration of the permit/deny attribute).*
3. Add entries to the access profile.
4. Apply the access profile.

Route maps are used to modify or filter routes redistributed between two routing domains. They are also used to modify or filter the routing information exchanged between the domains.

To use route maps, follow these steps:

1 Create a route map.

2 Add entries to the route map.

3 Add statements to the route map entries.

SSH

Secure Shell 2 (SSH2) is a feature of ExtremeWare that allows you to encrypt session data between a network administrator using SSH2 client software and the switch, or to send encrypted data from the switch to an SSH2 client on a remote system. Image and configuration files may also be transferred to the switch using the Secure Copy Program 2 (SCP2)

User Authentication

Remote Authentication Dial In User Service (RADIUS, RFC 2138) is a mechanism for authenticating and centrally administrating access to network nodes. The ExtremeWare RADIUS client implementation allows authentication for Telnet, Vista, or console access to the switch.

Extreme switches are also capable of sending RADIUS accounting information. You can configure RADIUS accounting servers to be the same as the authentication servers, but this is not required.

Terminal Access Controller Access Control System Plus (TACACS+) is a mechanism for providing authentication, authorization, and accounting on a centralized server, similar in function to the RADIUS client. The ExtremeWare version of TACACS+ is used to authenticate prospective users who are attempting to administer the switch. TACACS+ is used to communicate between the switch and an authentication database.

NOTE

You cannot use RADIUS and TACACS+ at the same time.

Network Login

Network Login is a feature designed to control the admission of user packets into a network by giving network access only to users that have been properly authenticated. Network Login is controlled by an administrator on a per port, per VLAN basis and uses an integration of DHCP, user authentication over the web interface or 802.1x client software, and, a RADIUS server to provide a user database or specific configuration details.

Network Login has two modes of operation:

- Campus mode, used when a port in a VLAN will move to another VLAN when authentication has been completed successfully. This mode is for the roaming user who will not always be using the

same port for authentication. Campus mode requires a DHCP server and a RADIUS server configured for Extreme Network Login.

- ISP mode, used when the port and VLAN used will remain constant. All network settings are configured for that VLAN.

A DHCP server is included to support Network Login functionality.

Denial of Service

You can configure ExtremeWare to protect your Extreme switches in the event of a denial of service attack. During a typical denial of service attack, the CPU on the switch gets flooded with packets from multiple attackers, potentially causing the switch to fail. To protect against this type of attack, you can configure the software so that when the number of packets received is more than the configured threshold limit of packets per second, a hardware ACL is enabled.

clear netlogin state

```
clear netlogin state port <portlist> vlan <vlan name>
```

Description

Clears and initializes the Network Login sessions on a VLAN port.

Syntax Description

portlist	Specifies the ports to clear.
vlan name	Specifies a VLAN to clear.

Default

None.

Usage Guidelines

Clear the states of every MAC learned on this VLAN port and put the port back to unauthenticated state. The port will be moved to its original VLAN if configured in Campus mode.

Example

The following example clears the Network Login state of port 9 in VLAN *corp*:

```
clear netlogin state port 9 vlan corp
```

History

This command was first available in ExtremeWare 7.0.0.

The MAC states were not cleared by this command until ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

clear netlogin state mac-address

```
clear netlogin state mac-address <hex-octet>
```

Description

Initialize/Reset the Network Login sessions for a specified supplicant.

Syntax Description

hex-octet	Specifies the MAC address of the supplicant.

Default

N/A

Usage Guidelines

This command is essentially equivalent to a particular supplicant logging out. The MAC address will be cleared from the FDB, the port is put back to its original VLAN (for Campus mode), and the port state is set to unauthenticated, if this was the last authenticated MAC on this port.

Example

The following example resets the Network Login session for the supplicant with the MAC address of 00:e0:18:01:32:1f:

```
clear netlogin state mac-address 00:e0:18:01:32:1f
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure access-profile add

```
configure access-profile <access profile> add {<seq_number>} {permit |
deny} [ipaddress <ip address> <mask> {exact} | as-path <path-expression> |
bgp-community [internet | no-export | no-advertise | no-export-subconfed |
<as_no:number> | number <community>] | ipxnet <netid> <netid mask> | ipxsap
<sap_type> <service_name> | vlan]
```

Description

Adds an entry to the access profile.

Syntax Description

access profile	Specifies an access profile name.
seq-number	Specifies the order of the entry within the access profile. If no sequence number is specified, the new entry is added to the end of the access-profile and is automatically assigned a value of 5 more than the sequence number of the last entry.
permit	Per-entry permit specification. The per-entry attribute only takes effect if the access-profile mode is none. Otherwise, the overall access profile type takes precedence.
deny	Per-entry deny specification. The per-entry attribute only takes effect if the access-profile mode is none. Otherwise, the overall access profile type takes precedence.
ip address/mask	Specifies an IP address and mask as an entry in the profile list.
exact	Specifies that an exact match with address and mask will be performed. Subnets within the address range will not match entry against entry.
path-expression	Specifies a regular expression string to match against the autonomous system path.
internet	Specifies a match against all routes, because all routes belong to the internet community.
no-export	Match against communities with the no-export attribute.
no-advertise	Match against communities with the no-advertise attribute.
no-export-subconfed	Match against communities with the no-export-subconfed attribute.
as_no:number	Match against a BGP community number, specified in as_no:number format.
community	Match against a BGP community number specified as an unsigned 32-bit integer in decimal format.
netid/netid mask	Specifies an IPX netID and mask as an entry in the profile list.
sap_type/service_name	Specifies an IPX SAP service type and service name as an entry in the profile list.
vlan	Specifies a VLAN name as an entry in the profile list (supported only on BlackDiamond 6800 MSM32 running ExtremeWare 4.1)

Default

N/A.

Usage Guidelines

You can specify the sequence number for each access profile entry. If you do not specify a sequence number, entries are sequenced in the order they are added. Each entry is assigned a value of 5 more than the sequence number of the last entry.

The explicit sequence number and the permit or deny attribute should be specified if the access profile mode is none.

The subnet mask specified in the access profile command is interpreted as a *reverse mask.* A reverse mask indicates the bits that are significant in the IP address. In other words, a reverse mask specifies the part of the address that must match the IP address to which the profile is applied.

The `as-path` keyword uses a regular expression string to match against the AS path. Regular expression notation can include any of the characters listed in Table 16.

Table 16: Regular Expression Notation

Character	Definition
N	AS number
N_1 - N_2	Range of AS numbers, where N_1 and N_2 are AS numbers and $N_1 < N_2$
[N_x ... N_y]	Group of AS numbers, where N_x and N_y are AS numbers or a range of AS numbers
[^N_x ... N_y]	Any AS numbers other than the ones in the group
.	Matches any number
^	Matches the beginning of the AS path
$	Matches the end of the AS path
–	Matches the beginning or end, or a space
-	Separates the beginning and end of a range of numbers
*	Matches 0 or more instances
+	Matches 1 or more instances
?	Matches 0 or 1 instance
{	Start of AS SET segment in the AS path
}	End of AS SET segment in the AS path
(	Start of a confederation segment in the AS path
)	End of a confederation segment in the AS path

Example

The following command adds an IP subnet address to access profile *nosales*, as the next available entry:

```
configure access-profile nosales add ipaddress 10.1.33.0/24
```

The following command configures the access profile AS1 to permit AS paths beginning with AS number 1, followed by any AS number from 2 - 8, and ending with either AS number 11, 13, or 15:

```
configure access-profile AS1 add 15 permit as-path "^1 2-8 [11 13 15]$"
```

History

This form of the command was available in ExtremeWare 6.1. Support for IPX NetID and IPX SAP matching was first available in ExtremeWare 6.2.

A limited version of this command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure access-profile delete

```
configure access-profile <access profile> delete <seq_number>
```

Description

Deletes an access profile entry using the sequence number.

Syntax Description

access profile	Specifies an access profile name.
seq-number	Specifies the order of the entry within the access profile. If no sequence number is specified, the new entry is added to the end of the access-profile and is automatically assigned a value of 5 more than the sequence number of the last entry.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the entry with sequence number 15 from the access profile AS1:

```
configure access-profile AS1 delete 15
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure access-profile mode

```
configure access-profile <access profile> mode [permit | deny | none]
```

Description

Configures the access profile mode to permit or deny access, or to require per-entry access control.

Syntax Description

access profile	Specifies an access profile name.
permit	Allows the addresses that match the access profile description.
deny	Denies the addresses that match the access profile description.
none	Permits and denies access on a per-entry basis. Each entry must be added to the profile as either type permit or deny.

Default

Permit.

Usage Guidelines

The access list mode determines whether the items in the list are to be permitted access or denied access.

Example

The following command configures the access profile *no_subnet_33* to deny access:

```
configure access-profile no_subnet_33 mode deny
```

The following command specifies that the access profile *no_subnet_33* uses per-entry access control:

```
configure access-profile no_subnet_33 mode none
```

History

This command was first available in ExtremeWare 4.0.

The per-entry access control was added in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure cpu-dos-protect

```
configure cpu-dos-protect [alert-threshold <packets per second>]
[notice-threshold <packets per second>] [timeout <seconds>] [messages [on |
off]] [filter-precedence <number>] [filter-type-allowed {destination |
source | destination source} {protocol}]
```

Description

Configures denial of service protection.

Syntax Description

alert-threshold	Configures the number of packets per second that the switch needs to receive on a port for an ACL to be enabled. Range is 150 to 100,000 packets per second. Default is 4000.
notice-threshold	Configures the number of packets per second that the switch needs to receive on a port for messages to be logged. Range is 150 to 100,000 packets per second. Default is 4000.
timeout	Configures a duration in seconds. Range is 2 to 300 seconds. Default is 15.
messages	Configures messaging to be on or off. Default is on.
filter-precedence	Configures the access list precedence. Default is 10.
filter-type-allowed	Configures the type of access list allowed. Default is destination
destination	Specifies that destination ACLs can be created
source	Specifies that source ACLs can be created
protocol	Specifies that an ACL will be created to block packets from a single protocol, either TCP, UDP, or other.

Default

The option defaults are:

- alert-threshold—4000
- notice-threshold—4000.
- timeout—15
- messages—on
- filter-precedence—10
- filter-type-allowed—destination

Usage Guidelines

This command configures denial of service protection for Extreme Networks switches. When heavy traffic reaches the alert threshold, a hardware ACL is created that blocks the traffic for the timeout number of seconds.

NOTE

If you set the filter-precedence to 0, the ACLs created by DoS protection will be overwritten by the default VLAN QoS profile.

Example

The following command configures denial of service protection to be invoked when 3000 or more packets per second are received by a port on the switch. This command configures logging to occur when the number of packets per second that the switch receives is 2000, the timeout is 15 seconds, and messages are on:

```
configure cpu-dos-protect alert-threshold 3000 notice-threshold 2000 timeout 15
messages on filter-precedence 10
```

History

This command was first available in ExtremeWare 6.2.2

The filter-type-allowed keyword was added in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure cpu-dos-protect trusted-ports

```
configure cpu-dos-protect trusted-ports [add <port number> | delete <port
number> | all | none]
```

Description

Configures ports as trusted, so that denial of service protection is not applied to port.

Syntax Description

port number	Specifies a port.
all	Specifies all ports as trusted.
none	Specifies that no ports are trusted.

Default

By default, no ports are trusted.

Usage Guidelines

Typically, you would use the `all` parameter when you want to set the denial of service protection to only a few of the ports on a switch. Use the `all` parameter, then use the command `configure cpu-dos-protect trusted-ports delete <port number>` to set ports that should not be trusted (that denial of service protection should be applied to).

Example

The following command configures a port as trusted, so that denial of service protection is not applied port 3:

```
configure cpu-dos-protect trusted-port add 3
```

History

This command was first available in ExtremeWare 7.0.0

Platform Availability

This command is available on all platforms.

configure netlogin base-url

```
configure netlogin base-url <url>
```

Description

Configures the base URL for Network Login.

Syntax Description

url	Specifies the base URL for Network Login.

Default

The base URL default value is “network-access.net”.

Usage Guidelines

When you login using a web browser, you are redirected to the specified base URL, which is the DNS name for the switch.

You must configure a DNS name of the type “www.xx…xx.xxx” or “xx…xx.xxx”.

This command applies only to the web-based authentication mode of Network Login.

Example

The following example configures the base URL as `access.net`:

```
configure netlogin base-url access.net
```

History

This command was first available in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

configure netlogin redirect-page

```
configure netlogin redirect-page <url>
```

Description

Configures the redirect URL for Network Login.

Syntax Description

url	Specifies the redirect URL for Network Login.

Default

The redirect URL default value is “http://www.extremenetworks.com”.

Usage Guidelines

In ISP mode, you can configure netlogin to be redirected to a base page after successful login using this command. If a RADIUS server is used for authentication, then base page redirection configured on the RADIUS server takes priority over this configuration.

You must configure a complete URL starting from either http:// or https://

This command applies only to the web-based authentication mode of Network Login.

Example

The following example configures the redirect URL as `http://www.extremenetworks.com`:

```
configure netlogin redirect-page http://www.extremenetworks.com
```

History

This command was first available in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

configure radius server

```
configure radius [primary | secondary] server [<ipaddress> | <hostname>]
{<udp_port>} client-ip [<ipaddress>]
```

Description

Configures the primary and secondary RADIUS authentication server.

Syntax Description

primary	Configures the primary RADIUS authentication server.
secondary	Configures the secondary RADIUS authentication server.
ipaddress	The IP address of the server being configured.
hostname	The host name of the server being configured.
udp_port	The UDP port to use to contact the RADIUS authentication server.
ipaddress	The IP address used by the switch to identify itself when communicating with the RADIUS authentication server.

Default

The default UDP port setting is 1645.

Usage Guidelines

Use this command to specify RADIUS server information.

Use of the <hostname> parameter requires that DNS be enabled.

The RADIUS server defined by this command is used for user name authentication and CLI command authentication.

Example

The following command configures the primary RADIUS server on host `radius1` using the default UDP port (1645) for use by the RADIUS client on switch 10.10.20.30:

```
configure radius primary server radius1 client-ip 10.10.20.30
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure radius shared-secret

```
configure radius [primary | secondary] shared-secret {encrypted} [<string>]
```

Description

Configures the authentication string used to communicate with the RADIUS authentication server.

Syntax Description

primary	Configures the authentication string for the primary RADIUS server.
secondary	Configures the authentication string for the secondary RADIUS server.
encrypted	Indicates that the secret should be encrypted
string	The string to be used for authentication.

Default

Unconfigured.

Usage Guidelines

The secret must be the same between the client switch and the RADIUS server.

The RADIUS server must first be configured for use with the switch as a RADIUS client.

Example

The following command configures the shared secret as “purplegreen” on the primary RADIUS server:

```
configure radius primary shared-secret purplegreen
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure radius timeout

```
configure radius timeout <seconds>
```

Description

Configures the timeout interval for RADIUS authentication requests.

Syntax Description

seconds	Specifies the number of seconds for authentication requests. Range is 3 to 120 seconds

Default

The default is 3 seconds.

Usage Guidelines

This command configures the timeout interval for RADIUS authentication requests. When the timeout has expired, another authentication attempt will be made. After three failed attempts to authenticate, the alternate server will be used. After five failed attempts, local user authentication will be used.

Example

This example configures the timeout interval for RADIUS authentication to 10 seconds. After 30 seconds (three attempts), the alternate RADIUS server will be used. After 50 seconds (five attempts) local user authentication is used:

```
configure radius timeout 10
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure radius-accounting server

```
configure radius-accounting [primary | secondary] server [<ipaddress> |
<hostname>] {<udp_port>} client-ip [<ipaddress>]
```

Description

Configures the RADIUS accounting server.

Syntax Description

primary	Configure the primary RADIUS accounting server.
secondary	Configure the secondary RADIUS accounting server.
ipaddress	The IP address of the accounting server being configured.
hostname	The host name of the accounting server being configured.
udp_port	The UDP port to use to contact the RADIUS accounting server.
ipaddress	The IP address used by the switch to identify itself when communicating with the RADIUS accounting server.

Default

The default UDP port setting is 1646.

Usage Guidelines

Use this command to specify the radius accounting server.

The accounting server and the RADIUS authentication server can be the same.

Use of the <hostname> parameter requires that DNS be enabled.

Example

The following command configures RADIUS accounting on host `radius1` using the default UDP port (1646) for use by the RADIUS client on switch 10.10.20.30:

```
configure radius-accounting primary server radius1 client-ip 10.10.20.30
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure radius-accounting shared-secret

```
configure radius-accounting [primary | secondary] shared-secret {encrypted}
[<string>]
```

Description

Configures the authentication string used to communicate with the RADIUS accounting server.

Syntax Description

primary	Configures the authentication string for the primary RADIUS accounting server.
secondary	Configures the authentication string for the secondary RADIUS accounting server.
encrypted	Indicates that the secret should be encrypted
string	The string to be used for authentication.

Default

Unconfigured.

Usage Guidelines

The secret must be the same between the client switch and the RADIUS accounting server.

Example

The following command configures the shared secret as “purpleaccount” on the primary RADIUS accounting server:

```
configure radius primary shared-secret purpleaccount
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure radius-accounting timeout

```
configure radius-accounting timeout <seconds>
```

Description

Configures the timeout interval for RADIUS-Accounting authentication requests.

Syntax Description

seconds	Specifies the number of seconds for authentication requests. Range is 3 to 120 seconds

Default

The default is 3 seconds.

Usage Guidelines

This command configures the timeout interval for RADIUS-Accounting authentication requests. When the timeout has expired, another authentication attempt will be made. After three failed attempts to authenticate, the alternate server will be used.

Example

This example configures the timeout interval for RADIUS-Accounting authentication to 10 seconds. After 30 seconds (three attempts), the alternate RADIUS server will be used:

```
configure radius-accounting timeout 10
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure route-map add

```
configure route-map <route-map> add <seq_number> [permit | deny] {match-one
| match-all} {set lpm-routing | set iphost-routing}
```

Description

Adds an entry in the route map with the specified sequence number and action.

Syntax Description

route-map	The name of the route map to which this entry should be added.
seq-number	Specifies a sequence number that uniquely identifies the entry, and determines the position of the entry in the route map.
permit	Permits the route.
deny	Denies the route. This is applied only if the match is successful.
match-one	The route map is successful as long as at least one of the matching statements is true.
match-all	The route map is successful only when all match statements are true. This is the default setting.

Default

N/A.

Usage Guidelines

The sequence number determines the order of the entry in the route map.

The action (permit or deny) specifies the action to be taken on a successful match against the statements in the route map.

After an entry has been added to the route map, statements must be added to define the routes that should be matched, using the `configure <route-map> add match` command.

This command may be used to override the VLAN LPM routing configuration for specific routes. The `lpm-routing` and `iphost-routing` keywords specify how packets are to be routed for route-map matched IP prefixes. If the `lpm-routing` property is added to a route-map, packets are forwarded to the IP prefixes' next hop by the ARM/MPLS module using LPM routing.

If the `iphost-routing` property is added to a route-map, packets are forwarded to the IP prefixes' next hop using the Inferno hardware host-based IP FDB. The `lpm-routing` keyword is only significant for routes learned on VLANs that are not LPM routing enabled. The `iphost-routing` keyword is only significant for routes learned on VLANs that are LPM routing enabled

Example

The following command adds an entry to the route-map named *bgp-out* that denies all matching routes:

```
configure route-map bgp-out add 10 deny
```

The following command adds an entry to the route-map named *bgp-out* that will be evaluated after the previous entry, and that permits all matching routes:

```
configure route-map bgp-out add 20 permit
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map add goto

```
configure route-map <route_map> <seq_number> add goto <new_route_map>
```

Description

Configures a route map `goto` statement to transfer evaluation to another route map.

Syntax Description

route-map	The name of the route map to which this statement should be added.
seq-number	Specifies the sequence number of the entry in the route map to which this statement should be added.
new-route-map	The name of another route map that should be evaluated.

Default

N/A.

Usage Guidelines

A route map `goto` statement is evaluated only after all `match` and `set` statements have been evaluated.

Example

The following command adds a `goto` statement to entry 25 in route map *map1* that causes evaluation control to transfer to route map *map2*:

```
configure route-map map1 25 add goto map2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map add match

```
configure route-map <route-map> <seq_number> add match [nlri-list
<access profile> | as-path [access-profile <access profile> | <as_number>]
| community [access-profile <access profile> | <as_number>:<number> |
number <community> | no-advertise | no-export | no-export-subconfed] |
next-hop <ip address> | med <number> | tag <number> | origin [igp | egp |
incomplete]]
```

Description

Configures a route map match statement.

Syntax Description

route-map	The name of the route map to which this statement should be added.
seq-number	Specifies the sequence number of the entry in the route map to which this statement should be added.
nlri-list <access profile>	Specifies an access profile against which the NLRI should be matched.
as-path access-profile	Specifies an access profile against which the AS path in the path attributes should be matched.
as-number	Specifies an AS number against which the AS path in the path attributes should be matched.
community access-profile	Specifies a BGP community access profile against which the community attribute should be matched.
as_number:number	Specifies a BGP community number, specified in as_number:number format, against which the community attribute should be matched.
community	Specifies a BGP community number, specified as an unsigned 32-bit integer in decimal format, against which the community attribute should be matched.
no-export	Specifies that the community attribute should be matched against the no-export attribute.
no-advertise	Specifies that the community attribute should be matched against the no-advertise attribute.
no-export-subconfed	Specifies that the community attribute should be matched against the no-export-subconfed attribute.
ipaddress	Specifies an IP address against which the next hop attribute in the path attribute should be matched.
med_number	Specifies a MED number against which the MED in the path attribute should be matched.
origin [igp | egp | incomplete]	Specifies an origin against which the origin in the path attribute should be matched. Values are igp, egp, or incomplete.
tag_number	Specifies a tag value against which the tag associated with the redistributed OSPF route should be matched.

Default

N / A.

Usage Guidelines

A match operation specifies a criteria that must be matched in order for the route to be successful. If there are multiple statements in a route table entry, match statements are evaluated before *set* or *goto* statements.

When an entry has multiple match statements, the primitive `match-one` or `match-all` in the entry determines how many matches are required for success. If an entry has no match statements, the entry is always considered a successful match.

Example

The following command adds a statement to entry 10 in route map *bgp-out* that matches the NLRI against the access profile named *iplist*:

```
configure bgp-out 10 add match nlri-list iplist
```

The following command adds a statement to entry 15 in route map *bgp-out* that matches the AS path attribute against the access profile named *aslist*:

```
configure bgp-out 15 add match as-path access-profile aslist
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map add set

```
configure route-map <route-map> <seq_number> add set [as-path <as_number> |
community [[access-profile <access-profile> | <as_number>:<number> | number
<community> | no-advertise | no-export | no-export-subconfed] | remove |
[add | delete] [access-profile <access-profile> | <as no> : <number> |
number <community> | no-advertise | no-export | no-export-subconfed]] |
next-hop <ip address> | med [internal | <med_number> | remove | [add |
delete] <med_number>] local-preference <number> | weight <number> | origin
[igp | egp | incomplete] | tag <tag_number> | accounting index
<index_number> value <value_number> | cost <number> | cost-type [ase-type-1
| ase-type-2]]
```

Description

Configures a route map set entry.

Syntax Description

route-map	The name of the route map to which this statement should be added.
seq-number	Specifies the sequence number of the entry in the route map to which this statement should be added.
as-number	Prepends the specified AS number to the AS path in the path attribute.
as_access_profile	Sets the community in path attribute to the specified access profile.
as_number:number	Sets the community in path attribute to the specified BGP community number, specified in as_number:number format, in the path attribute.
community	Sets the community in path attribute to the specified BGP community number, specified as an unsigned 32-bit integer in decimal format.
no-export	Sets the community in path attribute to the no-export attribute.
no-advertise	Sets the community in path attribute to the no-advertise attribute.
no-export-subconfed	Sets the community in path attribute to the no-export-subconfed attribute.
remove	Removes the community attribute, if present.
add | delete <as_access_profile>	Adds or deletes the specified access profile to or from the existing community in the path attribute.
add | delete <as_number:number>	Adds or deletes the specified BGP community number, specified in as_number:number format, to or from the existing community in the path attribute.
add | delete <community>	Adds or deletes the specified BGP community number, specified as an unsigned 32-bit integer in decimal format, to or from the existing community in the path attribute.
add | delete <no-export>	Adds or deletes the no-export attribute to or from the existing community in the path attribute.
add | delete <no-advertise>	Adds or deletes he no-advertise attribute to or from the existing community in the path attribute.
add | delete <no-export-subconfed>	Adds or deletes the no-export-subconfed attribute to or from the existing community in the path attribute.
next-hop <ipaddress>	Sets the next hop in the path attribute to the specified IP address.
internal	When used in the BGP neighbor output route map, sets the MED attribute to a value equal to the metric to reach the nexthop.
med_number	Sets the MED attribute to the specified value.

remove	Removes the MED attribute, if present.
add | delete <med_number>	Adds or deletes the specified value to or from the MED that is received. The final result is bound by 0 and 2147483647.
local-preference <number>	Sets the local preference in the path attribute to the specified local preference number.
weight <number>	Sets the weight associated with the NLRI to the specified number.
origin [igp | egp | incomplete]	Sets the origin in the path attributes to the specified origin.
tag <tag_number>	Sets the tag in the route to the specified number.
accounting index <index_number>	Specifies the index number of an accounting index to be set.
value <value_number>	Specifies the value to which the accounting index should be set.
cost <number>	Sets the cost of the route to the specified number.
cost-type <number>	Sets the cost type associated with the route (ase-type-1 or ase-type-2).

Default

N / A.

Usage Guidelines

Route map `set` statements are evaluated after `match` statements, but before the `goto` statement.

Changes to the route maps used to modify or filter NLRI information exchanged with neighbors is immediately effective on the routing information exchanged after the policy changes. The changes can be applied on the NLRI information that had been exchanged before the policy changes by issuing a soft reset on the ingress or egress side, depending on the changes. For soft resets to be applied on the ingress side, the changes must be previously enabled on the neighbor.

Changes to the route maps associated with network aggregation or redistribution commands becomes effective after a maximum interval of 30 seconds. You can immediately apply them by using the soft reconfiguration command.

Example

The following command modify the routing information for a route that matches a statement in entry 15 of route table *bgp-out* include a MED value of 200:

```
configure bgp-out 15 add set med 200
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map delete

```
configure route-map <route_map> delete <seq_number>
```

Description

Deletes an entry from the route map.

Syntax Description

route-map	The name of the route map to which this entry should be added.
seq-number	Specifies a sequence number that uniquely identifies the entry, and determines the position of the entry in the route map.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes the entry with sequence number 20 from the route-map named *bgp-out*:

```
configure route-map bgp-out delete 20
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map delete goto

```
configure route-map <route_map> <seq_number> delete goto <new_route_map>
```

Description

Deletes a route map `goto` statement.

Syntax Description

route-map	The name of the route map from which this statement should be deleted.
seq-number	The sequence number of the entry in the route map from which this statement should be deleted.
new-route-map	The name of another route map.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the `goto` statement from entry 25 in route map *map1* that specifies transfer to route map *map2*:

```
configure route-map map1 25 delete goto map2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map delete match

```
configure route-map <route-map> <seq_number> delete match [nlri-list
<access-profile> | as-path [access-profile <access-profile> | <as_number>]
| community [access-profile <access-profile> | <as_number>:<number> |
number <community> | no-advertise | no-export | no-export-subconfed] |
next-hop <ip address> | med <number> | tag <number> | origin [igp | egp |
incomplete]]
```

Description

Deletes a route map match statement.

Syntax Description

route-map	The name of the route map from which this statement should be deleted.
seq-number	The sequence number of the entry in the route map from which this statement should be deleted.
nrli_access_profile	Specifies an NRLI-list access profile.
as_access_profile	Specifies an AS path access profile.
as-number	Specifies an AS number.
com_access_profile	Specifies a BGP community access profile.
as_number:number	Specifies a BGP community number in as_number:number format.
community	Specifies a BGP community number, specified as an unsigned 32-bit integer in decimal format.
no-export	Specifies the no-export community attribute.
no-advertise	Specifies the no-advertise community attribute.
no-export-subconfed	Specifies the no-export-subconfed community attribute.
ipaddress	Specifies an IP address of the next hop attribute.
med_number	Specifies a MED number.
origin [igp | egp | incomplete]	Specifies an origin. Values are igp, egp, or incomplete.
tag_number	Specifies a tag value.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the statement from entry 15 in route map *bgp-out* that specifies that the access profile *aslist* should be used to match the AS path:

```
configure bgp-out 15 add match as-path access-profile aslist
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure route-map delete set

```
configure route-map <route-map> <seq_number> delete set [as-path
<as_number> | community [[access-profile <access-profile> |
<as_number>:<number> | number <community> | no-advertise | no-export |
no-export-subconfed] | remove | [add | delete] [access-profile
<access-profile> | <as_number>:<number> | number <community> | no-advertise
| no-export | no-export-subconfed]] | next-hop <ip address> | med <number>
| local-preference <number> | weight <number> | origin [igp | egp |
incomplete] | tag <number> | accounting index <number> value <number> |
cost <number> | cost-type [ase-type-1 | ase-type-2]]
```

Description

Deletes a route map set entry.

Syntax Description

route-map	The name of the route map from which this statement should be deleted.
seq-number	The sequence number of the entry in the route map from which this statement should be deleted.
as-number	Specifies an AS number.
as_access_profile	Specifies an AS path access profile.
as_number:number	Specifies a BGP community number, in as_number:number format.
community	Specifies a BGP community number, as an unsigned 32-bit integer in decimal format.
no-export	Specifies the no-export attribute.
no-advertise	Specifies the no-advertise attribute.
no-export-subconfed	Specifies the no-export-subconfed attribute.
remove	Specifies removing the community attribute.
add | delete <as_access_profile>	Specifies add or delete of the specified access profile.
add | delete <as_number:number>	Specifies add or delete of the specified BGP community number, in as_number:number format.
add | delete <community>	Specifies add or delete of the specified BGP community number, specified as an unsigned 32-bit integer in decimal format.
add | delete <no-export>	Specifies add or delete of the no-export attribute.
add | delete <no-advertise>	Specifies add or delete of the no-advertise attribute.
add | delete <no-export-subconfed>	Specifies add or delete of the no-export-subconfed attribute.
next-hop <ipaddress>	Specifies the IP address of the next hop.
internal	Specifies setting the MED attribute to a value equal to the metric to reach the nexthop.
med_number	Specifies setting the MED attribute to a specified value.
remove	Specifies removing the MED attribute.
add | delete <med_number>	Specifies add or delete of the specified value to or from the MED.
local-preference <number>	Specifies a local preference number.
weight <number>	Specifies a weight associated with the NLRI.

origin [igp | egp | incomplete]	Specifies the origin.
tag <tag_number>	Specifies the tag in the route to the specified number.
accounting index <index_number>	Specifies the index number of an accounting index to be set.
value <value_number>	Specifies a value for the accounting index.
cost <number>	Specifies the cost of the route.
cost-type <number>	Specifies the cost type.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the set statement from entry 15 of route table *bgp-out* that specified setting a MED value of 200:

```
configure bgp-out 15 delete set med 200
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure ssh2

```
configure ssh2 key {pregenerated}
```

Description

Generates the Secure Shell 2 (SSH2) host key.

Syntax Description

pregenerated	Indicates that the SSH2 authentication key has already been generated. The user will be prompted to enter the existing key.

Default

The switch generates a key for each SSH2 session.

Usage Guidelines

Secure Shell 2 (SSH2) is a feature of ExtremeWare that allows you to encrypt session data between a network administrator using SSH2 client software and the switch, or to send encrypted data from the switch to an SSH2 client on a remote system. Image and configuration files may also be transferred to the switch using the Secure Copy Program (SCP) or the Secure File Transfer Protocol (SFTP).

Before you can enable SSH2, you must first obtain a security license from Extreme Networks. After you receive the license, you must enable SSH2 and generate a host key. To enable SSH2, use the `enable ssh2` command. To generate an SSH2 host key, use the `configure ssh2 key` command.

An authentication key must be generated before the switch can accept incoming SSH2 sessions. This can be done automatically by the switch, or you can enter a previously generated key.

If you elect to have the key generated, you are prompted to enter a set of random characters to be used in generating the key. The key generation process takes approximately ten minutes, and cannot be canceled after it has started. Once the key has been generated, you should save your configuration to preserve the key.

To use a key that has been previously created, use the `pregenerated` keyword. You are prompted to enter the pregenerated key. You can use the `show configure` command to list the previously generated key, and then copy and paste it after the prompt from the `configure ssh2 key pregenerated` command.

The key generation process generates the SSH2 private host key. The SSH2 public host key is derived from the private host key, and is automatically transmitted to the SSH2 client at the beginning of an SSH2 session.

Example

The following command generates an authentication key for the SSH2 session:

```
configure ssh2 key
```

The command responds with the following messages:

```
WARNING: Generating new server host key
This will take approximately 10 minutes and cannot be canceled.
Continue? (y/n)
```

If you respond yes, the command prompts as follows:

```
Enter some random characters.  End with a newline
```

Type in a series of random characters, and then press the Enter or Return key. The key generation process will then proceed.

To configure an SSH2 session using a previously generated key, use the following command:

```
configure ssh2 key pregenerated
```

The command responds with the following message:

```
Please enter the server key
```

Enter the previously-generated key (you can copy and paste it from the saved configuration file).

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure tacacs server

```
configure tacacs [primary | secondary] server [<ipaddress> | <hostname>]
{<tcp_port>} client-ip <ipaddress>
```

Description

Configures the server information for a TACACS+ authentication server.

Syntax Description

primary	Configures the primary TACACS+ server.
secondary	Configures the secondary TACACS+ server.
ipaddress	The IP address of the TACACS+ server being configured.
hostname	The host name of the TACACS+ server being configured.
tcp_port	The TCP port to use to contact the TACACS+ server.
ipaddress	The IP address used by the switch to identify itself when communicating with the TACACS+ server.

Default

TACACS+ uses TCP port 49.

Usage Guidelines

Configure the server information for a TACACS+ server.

To remove a server, use the following command:

```
unconfigure tacacs server [primary | secondary]
```

Use of the <hostname> parameter requires that DNS be enabled.

Example

The following command configures server tacacs1 as the primary TACACS+ server for client switch 10.10.20.35:

```
configure tacacs primary server tacacs1 client-ip 10.10.20.35
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure tacacs shared-secret

```
configure tacacs [primary | secondary] shared-secret {encrypted} <string>
```

Description

Configures the shared secret string used to communicate with the TACACS+ authentication server.

Syntax Description

primary	Configures the authentication string for the primary TACACS+ server.
secondary	Configures the authentication string for the secondary TACACS+ server.
encrypted	Indicates that the secret should be encrypted.
string	The string to be used for authentication.

Default

N/A.

Usage Guidelines

The secret must be the same between the client switch and the TACACS+ server.

Example

The following command configures the shared secret as “purplegreen” on the primary TACACS+ server:

```
configure tacacs-accounting primary shared-secret purplegreen
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure tacacs timeout

```
configure tacacs timeout <seconds>
```

Description

Configures the timeout interval for TACAS+ authentication requests.

Syntax Description

seconds	Specifies the number of seconds for authentication requests. Range is 3 to 120 seconds

Default

The default is 3 seconds.

Usage Guidelines

This command configures the timeout interval for TACACS+ authentication requests. When the timeout has expired, another authentication attempt will be made to the next alternative authentication method.

Example

The following command configures the timeout interval for TACACS+ authentication to 10 seconds:

```
configure tacacs timeout 10
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure tacacs-accounting server

```
configure tacacs-accounting [primary | secondary] server [<ipaddress> |
<hostname>] {<udp_port>} client-ip <ipaddress>
```

Description

Configures the TACACS+ accounting server.

Syntax Description

primary	Configures the primary TACACS+ accounting server.
secondary	Configures the secondary TACACS+ accounting server.
ipaddress	The IP address of the TACACS+ accounting server being configured.
hostname	The host name of the TACACS+ accounting server being configured.
tcp_port	The TCP port to use to contact the TACACS+ server.
ipaddress	The IP address used by the switch to identify itself when communicating with the TACACS+ accounting server.

Default

Unconfigured.

Usage Guidelines

You can use the same TACACS+ server for accounting and authentication.

To remove a server, use the following command:

```
unconfigure tacacs server [primary | secondary]
```

Example

The following command configures server tacacs1 as the primary TACACS+ accounting server for client switch 10.10.20.35:

```
configure tacacs-accounting primary server tacacs1 client-ip 10.10.20.35
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure tacacs-accounting shared-secret

```
configure tacacs-accounting [primary | secondary] shared-secret {encrypted}
<string>
```

Description

Configures the shared secret string used to communicate with the TACACS+ accounting server.

Syntax Description

primary	Configures the authentication string for the primary TACACS+ accounting server.
secondary	Configures the authentication string for the secondary TACACS+ accounting server.
encrypted	Indicates that the secret should be encrypted.
string	The string to be used for authentication.

Default

N / A.

Usage Guidelines

Secret needs to be the same as on the TACACS+ server.

Example

The following command configures the shared secret as “tacacsaccount” on the primary TACACS+ accounting server:

```
configure tacacs-accounting primary shared-secret tacacsaccount
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure tacacs-accounting timeout

```
configure tacacs-accounting timeout <seconds>
```

Description

Configures the timeout interval for TACACS+ accounting authentication requests.

Syntax Description

seconds	Specifies the number of seconds for authentication requests. Range is 3 to 120 seconds

Default

The default is 3 seconds.

Usage Guidelines

This command configures the timeout interval for TACACS+ accounting authentication requests. When the timeout has expired, another authentication attempt will be made to the next alternative TACACS+ accounting server.

Example

The following command configures the timeout interval for TACACS+ accounting authentication to 10 seconds:

```
configure tacacs-accounting timeout 10
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure vlan access-profile

```
configure vlan <vlan name> access-profile [<access profile> | none]
```

Description

Configures a BlackDiamond 6800 running ExtremeWare 4.1 to control the routing of traffic between VLANs.

Syntax Description

vlan name	Specifies the name of an egress VLAN.
access profile	Specifies an access profile that contains a list of ingress VLANs.
none	Specifies that no access profile should be associated with this VLAN.

Default

N/A.

Usage Guidelines

This command configures a BlackDiamond 6800 to permit or deny the routing of IP traffic from the specified list of ingress VLANs to the specified egress VLAN. If the access profile uses permit mode, only traffic from the VLANs specified in the access profile will be routed to egress VLANs configured to use that access profile.

The VLAN must already exist. The access profile must be of type VLAN (supported only in ExtremeWare releases 4.0 and earlier).

Example

Given an access profile created and configured as follows:

```
create access-profile okprofile vlan
configure access-profile okprofile mode permit
configure access-profile okprofile add vlan exec
```

The following command permits traffic from VLAN *exec* to be routed to VLAN *vlan1*:

```
configure vlan vlan1 access-profile okprofile
```

History

This command was available in ExtremeWare 4.1.

Support for this command was discontinued in ExtremeWare 6.0.

Platform Availability

This command is available on the BlackDiamond 6800 MSM32 only.

configure vlan dhcp-address-range

```
configure vlan <name> dhcp-address-range <ipaddress1> - <ipaddress2>
```

Description

Configures a set of DHCP addresses for a VLAN.

Syntax Description

name	Specifies the VLAN on whose ports netlogin should be disabled.
ipaddress1	Specifies the first IP address in the DHCP address range to be assigned to this VLAN.
ipaddress2	Specifies the last IP address in the DHCP address range to be assigned to this VLAN.

Default

N/A.

Usage Guidelines

The DHCP server should be used with Network Login and not as a stand-alone DHCP server.

Example

The following command allocates the IP addresses between 192.168.0.20 and 192.168.0.100 for use by the VLAN *temporary*:

```
configure temporary dhcp-address-range 192.168.0.20 - 192.168.0.100
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan dhcp-lease-timer

```
configure vlan <name> dhcp-lease-timer <lease-timer>
```

Description

Configures the timer value in seconds returned as part of the DHCP response.

Syntax Description

name	Specifies the VLAN on whose ports netlogin should be disabled.
lease-timer	Specifies the timer value, in seconds.

Default

N/A.

Usage Guidelines

The timer value is specified in seconds.

The DHCP server should be used with Network Login and not as a stand-alone DHCP server.

Example

The following command configures the DHCP lease timer value for VLAN *corp*:

```
configure vlan corp dhcp-lease-timer <lease-timer>
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan dhcp-options

```
configure vlan <name> dhcp-options [default-gateway | dns-server |
wins-server] <ipaddress>
```

Description

Configures the DHCP options returned as part of the DHCP response by a switch configured as a DHCP server.

Syntax Description

name	Specifies a VLAN name.
default-gateway	Specifies the router option.
dns-server	Specifies the Domain Name Server (DNS) option.
wins-server	Specifies the NetBIOS name server (NBNS) option.
ipaddress	The IP address associated with the specified option.

Default

N/A.

Usage Guidelines

The DHCP server should be used with Network Login and not as a stand-alone DHCP server.

Example

The following command configures the DHCP server to return the IP address 10.10.20.8 as the router option:

```
configure vlan <name> dhcp-options default-gateway 10.10.20.8
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan netlogin-lease-timer

```
configure vlan <vlan name> netlogin-lease-timer <seconds>
```

Description

Configures the timer value returned as part of the DHCP response for clients attached to Network Login-enabled ports.

Syntax Description

vlan name	Specifies the VLAN to which this timer value applies.
seconds	Specifies the timer value, in seconds.

Default

10 seconds.

Usage Guidelines

The timer value is specified in seconds.

This command applies only to the web-based authentication mode of Network Login.

Example

The following command sets the timer value to 15 seconds for VLAN *corp*:

```
configure vlan corp netlogin-lease-timer 15
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

create access-list icmp destination source

```
create access-list <name> icmp destination [<dest_ipaddress>/<mask> | any]
source [<src_ipaddress>/<source_mask> | any] type <icmp_type> code
<icmp_code> [permit | deny] {<portlist>} {precedence <number>}
```

Description

Creates a named IP access list that applies to ICMP traffic.

Syntax Description

name	Specifies the access list name. The access list name can be between 1 and 31 characters.
dest_ipaddress/mask	Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.
	any specifies that any address will match.
src_ipaddress/source_mask	Specifies a source IP address and subnet mask.
	any specifies that any address will match.
icmp_type	Specifies the ICMP_TYPE number. The ICMP type is a number from 0 to 255.
icmp_code	Specifies the ICMP_CODE number. The ICMP code is a number from 0 to 255.
permit	Specifies that packets that match the access list description are permitted to be forward by this switch.
deny	Specifies that packets that match the access list description are filtered (dropped) by the switch.
portlist	Specifies the ingress port(s) on which this rule is applied.
number	Specifies the access list precedence number. The range is 1 to 25,600.

Default

N / A.

Usage Guidelines

The access list is applied to all ingress packets.

Example

This command creates an access list named *denyping* that filters out ping (ICMP echo) packets. ICMP echo packets are defined as type 8 code 0:

```
create access-list denyping icmp destination any source any type 8 code 0 deny ports
any
```

History

This command was first available in ExtremeWare 6.0, and replaced the `configure ipqos` command.

Platform Availability

This command is available on all platforms.

create access-list ip destination source ports

```
create access-list <name> ip destination [<dest_ipaddress>/<mask> | any]
source [<src_ipaddress>/<src_mask> | any] [permit {<qosprofile>} | deny]
ports [<portlist> | any] {precedence <prec_number>}
```

Description

Creates a named IP access list that applies to all IP traffic.

Syntax Description

name	Specifies the access list name. The access list name can be between 1 and 31 characters.
dest_ipaddress/mask	Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.
	any specifies that any address will match.
src_ipaddress/src_mask	Specifies a source IP address and subnet mask.
	any specifies that any address will match.
permit	Specifies that packets that match the access list description are permitted to be forward by this switch.
qosprofile	Specifies an optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.
deny	Specifies that packets that match the access list description are filtered (dropped) by the switch.
portlist	Specifies the ingress port(s) on which this rule is applied.
	any specifies that the rule will be applied to all ports.
prec_number	Specifies the access list precedence number. The range is 1 to 25,600.

Default

N / A.

Usage Guidelines

The access list is applied to all ingress packets.

Example

The following example defines an access list entry *allow102* with precedence 40 that permits all traffic on any ingress ports to the `10.2.x.x subnet`, and assigns QoS profile Qp3 to those packets:

```
create access-list allow102 ip dest 10.2.0.0/16 source 0.0.0.0/0 permit qosprofile qp3
ports any precedence 40
```

The following command defines a default entry that is used to specify an explicit deny:

```
create access-list denyall ip dest 0.0.0.0/0 source 0.0.0.0/0 deny ports any
```

History

This command was first available in ExtremeWare 6.0, and replaced the `configure ipqos` command.

Platform Availability

This command is available on all platforms.

create access-list tcp destination source ports

```
create access-list <name> tcp destination [<dest_ipaddress>/<mask> | any]
ip-port [<dst_port> | range <dst_port_min> <dst_port_max> | any]
source [<src_ipaddress>/<src_mask> | any] ip-port [<src_port> | range
<src_port_min> <src_port_max> | any] [permit <qosprofile> |
permit-established | deny] ports [<portlist> | any] {precedence
<precedence_num>}
```

Description

Creates a named IP access list that applies to TCP traffic.

Syntax Description

name	Specifies the access list name. The access list name can be between 1 and 31 characters.
dest_ipaddress/mask	Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.
	any specifies that any address will match.
dst_port	Specifies a TCP layer 4 port.
	any specifies that all TCP ports will match.
dst_port_min	Specifies the beginning of a TCP layer 4 port range.
dst_port_max	Specifies the end of a TCP layer 4 port range.
src_ipaddress/src_mask	Specifies a source IP address and subnet mask.
	any specifies that any address will match.
src_port	Specifies a TCP layer 4 port.
	any specifies that all TCP ports will match.
src_port_min	Specifies the beginning of a TCP layer 4 port range.
src_port_max	Specifies the end of a TCP layer 4 port range.
permit	Specifies that packets that match the access list description are permitted to be forward by this switch.
qosprofile	Specifies an optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.
permit-established	Specifies that a currently-established TCP session is allowed, but TCP packets from source to destination (uni-directional) with SYN=1 and ACK=0 (to initiate a new session) will be dropped.
deny	Specifies that packets that match the access list description are filtered (dropped) by the switch.
portlist	Specifies the ingress port(s) on which this rule is applied.
	any specifies that the rule will be applied to all ports.
prec_number	Specifies the access list precedence number. The range is 1 to 25,600.

Default

N / A.

Usage Guidelines

The access list is applied to all ingress packets.

Example

The following command defines an access-list rule named *allow10_23* with precedence 30 that permits TCP port 23 traffic destined for other 10.x.x.x networks, and assigns QoS profile *Qp4*:

```
create access-list allow10_23 tcp dest 10.0.0.0/8 ip-port 23 source any ip-port any
permit qosprofile qp4 ports any precedence 30
```

History

This command was first available in ExtremeWare 6.0, and replaced the `configure ipqos` command.

Platform Availability

This command is available on all platforms.

create access-list udp destination source ports

```
create access-list <name> udp destination [<dest_ipaddress>/<mask> | any]
ip-port [<dst_port> | range <dst_port_min> <dst_port_max> | any]
source [<src_ipaddress>/<src_mask> | any] ip-port [<src_port> | range
<src_port_min> <src_port_max> | any] [permit <qosprofile> | deny] ports
[<portlist> | any] {precedence <prec_number>}
```

Description

Creates a named IP access list that applies to UDP traffic.

Syntax Description

name	Specifies the access list name. The access list name can be between 1 and 31 characters.
dest_ipaddress/mask	Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.
	any specifies that any address will match.
dst_port	Specifies a UDP layer 4 port.
	any specifies that all UDP ports will match.
dst_port_min	Specifies the beginning of a UDP layer 4 port range.
dst_port_max	Specifies the end of a UDP layer 4 port range.
src_ipaddress/src_mask	Specifies a source IP address and subnet mask.
	any specifies that any address will match.
src_port	Specifies a UDP layer 4 port.
	any specifies that all UDP ports will match.
src_port_min	Specifies the beginning of a UDP layer 4 port range.
src_port_max	Specifies the end of a UDP layer 4 port range.
permit	Specifies that packets that match the access list description are permitted to be forward by this switch.
qosprofile	Specifies an optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.
deny	Specifies that packets that match the access list description are filtered (dropped) by the switch.
portlist	Specifies the ingress port(s) on which this rule is applied.
	any specifies that the rule will be applied to all ports.
prec_number	Specifies the access list precedence number. The range is 1 to 25,600.

Default

N/A.

Usage Guidelines

The access list is applied to all ingress packets.

Example

The following command defines an access-list rule named *allow10_35* with precedence 70 that permits udp port 35 traffic destined for other 10.X.X.X networks, and assigns QoS profile *Qp2*:

```
create access-list allow10_35 udp dest 10.0.0.0/8 ip-port 35 source any ip-port any
permit qosprofile qp2 ports any precedence 70
```

History

This command was first available in ExtremeWare 6.0, and replaced the `configure ipqos` command.

Platform Availability

This command is available on all platforms.

create access-profile

```
create access-profile <access profile> type [ipaddress | ipx-node | ipx-net
| ipx-sap | as-path | bgp-community | vlan]
```

Description

Creates an access profile.

Syntax Description

access profile	Specifies an access profile name.
ipaddress	Specifies that the profile entries will be a list of IP address/mask pairs.
ipx-node	Specifies that the profile entries will be a list of IPX node addresses.
ipx-net	Specifies that the profile entries will be a list of IPX NetIDs.
ipx-sap	Specifies that the profile entries will be a list of IPX SAP advertisements.
as-path	Specifies that the profile entries will be a list of AS path expressions.
bgp-community	Specifies that the profile entries will be a list of BGP community numbers.
vlan	Specifies that the profile entries will be a list of VLANs (supported only on BlackDiamond 6800 MSM32 running ExtremeWare 4.1)

Default

N/A.

Usage Guidelines

You must give the access profile a unique name (in the same manner as naming a VLAN, protocol filter, or Spanning Tree Domain).

After the access profile is created, you must configure the access profile mode. The access profile mode determines whether the items in the list are to be permitted access or denied access.

For version 4.0:

- Only type `ipaddress` was supported, and the `type` keyword was not used.
- On BlackDiamond 6800 MSM32 running ExtremeWare 4.1, the VLAN keyword specifies that profile entries will be a list of VLANs.

Example

The following command creates an access profile named *nosales* that will contain IP address/mask pairs:

```
create access-profile nosales type ipaddress
```

The following command creates an access profile that will contain AS path expressions:

```
create access-profile AS1 type as-path
```

History

This form of the command was available in ExtremeWare 6.1. Support for the IPX node, NetID and SAP advertisement types was added in ExtremeWare 6.2.

A limited version of this command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

create route-map

```
create route-map <name>
```

Description

Creates a route map statement.

Syntax Description

name	Specifies a route map name.

Default

N/A.

Usage Guidelines

Route maps are a mechanism that can be used to conditionally control the redistribution of routes between two routing domains, and to modify the routing information that is redistributed.

Route maps are used in conjunction with the match and set operations. A match operation specifies a criteria that must be matched. A set operation specifies a change that is made to the route when the match operation is successful.

After a route map statement has been created, you must add entries to the route-map, and then add statements to the route map entries.

Example

The following command creates a route-map named *bgp-out*:

```
create route-map bgp-out
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

delete access-list

```
delete access-list [<name> | all]
```

Description

Deletes an access list.

Syntax Description

name	Specifies the name of the access list to be deleted.
all	Specifies that all access lists should be deleted.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes access list *allow102*:

```
delete access-list allow102
```

History

This command was first available in ExtremeWare 6.0.

The command was modified in ExtremeWare 6.2.1 to provide the `all` option.

Platform Availability

This command is available on all platforms.

delete access-profile

```
delete access-profile <access profile>
```

Description

Deletes an access profile.

Syntax Description

access profile	Specifies an access profile name.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes an access profile named *nosales*:

```
delete access-profile nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

delete route-map

```
delete route-map <route map>
```

Description

Deletes a route map statement from the route map.

Syntax Description

route map	Specifies a route map name.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes a route-map named *bgp-out*:

```
delete route-map bgp-out
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable access-list

```
disable access-list <name> [counter | log]
```

Description

Disables message logging or the collection of access-list statistics.

Syntax Description

name	Specifies the name of the access list.
counter	Specifies that access-list statistics collection should be disable.
log	Specifies that message logging to the Syslog facility for each packet that matches the access-list description should be disabled.

Default

Counting is ON, logging is OFF.

Usage Guidelines

None.

Example

The following command disables statistics collection for access list *allow102*:

```
disable access-list allow102 counter
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable cpu-dos-protect

```
disable cpu-dos-protect
```

Description

Disables denial of service protection.

Syntax Description

There are no arguments or variables for this command.

Default

Default is disabled.

Usage Guidelines

None.

Example

The following command disables denial of service protection.

```
disable cpu-dos-protect
```

History

This command was first available in ExtremeWare 6.2.2

Platform Availability

This command is available on all platforms.

disable dhcp ports vlan

```
disable dhcp ports <portlist> vlan <vlan name>
```

Description

Disables DHCP on a specified port in a VLAN.

Syntax Description

portlist	Specifies the ports for which DHCP should be disabled.
vlan name	Specifies the VLAN on whose ports DHCP should be disabled.

Default

N/A.

Usage Guidelines

The DHCP server should be used with Network Login and not as a stand-alone DHCP server.

Example

The following command disables DHCP for port 9 in VLAN *corp*:

```
disable dhcp ports 9 vlan corp
```

History

This command was first available in ExtremeWare 6.2.

disable netlogin

```
disable netlogin [web-based |dot1x]
```

Description

Disables Network Login modes.

Syntax Description

web-based	Specifies web-based authentication.
dot1x	Specifies 802.1x authenticating.

Default

Both types of authentication are enabled.

Usage Guidelines

Both types, either type, or no type of authentication can be enabled on the same switch. To enable an authentication mode, use the following command:

```
enable netlogin [web-based | dot1x]
```

This command was first introduced as `disable netlogin`, which disabled the initial version of Network Login, the web-based mode. The original command was subsequently deprecated when the 802.1x mode of Network Login was introduced in ExtremeWare 7.1.0. The deprecated version of the command is temporarily supported in configurations. During an upgrade, the deprecated command:

```
disable netlogin
```

will be interpreted as:

```
disable netlogin web-based
disable netlogin dot1x
```

Example

The following command disables Network Login:

```
disable netlogin
```

History

The `web-based` and `dot1x` keywords were added in ExtremeWare 7.1.0, and the initial version of the command (without the new keywords) was deprecated.

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable netlogin logout-privilege

```
disable netlogin logout-privilege
```

Description

Disables Network Login logout window pop-up.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

This command controls the logout window pop-up on the web-based network client. This command applies only to the web-based authentication mode of Network Login. When disabled, the logout window pop-up will no longer appear.

Example

The following command disables Network Login logout-privilege:

```
disable netlogin logout-privilege
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable netlogin ports

```
disable netlogin ports <portlist> vlan <vlan name>
```

Description

Disables Network Login on a specified port in a VLAN.

Syntax Description

portlist	Specifies the ports for which netlogin should be disabled.
vlan name	Specifies the VLAN on whose ports netlogin should be disabled.

Default

N/A.

Usage Guidelines

Network Login must be disabled on a port before you can delete a VLAN that contains that port.

This command applies to both the web-based and 802.1x mode of Network Login. To control which authentication mode is used by Network Login, use the following commands:

```
enable netlogin [web-based | dot1x]
disable netlogin [web-based | dot1x]
```

Example

The following command disables Network Login on port 9 in VLAN *corp*:

```
disable netlogin ports 9 vlan corp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable netlogin session-refresh

```
disable netlogin session-refresh
```

Description

Disables Network Login session refresh.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Network Login sessions can refresh themselves after a configured timeout. After the user has been logged in successfully, a logout window opens which can be used to close the connection by clicking on the LogOut link. Any abnormal closing of this window is detected on the switch and the user is logged out after a time interval as configured for session refresh. The session refresh is enabled and set to five minutes by default.

This command applies only to the web-based authentication mode of Network Login.

Example

The following command disables Network Login session refresh:

```
disable netlogin session-refresh
```

History

This command was first available in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

disable radius

```
disable radius
```

Description

Disables the RADIUS client.

Syntax Description

This command has no arguments or variables.

Default

RADIUS authentication is disabled by default.

Usage Guidelines

None.

Example

The following command disables RADIUS authentication for the switch:

```
disable radius
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

disable radius-accounting

```
disable radius-accounting
```

Description

Disables RADIUS accounting.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables RADIUS accounting for the switch:

```
disable radius-accounting
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

disable ssh2

```
disable ssh2
```

Description

Disables the SSH2 server for incoming SSH2 sessions to switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

SSH2 session options (access profile and non-default port setting) are not saved when SSH2 is disabled.

To view the status of SSH2 Telnet sessions on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for SSH2 Telnet sessions.

SSH2 client connections can still be initiated from the switch when the SSH2 server is disabled.

Example

The following command disables the SSH2 server:

```
disable ssh2
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable tacacs

```
disable tacacs
```

Description

Disables TACACS+ authentication.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables TACACS+ authentication for the switch:

```
disable tacacs
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable tacacs-accounting

```
disable tacacs-accounting
```

Description

Disables TACACS+ accounting.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables TACACS+ accounting:

```
disable tacacs-accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable tacacs-authorization

```
disable tacacs-authorization
```

Description

Disables TACACS+ authorization.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This disable CLI command authorization but leaves user authentication enabled.

Example

The following command disables TACACS+ CLI command authorization:

```
disable tacacs-authorization
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable access-list

```
enable access-list <name> [counter | log]
```

Description

Enables message logging or the collection of access-list statistics.

Syntax Description

name	Specifies the name of the access list.
counter	Specifies that access-list statistics should be collected.
log	Specifies that a message should be logged to the Syslog facility for each packet that matches the access-list description. The message details the properties of the packet.

Default

Counting is ON, logging is OFF.

Usage Guidelines

None.

Example

The following command enables statistics collection for access list *allow102*:

```
enable access-list allow102 counter
```

The following command enables logging of packets for access list *allow102*:

```
enable access-list allow102 log
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable cpu-dos-protect

```
enable cpu-dos-protect
```

Description

Enables denial of service protection.

Syntax Description

There are no arguments or variables for this command.

Default

Default is disabled.

Usage Guidelines

None.

Example

The following command enables denial of service protection.

```
enable cpu-dos-protect
```

History

This command was first available in ExtremeWare 6.2.2

Platform Availability

This command is available on all platforms.

enable cpu-dos-protect simulated

```
enable cpu-dos-protect simulated
```

Description

Enables simulated denial of service protection.

Syntax Description

There are no arguments or variables for this command.

Default

Default is disabled.

Usage Guidelines

When simulated denial of service protection is enabled, no ACLs are created. This mode is useful to gather information about normal traffic levels on a switch. This will assist in configuring denial of service protection so that legitimate traffic is not blocked.

Example

The following command enables simulated denial of service protection.

```
enable cpu-dos-protect simulated
```

History

This command was first available in ExtremeWare 6.2.2

Platform Availability

This command is available on all platforms.

enable netlogin

```
enable netlogin [web-based | dot1x]
```

Description

Enables Network Login authentication modes.

Syntax Description

web-based	Specifies web-based authentication.
dot1x	Specifies 802.1x authenticating.

Default

Both types of authentication are enabled.

Usage Guidelines

Both types, either type, or no type of authentication can be enabled on the same switch. To disable an authentication mode, use the following command:

```
disable netlogin [web-based | dot1x]
```

This command was first introduced as `enable netlogin`, which enabled the initial version of Network Login, the web-based mode. The original command was subsequently deprecated when the 802.1x mode of Network Login was introduced in ExtremeWare 7.1.0. The deprecated version of the command is temporarily supported in configurations. During an upgrade, the deprecated command:

```
enable netlogin
```

will be interpreted as:

```
enable netlogin web-based
enable netlogin dot1x
```

Example

The following command enables web-based Network Login:

```
enable netlogin web-based
```

History

The `web-based` and `dot1x` keywords were added in ExtremeWare 7.1.0, and the initial version of the command (without the new keywords) was deprecated.

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable netlogin logout-privilege

```
enable netlogin logout-privilege
```

Description

Enables Network Login logout pop-up window.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

This command controls the logout window pop-up on the web-based network client. This command applies only to the web-based authentication mode of Network Login.

Example

The following command enables Network Login logout-privilege:

```
enable netlogin logout-privilege
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable netlogin ports

```
enable netlogin ports <portlist> vlan <vlan name>
```

Description

Enables Network Login on a specified port in a VLAN.

Syntax Description

portlist	Specifies the ports for which netlogin should be enabled.
vlan name	Specifies the VLAN on whose ports netlogin should be enabled.

Default

N/A.

Usage Guidelines

The VLAN you specify must exist and include the specified ports prior to enabling Network Login.

For campus mode login with web-based clients, the following conditions must be met:

- A DHCP server must be available, and a DHCP range must be configured for the port or ports in the VLAN on which you want to enable Network Login.
- The switch must be configured as a RADIUS client, and the RADIUS server must be configured to enable the Extreme Network Login capability.

For ISP mode login, no special conditions are required. A RADIUS server must be used for authentication.

Network Login is used on a per port, per VLAN basis. A port that is tagged can belong to more than one VLAN. In this case, Network Login can be enabled on one port for each VLAN.

Windows authentication is not supported via Network Login.

Example

The following command configures Network Login on port 9 in VLAN *corp*:

```
enable netlogin ports 9 vlan corp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable netlogin session-refresh

```
enable netlogin session-refresh {<minutes>}
```

Description

Disables Network Login session refresh.

Syntax Description

minutes	Specifies the session refresh time for Network Login in minutes.

Default

Disabled, with a value of three minutes for session refresh.

Usage Guidelines

Network Login sessions can refresh themselves after a configured timeout. After the user has been logged in successfully, a logout window opens which can be used to close the connection by clicking on the LogOut link. Any abnormal closing of this window is detected on the switch and the user is logged out after a time interval as configured for session refresh. The session refresh is enabled and set to three minutes by default. The value can range from 1 to 255 minutes. When you configure the Network Login session refresh for the logout window, ensure that the FDB aging timer is greater than the Network Login session refresh timer.

This command applies only to the web-based authentication mode of Network Login.

Use this command without the `minutes` parameter to reset the session refresh value to the default.

Example

The following command enables Network Login session refresh and sets the refresh time to ten minutes:

```
enable netlogin session-refresh 10
```

History

This command was first available in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

enable radius

```
enable radius
```

Description

Enables the RADIUS client on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

When enabled, all web and CLI logins are sent to the RADIUS servers for authentication. When used with a RADIUS server that supports ExtremeWare CLI authorization, each CLI command is sent to the RADIUS server for authorization before it is executed.

Example

The following command enables RADIUS authentication for the switch:

```
enable radius
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

enable radius-accounting

```
enable radius-accounting
```

Description

Enables RADIUS accounting.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

The RADIUS client must also be enabled.

Example

The following command enables RADIUS accounting for the switch:

```
enable radius-accounting
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

enable ssh2

```
enable ssh2 {access-profile [<access profile> | none]} {port
<tcp_port_number>}
```

Description

Enables SSH2 server to accept incoming sessions from SSH2 clients.

Syntax Description

access profile	Specifies an access profile.
none	Cancels a previously configured access profile.
port	Specifies a TCP port number. The default is port 22.

Default

The SSH2 feature is disabled by default.

Usage Guidelines

SSH2 enables the encryption of session data. You must be logged in as an administrator to enable SSH2, and you must obtain and enter a Security License Key to enable the SSH2 feature. To obtain a Security License Key, access the Extreme Networks website.

You can specify a list of predefined clients that are allowed SSH2 access to the switch. To do this, you must create an access profile that contains a list of allowed IP addresses. To create an access profile, use the `create access-profile` command. To configure an access profile, use the `configure access-profile` command.

Use the `none` option to cancel a previously configured access profile.

Use the `port` option to specify a TCP port number other than the default.

To view the status of SSH2 sessions on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for SSH2 sessions.

Example

The following command enables the SSH2 feature, with access allowed based on the access profile *management*:

```
enable ssh2 access-profile management
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable tacacs

```
enable tacacs
```

Description

Enables TACACS+ authentication.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

After they have been enabled, all web and CLI logins are sent to one of the two TACACS+ servers for login name authentication and accounting.

Example

The following command enables TACACS+ user authentication:

```
enable tacacs
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable tacacs-accounting

```
enable tacacs-accounting
```

Description

Enables TACACS+ accounting.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

If accounting is used, the TACACS+ client must also be enabled.

Example

The following command enables TACACS+ accounting for the switch:

```
enable tacacs-accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable tacacs-authorization

```
enable tacacs-authorization
```

Description

Enables CLI command authorization.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

When enabled, each command is transmitted to the remote TACACS+ server for authorization before the command is executed.

Example

The following command enables TACACS+ command authorization for the switch:

```
enable tacacs-authorization
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

scp2

```
scp2 {cipher [3des | blowfish]} {port <portnum>} {debug <debug_level>}
<user>@ [<hostname> | <ipaddress>] :<remote_file> [configuration
{incremental} | image [primary | secondary] | bootrom]
```

Description

Initiates an SCP2 client session to a remote SCP2 server and copies a file from the remote system to the switch.

Syntax Description

3des	Specifies that the 3des cipher should be used for encryption. This is the default.
blowfish	Specifies that the blowfish cipher should be used for encryption.
portnum	Specifies the TCP port number to be used for communicating with the SSH2 client. Default is port 22.
debug_level	Specifies a debug level. Default is 0.
user	Specifies a login name for the remote host.
host	Specifies the name of the remote host.
ipaddress	Specifies the IP address of the remote host.
remote file	Specifies the name of the remote file to be copied to the switch.
configuration	Specifies that the copied file is a switch configuration file. It the incremental option is not specified, it replaces the current switch configuration.
incremental	Specifies that the copied file should be handled like an incremental configuration download (only the commands in the file are executed).
image	Specifies that the copied file is an ExtremeWare image.
primary	Specifies that the image should be placed in the primary image area.
secondary	Specifies that the image should be placed in the secondary image area.
bootrom	Specifies that the copied file is a bootrom image.

Default

N/A.

Usage Guidelines

You must be running a security-enabled version of ExtremeWare 6.2.1 or later (which is under Export Control) in order to use the SCP2 command.

SSH2 does not need to be enabled on the switch in order to use this command.

This command logs into the remote host as <user> and accesses the file <remote_file>. You will be prompted for a password from the remote host, if required.

CAUTION

You can download a configuration to an Extreme Networks switch using SCP. If you do this, you cannot save this configuration. If you save this configuration and reboot the switch, the configuration will be corrupted.

Example

The following command copies a configuration file from the file *configpart1.save* on host *system1* to the switch as an incremental configuration:

```
scp2 admin@system1:configpart1.save configuration incremental
```

History

This command was first available in ExtremeWare 6.2.1

Platform Availability

This command is available on all platforms.

scp2 configuration

```
scp2 {cipher [3des | blowfish]} {port <portnum>} {debug <debug_level>}
configuration <user>@ [<hostname> | <ipaddress>]:<remote_file>
```

Description

Copies the configuration file from the switch to a remote system using SCP2.

Syntax Description

3des	Specifies that the 3des cipher should be used for encryption. This is the default.
blowfish	Specifies that the blowfish cipher should be used for encryption.
portnum	Specifies the TCP port number to be used for communicating with the SSH2 client. Default is port 22.
debug_level	Specifies a debug level. Default is 0.
user	Specifies a login name for the remote host.
host	Specifies the name of the remote host.
ipaddress	Specifies the IP address of the remote host.
remote file	Specifies the name of the file to be created on the remote host.

Default

N / A.

Usage Guidelines

You must be running a security-enabled version of ExtremeWare 6.2.1or later (which is under Export Control) in order to use the SCP2 command.

SSH2 does not need to be enabled on the switch in order to use this command. (SSH2 is enabled by default if you are running a security-enabled version of ExtremeWare).

This command logs into the remote host as `<user>` and creates the file `<remote_file>`.

Example

The following command copies the switch configuration and saves it as file c*onfig1.save* on host *system1*:

```
scp2 configuration admin@system1:config1.save
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

show access-list

```
show access-list {<name> | port <portlist>}
```

Description

Displays access list information and real-time statistics.

Syntax Description

name	Specifies the name of an access list to be displayed.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

Shows information for all access lists.

Usage Guidelines

To verify access list settings, you can view the access list configuration and see real-time statistics on which access list entries are being accessed when processing traffic.

Example

The following command shows information on all current the access lists:

```
show access-list
```

It produces output similar to the following:

```
Rule         Dest/mask:L4DP         Src/mask:L4SP        Flags  Hits
test1        0.0.0.0/ 0:   0          0.0.0.0/ 0:   0     I-P-X   1531

Flags: I=IP, T=TCP, U=UDP, E=Established, M=ICMP
       P=Permit Rule, D=Deny Rule
       N=Port Specific Rule, X=Any Port
```

The following command shows real-time access list statistics for ingress ports 5-7:

```
show access-list port 5-7
```

The following command shows information for access list *test1*:

```
show access-list test1
```

The command generates output similar to the following:

```
test1
       Protocol: ip    Action: permit qp1
       Destination: 0.0.0.0/0  any
       Source:  any    any
       Precedence: 0
       Rule Number: 0
       Hit Count: 4566 Flags: ac
       Ports:
              any
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show access-list-fdb

```
show access-list-fdb
```

Description

Displays the hardware access control list mapping.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the hardware access control list mapping:

```
show access-list-fdb
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show access-list-monitor

```
show access-list-monitor
```

Description

Initiates the access-list information display, and refreshes it until discontinued.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command initiates a display of real-time access list information. Use the keys as shown in Table 17 to change the view of the data. The [Esc] or [Return] keys will discontinue the display.

Table 17: Monitoring Display Keys

Key(s)	Description
U	Displays the previous page of ports.
D	Displays the next page of ports.
[Esc] or [Return]	Exits from the screen.
0	Clears all counters.

Example

The following command initiates the access-list information display:

```
show access-list-monitor
```

The command displays output similar to the following:

```
Access List     Proto   Destination     Source          Hit Count
=========================================================================
test1           ip      0.0.0.0/0       0.0.0.0/0         1922
```

The Hit Count continues to be updated until you exit from the display or enter “0” to reset the count to zero.

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show access-profile

```
show access-profile {<access profile>}
```

Description

Displays access-profile related information for the switch.

Syntax Description

access profile	Specifies an access profile.

Default

Shows all access profile information for the switch.

Usage Guidelines

None.

Example

The following command displays access-profile related information for access profile *nosales*:

```
show access-profile nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show cpu-dos-protect

```
show cpu-dos-protect
```

Description

Displays the status of denial of service protection.

Syntax Description

There are no arguments or variables for this command.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the status of denial of service protection.

```
show cpu-dos-protect
```

Following is the output from this command:

```
Denial-of-service protection to CPU is ENABLED
Notice level:     4000 new packets/second (level for logging)
Alert level:      4000 new packets/second (level for ACL creation)
Filter types: destination
ACL timeout:        15 seconds
ACL rule precedence: 10
Messages are ON
Trusted Ports:  none
ACL is active ports 48 to 192.168.3.1 proto all precedence 10
ACL should expire in 13 seconds
```

History

This command was first available in ExtremeWare 6.2.2

Platform Availability

This command is available on all platforms.

show netlogin

```
show netlogin {port <portlist> vlan <vlan name>}
```

Description

Shows status information for Network Login.

Syntax Description

portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
vlan name	Specifies the name of a VLAN.

Default

N / A.

Usage Guidelines

The information reported by this command is the following:

- Whether Network Login is enabled or disabled.
- The base-URL.
- The default redirect page.
- The logout privileges setting.
- The netlogin session-refresh setting and time.
- The MAC and IP address of supplicants
- The type of authentication, 802.1x or HTTP (web-based).

Example

The following command shows the summary Network Login information:

```
show netlogin
```

Following is the output from this command:

```
Netlogin Authentication Mode :  web-based ENABLED  ;   802.1x ENABLED

-----------------------------------------------
        Web-based Mode Global Configuration
-----------------------------------------------
Base-URL                              :  "network-access.net"
Default-Redirect-Page                 :  "http://www.extremenetworks.com"
Logout-privilege                      :   YES
Netlogin Session-Refresh              :   DISABLED ; 3 minutes
-----------------------------------------------
-----------------------------------------------
        802.1x Mode Global Configuration
-----------------------------------------------
```

```
Quiet Period                          :   60      secs
Client Response Timeout               :   30      secs
Default Reauthentication Timeout      :   3600    secs
Max. Number Authentication Failure    :   3
Periodic Reauthentication             :   ENABLED
--------------------------------

Port: 1:13,   Vlan: Default,  State: Unauthenticated
MAC                IP address      Auth   Type      ReAuth-Timer User
00:B0:D0:90:2F:72  0.0.0.0         No     802.1x    12           Unknown
------------------------------


Total Number of Authenticated MACs : 0
```

The following command shows the detailed Network Login information for the port 1:13 in the VLAN *Default*:

```
show netlogin ports 1:13 "Default"
```

Following is the output from this command before authentication:

```
Port: 1:13      Vlan: Default
Port State:     Unauthenticated
DHCP:           Not Enabled

MAC               IP address    Auth  Type   ReAuth-Timer User
------------------------------------------------------------------
00:B0:D0:90:2F:72  0.0.0.0       No   802.1x  30           Unknown
Quiet Period Timer            :  0      Num. Authentication Failed    :  1
------------------------------------------------------------------
```

Following is the output from this same command after authentication:

```
Port: 1:13      Vlan: Default
Port State:     Unauthenticated
DHCP:           Not Enabled

MAC               IP address    Auth  Type   ReAuth-Timer User
 ------------------------------------------------------------------
00:B0:D0:90:2F:72    0.0.0.0     Yes  802.1x  3600        auto20@dot1x.net
Quiet Period Timer            :  0      Num. Authentication Failed    :  0
------------------------------------------------------------------
                       IP address      Auth   Type      User     ReAuth-Timer
```

History

This command was modified to show the authentication type in ExtremeWare 7.1.0.

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show radius

```
show radius
```

Description

Displays the current RADIUS client configuration and statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The output from this command displays the status of the RADIUS and RADIUS accounting (enabled or disabled) and the primary and secondary servers for RADIUS and RADIUS accounting:

Example

The following command displays the current RADIUS client configuration and statistics:

```
show radius
```

Following is the output from this command:

```
Radius: enabled
Radius Accounting: enabled
Radius Server Connect Timeout sec: 3

Primary radius server:
        Server name:    172.17.1.123
        IP address:     172.17.1.123
        Server IP Port: 1645
        Client address: 172.17.1.221
        Shared secret:
        Access Requests:0        Access Accepts:0        Access Rejects:0
        Access Challenges:0      Access Retransmits:0    Client timeouts:0
        Bad authenticators:0     Unknown types:0         Round Trip Time:0 sec(s)
Secondary radius server:
        Server name:    172.17.1.123
        IP address:     172.17.1.123
        Server IP Port: 1645
        Client address: 172.17.1.221
        Shared secret:
        Access Requests:3        Access Accepts:0        Access Rejects:0
        Access Challenges:0      Access Retransmits:2    Client timeouts:0
        Bad authenticators:0     Unknown types:0         Round Trip Time:0


Radius Acct Server Connect Timeout sec: 3
```

```
Primary radius accounting server:
        Server name:    172.17.1.104
        Client address: 172.17.1.221
        Shared secret:  lf|nki
Secondary radius accounting server:
        Server name:    172.17.1.123
        Client address: 172.17.1.221
        Shared secret:  lf|nki
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

show radius-accounting

```
show radius-accounting
```

Description

Displays the current RADIUS accounting client configuration and statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The output from this command displays information about the status and configuration of RADIUS accounting

Example

The following command displays RADIUS accounting client configuration and statistics:

```
show radius-accounting
```

Following is the output from this command:

```
Radius Accounting: enabled
Radius Acct Server Connect Timeout sec: 3
Primary radius accounting server:
        Server name: 172.17.1.104
        IP address: 172.17.1.104
        Server IP Port: 1646
        Client address: 172.17.1.221
        Shared secret:  lf|nki
        Acct Requests:0  Acct Responses:0       Acct Retransmits:0      Timeouts:0
Secondary radius accounting server:
        Server name: 172.17.1.123
        IP address: 172.17.1.123
        Server IP Port: 1646
        Client address: 172.17.1.221
        Shared secret:  lf|nki
        Acct Requests:0  Acct Responses:0       Acct Retransmits:0      Timeouts:0
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

show route-map

```
show route-map <route map>
```

Description

Displays route map information.

Syntax Description

route map	Specifies a route map name.

Default

N/A.

Usage Guidelines

If you do not specify a route map name, information for all the route maps will be displayed.

Example

The following command displays the route-map named *bgp-out*:

```
show route-map bgp-out
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show tacacs

```
show tacacs
```

Description

Displays the current TACACS+ configuration and statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays TACACS+ client configuration and statistics:

```
show tacacs
```

Following is the output from this command:

```
TACACS+: enabled
TACACS+ Authorization: enabled
TACACS+ Accounting: enabled
TACACS+ Server Connect Timeout sec: 3

Primary TACACS+ Server:
        Server name:    172.17.1.104
        IP address:     172.17.1.104
        Server IP Port: 49
        Client address: 172.17.1.220
        Shared secret:  lf|nki
Secondary TACACS+ Server:
        Server name:    172.17.1.123
        IP address:     172.17.1.123
        Server IP Port: 49
        Client address: 172.17.1.220
        Shared secret:  lf|nki

TACACS+ Acct Server Connect Timeout sec: 3
Primary TACACS+ Accounting Server:
        Server name:    172.17.1.104
        Client address: 172.17.1.220
        Shared secret:  lf|nki
Secondary TACACS+ Accounting Server:
        Server name:    172.17.1.123
        Client address: 172.17.1.220
        Shared secret:  lf|nki
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show tacacs-accounting

```
show tacacs-accounting
```

Description

Displays the current TACACS+ accounting client configuration and statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None:

Example

The following command displays TACACS+ accounting client configuration and statistics:

```
show tacacs-accounting
```

Following is the output from this command:

```
TACACS+ Accounting: enabled
TACACS+ Acct Server Connect Timeout sec: 3

Primary TACACS+ Accounting Server:
        Server name: 172.17.1.104
        IP address: 172.17.1.104
        Server IP Port: 49
        Client address: 172.17.1.220
        Shared secret:  lf|nki
Secondary TACACS+ Accounting Server:
        Server name: 172.17.1.123
        IP address: 172.17.1.123
        Server IP Port: 49
        Client address: 172.17.1.220
        Shared secret:  lf|nki
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

ssh2

```
ssh2 {cipher [3des | blowfish]} {port <portnum>} {compression [on | off]}
{user <username>} {debug <debug_level>} {<username>@} [<host> |
<ipaddress>] {<remote command>}
```

Description

Initiates an SSH2 client session to a remote SSH2 server.

Syntax Description

3des	Specifies that the 3des cipher should be used for encryption. This is the default.
blowfish	Specifies that the blowfish cipher should be used for encryption.
portnum	Specifies the TCP port number to be used for communicating with the SSH2 client. Default is port 22.
compression	on specifies that data is to be compressed.
	`off` specifies that compression is not to be used. Default is `off`.
username	Specifies a login name for the remote host, as an alternate to the user@host parameter.
debug_level	Specifies a debug level. Default is 0
username	Specifies a login name for the remote host. May be omitted if it is the same as the username on the switch.
host	Specifies the name of the remote host
ipaddress	Specifies the IP address of the remote host
remote command	Specifies a command to be passed to the remote system for execution. Remote commands are not supported on switches. This option is only valid if the remote system is a system, such as a UNIX workstation, that can accept remote commands.

Default

N/A.

Usage Guidelines

You must be running a security-enabled version of ExtremeWare 6.2.1 or later (which is under Export Control) in order to use the SSH2 client command.

SSH2 does not need to be enabled on the switch in order to use this command.

Typically this command is used to establish a secure session to a remote switch. You will be prompted for your password. Once you have logged in successfully, all ExtremeWare commands you enter will be executed on the remote switch. When you terminate the remote session, commands will then resume being executed on the original switch.

The remote command option cannot be used with Extreme Networks switches. If you include a remote command, you will receive an error message.

Example

The following command establishes an SSH2 session on switch engineering1:

```
ssh2 admin@engineering1
```

The following command establishes an SSH2 session with the switch summit48i over TCP port 2050 with compression enabled:

```
ssh2 port 2050 compression on admin@summit48i
```

History

This command was first available in ExtremeWare 6.2.1

Platform Availability

This command is available on all platforms.

unconfigure cpu-dos-protect

```
unconfigure cpu-dos-protect
```

Description

Resets denial of service protection configuration to default parameter values.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command will not change whether denial of service protection is enabled or disabled. To enable or disable denial of service protection, use the following commands:

```
enable cpu-dos-protect
disable cpu-dos-protect
```

The default values for the denial of service protection parameters are as follows:

- alert-threshold—4000 packets per second
- notice-threshold—4000 packets per second
- timeout—15 seconds
- messages—on (messages are sent to syslog)
- filter-precedence—10

Example

The following command resets the denial of service protection configuration to the default values:

```
unconfigure cpu-dos-protect
```

History

This command was first available in ExtremeWare 7.0.0

Platform Availability

This command is available on all platforms.

unconfigure radius

```
unconfigure radius {server [primary | secondary]}
```

Description

Unconfigures the RADIUS client configuration.

Syntax Description

primary	Unconfigures the primary RADIUS server.
secondary	Unconfigures the secondary RADIUS server.

Default

Unconfigures both primary and secondary servers.

Usage Guidelines

None.

Example

The following command unconfigures the secondary RADIUS server for the client:

```
unconfigure radius server secondary
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

unconfigure radius-accounting

```
unconfigure radius-accounting {server [primary | secondary]}
```

Description

Unconfigures the RADIUS accounting client configuration.

Syntax Description

primary	Unconfigures the primary RADIUS accounting server.
secondary	Unconfigures the secondary RADIUS accounting server.

Default

Unconfigures both the primary and secondary accounting servers.

Usage Guidelines

None.

Example

The following command unconfigures the secondary RADIUS accounting server for the client:

```
unconfigure radius-accounting server secondary
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

unconfigure tacacs

```
unconfigure tacacs {server [primary | secondary]}
```

Description

Unconfigures the TACACS+ client configuration.

Syntax Description

primary	Unconfigures the primary TACACS+ server.
secondary	Unconfigures the secondary TACACS+ server.

Default

Unconfigures both the primary and secondary TACACS+ servers.

Usage Guidelines

None.

Example

The following command unconfigures all TACACS+ servers for the client:

```
unconfigure tacacs
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

unconfigure tacacs-accounting

```
unconfigure tacacs-accounting {server [primary | secondary]}
```

Description

Unconfigures the TACACS+ accounting client configuration.

Syntax Description

primary	Unconfigures the primary TACACS+ accounting server.
secondary	Unconfigures the secondary TACACS+ accounting server.

Default

Unconfigures both the primary and secondary TACACS+ accounting servers.

Usage Guidelines

None.

Example

The following command unconfigures all TACACS+ accounting servers for the client:

```
unconfigure tacacs-accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

12 EAPS Commands

This chapter describes commands for configuring and monitoring Ethernet Automatic Protection Switching (EAPS).

To use EAPS, you must enable EDP on the switch and the EAPS ring ports.

The EAPS protocol provides fast protection switching to layer 2 switches interconnected in an Ethernet ring topology, such as a metropolitan area network (MAN) or large campuses. EAPS protection switching is similar to what can be achieved with the Spanning Tree Protocol (STP), but offers the advantage of converging in less than a second when a link in the ring breaks.

To take advantage of the Spatial Reuse technology and broaden the use of the ring's bandwidth, EAPS supports multiple EAPS domains running on the ring at the same time.

EAPS operates by declaring an EAPS domain on a single ring. Any VLAN that warrants fault protection is configured on all ring ports in the ring, and is then assigned to an EAPS domain. On that ring domain, one switch, or node, is designated the *master* node, while all other nodes are designated as *transit* nodes.

One port of the master node is designated the master node's *primary* port (P) to the ring; another port is designated as the master node's *secondary* port (S) to the ring. In normal operation, the master node blocks the secondary port for all non-control traffic belonging to this EAPS domain. If the master node detects a break in the ring, it unblocks its secondary port and allows data traffic to be transmitted and received through it.

EAPS fault detection on a ring is based on a single *control* VLAN per EAPS domain. This EAPS domain provides protection to one or more data-carrying VLANs called *protected* VLANs. The control VLAN is used only to send and receive EAPS messages; the protected VLANs carry the actual data traffic. As long as the ring is complete, the EAPS master node blocks the protected VLANs from accessing its secondary port.

A master node detects a ring fault in any of three ways:

- "Link down" message sent by a transit node on the control VLAN
- Ring port down event from lower hardware layers
- Failed response to a periodic health-check packet on the control VLAN

When the master node detects a failure, it declares a "failed" state and opens its logically blocked secondary port on all the protected VLANs. The master node also flushes its forwarding database (FDB) and sends a message on the control VLAN to all of its associated transit nodes to flush their forwarding databases.

configure eaps add control vlan

```
configure eaps <name> add control vlan <vlan_name>
```

Description

Adds the specified control VLAN to the specified EAPS domain.

Syntax Description

name	Specifies the name of an EAPS domain.
vlan_name	Specifies the name of the control VLAN.

Default

N/A.

Usage Guidelines

You must configure one *control* VLAN for each EAPS domain. The control VLAN is used only to send and receive EAPS messages.

The VLAN that will act as the control VLAN must be configured as follows:

- The VLAN must NOT be assigned an IP address, to avoid loops in the network.
- Only ring ports may be added as members of the control VLAN.
- The ring ports of the control VLAN must be tagged. This ensures that EAPS control VLAN traffic is serviced before any other traffic and that control VLAN messages reach their intended destinations.
- The control VLAN must be assigned a QoS profile of QP8 with the QoS profile priority setting `HighHi`.

A control VLAN cannot belong to more than one EAPS domain.

Example

The following command adds the control VLAN “keys” to the EAPS domain “eaps_1.”

```
configure eaps eaps_1 add control vlan keys
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps add protect vlan

```
configure eaps <name> add protect vlan <vlan_name>
```

Description

Adds the specified protected VLAN to the specified EAPS domain.

Syntax Description

name	Specifies the name of an EAPS domain.
vlan_name	Specifies the name of the protected VLAN.

Default

N/A.

Usage Guidelines

You must configure one or more *protected* VLANs for each EAPS domain. The protected VLANs are the data-carrying VLANs.

When you configure the VLAN that will act as a protected VLAN, the ring ports of the protected VLAN must be tagged (except in the case of the default VLAN). As long as the ring is complete, the master node blocks the protected VLANs on its secondary port.

Example

The following command adds the protected VLAN "orchid" to the EAPS domain "eaps_1":

```
configure eaps eaps_1 add protect vlan orchid
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps delete control vlan

```
configure eaps <name> delete control vlan <vlan_name>
```

Description

Deletes the specified control VLAN from the specified EAPS domain.

Syntax Description

name	Specifies the name of an EAPS domain.
vlan_name	Specifies the name of the control VLAN.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the control VLAN “keys” from the EAPS domain “eaps_1”:

```
configure eaps eaps_1 delete control vlan keys
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps delete protect vlan

```
configure eaps <name> delete protect vlan <vlan_name>
```

Description

Deletes the specified protected VLAN from the specified EAPS domain.

Syntax Description

name	Specifies the name of an EAPS domain.
vlan_name	Specifies the name of the protected VLAN.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the protected VLAN “orchid” from the EAPS domain “eaps_1”:

```
configure eaps eaps_1 delete protect vlan orchid
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps failtime

```
configure eaps <name> failtime [<seconds>]
```

Description

Configures the value of the failtimer the master node uses for EAPS health-check packets.

Syntax Description

name	Specifies the name of an EAPS domain.
seconds	Specifies the number of seconds the master node waits to receive a health-check packet before the failtimer expires. Default is 3 seconds.

Default

The default is three seconds.

Usage Guidelines

Use the `failtime` keyword and its associated `seconds` parameter to specify the amount of time the master node waits before the failtimer expires. The `seconds` parameter must be set greater than the configured value for `hellotime`. The default value is three seconds.

Increasing the `failtime` value provides more protection by waiting longer to receive a health-check packet when the network is congested.

NOTE

In previous versions of ExtremeWare, the secondary port on the Master node would open when the failtimer expired. In ExtremeWare 7.1 the default behavior has been modified to not open the secondary port. You can configure the action taken when the failtimer expires by using the `configure failtimer expiry-action` *command.*

Example

The following command configures the failtimer value for the EAPS domain “eaps_1” to 15 seconds:

```
configure eaps eaps_1 failtime 15
```

History

This command was first available in ExtremeWare 6.2.

The behavior for this command was modified in ExtremeWare 7.1 to follow the parameters configured in `configure eaps failtime expiry-action`.

Platform Availability

This command is available on all platforms.

configure eaps failtime expiry-action

```
configure eaps <name> failtime expiry-action [ open-secondary-port |
send-alert]
```

Description

Configures the action taken when the failtimer expires.

Syntax Description

name	Specifies the name of an EAPS domain.
open-secondary-port	Specifies to open the secondary port when the failtimer expires.
send-alert	Specifies that a critical message is sent to the syslog when the failtimer expires.

Default

Default is send-alert.

Usage Guidelines

In earlier releases of ExtremeWare, when the failtimer of a master node expired, the default action was to open the secondary port. If the master node loses three Hello-PDUs in a row, the failtimer will expire, but there might not necessarily be a break in the ring. Opening the secondary port in this situation would create a loop.

The `configure eaps failtime expiry-action` command allows you to configure the action taken when the failtimer expires.

By default the action is to send an alert if the failtimer expires. Instead of going into a "Failed" state, the master node remains in a "Complete" or "Init" state, maintains the secondary port blocking, and writes a critical error message to syslog warning the user that there is a fault in the ring. An SNMP trap is also sent.

To use the failtimer expiry action of earlier releases, use the `open-secondary-port` parameter.

NOTE

You must explicitly configure the failtimer expiry action to `open-secondary-port` *if the EAPS ring includes a section composed of non-EAPS devices.*

NOTE

If you have a previous release of ExtremeWare and are upgrading to ExtremeWare 7.1, the failtimer expiry action will default to `send-alert`*.*

Example

The following command configures the failtimer expiry-action for EAPS domain “eaps_1”:

```
configure eaps eaps_1 failtime expiry-action open-secondary-port
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

configure eaps fast-convergence

```
configure eaps fast-convergence [on | off]
```

Description

Enables EAPS to converge more quickly.

Syntax Description

on	Turns fast-convergence on.
off	Turns fast-convergence off. Default is off.

Default

Default is off.

Usage Guidelines

In certain environments to keep packet loss to a minimum, configure EAPS with fast-convergence turned on. If fast convergence is turned on, it will be displayed under the `show eaps` command. For example:

```
ALP_2_22:2 # show eaps

EAPS Enabled: Yes
EAPS Fast-Convergence: On
Number of EAPS instances: 2
EAPSD-Bridge links: 4
```

NOTE

If fast-convergence is turned on, the link-filters on all EAPS ring-ports are turned off. This could result in a problem if the port's hardware had a problem and started "flapping" between link-up/link-down states.

Example

The following command configures fast convergence for EAPS domain "eaps_1":

```
configure eaps eaps_1 fast-convergence on
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms. This command is not supported on mini-GBICs on the Summit 48si.

configure eaps hellotime

```
configure eaps <name> hellotime <seconds>
```

Description

Configures the value of the hello timer the master node used for the EAPS health-check packet.

Syntax Description

name	Specifies the name of an EAPS domain.
seconds	Specifies the number of seconds to wait between transmission of the health-check packets on the control VLAN. Must be greater than 0.

Default

Default is 1 second.

Usage Guidelines

Use the `hellotime` keyword and its associated `seconds` parameter to specify the amount of time the master node waits between transmissions of health-check packets on the control VLAN. Increasing the `hellotime` value keeps the processor from sending and processing too many health-check packets. Increasing the `hellotime` value should not affect the network convergence time, because transit nodes are already sending "link down" notifications.

This command applies only to the master node. If you configure the polling timers for a transit node, they will be ignored. If you later reconfigure that transit node as the master node, the polling timer values will be used as the current values.

Example

The following command configures the hellotime value for the EAPS domain "eaps_1" to 2 seconds:

```
configure eaps eaps_1 hellotime 2
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps mode

```
configure eaps <name> mode [master | transit]
```

Description

Configures the switch as either the EAPS master node or as an EAPS transit node for the specified domain.

Syntax Description

name	Specifies the name of an EAPS domain.
master	Specifies that this switch should be the master node for the named EAPS domain.
transit	Specifies that this switch should be the transit node for the named EAPS domain.

Default

N/A.

Usage Guidelines

None.

Example

The following command identifies this switch as the master node for the domain named eaps_1:

```
configure eaps eaps_1 mode master
```

The following command identifies this switch as a transit node for the domain named eaps_1:

```
configure eaps eaps_1 mode transit
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps name

```
configure eaps <old_name> name <new_name>
```

Description

Renames an existing EAPS domain.

Syntax Description

old_name	Specifies the current name of an EAPS domain.
new_name	Specifies a new name for the EAPS domain.

Default

N/A.

Usage Guidelines

None.

Example

The following command renames EAPS domain “eaps-1” to “eaps-5”:

```
configure eaps eaps-1 name eaps-5
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps port

```
configure eaps <name> [primary | secondary] port <port number>
```

Description

Configures a node port as the primary or secondary port for the specified EAPS domain.

Syntax Description

name	Specifies the name of an EAPS domain.
primary	Specifies that the port is to be configured as the primary port.
secondary	Specifies that the port is to be configured as the secondary port.
port number	Specifies the port number.

Default

N/A.

Usage Guidelines

Each node on the ring connects through two ring ports. One port must be configured as the *primary* port; the other must be configured as the *secondary* port.

Example

The following command adds port 1 of the module installed in slot 8 of a BlackDiamond switch to the EAPS domain “eaps_1” as the primary port:

```
configure eaps eaps_1 primary port 8:1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure eaps shared-port link-id

```
configure eaps shared-port <port> link-id <id>
```

Description

Configures the link ID of the shared port.

Syntax Description

port	Specifies the port number of the common link port.
id	Specifies the link ID of the port.

Default

N/A.

Usage Guidelines

Each common link in the EAPS network must have a unique link ID. The controller and partner shared ports belonging to the same common link must have *matching* link IDs. No other instance in the network should have that link ID.

Example

The following command configures the EAPS shared port 1:1 to have a link ID of 1.

```
configure eaps shared-port 1:1 link-id 1
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

configure eaps shared-port mode

```
configure eaps shared-port <port> mode <controller | partner>
```

Description

Configures the mode of the shared port.

Syntax Description

port	Specifies the port number of the shared port.
controller	Specifies the controller mode. The controller is the end of the common link responsible for blocking ports when the common link fails thereby preventing the superloop.
partner	Specifies partner mode.

Default

N/A.

Usage Guidelines

The shared port on one end of the common link must be configured to be the *controller*. This is the end responsible for blocking ports when the common link fails thereby preventing the superloop.

The shared port on the other end of the common link must be configured to be the *partner*. This end does not participate in any form of blocking. It is responsible for only sending and receiving health-check messages.

Example

The following command configures the shared port 1:1 to be the controller.

```
configure eaps shared-port 1:1 mode controller
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

create eaps

```
create eaps <name>
```

Description

Creates an EAPS domain with the specified name.

Syntax Description

name	Specifies the name of an EAPS domain to be created. May be up to 32 characters in length.

Default

N/A.

Usage Guidelines

The name parameter is a character string of up to 32 characters that identifies the EAPS domain to be created. EAPS domain names and VLAN names must be unique: Do not use the same name string to identify both an EAPS domain and a VLAN.

Example

The following command creates EAPS domain eaps_1 on an "*i*" series switch:

```
create eaps eaps-1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

create eaps shared-port

```
create eaps shared-port <port>
```

Description

Creates an EAPS shared port on the switch.

Syntax Description

port	Specifies the port number of the common link port.

Default

N/A.

Usage Guidelines

To configure a common link, you must create a shared port on each switch of the common link.

Example

The following command creates a shared port on the EAPS domain.

```
create eaps shared-port 1:2
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

delete eaps

```
delete eaps <name>
```

Description

Deletes the EAPS domain with the specified name.

Syntax Description

name	Specifies the name of an EAPS domain to be deleted.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes EAPS domain eaps_1:

```
delete eaps eaps-1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

delete eaps shared-port

```
delete eaps shared-port <port>
```

Description

Deletes an EAPS shared port on a switch.

Syntax Description

port	Specifies the port number of the Common Link port.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes shared port 1:1.

```
delete eaps shared-port 1:1
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

disable eaps

```
disable eaps {<name>}
```

Description

Disables the EAPS function for a named domain or for an entire switch.

Syntax Description

name	Specifies the name of an EAPS domain.

Default

Disabled for the entire switch.

Usage Guidelines

None.

Example

The following command disables the EAPS function for entire switch:

```
disable eaps
```

The following command disables the EAPS function for the domain “eaps-1”:

```
disable eaps eaps-1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable eaps

```
enable eaps {<name>}
```

Description

Enables the EAPS function for a named domain or for an entire switch.

Syntax Description

name	Specifies the name of an EAPS domain.

Default

Disabled.

Default command enables for the entire switch.

Usage Guidelines

EDP must be enabled on the switch and EAPS ring ports.

Example

The following command disables the EAPS function for entire switch:

```
enable eaps
```

The following command disables the EAPS function for the domain “eaps-1”:

```
enable eaps eaps-1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show eaps

```
show eaps {<name>} {detail}
```

Description

Displays EAPS status information.

Syntax Description

name	Specifies the name of an EAPS domain.
detail	Specifies all available detail for each domain.

Default

N/A.

Usage Guidelines

If you enter the `show eaps` command without a keyword, the command displays less than with the `detail` keyword.

Use the optional domain name parameter to display status information for a specific EAPS domain.

The output displayed by this command depends on whether the node is a transit node or a master node. The display for a transit node contains information fields that are not shown for a master node. Also, some state values are different on a transit node than on a master node.

The fields displayed are as follows:

EAPS Enabled:	Current state of EAPS on this switch: • Yes—EAPS is enabled on the switch. • No—EAPS is not enabled.
EAPS Fast Convergence:	Displays only when Fast Convergence is on.
Number of EAPS instances:	Number of EAPS domains created. The maximum number of EAPS domains per switch is 64.
EAPSD-Bridge links:	The total number of EAPS bridge links in the system. The maximum count is 4096. Each time a VLAN is added to EAPS, this count increments by 1.
Name:	The configured name for this EAPS domain.
(instance=)	The instance number is created internally by the system.

State:	On a transit node, the command displays one of the following states: • Idle—The EAPS domain has been enabled, but the configuration is not complete. • Links-Up—This EAPS domain is running, and both its ports are up and in the FORWARDING state. • Links-Down—This EAPS domain is running, but one or both of its ports are down. • Preforwarding—This EAPS domain is running, and both of its ports are up, but one of them is in a temporary BLOCKED state. On a master node, the command displays one of the following states: • Idle—The EAPS domain has been enabled, but the configuration is not complete. • Init—The EAPS domain has started but has not yet determined the status of the ring. The secondary port is in a BLOCKED state. • Complete—The ring is in the COMPLETE state for this EAPS domain. • Failed—There is a break in the ring for this EAPS domain. • [Failtimer Expired]—When the failtimer expires and it's action is set to send-alert, this flag is set. This flag indicates there is a misconfiguration or hardware problem in the EAPS ring. The EAPS master node will continue to remain in COMPLETE or INIT state with it's secondary port blocking.
[Running: …]	• Yes—This EAPS domain is running. • No—This EAPS domain is not running.
Enabled:	Indicates whether EAPS is enabled on this domain. • Y—EAPS is enabled on this domain. • N—EAPS is not enabled.
Mode:	The configured EAPS mode for this switch: transit (T) or master (M).
Primary/Secondary port:	The port numbers assigned as the EAPS primary and secondary ports. On the master node, the port distinction indicates which port is blocked to avoid a loop.
Port status:	• Unknown—This EAPS domain is not running, so the port status has not yet been determined. • Up—The port is up and is forwarding data. • Down—The port is down. • Blocked—The port is up, but data is blocked from being forwarded.
Tag status:	Tagged status of the control VLAN: • Tagged—The control VLAN has this port assigned to it, and the port is tagged in the VLAN. • Untagged—The control VLAN has this port assigned to it, but the port is untagged in the control VLAN. • Undetermined—Either a VLAN has not been added as the control VLAN to this EAPS domain or this port has not been added to the control VLAN.
Hello Timer interval:	The configured value of the timer in seconds, specifying the time that the master node waits between transmissions of health check packets.
Fail Timer interval:	The configured value of the timer in seconds, specifying the time that the master node waits before the failtimer expires.

Failtimer expiry action:	Displays the action taken when the failtimer expires: • Send-alert—Sends a critical message to the syslog when the failtimer expires. • Open-secondary-port—Opens the secondary port when the failtimer expires. Displays only for master nodes.
Preforwarding Timer interval:[1]	The configured value of the timer. This value is set internally by the EAPS software.
Last update:[1]	Displayed only for transit nodes; indicates the last time the transit node received a hello packet from the master node (identified by its MAC address).
EAPS Domain has … Controller Vlans:	Lists the assigned name and ID of the control VLAN.
EAPS Domain has … Protected Vlans:[2]	Lists the assigned names and VLAN IDs of all the protected VLANs configured on this EAPS domain.
Number of Protected Vlans:	The count of protected VLANs configured on this EAPS domain.

1. These fields apply only to transit nodes; they are not displayed for a master node.
2. This list is displayed when you use the `detail` keyword in the `show eaps` command.

Example

The following command displays detailed EAPS information for domain “eaps2”:

```
show eaps eaps2 detail
```

The results for domain “eaps2” on a master node are shown as follows:

```
  Name: “eaps2” (instance=0)
  State: Complete        [Running: Yes]
  Enabled: Yes    Mode: Master
  Primary port: 14          Port status: Up        Tag status: Tagged
  Secondary port: 13        Port status: Blocked   Tag status: Tagged
  Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
   Fail Timer expiry action: Send alert
   Last update: From Master Id 00:01:30:B9:4B:E0, at Tue May 6 12:49:25 2003
  Eaps Domain has following Controller Vlan:
    Vlan Name            VID
    “rhsc”               0020
  EAPS Domain has following Protected Vlan(s):
    Vlan Name            VID
    “blue”               1003
    “traffic”            1001
  Number of Protected Vlans: 2
```

The following command displays detailed EAPS information:

```
show eaps detail
```

The results for a transit node are shown as follows:

```
EAPS Enabled: Yes
Number of EAPS instances: 1
EAPSD-Bridge links: 2

  Name: “eaps1” (instance=0)
  State: Links-Up          [Running: Yes]
  Enabled: Yes    Mode: Transit
```

```
  Primary port: 13          Port status: Up        Tag status: Tagged
  Secondary port: 14        Port status: Up        Tag status: Tagged
  Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
  Preforwarding Timer interval: 3 sec
  Last update: From Master Id 00:01:30:B9:4B:E0, at Tue May 6 12:49:25 2003
  Eaps Domain has following Controller Vlan:
    Vlan Name            VID       QosProfile
    “rhsc”               0020      QP8
  EAPS Domain has following Protected Vlan(s):
    Vlan Name            VID
    “traffic”            1001
  Number of Protected Vlans: 1
```

The following command displays EAPS information:

```
show eaps eaps2
```

The results for a transit node are shown as follows:

```
   Name: "eaps2" (instance=1)
   State: Link-Down       [Running: Yes]
   Enabled: Yes    Mode: Transit
   Primary port: 3           Port status: Down      Tag status: Tagged
   Secondary port: 2         Port status: Up        Tag status: Tagged
   Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
   Preforwarding Timer interval: 6 sec
   Last update: From Master Id 00:01:30:B9:4B:E0, at Tue May 6 12:49:25 2003
   EAPS Domain has following Controller Vlan:
      Vlan Name            VID             QosProfile
      "cv2"                4002            QP8
   Number of Protected Vlans: 2
```

The following command displays summary EAPS information:

```
show eaps summary
```

The results for this command are as follows:

```
EAPS Enabled: Yes
Number of EAPS instances: 1
EAPSD-Bridge links: 2

                                    Pri     Sec                         Vlan
Domain        State        Mo En   Port    Port     Control-Vlan (VID)Count
------------  ------------ -- -- ------- -------   ----------------------
eaps1         Complete     M  Y    1       2       cv1         (1001)    1
```

History

This command was first available in ExtremeWare 6.2.

The summary option was added in ExtremeWare 6.2.2.

This command was modified in ExtremeWare 7.1 to display primary and secondary ring-ports and show the status of the failtimer.

Platform Availability

This command is available on all platforms.

show eaps shared-port

```
show eaps shared-port [detail]
```

Description

Displays shared-port information for one or more EAPS domains.

Syntax Description

detail	Specifies to display the status of all segments and VLANs.

Default

N/A.

Usage Guidelines

If you enter the `show eaps shared-port` command without an argument or keyword, the command displays a summary of status information for all configured EAPS shared ports. You can use the `detail` keyword to display more detailed status information about the segments and VLANs associated with each shared port.

The fields displayed are as follows:

Field	Description
Shared Port	Displays the port number of the shared port.
Mode	Indicates whether the switch on either end of the common link is a controller or partner. The mode is configured by the user.
Link ID	The link ID configured by the user.
Up	Displays one of the following: • Yes—indicates that the link ID and the mode are configured. • No—indicates that the link ID or the mode is not configured.
State	Displays one of the following states: • Idle—Shared-port instance is not running. • Ready—The EAPS domain is running, the neighbor can be reached, and the common link is *up*. • Blocking—The EAPS domain is running, the neighbor cannot be reached, or the common link is *down*. • Preforwarding—The EAPS domain was in a blocking state, and the common link came up. To prevent a superloop, a temporary blocking state is created before going into Ready state.
Domain Count	• Indicates the number of EAPS domains sharing the common link.
VLAN Count	• Indicates the total number of VLANs that are protected under the EAPS domains sharing this common link.

Field	Description
Nbr	• Yes—Indicates that the EAPS instance on the other end of the common link is configured with matching link ID and opposite modes. For example, if one end of the common link is configured as a controller, the other end must be configured as a partner. • Err—Indicates that the EAPS instance on the other end of the common link is configured with a matching link ID, but the modes are configured the same. For example, both modes are configured as controller, or both modes are configured as partner. • No—The neighbor on the other end of the common link cannot be reached. Indicates one or more of the following: - The switch on the other end of the common link is not running. - The shared port has not been created. - The link IDs on each side of the common link do not match. - The common link, and any other segment, between the controller and partner are not fully connected.
RB State	• None—This EAPS shared-port is not the “root blocker”. • Active—This EAPS shared-port is the “root blocker” and is currently active. • Inactive—This EAPS shared-port is the “root blocker” but is currently inactive.
RB ID	The ID of the root blocker. If the value is none, there are not two or more common-link failures.
EAPS Domain List	• Lists the EAPS domains that share the common link.

Example

The following command displays shared-port statistics on “eaps2”, “eaps3”, and “eaps4”: The EAPS domain is in a “ready” state in this example:

```
show eaps shared-port
```

The results for this command are as follows:

```
BD_3_42:7 # show eaps shared-port

EAPS shared-port count: 1

                        Link                Domain Vlan       RB      RB
Shared-port  Mode       Id    Up  State     count  count  Nbr State   Id
-----------  ----------  ----  --  --------  ------ -----  --- ------- -----
1:1          Controller  2     Y   Ready       3     1     Yes None    None
EAPS Domain list: "eaps2" "eaps3" "eaps4"
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

show eaps summary

```
show eaps summary
```

Description

Displays summary information on one or more EAPS domains.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Displays EAPS domains and associated info such as Domain Name, Domain State, EAPS Mode, Enabled State, Control VLAN and VLAN ID and the Number of Protect VLANs in the domain. This is helpful when viewing the status info for large numbers of EAPS domains quickly.

Example

The following command displays summary EAPS information on a transit node:

```
show eaps summary
```

The results for this command are as follows:

```
EAPS Enabled: Yes
Number of EAPS instances: 3
EAPSD-Bridge links: 6

                                  Pri     Sec                          Vlan
Domain        State        Mo En  Port    Port     Control-Vlan (VID) count
------------  ------------ -- -- ------- -------   ----------------------
eaps4         Links-Up     T  Y    1:1     1:4     cv4         (1004)    1
eaps3         Links-Up     T  Y    1:1     1:3     cv3         (1003)    1
eaps2         Links-Up     T  Y    1:1     1:2     cv2         (1002)    1


EAPS shared-port count: 1

                         Link                Domain Vlan       RB       RB
Shared-port  Mode        Id    Up  State      count  count  Nbr State    Id
-----------  ----------  ----  --  ---------  ------ -----  --- ------- -----
1:1          Controller  2     Y   Ready        3     1     Yes None   None
EAPS Domain list: "eaps2" "eaps3" "eaps4"
```

History

This command was first available in ExtremeWare 6.2.

The `summary` option was added in ExtremeWare 6.2.2.

This command was modified in ExtremeWare 7.1 to show shared-port statistics.

Platform Availability

This command is available on all platforms.

unconfigure eaps shared-port link-id

```
unconfigure eaps shared-port <port> link-id
```

Description

Unconfigures an EAPS link ID on a shared port on the switch.

Syntax Description

port	Specifies the port number of the Common Link port.

Default

N/A.

Usage Guidelines

None.

Example

The following command unconfigures the link ID on shared port 1:1.

```
unconfigure eaps shared-port 1:1 link-id
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

unconfigure eaps shared-port mode

```
unconfigure eaps shared-port <port> mode
```

Description

Unconfigures the EAPS shared port mode.

Syntax Description

port	Specifies the port number of the Common Link port.

Default

N/A.

Usage Guidelines

None.

Example

The following command unconfigures the shared port mode on port 1:1.

```
unconfigure eaps shared-port 1:1 mode
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

unconfigure eaps port

```
unconfigure eaps <name> [primary | secondary] port
```

Description

Sets the specified port's internal configuration state to INVALID.

Syntax Description

name	Specifies the name of an EAPS domain.
primary	Specifies that the primary port should be unconfigured.
secondary	Specifies that the secondary port should be unconfigured.

Default

N / A.

Usage Guidelines

Unconfiguring an EAPS port sets its internal configuration state to INVALID, which causes the port to appear in the Idle state with a port status of Unknown when you use the `show eaps detail` command to display the status information about the port.

Example

The following command unconfigures this node's EAPS primary ring port on the domain eaps_1:

```
unconfig eaps eaps_1 primary port
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

13 STP Commands

This chapter describes:

- Commands related to creating, configuring, enabling, and disabling Spanning Tree Protocol (STP) on the switch
- Commands related to enabling and disabling Rapid Spanning Tree Protocol (RSTP) on the switch
- Commands related to displaying and resetting STP settings on the switch

The Spanning Tree Protocol (STP) is a bridge-based mechanism for providing fault tolerance on networks. STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP in terms used by the 802.1d specification, the switch will be referred to as a bridge.

STP allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational.
- A redundant path is enabled if the main path fails.

The Rapid Spanning Tree Protocol (RSTP; 802.1w) provides an enhanced spanning tree algorithm that improves the convergence speed of bridged networks. RSTP takes advantage of point-to-point links in the network and actively confirms that a port can safely transition to the forwarding state without relying on any timer configurations. If a network topology change or failure occurs, RSTP rapidly recovers network connectivity by confirming the change locally before propagating that change to other devices across the network. For broadcast links, there is no difference in convergence time between STP and RSTP.

RSTP supersedes legacy STP protocols, supports the existing STP parameters and configurations, and allows for seamless interoperability with legacy STP.

Spanning Tree Domains

The switch can be partitioned into multiple virtual bridges. Each virtual bridge can run an independent Spanning Tree instance. Each Spanning Tree instance is called a *Spanning Tree Domain* (STPD). Each STPD has its own root bridge and active path. After an STPD is created, one or more VLANs can be assigned to it.

A port can belong to multiple STPDs. In addition, a VLAN can span multiple STPDs.

The key points to remember when configuring VLANs and STP are:

- Each VLAN forms an independent broadcast domain.

- STP blocks paths to create a loop-free environment.
- When STP blocks a path, no data can be transmitted or received on the blocked port.
- Within any given STPD, all VLANs belonging to it use the same spanning tree.

If you delete a STPD, the VLANs that were members of that STPD are also deleted. You must remove all VLANs associated with the STP before deleting the STPD.

STPD Modes

An STPD has two modes of operation:

- 802.1d mode

  Use this mode for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1d. When configured in this mode, all rapid configuration mechanisms are disabled.

- 802.1w mode

  Use this mode for compatibility with Rapid Spanning Tree (RSTP). When configured in this mode, all rapid configuration mechanisms are enabled. This mode is available for point-to-point links only.

  RSTP is enabled or disabled on a per STPD basis only. You do not enable RSTP on a per port basis.

By default, the:

- STPD operates in 802.1d mode
- Default device configuration contains a single STPD called *s0*
- Default VLAN is a member of STPD s0

All STP parameters default to the IEEE 802.1d values, as appropriate.

Port Modes

An STP port has three modes of operation:

- 802.1d mode

  This mode is used for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1d. BPDUs are sent untagged in 1D mode. Because of this, on any given physical interface there can be only *one* STPD running in 1D mode.

- Extreme Multiple Instance Spanning Tree Protocol (EMISTP) mode

  EMISTP mode is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs. EMISTP adds significant flexibility to STP network design. BPDUs are sent with an 802.1Q tag having an STPD instance Identifier (StpdID) in the VLANid field.

- PVST+ mode

  This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.

These port modes are for STP ports, not for physical ports. When a physical port belongs to multiple STPDs, it is associated with multiple STP ports It is possible for the physical port to run in different modes for different domains to which it belongs.

configure stpd add vlan

```
configure stpd <spanning tree name> add vlan <vlan name> {ports <portlist>
[dot1d | emistp | pvst-plus]}
```

Description

Adds one or more VLANs, or a list of ports within a VLAN, to a specified STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
vlan name	Specifies a VLAN name.
ports	Specifies the port or ports to be included in the STPD. (6.2)
dot1d	Specifies the STP port mode of operation to be 802.1d. (6.2)
emistp	Specifies the STP port mode of operation to be EMISTP. (6.2)
pvst-plus	Specifies the STP port mode of operation to be PVST+. (6.2)

Default

For ExtremeWare 6.1 (or earlier), the default is N/A.

For ExtremeWare 6.2 (or later), all ports are in `emistp` mode, except those in STPD s0, whose default setting is `dot1d` mode.

Usage Guidelines

For version 6.2 or later, this command adds a list of ports within a VLAN to a specified STPD. If no ports are specified, the entire VLAN is added.

For versions up to 6.1, this command adds one or more VLANs to the STPD. All VLANs participating in the STPD elect a Root Bridge and create a loop free least-cost path to the bridge.

Care must be taken to ensure that ports in overlapping domains do not interfere with the orderly working of each domain's protocol.

You must create a VLAN to add a VLAN to the STPD. To create a VLAN, use the `create vlan <vlan name>` command.

You can create STP domains using the `create stpd <name>` command.

For version 6.2 or later:

Added keywords `dot1d`, `emistp`, and `pvst-plus` to specify STP port modes.

- `dot1d`—This mode is reserved for backward compatibility with previous STP versions. BPDUs are sent untagged in 802.1d mode. Because of this, on any given physical interface there can be only *one* STPD running in 802.1d mode.
- `emistp`—This mode sends BPDUs with an 802.1Q tag having an STPD instance Identifier (StpdID) in the VLANid field.

- pvst-plus—This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.

An StpdID is used to identify each STP domain. You assign the StpdID when configuring the domain. An StpdID must be identical to the VLANid of one of the member VLANs in that STP domain, and that VLAN cannot belong to another STPD.

NOTE

These port modes are for STP ports, not for physical ports. When a physical port belongs to multiple STPDs, it is associated with multiple STP ports. It is possible for the physical port to run in different modes for different domains for which it belongs.

When the switch boots, it automatically creates a VLAN named *default* with a tag value of 1, and STPD s0 with an StpdID of 1. The switch associates VLAN *default* to STPD s0. By default, all ports that belong to this VLAN and STPD are in 802.1d mode.

Example

Create a VLAN named *marketing* and an STPD named *STPD1* as follows:

```
create vlan marketing
create stpd stpd1
```

The following command adds the VLAN named *marketing* to the STPD *STPD1:*

```
configure stpd stpd1 add vlan marketing
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2 to support STP port mode configurations.

Platform Availability

This command is available on all platforms.

configure stpd delete vlan

```
configure stpd <spanning tree name> delete vlan <vlan name> {ports
<portlist>}
```

Description

Deletes a VLAN from and STPD or one or more ports in the specified VLAN from an STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
vlan name	Specifies a VLAN name.
ports	Specifies the port or ports to be removed from the STPD.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes a VLAN named *Marketing* from the STPD *STPD1:*

```
configure stpd stpd1 delete vlan marketing
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure stpd forwarddelay

```
configure stpd <spanning tree name> forwarddelay <seconds>
```

Description

Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the switch is the Root Bridge.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
seconds	Specifies the forward delay time in seconds.

Default

15 seconds.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The range for the <seconds> parameter is 4 through 30 seconds.

Example

The following command sets the forward delay from *STPD1* to 20 seconds:

```
configure stpd stpd1 forwarddelay 20
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure stpd hellotime

```
configure stpd <spanning tree name> hellotime <seconds>
```

Description

Specifies the time delay (in seconds) between the transmission of Bridge Protocol Data Units (BPDUs) from this STPD when it is the Root Bridge.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
seconds	Specifies the hello time in seconds.

Default

2 seconds.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The range for the <seconds> parameter is 1 through 10 seconds.

Example

The following command sets the time delay from *STPD1* to 10 seconds:

```
configure stpd stpd1 hellotime 10
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure stpd maxage

```
configure stpd <spanning tree name> maxage <seconds>
```

Description

Specifies the maximum age of a BPDU in the specified STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
seconds	Specifies the maxage time in seconds.

Default

20 seconds.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The range for the <seconds> parameter is 6 through 40 seconds.

Note that the time must be greater than, or equal to 2 * (Hello Time + 1) and less than, or equal to 2 * (Forward Delay –1).

Example

The following command sets the maximum age of *STPD1* to 30 seconds:

```
configure stpd stpd1 maxage 30
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure stpd mode

```
configure stpd <spanning tree name> mode [dot1d | dot1w]
```

Description

Configures the operational mode for the specified STP domain.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
dot1d	Specifies the STPD mode of operation to be 802.1d.
dot1w	Specifies the STPD mode of operation to be 802.1w, and rapid configuration is enabled.

Default

Operates in 802.1d mode.

Usage Guidelines

If you configure the STP domain in 802.1d mode, the rapid reconfiguration mechanism is disabled.

If you configure the STP domain in 802.1w mode, the rapid reconfiguration mechanism is enabled.

Example

The following command configures STPD *s1* to enable the rapid reconfiguration mechanism and operate in 802.1w mode:

```
configure stpd s1 mode dot1w
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

configure stpd ports cost

```
configure stpd <spanning tree name> ports cost <cost> <portlist>
```

Description

Specifies the path cost of the port in the specified STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
cost	Specifies a numerical port cost value. The range is 1 through 65,535.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

The switch automatically assigns a default path cost based on the speed of the port, as follows:

- For a 10Mbps port, the default cost is 100.
- For a 100Mbps port, the default cost is 19.
- For a 1000Mbps port, the default cost is 4.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The range for the `cost` parameter is 1 through 65,535. The switch automatically assigns a default path cost based on the speed of the port.

Example

The following command configures a cost of 100 to ports 1 through 5 in STPD *s0* on a stand-alone switch:

```
configure stpd s0 ports cost 100 1-5
```

The following command configures a cost of 100 to slot 2, ports 1 through 5 in STPD *s0* on a modular switch:

```
configure stpd s0 ports cost 100 2:1-2:5
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

configure stpd ports link-type

```
configure stpd <spanning tree name> ports link-type [auto | edge |
broadcast | point-to-point] <portlist>
```

Description

Configures the ports in the specified STPD as auto, edge, broadcast or point-to-point link types.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
auto	Specifies the switch to automatically determine the port link type. An auto link behaves like a point-to-point link if the link is in full duplex mode or if link aggregation is enabled on the port. Used for 802.1w configurations.
edge	Specifies a port that does not have a bridge attached. An edge port is placed and held in the STP forwarding state unless a BPDU is received by the port.
broadcast	Specifies a port attached to a LAN segment with more than two bridges. Used for 802.1d configurations. A port with broadcast link type cannot participate in rapid reconfiguration. By default, all ports are broadcast links.
point-to-point	Specifies a port attached to a LAN segment with only two bridges. A port with point-to-point link type can participate in rapid reconfiguration. Used for 802.1w configurations.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

All ports are broadcast link types.

Usage Guidelines

The default, broadcast links, supports legacy STP (802.1d) configurations.

If you configure a port to be an edge port, the port immediately enters the forwarding state. Edge ports remain in the forwarding state unless the port receives a BPDU.

RSTP does not send any BPDUs from an edge port, nor does it generate topology change events when an edge port changes its state.

RSTP rapidly moves the designated ports of a point-to-point link type into the forwarding state. This behavior is supported by RSTP only.

An auto link behaves like a point-to-point link if the link is in full duplex mode or if link aggregation is enabled on the port; otherwise, an auto link behaves like a broadcast link. If a non-STP switch exists between several switches operating in 802.1w mode with auto links, the non-STP switch may negotiate full duplex even though the broadcast domain extends over several STP devices. In this situation, an 802.1w port may advance to the “forwarding” state more quickly than desired.

If the switch operates in 802.1d mode, any configured port link type will behave the same as the broadcast link type.

Example

The following command configures ports 1 through 4 to be point-to-point links in STPD *s1* on a stand-alone switch:

```
configure stpd s1 ports link-type point-to-point 1-4
```

The following command configures slot 2, ports 1 through 4 to be point-to-point links in STPD *s1* on a modular switch:

```
configure stpd s1 ports link-type point-to-point 2:1-2:4
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

configure stpd ports mode

```
configure stpd <spanning tree name> ports mode [dot1d | emistp | pvst-plus]
<portlist>
```

Description

Configures the STP mode of operation for the specified port list.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
dot1d	Specifies IEEE 802.1d-compliant packet formatting. A physical port can only be a member of one STPD running it `dot1d` mode.
emistp	Specifies 802.1d formatting and 802.1q tagging.
pvst-plus	Specifies PVST+ packet formatting.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Ports in the default STPD (s0) are `dot1d` mode. Ports in user-created STPDs are in `emistp` mode.

Usage Guidelines

None.

Example

The following command configures STPD *s1* with PVST+ packet formatting for port 1 on a stand-alone switch:

```
configure stpd s1 ports mode pvst-plus 1
```

The following command configures STPD *s1* with PVST+ packet formatting for slot 2, port 1 on a modular switch:

```
configure stpd s1 ports mode pvst-plus 2:1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure stpd ports priority

```
configure stpd <spanning tree name> ports priority <priority> <portlist>
```

Description

Specifies the port priority of the port in the specified STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
priority	Specifies a numerical port priority value.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

For version 6.0 and later, the default setting is 16.

For version 2.0 and 4.0, the default setting is 128.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

By changing the priority of the port, you can make it more or less likely to become the root port or a designated port.

A setting of 0 indicates the highest priority.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

For version 6.0 and later:

- The range for the `priority` parameter is 0 through 31.

For version 2.0 and 4.0:

- The range for the `priority` parameter is 0 through 255.

Example

The following command assigns a priority of 1 to ports 1 through 5 in STPD *s0* on a stand-alone switch:

```
configure stpd s0 ports priority 1 1-5
```

The following command assigns a priority of 1 to slot 2, ports 1 through 5 in STPD *s0* on a modular switch:

```
configure stpd s0 ports priority 1 2:1-2:5
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to update the `priority` parameter.

This command was modified in ExtremeWare 4.0 to support modular switches.

Platform Availability

This command is available on all platforms.

configure stpd priority

```
configure stpd <spanning tree name> priority <priority>
```

Description

Specifies the bridge priority of the STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
priority	Specifies the bridge priority of the STPD.

Default

32,768.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

By changing the priority of the STPD, you can make it more or less likely to become the root bridge.

The range for the `priority` parameter is 0 through 65,535. A setting of 0 indicates the highest priority.

Example

The following command sets the bridge priority of *STPD1* to 16,384:

```
configure stpd stpd1 priority 16384
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure stpd tag

```
configure stpd <spanning tree name> tag <vlan tag>
```

Description

Assigns an StpdID to an STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
vlan tag	Specifies the VLANid of a VLAN that is owned by the STPD.

Default

N/A.

Usage Guidelines

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

An StpdID is used to identify each STP domain. You assign the StpdID when configuring the domain. An StpdID must be identical to the VLANid of one of the member VLANs in that STP domain, and that VLAN cannot belong to another STPD. Unless all ports are running in 802.1d mode, an STPD must be configured with an StpdID.

You must create and configure the VLAN, along with the tag, before you can configure the STPD tag. To create a VLAN, use the `create vlan` command. To configure the VLAN, use the `configure vlan` command.

In addition to the VLAN attributes that you will use in the STPD, you must first create an STPD. To create an STPD, use the `create stpd` command.

Example

The following command assigns an StpdID to the `purple_st` STPD:

```
configure stpd purple_st tag 200
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan add ports stpd

```
configure vlan <vlan name> add ports [all | <portlist>] stpd <spanning tree
name> {[dot1d | emistp | pvst-plus]}
```

Description

Adds a list of ports within a VLAN to a specified STPD.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all of the ports to be included in the STPD.
portlist	Specifies the port or ports to be included in the STPD.
spanning tree name	Specifies an STPD name on the switch.
dot1d	Specifies the STP port mode of operation to be 802.1d.
emistp	Specifies the STP port mode of operation to be EMISTP.
pvst-plus	Specifies the STP port mode of operation to be PVST+.

Default

All ports are in `emistp` mode, except those in STPD s0, whose default setting is `dot1d` mode.

Usage Guidelines

This command performs the same function as the `configure stpd add vlan` command with the ports option included.

This command adds a list of ports within a VLAN to a specified STPD, and specifies the mode for those ports.

- `dot1d`—In this mode, BPDUs are sent untagged in 802.1d mode. Because of this, on any given physical interface there can be only *one* STPD running in 802.1d mode. This mode supports the industry standard implementation, and can be used with non-Extreme devices. It can also be used for backward compatibility with previous STP versions.
- `emistp`—This mode sends BPDUs with an 802.1Q tag having an STPD instance Identifier (StpdID) in the VLANid field. This is an Extreme proprietary mode, and cannot be used with non-Extreme devices.
- `pvst-plus`—This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.

These port modes are for STP ports, not for physical ports. When a physical ports belongs to multiple STPDs, it is associated with multiple STP ports. It is possible for the physical port to run in different modes for different domains for which it belongs.

Example

The following command adds ports 2 and 3, members of a VLAN named *Marketing*, to the STPD named *STPD1, and specifies that they be in EMISTP mode:*

```
configure vlan marketing add ports 2-3 stpd stpd1 emistp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

create stpd

```
create stpd <name>
```

Description

Creates a user-defined STPD.

Syntax Description

name	Specifies a user-defined STPD name.

Default

The default device configuration contains a single STPD called *s0*.

When an STPD is created, the STPD has the following default parameters:

- State—disabled
- StpdID—none
- Assigned VLANs—none
- Bridge priority—32,768
- Hello time—2 seconds
- Forward delay—15 seconds
- Operational mode—802.1d
- Rapid Root Failover—disabled state
- Port mode—Ports in the default STPD (s0) are 802.1d mode. Ports in user-created STPDs are in `emistp` mode.

Usage Guidelines

Each STPD name must be unique, and cannot duplicate any other named elements on the switch (such as VLANs, QoS profiles, Access profiles, or route maps). If you are uncertain about the VLAN profile names on the switch, use the `show vlan` command to view the VLAN profiles. If you are uncertain about QoS profile names on the switch, use the `show qos <qos profile>` command to view the QoS profiles.

Each STPD has its own Root Bridge and active path. After the STPD is created, one or more VLANs can be assigned to it.

Example

The following example creates an STPD named *purple_st*:

```
create stpd purple_st
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

delete stpd

```
delete stpd <spanning tree name>
```

Description

Removes a user-defined STPD from the switch.

Syntax Description

spanning tree name	Specifies a user-defined STPD name on the switch.

Default

N/A.

Usage Guidelines

If you remove an STPD, the VLANs that were members of that STPD are also deleted. An STPD can only be removed if all VLANs have been deleted from it.

The default STPD, *s0*, cannot be deleted.

Example

The following command deletes an STPD named *purple_st*:

```
delete stpd purple_st
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable ignore-bpdu vlan

```
disable ignore-bpdu vlan <vlan name>
```

Description

Allows the switch to recognize STP BDUs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

By default, STP processes all of the BPDUs received on a VLAN.

Use the `enable ignore-bpdu vlan <vlan name>` command to allow a BPDU to traverse a VLAN without being processed by STP, even if STP is enabled on the port. If you have a known topology and have switches outside of your network within your STPD, use this feature to keep the root bridge within your network.

Example

The following command disables the ignore-bpdu option on the VLAN *accounting*:

```
disable ignore-bpdu accounting
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable ignore-stp vlan

```
disable ignore-stp vlan <vlan name>
```

Description

Allows a VLAN to use STP port information.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

The `vlan` keyword is optional.

Example

The following command disables the ignore-stp option on the VLAN *accounting*:

```
disable ignore-stp accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable stpd

```
disable stpd {<spanning tree name>}
```

Description

Disables the STP protocol on a particular STPD or for all STPDs.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.

Default

Disabled.

Usage Guidelines

All VLANs belong to an STPD. If you do not want to run STP on a VLAN, you must add the VLAN to an STPD that is disabled.

The `spanning tree name` keyword is optional. You do not need to indicate an STPD name if you disable the STP protocol for all STPDs.

Example

The following command disables an STPD named *purple_st*:

```
disable stpd purple_st
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable stpd ports

```
disable stpd <spanning tree name> ports {<portlist>}
```

Description

Disables STP on one or more ports for a given STPD.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

N / A.

Usage Guidelines

Disabling STP on one or more ports puts those ports in *forwarding* state; all Bridge Protocol Data Units (BPDUs) received on those ports will be disregarded and dropped.

The `portlist` keyword is optional. You do not need to indicate a list of ports if you want to disable STP on all ports in the STPD.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

You must create one or more STP domains, configure, and enable an STPD before you can use the `disable stpd port` command.

Example

The following command disables port 4 on an STPD named *Backbone_st* on a stand-alone switch:

```
disable stpd backbone_st ports 4
```

The following command disables slot 2, port 4 on an STPD named *Backbone_st* on a modular switch:

```
disable stpd backbone_st ports 2:4
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular devices.

Platform Availability

This command is available on all platforms.

disable stpd rapid-root-failover

```
disable stpd <spanning tree name> rapid-root-failover
```

Description

Disables rapid root failover for STP recovery times.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.

Default

Disabled.

Usage Guidelines

To view the status of rapid root failover on the switch, use the `show stpd` command. The `show stpd` command displays information about the STPD configuration on the switch including the enable / disable state for rapid root failover.

Example

The following command disables rapid root fail over on STPD *Backbone_st*:

```
disable stpd backbone_st rapid-root-failover
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable ignore-bpdu vlan

```
enable ignore-bpdu vlan <vlan name>
```

Description

Configures the switch to ignore the STP BPDUs, which prevents ports in the VLAN from becoming part of an STPD.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

This command is useful when you have a known topology with switches outside your network, and you wish to keep the root bridge within your network.

Example

The following command configures the switch to ignore STP BPDUs on the VLAN *accounting*:

```
enable ignore-bpdu vlan accounting
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable ignore-stp vlan

```
enable ignore-stp vlan <vlan name>
```

Description

Configures the switch to ignore the STP protocol and not block traffic for the VLAN(s).

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

This command is useful when multiple VLANs share the same physical ports, but only some of the VLANs require STP protection.

Example

The following command enables the ignore-stp option on the VLAN *accounting*:

```
enable ignore-stp accounting
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable stpd

```
enable stpd {<spanning tree name>}
```

Description

Enables the STP protocol for one or all STPDs.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.

Default

Disabled.

Usage Guidelines

You must create one or more STP domains and configure an STPD before you can use the `enable stpd` command. Use the `create stpd <name>` command to create an STPD.

The `spanning tree name` keyword is optional. You do not need to indicate an STPD name if you enable the STP protocol for all STPDs.

Example

The following command enables an STPD named *Backbone_st*:

```
enable stpd backbone_st
```

History

This command was first available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable stpd rapid-root-failover

```
enable stpd <spanning tree name> rapid-root-failover
```

Description

Enables rapid root failover for faster STP recovery times.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.

Default

Disabled.

Usage Guidelines

To view the status of rapid root failover on the switch, use the `show stpd` command. The `show stpd` command displays information about the STPD configuration on the switch including the enable/disable state for rapid root failover.

Example

The following command enables rapid root fail over on STPD *Backbone_st*:

```
enable stpd backbone_st rapid-root-failover
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable stpd ports

```
enable stpd <spanning tree name> ports <portlist>
```

Description

Enables the STP protocol on one or more ports.

Syntax Description

spanning tree name	Specifies an STPD on the switch.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Enabled.

Usage Guidelines

If STPD is enabled for a port, Bridge Protocol Data Units (BPDUs) will be generated on that port if STP is enabled for the associated STPD.

You must create and configure one or more STP domains before you can use the `enable stpd ports` command. Use the `create stpd <name>` command to create an STP domain. If you have considerable knowledge and experience with STP, you can configure the STPD using the `configure stpd` commands. However, the default STP parameters are adequate for most networks.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

Example

The following command enables port 4 on an STPD named *Backbone_st* on a stand-alone switch:

```
enable stpd backbone_st ports 4
```

The following command enables slot 2, port 4 on an STPD named *Backbone_st* on a modular switch:

```
enable stpd backbone_st ports 2:4
```

History

This command was first available in ExtremeWare 2.0.

Support for modular switches was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show stpd

```
show stpd {<spanning tree name> | detail}
```

Description

Displays STPD settings on the switch.

Syntax Description

spanning tree name	Specifies an STPD on the switch.
detail	Specifies that STPD settings should be shown for each STPD.

Default

N/A.

Usage Guidelines

The command displays the following STPD information:

- STPD name
- STPD state
- STPD mode of operation
- Rapid Root Failover
- Tag
- Ports
- Active VLANs
- Bridge Priority
- Bridge ID
- Designated root
- STPD configuration information

You can create, configure, and enable one or more STP domains and use the `show stpd` command to display STP configurations. Use the `create stpd <name>` command to create an STP domain. Use the `enable stpd {<spanning tree name>}` command to enable an STPD. If you have considerable knowledge and experience with STP, you can configure the STPD using the `configure stpd` commands. However, the default STP parameters are adequate for most networks.

Example

The following command displays STPD settings on an STPD named *Backbone_st:*

```
show stpd backbone_st
```

The results for this command are as follows:

```
* Alpine3804:47 # show stpd Backbone_st
Stpd: Backbone_st Stp: ENABLED            Number of Ports: 0
```

```
Rapid Root Failover: Disabled
Operational Mode: 802.1W
802.1Q Tag: (none)
Ports:2:5,2:6,3:1,3:2,3:3,3:4,3:5,3:6,3:7,3:8,4:1,4:2
       4:3,4:4
Active Vlans:  Default
Bridge Priority: 32768
BridgeID:               80:00:00:01:30:23:c1:00
Designated root:        80:00:00:01:30:23:c1:00
RootPathCost: 0         Root Port: ----
MaxAge: 20s             HelloTime: 2s           ForwardDelay: 15s
CfgBrMaxAge: 20s        CfgBrHelloTime: 2s      CfgBrForwardDelay: 15s
Topology Change Time: 35s                       Hold time: 1s
Topology Change Detected: FALSE                 Topology Change: FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 5192295s
```

History

This command was first available in ExtremeWare 2.0.

Support for the `detail` keyword was introduced in ExtremeWare 6.2.

Support for displaying RSTP data was introduced in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

show stpd ports

```
show stpd <spanning tree name> ports <portlist> {detail}
```

Description

Displays the STP state of a port.

Syntax Description

spanning tree name	Specifies an STPD name.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
detail	Specifies that STPD state information should be displayed for all ports, or for the ports in the port list.

Default

N/A.

Usage Guidelines

This command displays the following:

- STPD port configuration
- STPD port mode of operation
- STPD path cost
- STPD priority
- STPD state (root bridge, and so on)
- Port role (root bridge, edge port, etc.)
- STPD port state (forwarding, blocking, and so on)
- Configured port link type
- Operational port link type

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see "Modular Switch Numerical Ranges" or "Stand-alone Switch Numerical Ranges" in Chapter 1.

For version 6.2 and later:

- Use the `detail` option to display detailed formats for all ports.

Example

The following command displays the state of port 4 on an STPD named *Backbone_st* on a stand-alone switch:

```
show stpd Backbone_st ports 4
```

The following command displays the state of slot 3, ports 1 through 3 on an STPD named *s0* on a modular switch:

```
show stpd S0 ports 3:1-3:3
```

The results for this command are as follows:

```
* Alpine3804:4 # show stpd s0 ports 3:1-3:3
Port Mode   State      Cost   Flags Priority Port ID Designated Bridge
3:1  802.1D FORWARDING 100    e------- 16    16641   00:00:00:00:00:00:00:00
3:2  802.1D FORWARDING 100    e------- 16    16642   00:00:00:00:00:00:00:00
3:3  802.1D FORWARDING 100    e------- 16    16643   00:00:00:00:00:00:00:00

Total Ports: 14

 ------------------------- Flags: ----------------------------
1:                e=Enable, d=Disable
2:                L = Loopback port
3: (Port role)    R=Root, D=Designated, A=Alternate, B=Backup
4: (Config type)  b=broadcast, p=point-to-point, e=edge, a=auto
5: (Oper. type)   b=broadcast, p=point-to-point, e=edge
6:                p=proposing, a=agree
7: (partner mode) d = 802.1d, w = 802.1w
8:                i = edgeport inconsistency
```

History

This command was first available in ExtremeWare 2.0.

Support for modular switches was introduced in ExtremeWare 4.0.

Support for the `all` keyword was introduced in ExtremeWare 4.0.

Support for the `detail` keyword was introduced in ExtremeWare 6.2 and replaced the `all` keyword.

Support for displaying RSTP data was introduced in ExtremeWare 7.1.

Platform Availability

This command is available on all platforms.

show vlan stpd

```
show vlan <vlan name> stpd
```

Description

Displays the STP configuration of the ports assigned to a specific VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

If you have a VLAN that spans multiple STPDs, use this command to display the STP configuration of the ports assigned to that specific VLAN.

This command displays the following:

- STPD port configuration
- STPD port mode of operation
- STPD path cost
- STPD priority
- STPD state (root bridge, and so on)
- Port role (root bridge, edge port, etc.)
- STPD port state (forwarding, blocking, and so on)
- Configured port link type
- Operational port link type

Example

The following command displays the spanning tree configurations for the vlan *Default*:

```
show vlan default stpd
```

The results for this command are as follows:

```
* Summit1iTx:30 # show vlan "Default" stpd
s0(enabled)  Tag: (none)  Ports: 8  Root/P/C: 80:00:00:01:30:1d:48:30/2/4

Port Mode   State      Cost   Flags Priority Port ID Designated Bridge
1    802.1D FORWARDING 19     e-Dbb-d- 16    16385   80:00:00:01:30:b6:99:10
2    802.1D FORWARDING 4      e-Rbb-w- 16    16386   80:00:00:01:30:1d:48:30
3    802.1D DISABLED   4      e------- 16    16387   00:00:00:00:00:00:00:00
4    802.1D DISABLED   4      e------- 16    16388   00:00:00:00:00:00:00:00
5    802.1D FORWARDING 19     e-Dbb-w- 16    16389   80:00:00:01:30:b6:99:10
```

```
6    802.1D DISABLED   4      e------- 16    16390   00:00:00:00:00:00:00:00
7    802.1D DISABLED   4      e------- 16    16391   00:00:00:00:00:00:00:00
8    802.1D DISABLED   4      e------- 16    16392   00:00:00:00:00:00:00:00

 ------------------------- Flags: ----------------------------
1:                e=Enable, d=Disable
2:                L = Loopback port
3: (Port role)    R=Root, D=Designated, A=Alternate, B=Backup
4: (Config type)  b=broadcast, p=point-to-point, e=edge, a=auto
5: (Oper. type)   b=broadcast, p=point-to-point, e=edge
6:                p=proposing, a=agree
7: (partner mode) d = 802.1d, w = 802.1w
8:                i = edgeport inconsistency
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

unconfigure stpd

```
unconfigure stpd {<spanning tree name>}
```

Description

Restores default STP values to a particular STPD or all STPDs.

Syntax Description

spanning tree name	Specifies an STPD name on the switch.

Default

N / A.

Usage Guidelines

Use this command to restore default STP values to a particular STPD. If you want to restore default STP values on all STPDs, do not specify a spanning tree name.

For version 2.0:

- You can use the `all` parameter to specify all STPDs.

Example

The following command restores default values to an STPD named *Backbone_st*:

```
unconfigure stpd backbone_st
```

History

This command was first available in ExtremeWare 2.0.

Support for the `all` parameter was discontinued in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

14 ESRP Commands

This chapter describes the following commands:

- Commands for enabling and disabling ESRP
- Commands for performing basic ESRP configuration
- Commands for enabling and disabling port restart and failure tracking for ESRP
- Commands for displaying ESRP configuration information
- Commands for enabling and disabling ELRP in an ESRP environment

ESRP is a feature of ExtremeWare that allows multiple switches to provide redundant layer 3 routing services to users. In addition to providing layer 3 routing redundancy, ESRP also provides for layer 2 redundancy. These "layered" redundancy features can be used in combination or independently. The layer 2 redundancy features of ESRP offer fast failure recovery and provide for dual-homed system design. In some instances, depending on network system design, ESRP can provide better resiliency than using the Spanning Tree Protocol (STP) or Virtual Router Redundancy Protocol (VRRP).

Extreme switches that are not running ESRP, but are connected on a network that has other Extreme switches running ESRP are ESRP-*aware*. This means that when Extreme switches are attached to the ESRP-enabled switches, the non-ESRP switches reliably perform fail-over and fail-back scenarios in the prescribed recovery times. No configuration of this feature is necessary.

NOTE

If you disable EDP on the switch, the switch is no longer ESRP-aware.

ESRP is configured on a per-VLAN basis on each switch. A maximum of four switches can participate in providing redundant layer 3 or layer 2 services to a single VLAN. A maximum of 3000 VLANs can run ESRP simultaneously on a single switch. The switches exchange keep-alive packets for each VLAN independently. Only one switch can actively provide layer 3 routing and / or layer 2 switching for each VLAN. The switch performing the forwarding for a particular VLAN is considered the "master" for that VLAN. Other participating switches for the VLAN are in slave mode.

To have two or more switches participate in ESRP, the following must be true:

- For each VLAN to be made redundant, the switches must have the ability to exchange packets on the same layer 2 broadcast domain for that VLAN. Multiple paths of exchange can be used.
- For a VLAN to be recognized as participating in ESRP, the assigned IP address or the IPX NETid for the separate switches must be *identical*. Other aspects of the VLAN, including its name, are ignored.

- ESRP must be enabled on the desired VLANs for each switch. ESRP cannot be enabled on the VLAN "default."
- Extreme Discovery Protocol (EDP) must be enabled on the ports that are members of the ESRP VLANs. (The default setting is enabled.)

ESRP can also be enabled on super-VLANs. The super-VLAN must be configured with all the ports as the sub-VLANs.

It is highly recommended that all switches participating in ESRP run the same version of ExtremeWare. Not all ESRP features are available in all ExtremeWare software releases.

Extreme Loop Recovery Protocol (ELRP) is a feature of ExtremeWare that allows you to prevent, detect, and recover from layer 2 loops in the network. You can use ELRP with other protocols such as ESRP.

With ELRP, each switch, except for the sender, treats the ELRP PDU as a layer 2 multicast packet. The sender uses the source and destination MAC addresses to identify the packet it sends and receives. When the sender receives its original packet back, that triggers loop detection and prevention. Once a loop is detected, the loop recovery agent is notified of the event and takes the necessary actions to recover from the loop. ELRP operates only on the sending switch; therefore, ELRP operates transparently across the network.

NOTE

Because ELRP introduces the pre-master state to ESRP, you must upgrade all ESRP-enabled switches within an ESRP domain to ExtremeWare 6.2.2b134 (or later) for ESRP to operate correctly. Earlier ExtremeWare releases do not recognize the pre-master state.

clear elrp stats

```
clear elrp stats {vlan <vlan name>}
```

Description

Clears the transmitted and received ELRP packet counters.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

N/A.

Usage Guidelines

If you do not specify the optional `vlan name` parameter, you clear the system level ELRP counters, the VLAN counters, and the global counters.

If you specify the optional `vlan name` parameter, you clear the counters for a specific VLAN.

Example

The following command clears the ELRP system counters:

```
clear elrp stats
```

The following command clears the VLAN counters on VLAN *elrp1*:

```
clear elrp stats elrp1
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure esrp port-mode ports

```
configure esrp port-mode [host | normal] ports <portlist> {don't-count}
```

Description

Configures the ESRP port mode for ESRP host attach.

Syntax Description

host	Specifies that the ports should be configured as host ports.
normal	Specifies that the ports should be configured as normal ports.
portlist	Specifies the list of ports that should be configured. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
don't-count	Specifies that ports should not be counted as active ports.

Default

Normal.

Usage Guidelines

This feature is useful in dual-homed server environments in conjunction with high availability server load-balancing (SLB) configurations.

Ports configured as normal ports do not accept or transmit Layer 2 or Layer 3 traffic when the local ESRP device is a slave.

Ports configured as host ports allow configured ports that do not represent loops to the network to continue operation independent of ESRP status. The command sets the port to forward, allowing those ports directly attached to the slave's hosts to communicate with other hosts that are connected to the master. If you use load sharing with the host attach feature, configure all ports in the same load sharing groups as host attach ports.

`don't-count` has the effect of not counting the host ports and normal ports as active ports. This has the convenience of minimal ESRP state changes due to frequent client activities like reboots and unplugging laptops. If you use load sharing with the don't count feature, configure all ports in the same load sharing group as don't count ports.

An L2 connection for VLANs between ESRP switches is required.

Example

The following command configures ports 1 through 5 as host ports, and prevents them from being counted as active ports:

```
configure esrp port-mode host ports 1-5 don't-count
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure vlan add domain-member vlan

```
configure vlan <super_esrp_vlan> add domain-member vlan <sub_esrp_vlan>
```

Description

Adds a VLAN to an ESRP domain.

Syntax Description

super_esrp_vlan	Specifies the name of an ESRP-enabled domain master-VLAN.
sub_esrp_vlan	Specifies the name of a domain member-VLAN.

Default

N/A.

Usage Guidelines

ESRP is performed in the domain master VLAN only, and not the other domain members. The domain master VLAN controls member VLANs whether they are in forward or blocked states.

The domain master does not need to have all the ports as the domain members. Domain master VLANs can have their own set of ports and the members can have different ports.

Example

The following command adds the domain member-VLAN *sub_esrp1* to ESRP-enabled domain master-VLAN *esrp-super*:

```
configure vlan esrp-super add domain-member vlan sub_esrp1
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan add elrp-poll ports

```
configure vlan <vlan name> add elrp-poll ports [<portlist> | all]
```

Description

Configures the ports of a VLAN where ELRP packet transmission is requested by ESRP.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports in the VLAN.

Default

All ports of an ESRP-enabled VLAN have ELRP transmission enabled.

Usage Guidelines

This command allows you to configure the ports in your network that might experience loops, such as ports that connect to master, slave, or ESRP-aware switches, to receive ELRP packets. You do not need to send ELRP packets to host ports.

Example

The following command enables ELRP packet transmission for ports 3-5 on VLAN *esrp1*:

```
configure vlan esrp1 add elrp-poll ports 3-5
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan add ports no-restart

```
configure vlan <vlan name> add ports [<portlist> | all] no-restart
```

Description

Disables port restart for a port.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports.

Default

N/A.

Usage Guidelines

To disable port restart, you either delete the ports and then add them again with the `no-restart` option, or directly add the ports with the `no-restart` option.

Example

The following command disables port restart for ports 7-9 on VLAN *esrp1*:

```
configure vlan esrp1 add ports 7-9 no-restart
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan add ports restart

```
configure vlan <vlan name> add ports [<portlist> | all] restart
```

Description

Configures ESRP to restart ports if there is a state change and the downstream switch is from another vendor.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports.

Default

N/A.

Usage Guidelines

If a VLAN becomes a slave, ESRP disconnects member ports that have port restart enabled. The disconnection of these ports causes downstream devices to remove the ports from their FDB tables. After 3 seconds the ports re-establish connection with the ESRP-enabled device. This feature allows you to use ESRP in networks that include equipment from other vendors.

Example

The following command enables port restart for ports 7-9 on VLAN *esrp1*:

```
configure vlan esrp1 add ports 7-9 restart
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure vlan add track-bgp

```
configure vlan <vlan name> add track-bgp failover <priority>
```

Description

Configures an ESRP-enabled VLAN to track any available BGP route.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
priority	Specifies a number between 0 and 255.

Default

No BGP route tracking.

Usage Guidelines

If no BGP routes are detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and makes it ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example

The following command enables BGP failure tracking, and specifies that the ESRP priority for VLAN *esrp-1* be set to 10 when no BGP routes are reachable.

```
configure vlan esrp-1 add track-bgp failover 10
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan add track-diagnostic

```
configure vlan <vlan name> add track-diagnostic failover <priority>
```

Description

Configures backplane diagnostics failure tracking for an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
priority	Specifies a number between 0 and 255.

Default

No diagnostic tracking.

Usage Guidelines

If a diagnostic failure is detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and makes it ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example

The following command enables diagnostic failure tracking, and specifies that the ESRP priority for VLAN *esrp-1* be set to 10 upon a diagnostic failure.

```
configure vlan esrp-1 add track-diagnostic failover 10
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure vlan add track-environment

```
configure vlan <vlan name> add track-environment failover <priority>
```

Description

Configures an ESRP-enabled VLAN to track environmental failures.

Syntax Description

vlan name	Specifies a VLAN name.
priority	Specifies a number between 0 and 255.

Default

No environmental tracking.

Usage Guidelines

Environmental tracking tracks fan, power supply, and chassis temperature status.

If a failure is detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example

The following command enables diagnostic failure tracking, and specifies that the ESRP priority for VLAN *esrp-1* be set to 10 upon a diagnostic failure.

```
configure vlan esrp-1 add track-environment failover 10
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure vlan add track-iproute

```
configure vlan <vlan name> add track-iproute <ip address>/<masklength>
```

Description

Configures an ESRP-enabled VLAN or a VRRP VLAN to track a route entry in the kernel route table.

Syntax Description

vlan name	Specifies an ESRP-enabled or VRRP VLAN name.
ip address	Specifies the IP address of the route entry to be tracked.

Default

No route tracking.

Usage Guidelines

If the specified routes are not reachable, the device automatically relinquishes master status and remains in slave mode (for ESRP) or backup mode (for VRRP).

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command enables IP route failure tracking for routes to the specified subnet:

```
configure vlan esrp-1 add track-iproute 192.168.46.0/24
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan add track-ospf

```
configure vlan <vlan name> add track-ospf failover <priority>
```

Description

Configures an ESRP-enabled VLAN to track any available OSPF route.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
priority	Specifies a number between 0 and 255.

Default

No OSPF route tracking.

Usage Guidelines

The switch cannot be the ESRP master if none of the specified routes are reachable.

If no OSPF routes are detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example

The following command enables OSPF route failure tracking, and specifies that the ESRP priority for VLAN *esrp-1* be set to 10 when all OSPF routes become unreachable:

```
configure vlan esrp-1 add track-ospf failover 10
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan add track-ping

```
configure vlan <vlan name> add track-ping <ip address> frequency <seconds>
miss <number>
```

Description

Configures an ESRP-enabled VLAN or VRRP VLAN to track an external gateway using ping.

Syntax Description

vlan name	Specifies an ESRP-enabled or VRRP VLAN name.
ip address	Specifies the IP address of the external gateway.
seconds	Specifies the interval in seconds between ping requests.
number	Specifies the number of consecutive ping failures that will initiate failover to an ESRP slave or VRRP backup router.

Default

No ping tracking. Default miss number for VRRP is 3 consecutive missed ping responses.

Usage Guidelines

If the external gateway is not reachable as indicated by consecutive ping failures, the device automatically relinquishes master status and remains in slave mode (for ESRP) or backup mode (for VRRP).

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command enables ping tracking for the external gateway at 10.207.29.17, pinging every 10 seconds, and considering the gateway to be unreachable if no response is received to 5 consecutive pings:

```
configure vlan esrp-1 add track-ping 10.207.29.17 frequency 10 miss 5
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan add track-rip

```
configure vlan <vlan name> add track-rip failover <priority>
```

Description

Configures an ESRP-enabled VLAN to track any available RIP route.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
priority	Specifies a number between 0 and 255.

Default

No RIP route tracking.

Usage Guidelines

If no RIP routes are detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the following should be true:

- The priority field should be given precedence over the other election factors by assigning the `priority-ports-track-mac` election algorithm to the VLAN.
- The normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example

The following command enables RIP route tracking, and specifies that the ESRP priority for VLAN *esrp-1* be set to 10 upon a diagnostic failure:

```
configure vlan esrp-1 add track-rip failover 10
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan add track-vlan

```
configure vlan <vlan name> add track-vlan <vlan_tracked>
```

Description

Configures an ESRP-enabled VLAN or a VRRP VLAN to track port connectivity to a specified VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled or VRRP VLAN name.
vlan_tracked	Specifies the VLAN to be tracked.

Default

Disabled.

Usage Guidelines

If no active ports remain on the specified VLANs, the device automatically relinquishes master status and remains in slave mode (for ESRP) or backup mode (for VRRP).

An ESRP or VRRP VLAN can track one VLAN.

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command enables ESRP-enabled VLAN *esrp-1* to track port connectivity to VLAN *engineering*:

```
configure vlan esrp-1 add track-vlan engineering
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure vlan delete domain-member vlan

```
configure vlan <super_esrp_vlan> delete domain-member vlan <sub_esrp_vlan>
```

Description

Deletes a VLAN from an ESRP domain.

Syntax Description

super_esrp_vlan	Specifies a domain master-VLAN name.
sub_esrp_vlan	Specifies a domain member-VLAN name.

Default

N / A.

Usage Guidelines

The domain master does not need to have all the ports as the domain members. Domain master VLANs can have their own set of ports and the members can have different ports.

Example

The following command deletes the domain member-VLAN *sub_esrp1* from ESRP-enabled domain master-VLAN *esrp-super*:

```
configure vlan esrp-super delete domain-member vlan sub_esrp1
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan delete elrp-poll ports

```
configure vlan <vlan name> delete elrp-poll ports [<portlist> | all]
```

Description

Disables ELRP packet transmission on ports of an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.
all	Specifies all ports in the VLAN.

Default

All ports of an ESRP-enabled VLAN have ELRP transmission enabled.

Usage Guidelines

If you have host ports on an ESRP-enabled VLAN, you do not need to send ELRP packets to those ports.

If you change your network configuration, and a port no longer connects to a master, slave, or ESRP-aware switch, you can disable ELRP transmission on that port.

Example

The following command disables ELRP packet transmission for ports 3-5 on VLAN *esrp1*:

```
configure vlan esrp1 delete elrp-poll ports 3-5
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan delete track-bgp

```
configure vlan <vlan name> delete track-bgp
```

Description

Disables BGP route tracking for an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables BGP tracking for VLAN *esrp-1*:

```
configure vlan esrp-1 delete track-bgp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan delete track-diagnostic

```
configure vlan <vlan name> delete track-diagnostic
```

Description

Disables diagnostics failure tracking for an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables diagnostic failure tracking for VLAN *esrp-1*:

```
configure vlan esrp-1 delete track-diagnostic
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure vlan delete track-environment

```
configure vlan <vlan name> delete track-environment
```

Description

Disables environmental failure tracking.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables environmental failure tracking for VLAN *esrp-1*:

```
configure vlan esrp-1 delete track-environment
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure vlan delete track-iproute

```
configure vlan <vlan name> delete track-iproute <ipaddress>/<masklength>
```

Description

Disables route table entry tracking for an ESRP-enabled VLAN or a VRRP VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled or VRRP VLAN name.
ipaddress	Specifies the IP address of the route entry to be tracked.

Default

N/A.

Usage Guidelines

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command disables tacking of routes to the specified subnet for VLAN *esrp-1*:

```
configure vlan esrp-1 delete track-iproute 192.168.46.0/24
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan delete track-ospf

```
configure vlan <vlan name> delete track-ospf
```

Description

Disables OSPF route tracking for an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables OSPF route tracking for VLAN *esrp-1*:

```
configure vlan esrp-1 delete track-ospf
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan delete track-ping

```
configure vlan <vlan name> delete track-ping <ipaddress>
```

Description

Disables the tracking of an external gateway using ping.

Syntax Description

vlan name	Specifies an ESRP-enabled or VRRP VLAN name.
ipaddress	Specifies the IP address of the external gateway.

Default

N/A.

Usage Guidelines

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command disables ping tracking for the external gateway at 10.207.29.17:

```
configure vlan esrp-1 delete track-ping 10.207.29.17
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure vlan delete track-rip

```
configure vlan <vlan name> delete track-rip
```

Description

Disables RIP route tracking for an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

No RIP route tracking.

Usage Guidelines

None.

Example

The following command disables RIP route failure tracking for VLAN *esrp-1*:

```
configure vlan esrp-1 delete track-rip
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vlan delete track-vlan

```
configure vlan <vlan name> delete track-vlan <vlan_tracked>
```

Description

Disables the tracking of port connectivity to a specified VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled or VRRP VLAN name.
vlan_tracked	Specifies the VLAN to be tracked.

Default

N/A.

Usage Guidelines

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command disables the tracking of port connectivity to VLAN *engineering*:

```
configure vlan esrp-1 delete track-vlan engineering
```

History

This command was first available in ExtremeWare 4.1.

Platform Availability

This command is available on all platforms.

configure vlan esrp elrp-master-poll disable

```
configure vlan <vlan name> esrp elrp-master-poll disable
```

Description

Disables the use of ELRP by ESRP in the master state.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

Disabled.

Usage Guidelines

Use this command to disable the use of ELRP by ESRP in the master state. When you disable ELRP, the ESRP master switch no longer transmits ELRP PDUs to detect network loops.

Example

The following command disables the use of ELRP in the master state on the ESRP-enabled VLAN *elrp1*:

```
configure vlan elrp1 esrp elrp-master poll disable
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan esrp elrp-master-poll enable

```
configure vlan <vlan name> esrp elrp-master-poll enable {interval
<seconds>}
```

Description

Enables the use of ELRP by ESRP in the master state, and configures how often the master checks for loops in the network.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
seconds	Specifies how often, in seconds, successive ELRP packets are sent. The default is 1 second. The range is 1 to 32 seconds.

Default

- Use of ELRP in the master state—disabled
- Interval—1 second

Usage Guidelines

Use this command to enable the use of ELRP by ESRP in the master state. When an ESRP-enabled switch is in the master state, and you enable elrp-master-poll, the switch periodically sends ELRP PDUs at the configured interval level. If a loop is detected in the network, the transmitted PDUs are received by the switch. The ESRP master switch then transitions to the slave state to break the network loop.

Specify the `interval` parameter to configure how often successive ELRP PDUs are sent while in the master state. If you do not specify an interval value, the default value is used.

Example

The following command enables the use of ELRP in the master state on the ESRP-enabled VLAN *`elrp1`*:

```
configure vlan elrp1 esrp elrp-master poll enable
```

The following command configures the ESRP master to check for loops in the network every 3 seconds:

```
configure vlan elrp1 esrp elrp-master-poll enable interval 3
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan esrp elrp-premaster-poll disable

```
configure vlan <vlan name> esrp elrp-premaster-poll disable
```

Description

Disables the use of ELRP by ESRP in the pre-master state.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

Disabled.

Usage Guidelines

Use this command to disable the use of ELRP by ESRP in the pre-master state. When you disable ELRP in the pre-master state, the ESRP pre-master switch no longer transmits ELRP PDUs to detect network loops prior to changing to the master state.

Example

The following command disables the use of ELRP in the pre-master state on the ESRP-enabled VLAN *elrp1*:

```
configure vlan elrp1 esrp elrp-premaster poll disable
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan esrp elrp-premaster-poll enable

```
configure vlan <vlan name> esrp elrp-premaster-poll enable {count <number>
| interval <seconds>}
```

Description

Enables the use of ELRP by ESRP in the pre-master state, and configures how many times the switch sends ELRP PDUs and how often the switch sends ELRP PDUS in the pre-master state.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
number	Specifies the number of times the switch sends ELRP PDUs. The default is 3. The range is 1to 32.
seconds	Specifies how often, in seconds, the ELRP PDUs are sent. The default is 1 second. The range is 1 to 32 seconds.

Default

- Use of ELRP in the pre-master state—disabled
- Count—3 times
- Interval—1 second

Usage Guidelines

Use this command to enable the use of ELRP by ESRP in the pre-master state to prevent network loops from occurring. When an ESRP-enabled switch is in the pre-master state (waiting to become the master), and you enable elrp-premaster-poll, the switch periodically sends ELRP PDUs at the configure level for a specified number of times. If there is a loop in the network, the transmitted PDUs are received by the switch. If this happens, the ESRP pre-master switch does not transition to the master state; rather, the switch transitions to the slave state.

If you do not specify the optional `count` or `interval` parameters, the default values are used.

If no packets are received by the sender, there is no loop in the network.

Example

The following command enables the use of ELRP in the pre-master state on the ESRP-enabled VLAN *elrp1*:

```
configure vlan elrp1 esrp elrp-premaster poll enable
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan esrp esrp-election

```
configure vlan <vlan name> esrp esrp-election [ports-track-priority |
ports-track-priority-mac | track-ports-priority | track-ports-priority-mac
| priority-ports-track-mac | priority-track-ports-mac | priority-mac-only]
```

Description

Configures the election algorithm on the switch.

Syntax Description

vlan name	Specifies a VLAN name.
ports-track-priority	Specifies that this VLAN should consider election factors in the following order: Active ports, tracking information, ESRP priority.
ports-track-priority-mac	Specifies that this VLAN should consider election factors in the following order: Active ports, tracking information, ESRP priority, MAC address. This is the default election algorithm.
track-ports-priority	Specifies that this VLAN should consider election factors in the following order: Tracking information, active ports, ESRP priority.
track-ports-priority-mac	Specifies that this VLAN should consider election factors in the following order: Tracking information, active ports, ESRP priority, MAC address.
priority-ports-track-mac	Specifies that this VLAN should consider election factors in the following order: ESRP priority, active ports, tracking information, MAC address.
priority-track-ports-mac	Specifies that this VLAN should consider election factors in the following order: ESRP priority, tracking information, active ports, MAC address.
priority-mac-only	Specifies that this VLAN should consider election factors in the following order: ESRP priority, MAC address.

Default

`ports_track_priority_mac` election algorithm.

Usage Guidelines

The election algorithm determines the order of precedence of the election factors used to determine the ESRP Master. The election factors are:

- Active Ports (`ports`): the number of active ports (the switch with the highest number takes priority)
- Tracking Information (`track`): whether the switch is using ESRP tracking. A switch using tracking has priority.
- ESRP Priority (`priority`): a user-defined priority number between 0 and 254. A higher number has higher priority. The default priority setting is 0. A priority setting of 255 makes an ESRP switch remain in slave mode and is the recommended setting for system maintenance. A switch with a priority setting of 255 will never become the master.
- MAC address (`mac`): the switch MAC address. A higher-number address has priority.

The election algorithm must be the same on all switches for a particular VLAN.

The ports-track-priority or track-ports-priority options can be used to ensure that there is no failback if the original Master recovers (the Master will have the same ports, tracks and priority, but a higher MAC).

If a switch is master, it actively provides layer 3 routing services to other VLANs, and layer 2 switching between all the ports of that VLAN. Additionally, the switch exchanges ESRP packets with other switches that are in slave mode.

If a switch is in slave mode, it exchanges ESRP packets with other switches on that same VLAN. When a switch is in slave mode, it does not perform layer 3 routing or layer 2 switching services for the VLAN.

Example

The following command configures the election algorithm to use tracking information as the first criteria for determining the ESRP master switch for VLAN *esrp-1*:

```
configure vlan esrp-1 esrp esrp-election track-ports-priority-mac
```

History

This command was first available in ExtremeWare 6.0.

The ports-track-priority and track-ports-priority election algorithms were added in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure vlan esrp esrp-premaster-timeout

```
configure vlan <vlan name> esrp esrp-premaster-timeout <premaster-timer
(0-512, 0 restores dflt)>
```

Description

Configures the ESRP pre-master timeout value.

Syntax Description

vlan name	Specifies a VLAN name.
premaster-timer	Specifies the maximum length of time, in seconds, that the transitioning master VLAN remains in the pre-master state. The range is 0 to 512.

Default

The default timeout is 6 seconds (three times the hello timer).

Usage Guidelines

The `premaster-timer` range is 0 - 512. If you set the `premaster-timer` to 0, ESRP uses the default. To see the `premaster-timer` settings, use the `show vlan esrp` command.

CAUTION

Configure the pre-master state timeout only with guidance from Extreme Networks personnel. Misconfiguration can severely degrade the performance of ESRP and your switch.

Example

The following command configures the pre-master timeout to 10 seconds for the VLAN *esrp-1*:

```
configure vlan esrp-1 esrp esrp-premaster-timeout 10
```

History

This command was first available in ExtremeWare 7.1.0, and replaced the `configure vlan esrp esrp-neutral-timeout` command.

Platform Availability

This command is available on all platforms.

configure vlan esrp priority

```
configure vlan <vlan name> esrp priority <value>
```

Description

Configures the ESRP priority.

Syntax Description

vlan name	Specifies a VLAN name.
value	Specifies a number between 0 and 255.

Default

Priority = 0.

Usage Guidelines

The ESRP priority is one of the factors used by the ESRP election algorithm in determining which switch is the Master switch.

The range of the priority value is 0 to 254, with 0 being the lowest priority, 254 being the highest. If the ESRP priority is the determining criteria for the election algorithm, the highest priority value determines which switch will act as master for a particular VLAN.

Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master. This feature is typically used to ensure a switch cannot become the ESRP master while it is offline for servicing.

Example

The following command configures the ESRP priority to the highest priority on VLAN *esrp-1*:

```
configure vlan esrp-1 esrp priority 254
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure vlan esrp timer

```
configure vlan <vlan name> esrp timer <timervalue> {esrp-nbr-timeout
<timeoutvalue>}
```

Description

Configures the ESRP timer values.

Syntax Description

vlan name	Specifies a VLAN name.
timervalue	Specifies the number of seconds between keep-alive packets. The range is 1 to 255 seconds.
esrp-nbr-timeout	Specifies the number of seconds after which an ESRP neighbor times out. The range is 3 to 7650 seconds.

Default

The default `timervalue` is 2 seconds.

The default neighbor timeout is 3 times the `timervalue`.

Usage Guidelines

The timer specifies the interval, in seconds, for exchanging keep-alive packets between the ESRP switches for this VLAN. A lower value specifies a more frequent exchange of keep-alive messages, resulting in the faster detection of a failover condition. The timer setting must be configured identically for the VLAN across all participating switches. If your configuration contains more than 2,500 ESRP VLANs and 256,000 FDB entries, we recommend a timer setting greater than 3 seconds.

The neighbor timeout specifies the amount of time that ESRP waits before considering the neighbor down. The timeout value must be at least 3 times, but not more than 30 times the timervalue. Entering a value outside of that range generates an error message.

In a large ESRP configuration, the slave ESRP VLAN might inadvertently become the master ESRP VLAN. This can occur when FDB entries are flushed during a master-slave transition. To avoid this we recommend the general neighbor timeout guidelines listed in Table 18.

Table 18: General neighbor timeout

Number of Domains	Number of VLANs	Number of Active ports	Suggested Neighbor Timeout
64	1000	6 or more	> 8
48 or more	1500	4 or more	> 10
48 or more	2000	4 or more	> 11

Example

The following command configures the ESRP timer to 60 seconds and the ESRP neighbor timeout to 12 seconds:

```
configure vlan esrp-1 esrp timer 60 esrp-nbr-timeout 12
```

History

This command was first available in ExtremeWare 4.0.

This command was modified to include the `esrp-nbr-timeout` option in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure vlan esrp group

```
configure vlan <vlan name> esrp group <group_number>
```

Description

Configures the group number to be used for the ESRP VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
group_number	Specifies the ESRP group to which this VLAN should be added.

Default

The default group number is 0.

Usage Guidelines

Each group runs an instance of ESRP within the same VLAN or broadcast domain. A maximum of four ESRP groups can be defined within the same networked broadcast domain. In addition a maximum of four distinct ESRP groups can be supported on a single ESRP switch.You can configure a maximum of 32 ESRP groups in a network.

The most typical application for multiple ESRP groups is when two or more sets of ESRP switches are providing fast-failover protection within a common subnet for two or more groups of users. An additional use for ESRP groups is ESRP Host Attach; ESRP VLANs that share ESRP HA ports must be members of different ESRP groups.

Example

The following command configures VLAN *esrp-1* to be a member of ESRP group 2:

```
configure vlan esrp-1 esrp group 2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure vlan esrp group add esrp-aware-ports

```
configure vlan <vlan name> esrp group <group_number> add esrp-aware-ports
[all | <portlist>]
```

Description

Enables selective forwarding on an ESRP-aware VLAN.

Syntax Description

vlan name	Specifies an ESRP-aware VLAN name.
group_number	Specifies the ESRP group to which this ESRP-aware VLAN belongs.
all	Specifies all of the ports to be configured.
portlist	Specifies the ports to be configured. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

An ESRP-aware switch floods ESRP PDUs to all ports in an ESRP-aware VLAN and the CPU. This flooding increases the amount of network traffic because all ports, regardless if they are connected to switches running the same ESRP group or not, receive ESRP PDUs. To reduce the amount of traffic, you can select the ports that receive ESRP PDUs by configuring selective forwarding on an ESRP-aware VLAN. By configuring selective forwarding, you create a portlist for the ESRP groups associated with an ESRP-aware VLAN, and that portlist is used for forwarding ESRP PDUs on the relevant ports only.

The ESRP group number must be the same as the ESRP-aware VLAN number.

If you specify the `all` or `portlist` options, the ports must be connected to switches running ESRP, and the ports must connect to the ESRP master and slave switches.

When an ESRP-aware switch receives an ESRP PDU, the software will lookup the group to which the PDU belongs and will forward the ESRP PDU to the group's portlist and the CPU.

You cannot enable selective forwarding on an ESRP-enabled VLAN. If you try to enable selective forwarding on an ESRP-enabled VLAN, you see the following message:

```
ERROR: vlan meg is esrp enabled. Cannot enable selective forwarding on esrp vlans
```

Example

The following command configures ESRP-aware VLAN *purple* to receive ESRP PDUs on ports 1, 2, 3, and 4:

```
configure vlan purple esrp group 1 add esrp-aware-ports 1-4
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure vlan esrp group delete esrp-aware-ports

```
configure vlan <vlan name> esrp group <group_number> delete
esrp-aware-ports [all | <portlist>]
```

Description

Disables selective forwarding on an ESRP-aware VLAN.

Syntax Description

vlan name	Specifies an ESRP-aware VLAN name.
group_number	Specifies the ESRP group to which this ESRP-aware VLAN belongs.
all	Specifies all of the ports to be disabled.
portlist	Specifies the ports to be disabled. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.

Default

Disabled.

Usage Guidelines

An ESRP-aware switch floods ESRP PDUs to all ports in an ESRP-aware VLAN and the CPU. This flooding increases the amount of network traffic because all ports, regardless if they are connected to switches running the same ESRP group or not, receive ESRP PDUs. To reduce the amount of traffic, you can select the ports that receive ESRP PDUs by configuring selective forwarding on an ESRP-aware VLAN. By configuring selective forwarding, you create a portlist for the ESRP groups associated with an ESRP-aware VLAN, and that portlist is used for forwarding ESRP PDUs on the relevant ports only.

If all ports are removed from the esrp-aware-ports list, selective forwarding is disabled.

You cannot enable selective forwarding on an ESRP-enabled VLAN. If you try to enable selective forwarding on an ESRP-enabled VLAN, you see the following message:

```
ERROR: vlan meg is esrp enabled. Cannot enable selective forwarding on esrp vlans
```

Example

The following command disables selective forwarding for ESRP-aware VLAN *purple*:

```
configure vlan purple esrp group 1 delete esrp-aware-ports 1-4
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

disable esrp vlan

```
disable esrp vlan <vlan name>
```

Description

Disables ESRP on a VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

Disabled.

Usage Guidelines

None.

Example

The following command disables ESRP on the VLAN *accounting*:

```
disable esrp vlan accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

enable esrp vlan

```
enable esrp vlan <vlan name>
```

Description

Enables ESRP on a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

EDP must be enabled on all ports participating in ESRP.

ESRP cannot be enabled on the VLAN *default*.

Example

The following command enables ESRP on the VLAN *esrp-1*:

```
enable esrp vlan esrp-1
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show elrp

```
show elrp {<vlan name> | detail}
```

Description

Displays ELRP information.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
detail	Specifies detail for each switch in the ESRP VLAN.

Default

N/A.

Usage Guidelines

If you enter the `show elrp` command without a keyword, the command displays the:

- Total number of clients registered with ELRP
- ELRP packets transmitted
- ELRP packets received

If you enter the `detail` keyword, more detailed status information for VLANs in the master and pre-master states is displayed. If you enter a `vlan name`, the command displays ELRP information for that specific VLAN.

The additional table output for the `detail` keyword or a specific VLAN name includes the following:

Client name	Displays the name of the ELRP client.
VLAN	Displays the name of the VLAN with ELRP enabled.
Interval	Displays the configured interval. An interval of 3 indicates that ELRP PDUs are transmitted every 3 seconds.
Count	Lists the configured number of ELRP PDUs that are transmitted. The PDUs are transmitted at the configured interval. This method of ELRP PDU transmission is used by ESRP in the pre-master state. A count of 0 indicates continuous PDU transmission. If the Cyclic value is `Yes`, the count is always 0.
Cyclic	Indicates whether ELRP PDUs are being continuously sent. The column shows `Yes` for the master VLAN because that VLAN is continuously sending ELRP PDUs for loop detection. When a VLAN is in the pre-master state, it only sends three ELRP PDUs before changing to master or slave. During this time the column shows `No` for that VLAN.
Pkts-Xmit	Displays the number of ELRP PDUs transmitted.
Pkts-Rcvd	Displays the number of ELRP PDUs received.

Example

The following command displays summary ELRP status information on the switch:

```
show elrp
```

The following sample output is displayed:

```
Number of ELRP Clients          = 1
Number of ELRP pkts transmitted = 69345
Number of ELRP pkts Received    = 150
```

The following command displays detailed ELRP status information on the switch:

```
show elrp detail
```

The following sample output is displayed:

```
Number of ELRP Clients          = 1
Number of ELRP pkts transmitted = 70305
Number of ELRP pkts Received    = 150

    Client     VLAN    Interval Count Cyclic    Pkts-Xmit    Pkts-Rcvd
--------------------------------------------------------------------------------
   tEsrpTask   uj-mas64  3        0    Yes        1095          0
   tEsrpTask   uj-mas63  3        0    Yes        1095          0
   tEsrpTask   uj-mas62  3        0    Yes        1095          0
   tEsrpTask   uj-mas61  3        0    Yes        1095          0
   tEsrpTask   uj-mas60  3        0    Yes        1095          0
   tEsrpTask   uj-mas59  3        0    Yes        1095          0
   tEsrpTask   uj-mas58  3       0     Yes        1095          0
   tEsrpTask   uj-mas57  3        0    Yes        1095          0
   tEsrpTask   uj-mas56  3        0    Yes        1095          0
   tEsrpTask   uj-mas55  3        0    Yes        1095          0
   tEsrpTask   uj-mas54  3        0    Yes        1095          0
   tEsrpTask   uj-mas53  3        0    Yes        1095          0
   tEsrpTask   uj-mas52  3        0    Yes        1095          0
   tEsrpTask   uj-mas51  3        0    Yes        1095          0
   tEsrpTask   uj-mas50  3        0    Yes        1095          0
   tEsrpTask   uj-mas49  3        0    Yes        1095          0
```

The following command displays the ELRP status information for VLAN *uj-mas*:

```
show elrp uj-mas
```

The following sample output is displayed:

```
   Client      VLAN    Interval Count Cyclic    Pkts-Xmit    Pkts-Rcvd
--------------------------------------------------------------------------------
   tEsrpTask   uj-mas   3        0    Yes        1095          0
```

History

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show esrp

```
show esrp {detail}
```

Description

Displays ESRP configuration information.

Syntax Description

detail	Specifies detail for each switch in the ESRP VLAN.

Default

Shows summary ESRP information.

Usage Guidelines

This command shows information about the state of an ESRP VLAN and its neighbors. This includes information about tracked devices.

In addition to ESRP information, ELRP status information is also displayed. This includes information about the master and pre-master states, number of transitions to the pre-master state, and the ports where ELRP is disabled.

Example

The following command displays summary ESRP status information for the VLANs on the switch:

```
show esrp
```

It produces output similar to the following:

```
VLAN Name VID Virtual IP/IPX  State Master MAC Addres NbrPri/Gr/Prt/In/TR/TP/T
   uj-mas1 0001 192.169.1.1          Master  00:E0:2B:80:E6:00  1
070/10/004/00/01/00/02

Nbr - Number of Neighbors, Pri - Priority In Use, Gr - Group
Prt - Number of ActivePorts, In - Internal Ports, TR - Tracked Rt/Ping/LSP
TP - Tracked Ports, T - Hello Time.
        Host (Direct-attach) Ports on System:
        No-count ports on the System:
```

The following command displays detailed ESRP status information for the VLANs on the switch:

```
show esrp detail
```

It produces output similar to the following:

```
VLAN Interface(Layer 2): demo_esrp
        Priority:               0 (Priority In Use: 0)
        Active Ports:           2
        Internal Ports:         0
        Tracked Rt/Ping/LSP:    0
        Tracked Ports:          0
        Tracked Diag:           -
```

```
Tracked Env:            -
Tracked RIP:            -
Tracked OSPF:           -
Tracked BGP:            -
Tracked LSP:            None
ELRP in Premaster(Int, Cnt):Enabled(1, 3)
ELRP in Master(Int):    Enabled(1)
Election Algorithm:     ports-track-priority-mac
Group:                  0
Hello Timer:            2
Esrp Nbr Timeout:       6
Premaster Timeout:      6
State:                  Enabled(Slave) on Mon Jun 2 10:09:48 2003
State Trans Counters:   ToMaster:(1)    ToPremaster:(1) ToSlave:(2)

Host (Direct-Attach) ports : None
No-count ports: None
Restart Ports: None
Tracked VLANs: None
Tracked Ip Routes: None
Tracked Pings/Freq/N_miss:
192.12.1.1/5/2*
Neighbours:
[1]     Nbr Active Ports:               3
        Nbr Internal Ports:             0
        Nbr Tracked Rt/Ping/LSP:        0
        Nbr Tracked Ports:              0
        Nbr Priority:                   0
        Nbr MacID:                      00:01:30:33:28:00
        Nbr HelloTimer:                 2
        Nbr ESRP State:                 Master
```

History

This command was first available in ExtremeWare 4.0.

This command was updated to support ELRP data in ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0. ELRP data is not displayed in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

show esrp-aware-ports

```
show esrp-aware-ports
```

Description

Displays the ESRP-aware VLAN(s), the ESRP group(s), and the ESRP-aware port(s) that receive ESRP PDUs.

Syntax Description

This command has not arguments or variables.

Default

N/A.

Usage Guidelines

To reduce the amount of traffic, you can select the ports that receive ESRP PDUs by configuring selective forwarding on ESRP-aware VLANs. By configuring selective forwarding, you create a portlist of the ESRP groups associated with an ESRP-aware VLAN, and that portlist is used for forwarding ESRP PDUs on the relevant ports only. Use the `show-esrp-aware-ports` command to view the ESRP group portlist that forwards ESRP PDUs.

Example

The following command displays selective forwarding statistics:

```
show esrp-aware-ports
```

The `show esrp-aware-ports` command produces output similar to the following:

```
VLAN  tt
--------
ESRP Group 0: 1:2 1:1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show esrp-aware vlan

```
show esrp-aware vlan <vlan name>
```

Description

Displays ESRP-aware information for a specific VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.

Default

Displays summary information for the VLAN.

Usage Guidelines

The display includes the group number, MAC address for the master of the group, and age of the information.

Example

The following command displays ESRP-aware status information for ESRP-aware VLAN *demo-esrp-aware*:

```
show esrp-aware vlan demo-esrp-aware
```

On an ESRP-aware switch, it produces output similar to the following:

```
Summit48i:24 # sh esrp-aware
VLAN Interface: [demo-esrp-aware1]. DisableLearnTimeout=0 secs, Total-Fdb-Flushes=6
          Last EsrpAware Fdb-Flush on Mon Nov 18 05:22:26 2002
          Esrp-Group:0  Esrp-Master-Mac=00:01:30:08:36:00,  Age=1 secs

VLAN Interface: [demo-esrp-aware2]. DisableLearnTimeout=0 secs, Total-Fdb-Flushes=6
          Last EsrpAware Fdb-Flush on Mon Nov 18 05:22:26 2002
          Esrp-Group:0  Esrp-Master-Mac=00:01:30:08:36:00,  Age=0 secs
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

show esrp vlan

```
show esrp vlan <vlan name> {counters}
```

Description

Displays ESRP configuration information for a specific VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
counters	Displays ESRP counters.

Default

Displays summary ESRP and ELRP information for the VLAN.

Usage Guidelines

None.

Example

The following command displays ESRP status information for ESRP-enabled VLAN *demo-esrp*:

```
show esrp vlan demo-esrp
```

It produces output similar to the following:

```
VLAN Interface(Layer 2): demo_esrp
        Priority:               0 (Priority In Use: 0)
        Active Ports:           2
        Internal Ports:         0
        Tracked Rt/Ping/LSP:    0
        Tracked Ports:          0
        Tracked Diag:           -
        Tracked Env:            -
        Tracked RIP:            -
        Tracked OSPF:           -
        Tracked BGP:            -
        Tracked LSP:            None
        ELRP in Premaster(Int, Cnt):Enabled(1, 3)
        ELRP in Master(Int):    Enabled(1)
        Election Algorithm:     ports-track-priority-mac
        Group:                  0
        Hello Timer:            2
        Esrp Nbr Timeout:       6
        Premaster Timeout:      6
        State:                  Enabled(Slave) on Mon Jun 2 10:09:48 2003
        State Trans Counters:   ToMaster:(1)    ToPremaster:(1) ToSlave:(2)

        Host (Direct-Attach) ports : None
        No-count ports: None
        Restart Ports: None
```

```
Tracked VLANs: None
Tracked Ip Routes: None
Tracked Pings/Freq/N_miss:
192.12.1.1/5/2*
Neighbours:
[1]     Nbr Active Ports:              3
        Nbr Internal Ports:            0
        Nbr Tracked Rt/Ping/LSP:       0
        Nbr Tracked Ports:             0
        Nbr Priority:                  0
        Nbr MacID:                     00:01:30:33:28:00
        Nbr HelloTimer:                2
        Nbr ESRP State:                Master
```

The following command displays the ESRP counters for ESRP-enabled VLAN *demo-esrp*:

```
show esrp vlan demo-esrp counters
```

It produces output similar to the following:

```
VLAN=demo_esrp Current-time: Mon Jun 2 08:40:15 2003
Rx-Esrp-Pkts=0  Tx-Esrp-Pkts=0
Rx-Aware-Esrp-Pkts=0, Rx-Elrp-Pkts=0
```

History

This command was first available in ExtremeWare 6.0.

This command was updated to support ELRP data in ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0. ELRP data is not displayed in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

15 VRRP Commands

This chapter describes the following commands:

- Commands for enabling and disabling Virtual Router Redundancy Protocol (VRRP)
- Commands for performing basic VRRP configuration

NOTE

Commands for enabling and disabling port restart and enabling and disabling failure tracking for VRRP are described in Chapter 14, covering ESRP commands.

Like ESRP, VRRP is a protocol that allows multiple switches to provide redundant routing services to users. A virtual router is a group of one or more physical devices that acts as the default gateway for hosts on the network. The virtual router is identified by a virtual router identifier (VRID) and an IP address. All of the VRRP routers that participate in the virtual router are assigned the same VRID.

Extreme Networks' VRRP implementation is compliant with RFC 2338, Virtual Router Redundancy Protocol.

The following points pertain to VRRP:

- VRRP packets are encapsulated IP packets.
- The VRRP multicast address is 224.0.0.18.
- The virtual router MAC address is `00 00 5E 00 01 <vrid>`
- An interconnect link between VRRP routers should not be used, except when VRRP routers have hosts directly attached.
- A maximum of 64 VRID instances are supported on the router.
- Up to 4 unique VRIDs can be configured on an interface. VRIDs can be re-used, but not on the same interface.
- VRRP and Spanning Tree can be simultaneously enabled on the same switch.
- VRRP and ESRP cannot be simultaneously enabled on the same switch.

VRRP uses an election algorithm to dynamically assign responsibility for the master router to one of the VRRP routers on the network. A VRRP router is elected master if one of the following is true:

- The router is the IP address owner (router that has the IP address of the virtual router configured as its real interface address).
- The router is configured with the highest priority (the range is 1 - 255).

If the master router becomes unavailable, the election process provides dynamic failover and the backup router that has the highest priority assumes the role of master.

A new master is elected when one of the following things happen:

- VRRP is disabled on the master router.
- Communication is lost between master and backup router(s). The master router sends periodic advertisements to the backup routers to indicate that it is alive.

VRRP also supports the following tracking options:

- VRRP VLAN tracking
- VRRP route table tracking
- VRRP ping tracking

If a tracking option is enabled, and the object being tracked becomes unreachable, the master device will fail over. These tracking features are documented in the chapter on ESRP.

VRRP also supports port restart. Like the tracking features, the commands to enable and disable this feature are described in the chapter on ESRP.

configure vrrp add vlan

```
configure vrrp add vlan <vlan name>
```

Description

Enables VRRP on a particular VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following enables VRRP on VLAN *vrrp-1*:

```
configure vrrp add vlan vrrp-1
```

History

This command was first available in ExtremeWare 6.2

Platform Availability

This command is available on all platforms.

configure vrrp delete

```
configure vrrp delete [vlan <vlan name> | all]
```

Description

Disables VRRP on one or all VLANs.

Syntax Description

vlan name	Specifies the name of a VLAN on which to disable VRRP.
all	Specifies that VRRP should be disabled on all VLANs on this device.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables VRRP on VLAN *vrrp-1*:

```
configure vrrp delete vlan vrrp-1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vrrp vlan add

```
configure vrrp vlan <vlan name> add [master | backup] vrid <number> <ip
address>
```

Description

Configures the VRID instance on the VRRP VLAN as master or backup.

Syntax Description

vlan name	Specifies the name of a VRRP VLAN.
master	Specifies that this device is the master router for the virtual router.
backup	Specifies that this device is a backup router for this VLAN.
number	Specifies a Virtual Router ID (VRID). Value can be in the range of 1-255.
ip address	Specifies the IP address of the virtual router in which this device participates.

Default

N/A.

Usage Guidelines

The IP address must be the same on all VRRP routers that make up the virtual router for this VLAN. If the IP address is the same as the actual interface address of the device, this device is the IP address owner, and is automatically elected as the master router as long as it remains functional.

Example

The following command sets up this device as the master router for VLAN *vrrp-1*, using IP address 192.168.1.3 as the virtual router IP address:

```
configure vrrp vlan vrrp-1 add master vrid 1 192.168.1.3
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vrrp vlan authentication

```
configure vrrp vlan <vlan name> authentication [none | simple-password
<simple password>]
```

Description

Configures VRRP authentication.

Syntax Description

vlan name	Specifies the name of a VRRP VLAN.
none	Specifies that no password is required.
simple password	Specifies the password for VRRP authentication. The maximum password length is eight characters.

Default

N/A.

Usage Guidelines

None.

Example

The following command configures authentication for VRRP VLAN *vrrp-1* with the password `newvrrp`:

```
configure vrrp vlan vrrp-1 authentication simple-password newvrrp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vrrp vlan delete vrid

```
configure vrrp vlan <vlan name> delete vrid [<number> | all]
```

Description

Deletes one or all VRIDs.

Syntax Description

vlan name	Specifies the name of a VRRP VLAN.
number	Specifies a Virtual Router ID (VRID). Value can be in the range of 1-255.
all	Specifies that all virtual routers should be deleted for this VLAN on this device.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the virtual router identified by VRID 2:

```
configure vrrp vlan vrrp-1 delete vrid 2
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure vrrp vlan vrid

```
configure vrrp vlan <vlan name> vrid <number> [priority <priority_number> |
advertisement-interval <ad_interval_number> | dont_preempt | preempt]
```

Description

Configures VRRP parameters.

Syntax Description

vlan name	Specifies the name of a VRRP VLAN.
number	Specifies a Virtual Router ID (VRID). Value can be in the range of 1-255.
priority_number	Specifies the priority value to be used by this VRRP router in the master election process. The range is 1 - 254. The default value is 100.
ad_interval_number	Specifies the time interval between advertisements, in seconds. The range is 1 - 255. The default value is 1 second.
dont_preempt	Specifies that this router, as master, may not be preempted by a higher priority backup router.
preempt	Specifies that this router, as master, may be preempted by a higher-priority backup router. This is the default.

Default

N / A.

Usage Guidelines

This command may be used to configure a VRRP router priority, advertisement interval, and preempt mode.

The priority is used to determine which VRRP router takes over when the master fails over. A value of 255 is reserved for the router that is configured with the virtual router IP address. A value of 0 is reserved for the master router's use to indicate it is releasing responsibility for the virtual router.

The advertisement interval specifies the interval between advertisements sent by the master router to inform the backup routers that it is alive. The master down interval is the interval that a backup router waits after the last received advertisement before it determines that the master router is down.

If you have an extremely busy CPU, a short dual master situation can occur. To avoid this, increase the advertisement interval.

The preempt mode controls whether a higher priority backup router preempts a lower priority master. `preempt` allows preemption. `dont_preempt` prohibits preemption. The default setting is `preempt`. The router that owns the virtual router IP address always preempts, independent of the setting of this parameter.

Example

The following commands set a priority and advertisement interval for the VRRP router on VLAN vrrp-1, and sets the preempt mode to disallow preemption:

```
configure vrrp vlan vrrp-1 vrid 2 priority 200
```

```
configure vrrp vlan vrrp-1 vrid 2 advertisement-interval 15
configure vrrp vlan vrrp-1 vrid 2 dont_preempt
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable vrrp

```
disable vrrp
```

Description

Disables VRRP on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This disables VRRP on the device. All virtual routers defined on this device will also be disabled.

Example

The following command disables VRRP on the device:

```
disable vrrp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable vrrp

```
enable vrrp
```

Description

Enables VRRP on the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

IGMP snooping must be enabled for VRRP to operate correctly. Use the following command to enable IGMP snooping:

```
enable igmp snooping
```

Example

The following command enables VRRP on this device:

```
enable vrrp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show vrrp

```
show vrrp [vlan <vlan name> | all] {detail}
```

Description

Displays VRRP configuration information for one or all VLANs.

Syntax Description

vlan name	Specifies the name of a VRRP VLAN.
all	Specifies that information should be displayed for all VLANs.
detail	Specifies detail information.

Default

N/A.

Usage Guidelines

Use the `detail` option for a detailed display.

Example

The following command displays summary status information for VRRP:

```
show vrrp
```

It produces output similar to the following:

```
VRRP Router: Enabled
   VLAN Name VRID Pri Virtual IP Addr State Master Mac Addres Prt/TR/TPr/W/M/T
 demo_vr(En) 0001 100 192.168.1.1      MSTR 00:00:5E:00:01:01   1  0   0 Y Y 1
```

En-Enabled, Ds-Disabled, Pri-Priority, T-Advert Timer, M-Preempt

Prt-Active Ports, TR-Tracked Routes/Pings, TPr-Tracked Ports, W-TrackWinner

The following command displays detail status information for VRRP:

```
show vrrp detail
```

It produces output similar to the following:

```
VRRP Router: Enabled
 Vlan:demo_vrrp IpAddress Owner=192.168.1.2 Vrrp:ENABLED Router:ENABLED
 Authentication: None
 Tracked VLANs:         -
 Tracked Ip Routes:     -
 Tracked Pings/Freq/N_miss:  -
 Tracked Diag:          -
 Tracked Env:           -
 Track Winner:          Yes
    1) Backup-Vrid:1 Virtual-IP:192.168.1.1 Priority:100
       Active Ports:1, Advert-Interval:1, Preempt:Yes
       State:MASTER on Wed Jan 23 10:17:42 2002
```

```
Transition Counters: ToMaster:1  ToBackup:1
Skew:0.609375 Master-Dn-Int:3.60938
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show vrrp vlan stats

```
show vrrp vlan <vlan name> stats
```

Description

Displays VRRP statistics for a particular VLAN.

Syntax Description

vlan name	Specifies the name of a VRRP VLAN.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays statistics for VLAN *vrrp-1*:

```
show vrrp vlan vrrp-1 stats
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

16 IP Unicast Commands

Extreme Networks switches provide full layer 3, IP unicast routing. They exchange routing information with other routers on the network using either the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol. The switches dynamically build and maintain routing tables and determine the best path for each of its routes.

Each host that uses the IP unicast routing functionality of the switch must have a unique IP address assigned. In addition, the default gateway assigned to the host must be the IP address of the router interface.

The routing software and hardware directs IP traffic between router interfaces. A router interface is simply a VLAN that has an IP address assigned to it.

As you create VLANs with IP addresses belonging to different IP subnets, you can also choose to route between the VLANs. The VLAN switching and IP routing functions occur within the switch.

Each IP address and mask assigned to a VLAN must represent a unique IP subnet. You cannot configure the same IP subnet on different VLANs.

The Extreme Networks switch maintains an IP routing table for network routes and host routes. The table is populated from the following sources:

- Dynamically, by way of routing protocol packets or by ICMP redirects exchanged with other routers
- Statically, by way of routes entered by the administrator
  - Default routes, configured by the administrator
  - Locally, by way of interface addresses assigned to the system
  - By other static routes, as configured by the administrator

Dynamic routes are typically learned by way of RIP or OSPF. Routers that use RIP or OSPF exchange information in their routing tables in the form of advertisements. Using dynamic routes, the routing table contains only networks that are reachable.

Dynamic routes are aged out of the table when an update for the network is not received for a period of time, as determined by the routing protocol.

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure up to 64 static unicast routes on the switch.

Static routes can also be used for security reasons, to control which routes you want advertised by the router. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

When there are multiple, conflicting choices of a route to a particular destination, the router picks the route with the longest matching network mask. If these are still equal, the router picks the route using the following criteria (in the order specified):

- Directly attached network interfaces
- ICMP redirects
- Static routes
- Directly attached network interfaces that are not active

If you define multiple default routes, the route that has the lowest metric is used. If there are multiple default routes that have the same lowest metric, the system picks one of the routes.

You can also configure *blackhole* routes—traffic to these destinations is silently dropped.

Internet Control Message Protocol (ICMP) is used to transmit information needed to control IP traffic. It is used mainly to provide information about routes to destination addresses. ICMP redirect messages inform hosts about more accurate routes to other systems, whereas ICMP unreachable messages indicate problems with a route.

Additionally, ICMP can cause TCP connection to terminate gracefully if the route becomes unavailable.

After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being service by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95.

UDP-forwarding is a flexible and generalized routing utility for handling the directed forwarding of broadcast UDP packets. UDP-forwarding allows applications, such as multiple DHCP relay services from differing sets of VLANs, to be directed to different DHCP servers. The following rules apply to UDP broadcast packets handled by this feature:

- If the UDP profile includes BOOTP or DHCP, the packet is handled according to guidelines in RFC 1542.
- If the UDP profile includes other types of traffic, these packets have the IP destination address modified as configured, and changes are made to the IP and UDP checksums and decrements to the TTL field, as appropriate.

If the UDP-forwarding is used for BOOTP or DHCP forwarding purposes, do not configure or use the existing `bootprelay` function. However, if the previous `bootprelay` functions are adequate, you can continue to use them.

To configure UPD-forwarding, you must first create a UDP-forward destination profile. The profile describes the types of UDP packets (by port number) that are used and where they are to be forwarded. You must give the profile a unique name, in the same manner as a VLAN, protocol filter, or Spanning Tree Domain (STD).

Next, configure a VLAN to make use of the UDP-forwarding profile. As a result, all incoming traffic from the VLAN that matches the UDP profile is handled as specified in the UDP-forwarding profile.

A maximum of 10 UDP-forwarding profiles can be defined. Each named profile may contain a maximum of eight “rules” defining the UDP port, and destination IP address or VLAN. A VLAN can

use a single UDP-forwarding profile. UDP packets directed toward a VLAN use an all-ones broadcast on that VLAN.

Proxy Address Resolution Protocol (ARP) was first developed so that ARP-capable devices could respond to ARP Request packets on behalf of ARP-incapable devices. Proxy ARP can also be used to achieve router redundancy and simplify IP client configuration. The Extreme Networks switch supports proxy ARP for this type of network configuration.

Once IP ARP is configured, the system responds to ARP Requests on behalf of the device, as long as the following conditions are satisfied:

- The valid IP ARP Request is received on a router interface.
- The target IP address matches the IP address configured in the proxy ARP table.
- The proxy ARP table entry indicates that the system should always answer this ARP Request, regardless of the ingress VLAN (the `always` parameter must be applied).

After all the proxy ARP conditions have been met, the switch formulates an ARP Response using the configured MAC address in the packet.

In some networks, it is desirable to configure the IP host with a wider subnet than the actual subnet mask of the segment. Proxy ARP can be used so that the router answers ARP Requests for devices outside of the subnet. As a result, the host communicates as if all devices are local. In reality, communication with devices outside of the subnet are proxied by the router.

clear iparp

```
clear iparp {<ip address> | vlan <vlan name>}
```

Description

Removes dynamic entries in the IP ARP table.

Syntax Description

ip address	Specifies an IP address.
vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

Permanent IP ARP entries are not affected.

Example

The following command removes a dynamically created entry from the IPARP table:

```
clear iparp 10.1.1.5/24
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

clear ipfdb

```
clear ipfdb {<ip address> <netmask>| vlan <vlan name>}
```

Description

Removes the dynamic entries in the IP forwarding database.

Syntax Description

ip address	Specifies an IP address.
netmask	Specifies a subnet mask.
vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

If no options are specified, all IP FDB entries are removed.

Example

The following command removes dynamically created entries in the IP forwarding database:

```
clear ipfdb 10.1.2.1/24
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure bootprelay add

```
configure bootprelay add <ip address>
```

Description

Configures the addresses to which BOOTP requests should be directed.

Syntax Description

ip address	Specifies an IP address.

Default

N / A.

Usage Guidelines

After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:

   ```
   enable bootprelay
   ```

3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

   ```
   configure bootprelay add <ip address>
   ```

Example

The following command configures BOOTP requests to be directed to 123.45.67.8:

```
configure bootprelay add 123.45.67.8
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms

configure bootprelay delete

```
configure bootprelay delete [<ip address> | all]
```

Description

Removes one or all IP destination addresses for forwarding BOOTP packets.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all IP address entries.

Default

N/A.

Usage Guidelines

After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:

   ```
   enable bootprelay
   ```

3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

   ```
   configure bootprelay add <ip address>
   ```

Example

The following command removes the destination address:

```
configure bootprelay delete 123.45.67.8
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iparp add

```
configure iparp add <ip address> <mac_address>
```

Description

Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.

Syntax Description

ip address	Specifies an IP address.
mac_address	Specifies a MAC address.

Default

N / A.

Usage Guidelines

Add a permanent IP ARP entry to the system. The `ip address` is used to match the IP interface address to locate a suitable interface.

Example

The following command adds a permanent IP ARP entry to the switch for IP address *10.1.2.5*:

```
configure iparp add 10.1.2.5 00:11:22:33:44:55
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iparp add proxy

```
configure iparp add proxy <ip address> {<mask>} {<mac_address>} {always}
```

Description

Configures the switch to respond to ARP Requests on behalf of devices that are incapable of doing so. Up to 64 proxy ARP entries can be configured.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.
mac_address	Specifies a MAC address.
always	Specifies all ARP Requests.

Default

N/A.

Usage Guidelines

When `mask` is not specified, an address with the mask 255.255.255.255 is assumed. When `mac_address` is not specified, the MAC address of the switch is used in the ARP Response. When `always` is specified, the switch answers ARP Requests without filtering requests that belong to the same subnet of the receiving router interface.

After IP ARP is configured, the system responds to ARP Requests on behalf of the device as long as the following conditions are satisfied:

- The valid IP ARP Request is received on a router interface.
- The target IP address matches the IP address configured in the proxy ARP table.
- The proxy ARP table entry indicates that the system should always answer this ARP Request, regardless of the ingress VLAN (the `always` parameter must be applied).

After all the proxy ARP conditions have been met, the switch formulates an ARP Response using the configured MAC address in the packet.

Example

The following command configures the switch to answer ARP Requests for all devices with the address range of 100.101.45.1 to 100.101.45.255:

```
configure iparp add proxy 100.101.45.0/24
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iparp delete

```
configure iparp delete <ip address>
```

Description

Deletes an entry from the ARP table. Specify the IP address of the entry.

Syntax Description

ip address	Specifies an IP address.

Default

N/A.

Usage Guidelines

Removes any IP ARP entry (dynamic or permanent) from the table. The `ip address` is used to match the IP interface address to locate a suitable interface.

Example

The following command deletes an IP address entry from the ARP table:

```
configure iparp delete 10.1.2.5
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iparp delete proxy

```
configure iparp delete proxy [<ip address> {<mask>} | all]
```

Description

Deletes one or all proxy ARP entries.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.
all	Specifies all ARP entries.

Default

Not Always.

Usage Guidelines

Proxy ARP can be used for two purposes:

1. To support host that cannot process ARP traffic. In this case, the switch answers the ARP Request for that host.
2. To hide the IP topology from the host. The network administrator can configure a large network on the host machine (16-bit mask) and a smaller network on each router interface (for example, 22-bit mask). When the host sends ARP Request for another host on another subnet, the switch answers the ARP Request and all subsequent traffic will be sent directly to the router.

You can configure up to 64 proxy ARP entries. When the `mask` is not specified, then software will assume a host address (that is, a 32-bit mask). When the MAC address is not specified, then the software uses the switch's MAC address as the proxy host. Always should be specified for type-1 usage, not always is the default (type-2).

Example

The following command deletes the IP ARP proxy entry 1*00.101.45.0/24*:

```
configure iparp delete proxy 100.101.45.0/24
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iparp max-entries

```
configure iparp max-entries <number>
```

Description

Configures the maximum allowed IP ARP entries.

Syntax Description

number	Specifies a number of maximum IP ARP entries.

Default

4096.

Usage Guidelines

Range: 1 - 20480. The maximum IP ARP entries include dynamic, static, and incomplete IP ARP entries.

Example

The following command sets the maximum IP ARP entries to 2000 entries:

```
configure iparp max-entries 2000
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure iparp max-pending-entries

```
configure iparp max-pending-entries <number>
```

Description

Configures the maximum allowed incomplete IP ARP entries.

Syntax Description

number	Specifies a number of maximum IP ARP entries.

Default

256.

Usage Guidelines

Range: 1 - 20480, but cannot be greater than the configured IP ARP max-entries value.

Example

The following command sets the maximum IP ARP entries to 500 entries:

```
configure iparp max-pending-entries 500
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure iparp timeout

```
configure iparp timeout <minutes>
```

Description

Configures the IP ARP timeout period.

Syntax Description

minutes	Specifies a time in minutes.

Default

20 minutes.

Usage Guidelines

A setting of 0 disables ARP aging.

Example

The following command sets the IP ARP timeout period to 10 minutes:

```
configure iparp timeout 10
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure ip-down-vlan-action

```
configure ip-down-vlan-action [consume | drop | forward]
```

Description

Configures the forwarding functionality destined to nonworking IP interfaces.

Syntax Description

consume	Specifies the consume function.
drop	Specifies the drop function.
forward	Specifies the forwarding function.

Default

N/A.

Usage Guidelines

None.

Example

The following command configures the forwarding functionality destined to nonworking IP interfaces:

```
configure ip-down-vlan-action forward
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure ipfdb route-add

```
configure ipfdb route-add [clear-all | clear-subnet]
```

Description

Specifies which routes are deleted and reinstalled with a new gateway.

Syntax Description

clear-all	Clears all IPFDB entries associated with a route if a more specific route is installed.
clear-subnet	Clears only the IPFDB entries associated with the new route's subnet.

Default

The default is `clear-all`.

Usage Guidelines

To see the current setting, use the `show ipconfig` command.

Example

The following command clears only the IPFDB entries associated with the new route's subnet:

```
configure ipfdb route-add clear-subnet
```

History

This command was first available in ExtremeWare 7.0.

Platform Availability

This command is available on all platforms.

configure iproute add

```
configure iproute add <ip address> <mask> <gateway> <metric>
```

Description

Adds a static address to the routing table.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.
gateway	Specifies a VLAN gateway.
metric	Specifies a cost metric.

Default

N/A.

Usage Guidelines

Use a value of 255.255.255.255 for mask to indicate a host entry.

Example

The following command adds a static address to the routing table:

```
configure iproute add 10.1.1.1/24 123.45.67.1 5
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iproute add blackhole

```
configure iproute add blackhole <ip address> <mask>
```

Description

Adds a blackhole address to the routing table. All traffic destined for a configured blackhole IP address is silently dropped, and no Internet Control Message Protocol (ICMP) message is generated.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.

Default

N/A.

Usage Guidelines

A blackhole entry configures packets with a specified MAC destination address to be discarded. Blackhole entries are useful as a security measure or in special circumstances where a specific destination address must be discarded. Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged out of the forwarding database (FDB).

Example

The following command adds a blackhole address to the routing table for packets with a destination address of 100.101.145.4:

```
configure iproute add blackhole 100.101.145.4
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iproute add blackhole default

```
configure iproute add blackhole default
```

Description

Adds a default blackhole route to the routing table. All traffic destined for an unknown IP destination is silently dropped, and no Internet Control Message Protocol (ICMP) message is generated.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

While a default route is for *forwarding* traffic destined to an unknown IP destination, and a blackhole route is for *discarding* traffic destined to a specified IP destination, a *default blackhole* route is for *discarding* traffic to the unknown IP destination.

Using this command, all traffic with an unknown destination is discarded. If there is another static default route existing in the routing table, the `blackhole default` route takes higher route priority.

The default blackhole route is treated like a permanent entry in the event of a switch reset or power off/on cycle. The default blackhole route's origin is "b" or "blackhole" and the gateway IP address for this route is 0.0.0.0.

Example

The following command adds a blackhole default route into the routing table:

```
configure iproute add blackhole default
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure iproute add default

```
configure iproute add default <gateway> {<metric>}
```

Description

Adds a default gateway to the routing table.

Syntax Description

gateway	Specifies a VLAN gateway
metric	Specifies a cost metric. If no metric is specified, the default of 1 is used.

Default

If no metric is specified, the default metric of 1 is used.

Usage Guidelines

Default routes are used when the router has no other dynamic or static route to the requested destination. A default gateway must be located on a configured IP interface. Use the `unicast-only` or `multicast-only` options to specify a particular traffic type. If not specified, both unicast and multicast traffic uses the default route.

Example

The following command configures a default route for the switch:

```
configure iproute add default 123.45.67.1
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iproute delete

```
configure iproute delete <ip address> <mask> <gateway>
```

Description

Deletes a static address from the routing table.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.
gateway	Specifies a VLAN gateway.

Default

N / A.

Usage Guidelines

Use a value of 255.255.255.255 for mask to indicate a host entry.

Example

The following command deletes an address from the gateway:

```
configure iproute delete 10.101.0.250/24 10.101.0.1
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iproute delete blackhole

```
configure iproute delete blackhole <ip address> <mask>
```

Description

Deletes a blackhole address from the routing table.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes a blackhole address from the routing table:

```
configure iproute delete blackhole 100.101.145.4
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iproute delete blackhole default

```
configure iproute delete blackhole default
```

Description

Deletes a default blackhole route from the routing table.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes a blackhole default route from the routing table:

```
configure iproute delete blackhole default
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure iproute delete default

```
configure iproute delete default <gateway>
```

Description

Deletes a default gateway from the routing table.

Syntax Description

gateway	Specifies a VLAN gateway.

Default

N / A.

Usage Guidelines

Default routes are used when the router has no other dynamic or static route to the requested destination. A default gateway must be located on a configured IP interface.

Example

The following command deletes a default gateway:

```
configure iproute delete default 123.45.67.1
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure iproute priority

```
configure iproute priority [rip | bootp | icmp | static | ospf-intra |
ospf-inter | ospf-as-external | ospf-extern1 | ospf-extern2] <priority>
```

Description

Changes the priority for all routes from a particular route origin.

Syntax Description

rip	Specifies RIP.
bootp	Specifies BOOTP.
icmp	Specifies ICMP.
static	Specifies static routes.
ospf-intra	Specifies OSPFIntra routing.
ospf-inter	Specifies OSPFInter routing.
ospf-as-external	Specifies OSPF as External routing.
ospf-extern1	Specifies OSPF External 1 routing.
ospf-extern2	Specifies OSPF External 2 routing.
priority	Specifies a priority number.

Default

Table 19 lists the relative priorities assigned to routes depending upon the learned source of the route.

Table 19: Relative Route Priorities

Route Origin	Priority
Direct	10
Blackhole	50
Static	1100
ICMP	1200
OSPFIntra	2200
OSPFInter	2300
RIP	2400
OSPF External 1	3200
OSPF External 2	3300
BOOTP	5000

Usage Guidelines

Although these priorities can be changed, do not attempt any manipulation unless you are expertly familiar with the possible consequences.

Example

The following command sets IP route priority for static routing to 1200:

```
configure iproute priority static 1200
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure iproute route-map

```
configure iproute route-map [bgp | direct | e-bgp | i-bgp | ospf |
ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | rip | static]
[<route map> | none]
```

Description

Configures the contents of the IP routing table.

Syntax Description

bgp	Specifies BGP routing.
direct	Specifies direct routing.
e-bgp	Specifies E-BGP routing.
i-bgp	Specifies I-BGP routing.
opsf	Specifies OSPF routing.
ospf-extern1	Specifies OSPF External 1 routing.
ospf-extern2	Specifies OSPF External 2 routing.
ospf-inter	Specifies OSPFInter routing.
ospf-intra	Specifies OSPFIntra routing.
rip	Specifies RIP routing.
static	Specifies static routing.
route map	Specifies a route map.
none	Specifies not to use a route map.

Default

N / A.

Usage Guidelines

Route maps for IP routing can be configured based on the route origin. When routes are added to the IP routing table from various sources, the route map configured for the origin of the route is applied to the route. After matching on specified characteristics, the characteristics for the route can be modified using the route maps. The characteristics that can be matched and modified are dependent on the origin of the route. Route maps for IP routing can be dynamically changed. In the case of direct and static route origins, the changes are reflected immediately. In the case of routes that are sourced from other origin, the changes are reflected within 30 seconds.

MPLS uses route map-based filters for controlling label advertisement and label propagation. The implementation of the `delete route-map <route-map>` command has been augmented to support the MPLS module.

Example

The following command configures the IP routing table *bgp_out* to BGP routing:

```
configure iproute route-map bgp_out bgp
```

History

This command was first available in ExtremeWare 6.1.5.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

configure irdp

```
configure irdp [multicast | broadcast]
```

Description

Configures the destination address of the router advertisement messages.

Syntax Description

multicast	Specifies multicast setting.
broadcast	Specifies broadcast setting.

Default

Multicast (224.0.0.1).

Usage Guidelines

None.

Example

The following command sets the address of the router advertiser messages to multicast:

```
configure irdp multicast
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure irdp

```
configure irdp <mininterval> <maxinterval> <lifetime> <preference>
```

Description

Configures the router advertisement message timers, using seconds.

Syntax Description

mininterval	Specifies the minimum amount of time between router advertisements in seconds. The default setting is 450 seconds.
maxinterval	Specifies the maximum amount of time between router advertisements in seconds. The default setting is 600 seconds.
lifetime	Specifies the client aging time. The default setting is 1,800 seconds.
preference	Specifies the preference level of the router. The default setting is 0.

Default

N/A.

Usage Guidelines

All arguments need to be specified. All time intervals are in seconds.

An ICMP Router Discover Protocol (IRDP) client always uses the router with the highest preference level. Change the preference setting to encourage or discourage the use of this router. The default setting is 0.

Example

The following command configures the router advertisement message timers:

```
configure irdp 30 40 300 1
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure udp-profile add

```
configure udp-profile <profile_name> add <udp_port> [vlan <vlan name> | ip
address <dest_ipaddress>]
```

Description

Configures a UDP-forwarding profile.

Syntax Description

profile_name	Specifies a UDP profile name.
udp_port	Specifies a UDP port number.
vlan name	Specifies a VLAN name.
dest_ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

A maximum of 10 UDP-forwarding profiles can be defined. Each named profile may contain a maximum of eight “rules” defining the UDP port, and destination IP address or VLAN. A VLAN can make use of a single UDP-forwarding profile. UDP packets directed toward a VLAN use an all-ones broadcast on that VLAN.

Example

The following command adds port 34 to UDP profile *port_34_to_server*:

```
configure udp-profile port_34_to_server add 34 ip address 10.1.1.1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure udp-profile delete

```
configure udp-profile <profile_name> delete <udp_port> [vlan <vlan name> |
ip address <dest_ipaddress>]
```

Description

Deletes a forwarding entry from the specified UDP-profile.

Syntax Description

profile_name	Specifies a UDP profile name.
udp_port	Specifies a UDP port number.
vlan name	Specifies a VLAN name.
dest_ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes port 34 from UDP profile *port_34_to_server*:

```
configure udp-profile port_34_to_server delete 34 ip address 10.1.1.1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure vlan subvlan address range

```
configure vlan <vlan name> subvlan-address-range <ip address1> - <ip
address2>
```

Description

Configures sub-VLAN address ranges on each sub-VLAN to prohibit the entry of IP addresses from hosts outside of the configured range.

Syntax Description

vlan name	Specifies a super-VLAN name.
ip address1	Specifies an IP address.
ip address2	Specifies another IP address.

Default

N/A.

Usage Guidelines

There is no error checking to prevent the configuration of overlapping sub-VLAN address ranges between multiple sub-VLANs. Doing so can result in unexpected behavior of ARP within the super-VLAN and associated sub-VLANs.

Example

The following command configures the super-VLAN *vsuper* to prohibit the entry of IP addresses from hosts outside of the configured range of IP addresses:

```
configure vlan vsuper subvlan-address-range 10.1.1.1 - 10.1.1.255
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure vlan upd-profile

```
configure vlan <vlan name> udp-profile <profile_name>
```

Description

Assigns a UDP-forwarding profile to the source VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
profile_name	Specifies a UDP profile name.

Default

N/A.

Usage Guidelines

After the UDP profile has been associated with the VLAN, the switch picks up any broadcast UDP packets that match the user-configured UDP port number, and forwards those packets to the user-defined destination. If the UDP port is the DHCP/BOOTP port number, appropriate BOOTP/DHCP proxy functions are invoked.

Example

The following command assigns a UDP profile to VLAN *accounting*:

```
configure vlan accounting udp-profile port_34_to_server
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure vlan secondary-ip

```
configure vlan <super-vlan name> [add | delete] secondary-ip <ip address>
{<mask>}
```

Description

Adds or deletes a secondary IP address to the super-VLAN for responding to ICMP ping requests.

Syntax Description

super-vlan name	Specifies a super-VLAN name.
add	Specifies to add a secondary IP address.
delete	Specifies to delete a secondary IP address.
ip address	Specifies an IP address.
mask	Specifies a netmask.

Default

N / A.

Usage Guidelines

- All broadcast and unknown traffic remains local to the sub-VLAN and does not cross the sub-VLAN boundary. All traffic within the sub-VLAN is switched by the sub-VLAN, allowing traffic separation between sub-VLANs (while using the same default router address among the sub-VLANs).
- Hosts are located on the sub-VLAN. Each host can assume any IP address within the address range of the super-VLAN router interface. Hosts on the sub-VLAN are expected to have the same network mask as the super-VLAN and have their default router set to the IP address or the super-VLAN.
- All traffic (IP unicast and IP multicast) between sub-VLANs is routed through the super-VLAN. For example, no ICMP redirects are generated for traffic between sub-VLANs, because the super-VLAN is responsible for sub-VLAN routing. Unicast IP traffic across the sub-VLANs is facilitated by the automatic addition of an ARP entry (similar to a proxy ARP entry) when a sub-VLAN is added to a super-VLAN. This feature can be disabled for security purposes.

IP multicast traffic between sub-VLANs is routed when an IP multicast routing protocol is enabled on the super-VLAN.

Example

The following command adds a secondary IP address to the super-VLAN *vsuper* for responding to ICMP ping requests:

```
configure vlan vsuper add secondary-ip 10.1.1.1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure vlan subvlan

```
configure vlan <super-vlan name> [add | delete] subvlan <sub-vlan name>
```

Description

Adds or deletes a sub-VLAN to a super-VLAN.

Syntax Description

super-vlan name	Specifies a super-VLAN name
add	Specifies to add the sub-VLAN to the super-VLAN
delete	Specifies to delete the sub-VLAN from the super-VLAN
sub-vlan name	Specifies a sub-VLAN name.

Default

N/A.

Usage Guidelines

- All broadcast and unknown traffic remains local to the sub-VLAN and does not cross the sub-VLAN boundary. All traffic within the sub-VLAN is switched by the sub-VLAN, allowing traffic separation between sub-VLANs (while using the same default router address among the sub-VLANs).
- Hosts are located on the sub-VLAN. Each host can assume any IP address within the address range of the super-VLAN router interface. Hosts on the sub-VLAN are expected to have the same network mask as the super-VLAN and have their default router set to the IP address or the super-VLAN.
- All traffic (IP unicast and IP multicast) between sub-VLANs is routed through the super-VLAN. For example, no ICMP redirects are generated for traffic between sub-VLANs, because the super-VLAN is responsible for sub-VLAN routing. Unicast IP traffic across the sub-VLANs is facilitated by the automatic addition of an ARP entry (similar to a proxy ARP entry) when a sub-VLAN is added to a super-VLAN. This feature can be disabled for security purposes.

IP multicast traffic between sub-VLANs is routed when an IP multicast routing protocol is enabled on the super-VLAN.

Example

The following command adds the sub-VLAN *vsub1*to the super-VLAN *vsuper*:

```
configure vlan vsuper add subvlan vsub1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

create udp-profile

```
create udp-profile <profile_name>
```

Description

Creates a UDP-forwarding destination profile that describes the types of UDP packets (by port number) that are used, and where they are to be forwarded.

Syntax Description

profile_name	Specifies a UDP profile name.

Default

N / A.

Usage Guidelines

You must give the profile a unique name, in the same manner as a VLAN, protocol filter, or Spanning Tree Domain (STD). A maximum of 10 UDP-forwarding profiles can be defined.

Example

The following command creates a UPD profile named *backbone*:

```
create udp-profile backbone
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

delete udp-profile

```
delete udp-profile <profile_name>
```

Description

Deletes a UDP-forwarding profile.

Syntax Description

profile_name	Specifies a UDP profile name.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes a UPD profile named *backbone*:

```
delete udp-profile backbone
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

disable bootp vlan

```
disable bootp vlan [<vlan name> | all]
```

Description

Disables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

Enabled for all VLANs.

Usage Guidelines

None.

Example

The following command disables the generation and processing of BOOTP packets on a VLAN named *accounting*:

```
disable bootp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable bootprelay

```
disable bootprelay
```

Description

Disables the BOOTP relay function.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:

   ```
   enable bootprelay
   ```

3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

   ```
   configure bootprelay add <ip address>
   ```

Example

The following command disables the forwarding of BOOTP requests:

```
disable bootprelay
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable icmp address-mask

```
disable icmp address-mask {vlan <vlan name>}
```

Description

Disables the generation of an ICMP address-mask reply on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Disables the generation of an ICMP address-mask reply (type 18, code 0) when an ICMP address mask request is received. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command disables the generation of an ICMP address-mask reply on VLAN *accounting*:

```
disable icmp address-mask vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable icmp parameter-problem

```
disable icmp parameter-problem {vlan <vlan name>}
```

Description

Disables the generation of an ICMP parameter-problem message on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Disables the generation of an ICMP parameter-problem message (type 12) when the switch cannot properly process the IP header or IP option information. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command disables the generation of an ICMP parameter-problem message on VLAN *accounting*:

```
disable icmp parameter-problem vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable icmp port-unreachables

```
disable icmp port-unreachables {vlan <vlan name>}
```

Description

Disables the generation of ICMP port unreachable messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Disables the generation of ICMP port unreachable messages (type 3, code 3) when a TPC or UDP request is made to the switch, and no application is waiting for the request, or access policy denies the request. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command disables ICMP port unreachable messages on VLAN *accounting*:

```
disable icmp port-unreachables vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable icmp redirects

```
disable icmp redirects {vlan <vlan name>}
```

Description

Disables generation of ICMP redirect messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

This option only applies to the switch when the switch is not in routing mode.

Example

The following command disables ICMP redirects from VLAN *accounting*:

```
disable icmp redirects vlan accounting
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

disable icmp time-exceeded

```
disable icmp time-exceeded {vlan <vlan name>}
```

Description

Disables the generation of ICMP time exceeded messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Disables the generation of an ICMP time exceeded message (type 11) when the TTL field expires during forwarding. IP multicast packets do not trigger ICMP time exceeded messages. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command disables the generation of ICMP time exceeded messages on VLAN *accounting*:

```
disable icmp time-exceeded vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

disable icmp timestamp

```
disable icmp timestamp {vlan <vlan name>}
```

Description

Disables the generation of an ICMP timestamp response on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Disables the generation of an ICMP timestamp response (type 14, code 0) when an ICMP timestamp request is received. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command disables the generation of an ICMP timestamp response on VLAN *accounting*:

```
disable icmp timestamp vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable icmp unreachables

```
disable icmp unreachables {vlan <vlan name>}
```

Description

Disables the generation of ICMP unreachable messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables the generation of ICMP unreachable messages on all VLANs:

```
disable icmp unreachables
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

disable icmp useredirects

```
disable icmp useredirects
```

Description

Disables the modification of route table information when an ICMP redirect message is received.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This option only applies to the switch when the switch is not in routing mode.

Example

The following command disables the changing of routing table information:

```
disable icmp useredirects
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable iparp checking

```
disable iparp checking
```

Description

Disable checking if the ARP Request source IP address is within the range of the local interface or VLAN domain.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables IP ARP checking:

```
disable iparp checking
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable iparp refresh

```
disable iparp refresh
```

Description

Disables IP ARP to refresh its IP ARP entries before timing out.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

IP ARP refresh can only be disabled if IP forwarding is disabled. The purpose of disabling ARP refresh is to reduce ARP traffic in a high node count layer 2 switching only environment.

Example

The following command disables IP ARP refresh:

```
disable iparp refresh
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable ipforwarding

```
disable ipforwarding {[broadcast | fast-direct-broadcast |
ignore-broadcast]} {vlan <vlan name>}
```

Description

Disables routing (or routing of broadcasts) for one or all VLANs. If no argument is provided, disables routing for all VLANs.

Syntax Description

broadcast	Specifies broadcast IP forwarding.
fast-direct-broadcast	Specifies fast direct broadcast forwarding.
ignore-broadcast	Specifies to ignore broadcast forwarding.
vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

Disabling IP forwarding also disables broadcast forwarding. Broadcast forwarding can be disabled without disabling IP forwarding. When new IP interfaces are added, IP forwarding (and IP broadcast forwarding) is disabled by default.

Other IP related configuration is not affected.

Example

The following command disables forwarding of IP broadcast traffic for a VLAN named *accounting*:

```
disable ipforwarding broadcast vlan accounting
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

disable ipforwarding lpm-routing

```
disable ipforwarding lpm-routing {vlan <vlan name>}
```

Description

Disables Longest Prefix Match (LPM) routing for the specified VLAN. If no argument is provided, disables LPM routing for all VLANs except the management VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

Disabling LPM routing does not disable IP forwarding.

Example

The following command disables LPM routing for all configured VLANs:

```
disable ipforwarding lpm-routing
```

The following command disables LPM routing for a VLAN named *accounting*:

```
disable ipforwarding lpm-routing accounting
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond series chassis-based systems only.

disable ip-option loose-source-route

```
disable ip-option loose-source-route
```

Description

Disables the loose source route IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables the loose source route IP option:

```
disable ip-option loose-source-route
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable ip-option record-route

```
disable ip-option record-route
```

Description

Disables the record route IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables the record route IP option:

```
disable ip-option record-route
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable ip-option record-timestamp

```
disable ip-option record-timestamp
```

Description

Disables the record timestamp IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables the record timestamp IP option:

```
disable ip-option record-timestamp
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable ip-option strict-source-route

```
disable ip-option strict-source-route
```

Description

Disables the strict source route IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables the strict source route IP option:

```
disable ip-option strict-source-route
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable ip-option use-router-alert

```
disable ip-option use-router-alert
```

Description

Disables the generation of the router alert IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command disables generation of the router alert IP option:

```
disable ip-option use-router-alert
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable iproute sharing

```
disable iproute sharing
```

Description

Disables load sharing if multiple routes to the same destination are available. When multiple routes to the same destination are available, load sharing can be enabled to distribute the traffic to multiple destination gateways. Only paths with the same lowest cost is will be shared.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

IP route sharing allows multiple equal-cost routes to be used concurrently. IP route sharing can be used with static routes or with OSPF routes. In OSPF, this capability is referred to as *equal cost multipath* (ECMP) routing.

Configure static routes and/or OSPF as you would normally. ExtremeWare supports unlimited route sharing across static routes and up to 12 ECMP routes for OSPF.

Route sharing is useful only in instances where you are constrained for bandwidth. This is typically not the case using Extreme switches. Using route sharing makes router troubleshooting more difficult because of the complexity in predicting the path over which the traffic will travel.

Example

The following command disables load sharing for multiple routes:

```
disable iproute sharing
```

History

This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.2 to allow support of up to 12 ECMP routes for OSPF.

Platform Availability

This command is available on all platforms.

disable irdp

```
disable irdp {vlan <vlan name>}
```

Description

Disables the generation of ICMP router advertisement messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

If no optional argument is specified, all the IP interfaces are affected.

Example

The following command disables IRDP on VLAN *accounting*:

```
disable irdp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable loopback-mode vlan

```
disable loopback-mode vlan [<vlan name> | all]
```

Description

Disallows a VLAN to be placed in the UP state without an external active port. This allows (disallows) the VLANs routing interface to become active.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N / A.

Usage Guidelines

Use this command to specify a stable interface as a source interface for routing protocols. This decreases the possibility of route flapping, which can disrupt connectivity.

Example

The following command disallows the VLAN *accounting* to be placed in the UP state without an external active port:

```
disable loopback-mode vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable multinetting

```
disable multinetting
```

Description

Disables IP multinetting on the system.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The multinetting features requires the user to change the MAC FDB aging timer to be at least 3000 seconds on the switch. This command will automatically change the FDB timer to 3000 seconds if it is shorter than 3000 seconds.

Example

The following command disables multinetting on the system:

```
disable multinetting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable subvlan-proxy-arp vlan

```
disable subvlan-proxy-arp vlan [<super-vlan name> | all]
```

Description

Disables the automatic entry of sub-VLAN information in the proxy ARP table.

Syntax Description

super-vlan name	Specifies a super-VLAN name.
all	Specifies all VLANs.

Default

Enabled.

Usage Guidelines

To facilitate communication between sub-VLANs, by default, an entry is made in the IP ARP table of the super-VLAN that performs a proxy ARP function. This allows clients on one sub-VLAN to communicate with clients on another sub-VLAN. In certain circumstances, intra-sub-VLAN communication may not be desired for isolation reasons.

NOTE

The isolation option works for normal, dynamic, ARP-based client communication.

Example

The following command disables the automatic entry of sub-VLAN information in the proxy ARP table of the super-VLAN *vsuper*:

```
disable subvlan-proxy-arp vlan vsuper
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable udp-echo-server

```
disable udp-echo-server
```

Description

Disables UDP echo server support.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

UDP Echo packets are used to measure the transit time for data between the transmitting and receiving end.

Example

The following command disables UDP echo server support:

```
disable udp-echo-server
```

History

This command was available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

enable bootp vlan

```
enable bootp vlan [<vlan name> | all]
```

Description

Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

Enabled for all VLANs.

Usage Guidelines

None.

Example

The following command enables the generation and processing of BOOTP packets on a VLAN named *accounting*:

```
enable bootp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable bootprelay

```
enable bootprelay
```

Description

Enables the BOOTP relay function.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:

   ```
   enable bootprelay
   ```

3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

   ```
   configure bootprelay add <ip address>
   ```

Example

The following command enables the forwarding of BOOTP requests:

```
enable bootprelay
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable icmp address-mask

```
enable icmp address-mask {vlan <vlan name>}
```

Description

Enables the generation of an ICMP address-mask reply on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Enables the generation of an ICMP address-mask reply (type 18, code 0) when an ICMP address mask request is received.The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command enables the generation of an ICMP address-mask reply on VLAN *accounting*:

```
enable icmp address-mask vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable icmp parameter-problem

```
enable icmp parameter-problem {vlan <vlan name>}
```

Description

Enables the generation of an ICMP parameter-problem message on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Enables the generation of an ICMP parameter-problem message (type 12) when the switch cannot properly process the IP header or IP option information. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command enables the generation of an ICMP parameter-problem message on VLAN *accounting*:

```
enable icmp parameter-problem vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable icmp port-unreachables

```
enable icmp port-unreachables {vlan <vlan name>}
```

Description

Enables the generation of ICMP port unreachable messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Enables the generation of ICMP port unreachable messages (type 3, code 3) when a TPC or UDP request is made to the switch, and no application is waiting for the request, or access policy denies the request. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command enables ICMP port unreachable messages on VLAN *accounting*:

```
enable icmp port-unreachables vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable icmp redirects

```
enable icmp redirects {vlan <vlan name>}
```

Description

Enables generation of ICMP redirect messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

This option only applies to the switch when the switch is not in routing mode.

Example

The following command enables the generation of ICMP redirect messages on all VLANs:

```
enable icmp redirects
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

enable icmp time-exceeded

```
enable icmp time-exceeded {vlan <vlan name>}
```

Description

Enables the generation of ICMP time exceeded messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Enables the generation of an ICMP time exceeded message (type 11) when the TTL field expires during forwarding. IP multicast packets do not trigger ICMP time exceeded messages. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command enables the generation of ICMP time exceeded messages on VLAN *accounting*:

```
enable icmp time-exceeded vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

enable icmp timestamp

```
enable icmp timestamp {vlan <vlan name>}
```

Description

Enables the generation of an ICMP timestamp response on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Enables the generation of an ICMP timestamp response (type 14, code 0) when an ICMP timestamp request is received. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example

The following command enables the generation of an ICMP timestamp response on VLAN *accounting*:

```
enable icmp timestamp vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable icmp unreachables

```
enable icmp unreachables {vlan <vlan name>}
```

Description

Enables the generation of ICMP unreachable messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables the generation of ICMP unreachable messages on all VLANs:

```
enable icmp unreachables
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

enable icmp useredirects

```
enable icmp useredirects
```

Description

Enables the modification of route table information when an ICMP redirect message is received.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This option only applies to the switch when the switch is not in routing mode.

Example

The following command enables the modification of route table information:

```
enable icmp useredirects
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable iparp checking

```
enable iparp checking
```

Description

Enables checking if the ARP Request source IP address is within the range of the local interface or VLAN domain.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables IP ARP checking:

```
enable iparp checking
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable iparp refresh

```
enable iparp refreshenable iparp refresh
```

Description

Enables IP ARP to refresh its IP ARP entries before timing out.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

IP ARP refresh can only be disabled if IP forwarding is disabled. The purpose of disabling ARP refresh is to reduce ARP traffic in a high node count layer 2 switching only environment.

Example

The following command enables IP ARP refresh:

```
enable iparp refresh
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable ipforwarding

```
enable ipforwarding {[broadcast | fast-direct-broadcast |
ignore-broadcast]} {vlan <vlan name>}
```

Description

Enables IP routing or IP broadcast forwarding for one or all VLANs. If no argument is provided, enables IP routing for all VLANs that have been configured with an IP address.

Syntax Description

broadcast	Specifies broadcast IP forwarding.
fast-direct-broadcast	Specifies fast direct broadcast forwarding.
ignore-broadcast	Specifies to ignore broadcast forwarding.
vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

IP forwarding must first be enabled before IP broadcast forwarding can be enabled. When new IP interfaces are added, IP forwarding (and IP broadcast forwarding) is disabled by default.

Other IP related configuration is not affected.

Example

The following command enables forwarding of IP traffic for all VLANs with IP addresses:

```
enable ipforwarding
```

The following command enables forwarding of IP broadcast traffic for a VLAN named *accounting*:

```
enable ipforwarding broadcast vlan accounting
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

enable ipforwarding lpm-routing

```
enable ipforwarding lpm-routing {vlan <vlan name>}
```

Description

Enables Longest Prefix Match (LPM) routing for the specified VLAN. If no argument is provided, enables LPM routing for all VLANs except the management VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

This command enables Longest Prefix Match (LPM) routing for a specified VLAN. When either an ARM or MPLS module is installed in a BlackDiamond switch, the module can be configured to forward IP packets for specified VLANs using LPM routing. If no VLAN is specified, LPM routing is enabled for all configured VLANs except the management VLAN.

Example

The following command enables LPM routing for all configured VLANs:

```
enable ipforwarding lpm-routing
```

The following command enables LPM routing for a VLAN named *accounting*:

```
enable ipforwarding lpm-routing accounting
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

enable ip-option loose-source-route

```
enable ip-option loose-source-route
```

Description

Enables the loose source route IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables the loose source route IP option:

```
enable ip-option loose-source-route
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable ip-option record-route

```
enable ip-option record-route
```

Description

Enables the record route IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables the record route IP option:

```
enable ip-option record-route
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable ip-option record-timestamp

```
enable ip-option record-timestamp
```

Description

Enables the record timestamp IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables the record timestamp IP option:

```
enable ip-option record-timestamp
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable ip-option strict-source-route

```
enable ip-option strict-source-route
```

Description

Enables the strict source route IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables the strict source route IP option:

```
enable ip-option strict-source-route
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable ip-option use-router-alert

```
enable ip-option use-router-alert
```

Description

Enables the generation of the router alert IP option.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

None.

Example

The following command enables generation of the router alert IP option:

```
enable ip-option use-router-alert
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable iproute sharing

```
enable iproute sharing
```

Description

Enables load sharing if multiple routes to the same destination are available. When multiple routes to the same destination are available, load sharing can be enabled to distribute the traffic to multiple destination gateways. Only paths with the same lowest cost is will be shared.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

IP route sharing allows multiple equal-cost routes to be used concurrently. IP route sharing can be used with static routes or with OSPF routes. In OSPF, this capability is referred to as *equal cost multipath* (ECMP) routing.

Configure static routes and/or OSPF as you would normally. ExtremeWare supports unlimited route sharing across static routes and up to 12 ECMP routes for OSPF.

Route sharing is useful only in instances where you are constrained for bandwidth. This is typically not the case using Extreme switches. Using route sharing makes router troubleshooting more difficult because of the complexity in predicting the path over which the traffic will travel.

Example

The following command enables load sharing for multiple routes:

```
enable iproute sharing
```

History

This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.2 to allow support of up to 12 ECMP routes for OSPF.

Platform Availability

This command is available on all platforms.

enable irdp

```
enable irdp {vlan <vlan name>}
```

Description

Enables the generation of ICMP router advertisement messages on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

If no optional argument is specified, all the IP interfaces are affected.

Example

The following command enables IRDP on VLAN *accounting*:

```
enable irdp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable loopback-mode vlan

```
enable loopback-mode vlan [<vlan name> | all]
```

Description

Allows a VLAN to be placed in the UP state without an external active port. This allows (disallows) the VLANs routing interface to become active.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N / A.

Usage Guidelines

Use this command to specify a stable interface as a source interface for routing protocols. This decreases the possibility of route flapping, which can disrupt connectivity.

Example

The following command allows the VLAN *accounting* to be placed in the UP state without an external active port:

```
enable loopback-mode vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable multinetting

```
enable multinetting
```

Description

Enables IP multinetting on the system.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The multinetting features requires the user to change the MAC FDB aging timer to be at least 3000 seconds on the switch. This command will automatically change the FDB timer to 3000 seconds if it is shorter than 3000 seconds.

Example

The following command enables multinetting on the system:

```
enable multinetting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable subvlan-proxy-arp vlan

```
enable subvlan-proxy-arp vlan [<super-vlan name> | all]
```

Description

Enables the automatic entry of sub-VLAN information in the proxy ARP table.

Syntax Description

super-vlan name	Specifies a super-VLAN name.
all	Specifies all VLANs.

Default

Enabled.

Usage Guidelines

To facilitate communication between sub-VLANs, by default, an entry is made in the IP ARP table of the super-VLAN that performs a proxy ARP function. This allows clients on one sub-VLAN to communicate with clients on another sub-VLAN. In certain circumstances, intra-sub-VLAN communication may not be desired for isolation reasons.

NOTE

The isolation option works for normal, dynamic, ARP-based client communication.

Example

The following command enables the automatic entry of sub-VLAN information in the proxy ARP table opf the super-VLAN *vsuper*:

```
enable subvlan-proxy-arp vlan vsuper
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable udp-echo-server

```
enable udp-echo-server
```

Description

Enables UDP echo server support.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

UDP Echo packets are used to measure the transit time for data between the transmitting and receiving end.

Example

The following command enables UDP echo server support:

```
enable udp-echo-server
```

History

This command was available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

rtlookup

```
rtlookup [<ip address> | <hostname>]
```

Description

Performs a look-up in the route table to determine the best route to reach an IP address or host.

Syntax Description

hostname	Specifies a hostname.
ip address	Specifies an IP address.

Default

N/A.

Usage Guidelines

The output of the `rtlookup` command has been enhanced to include information about MPLS LSPs associated with the routes. The flags field displayed by this command has been enhanced to indicate the presence of MPLS next hops. An uppercase `L` indicates the presence of a direct LSP next hop for the route. A lowercase `l` indicates the presence of an indirect LSP next hope for the route.

An optional `mpls` keyword has been added to the `rtlookup` command. When the `mpls` keyword is specified, the information displayed is modified; some of the information normally displayed is omitted, and the LSP endpoint and outgoing MPLS label are displayed instead. The LSP endpoint is the IP address/prefix of the FEC associated with the LSP. The LSP endpoint matches the destination for direct LSPs and is a 32-bit prefix address of a proxy router for indirect LSPs.

Example

The following command performs a look up in the route table to determine the best way to reach the specified hostname:

```
rtlookup berkeley.edu
```

History

This command was available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

run ipfdb-check

```
run ipfdb-check [index <bucket> <entry> | <ip-address> {<ip-address>}]
{extended} {detail}
```

Description

Checks IP FDB entries for consistency.

Syntax Description

bucket	Specifies the bucket portion of the FDB hash index.
entry	Specifies the entry portion of the FDB hash index.
ip-address	Specifies an IP address. FDB entries with this IP address will be checked.
ip-address	Specifies a second IP address, for checking bi-directional entries.
extended	Enables OTP index checking in the MAC entry and VPST of the egress port.
detail	Specifies that more detailed debug information should be logged.

Default

N / A.

Usage Guidelines

The IP FDB error checking function logs the error count into the system log. Use the `detail` option to log more detailed debug information.

Example

The following command will do consistency checking on IP FDB entries for IP address 10.20.30.55:

```
run ipfdb-check 10.20.30.55
```

History

This command was first available in ExtremeWare 6.1.9

Platform Availability

This command is available on all platforms.

The `extended` option is available on the BlackDiamond switch only.

show iparp

```
show iparp {<ip address> | <mac_address> | vlan <vlan name> | permanent}
```

Description

Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, MAC address, VLAN, or permanent entries.

Syntax Description

ip address	Specifies an IP address.
mac_address	Specifies a MAC address.
vlan name	Specifies a VLAN name.
permanent	Specifies permanent entries.

Default

Show all entries.

Usage Guidelines

Displays the IP ARP table, including:

- IP address
- MAC address
- Aging timer value
- VLAN name, VLAN ID and port number
- Flags

Example

The following command displays the IP ARP table:

```
show iparp 10.1.1.5/24
```

History

This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.1 to provide the MAC address option.

Platform Availability

This command is available on all platforms.

show iparp proxy

```
show iparp proxy {<ip address> {<mask>}}
```

Description

Displays the proxy ARP table.

Syntax Description

ip address	Specifies an IP address.
mask	Specifies a subnet mask.

Default

N/A.

Usage Guidelines

If no argument is specified, then all proxy ARP entries are displayed.

Example

The following command displays the proxy ARP table:

```
show iparp proxy 10.1.1.5/24
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ipconfig

```
show ipconfig {vlan <vlan name>} {detail}
```

Description

Displays configuration information for one or more VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
detail	Specifies to display global IP configuration information in the detailed format.

Default

N/A.

Usage Guidelines

If no VLAN information is specified, then global IP configuration is displayed. Otherwise, specific VLAN(s) information will be displayed. Global IP configuration information includes:

- IP address/netmask/etc.
- IP forwarding information / IP multicast forwarding information
- BOOTP configuration
- VLAN name and VLANID
- ICMP configuration (global)
- IGMP configuration (global)
- IRDP configuration (global)

Example

The following command displays configuration information on a VLAN named *accounting*:

```
show ipconfig vlan accounting
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

show ipfdb

```
show ipfdb {<ip address> <netmask> | vlan <vlan name>}
```

Description

Displays the contents of the IP forwarding database (FDB) table. Used for technical support purposes. If no option is specified, all IP FDB entries are displayed.

Syntax Description

ip address	Specifies an IP address.
netmask	Specifies a subnet mask.
vlan name	Specifies a VLAN name.

Default

Default is to show all IP FDB entries.

Usage Guidelines

Displays IP FDB table content including:

Dest IP Addr	IP address
TblIdx	IP FDB hash index and entry number
MacIdx	MAC FDB hash index and entry number
Flag	Flags
FlowInfo	
MAC Address	Next hop router MAC address
VLAN	Egress VLAN ID
Port	Egress port number

Example

The following command displays the contents of the IP FDB table on a VLAN named *accounting*:

```
show ipfdb vlan accounting
```

```
Dest IP Addr  TblIdx MacIdx Flag FlowInfo   MAC Address     VLAN Port
--------------- ------ ------ ---- -------- ----------------- ---- ----
10.205.4.201    00C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.200    01C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.203    02C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.202    03C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.205    04C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.0.5.0        050F.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.204    05C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.207    06C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.206    07C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
```

```
10.205.0.202    07C7.0 4646.0          0000 00:10:E3:1D:00:1E 4000 1
10.205.4.193    08C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
10.205.4.192    09C3.0 9C32.0          0000 00:E0:2B:04:DA:00 4000 1
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show iproute

```
show iproute {priority | vlan <vlan name> | permanent | <ip address>
<netmask> | route-map |origin [direct | static | blackhole | rip | bootp |
icmp | ospf-intra | ospf-inter | ospf-as-external | ospf-extern1 |
ospf-extern2]} {mpls} {sorted}
```

Description

Displays the contents of the IP routing table or the route origin priority.

Syntax Description

priority	Specifies a route priority.
vlan name	Specifies a VLAN name.
permanent	Specifies permanent routing.
ip address	Specifies an IP address.
netmask	Specifies a subnet mask.
route-map	Specifies display of route maps for direct, static, blackhole, RIP, BOOTP, ICMP, OSPF-intra, OSPF-inter, OSPF as External, OSPF External 1, and OPPF External 2 routing.
origin	Specifies a display of the route map origin.
mpls	Specifies to display MPLS information.
sorted	Specifies to sort the information displayed.

Default

N/A.

Usage Guidelines

Route maps for IP routing can be configured based on the route origin. When routes are added to the IP routing table from various sources, the route map configured for the origin of the route is applied to the route. After matching on specified characteristics, the characteristics for the route can be modified using the route maps. The characteristics that can be matched and modified are dependent on the origin of the route. Route maps for IP routing can be dynamically changed. In the case of direct and static route origins, the changes are reflected immediately. In the case of routes that are sourced from other origin, the changes are reflected within 30 seconds.

The output of the `show iproute` command has been enhanced to include information about MPLS LSPs associated with the routes. The flags field displayed by this command has been enhanced to indicate the presence of MPLS next hops. An uppercase `L` indicates the presence of a direct LSP next hop for the route. A lowercase `l` indicates the presence of an indirect LSP next hope for the route.

An optional `mpls` keyword has been added to the `show iproute` command. When the `mpls` keyword is specified, the information displayed is modified; some of the information normally displayed is omitted, and the LSP endpoint and outgoing MPLS label are displayed instead. The LSP endpoint is the IP address/prefix of the FEC associated with the LSP. The LSP endpoint matches the destination for direct LSPs and is a 32-bit prefix address of a proxy router for indirect LSPs.

The mpls keyword only applies to some of the options available on the show iproute command. The mpls keyword is ignored when specified in conjunction with the following options:

- priority
- route-map
- summary

If a route is active and in use, it is preceded in the display by an "*". If there are multiple routes to the same destination network, the "*" will indicate which route is the most preferable route.

The Use and M-Use fields indicate the number of times the route table entry is being used for packet forwarding decisions. The Use field indicates a count for unicast routing while the M-Use field indicates a count for multicast routing. If the use count is going up unexpectedly, the software is making route decisions and should be investigated further.

Example

The following command displays detailed information about all IP routing:

```
show iproute detail
```

Following is the output from this command:

```
Destination: 10.10.121.111/30
  Gateway: 10.10.121.201     VLAN   : helium          Origin : *d
  Metric : 1                   Flags  : U------u-       Time   : 13:15:26:49
  Use    : 14409               M-Use  : 0               Acct-1 : 0

 Destination: 10.11.166.112/29
  Gateway: 10.17.0.1          VLAN   : helium          Origin : *be
  Metric : 2                   Flags  : UG-----um       Time   : 01:11:23:49
  Use    : 0                   M-Use  : 0               Acct-1 : 0

 Destination: 10.13.105.112/29
  Gateway: 10.11.110.123     VLAN   : helium          Origin : *be
  Metric : 2                   Flags  : UG-----um       Time   : 00:29:09:23
  Use    : 0                   M-Use  : 0               Acct-1 :
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare 6.1.8b12 to support MPLS modules.

This command was modified to include a timestamp in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

show ipstats

```
show ipstats {vlan <vlan name>}
```

Description

Displays IP statistics for the CPU for the switch or for a particular VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

This command only shows statistics of the CPU-handled packets. Not all packets are handled by the CPU.

The fields displayed in the `show ipstats` command are defined in Table 20 though Table 24.

Table 20: Global IP Statistics Field Definitions

Field	Definition
InReceives	Total number of incoming IP packets processed by the CPU.
InUnicast	Total number of unicast IP packets processed by the CPU.
InBcast	Total number of broadcast IP packets processed by the CPU.
InMcast	Total number of multicast IP packets processed by the CPU.
InHdrEr	Total number of packets with an IP Header Error forwarded to the CPU.
Bad vers	Total number of packets with a version other than IP v4 in the IP version field.
Bad chksum	Total number of packets with a bad IP checksum forwarded to the CPU.
Short pkt	IP packets that are too short.
Short hdr	IP packets with a header that is too short.
Bad hdrlen	IP packets with a header length that is less than the length specified.
Bad length	IP packets with a length less than that of the header.
InDelivers	IP packets passed to upper layer protocols.
Bad Proto	IP packets with unknown (not standard) upper layer protocol.
OutRequest	IP packets sent from upper layers to the IP stack.
OutDiscard	IP packets that are discarded due to lack of buffer space or the router interface being down, or broadcast packets with broadcast forwarding disabled.
OutNoRoute	IP packets with no route to the destination.
Forwards	ForwardOK and Fwd Err aggregate count.
ForwardOK	Total number of IP packets forwarded correctly.
Fwd Err	Total number of IP packets that cannot be forwarded.

Table 20: Global IP Statistics Field Definitions (continued)

Field	Definition
NoFwding	Aggregate number of IP packets not forwarded due to errors.
Redirects	IP packets forwarded on the same network.
No route	Not used.
Bad TTL	IP packets with a bad time-to-live.
Bad MC TTL	IP packets with a bad multicast time-to-live.
Bad IPdest	IP packets with an address that does not comply with the IP v4 standard.
Blackhole	IP packets with a destination that is a blackhole entry.
Output err	Not used. This is the same as Fwd Err.
MartianSrc	IP packets with an invalid source address.

Table 21: Global ICMP Statistics Field Definitions

Field	Definition
OutResp	Echo replies sent from the CPU.
OutError	Redirect from broadcast or multicast source addresses.
InBadcode	Incoming ICMP packets with an invalid CODE value.
InTooshort	Incoming ICMP packets that are too short.
Bad chksum	Incoming ICMP packets with checksum errors.
In Badlen	Incoming ICMP packets with length errors.
echo reply (In/Out):	ICMP “echo reply” packets that are received and transmitted.
destination unreachable (In/Out):	ICMP packets with destination unreachable that are received and transmitted.
port unreachable (In/Out):	ICMP packets with port unreachable that are received and transmitted.
echo (In/Out):	ICMP echo packets that are received and transmitted.

Table 22: Global IGMP Statistics Field Definitions

Field	Definition
Out Query	Number of IGMP query messages sent by the router.
Out Report	Number of reports sent on an active multicast route interface for reserved multicast addresses and for regular IGMP reports forwarded by the query router.
Out Leave	Number of IGMP out leave messages forwarded for IP multicast router interfaces.
In Query	Number of IGMP query messages received.
In Report	Number of IGMP report messages received (mostly from hosts).
In Leave	Number of IGMP leave messages received (mostly from hosts).
In Error	Number of IGMP packets with bad header fields or checksum failures.

Table 23: DHCP/BOOTP Statistics Field Definitions

Field	Definition
Received to server	Number of DHCP packets forwarded to server.
Received to client	Number of DHCP packets received by clients.
Requests relayed	Number of DHCP request packets relayed.
Responses relayed	Number of DHCP response packets relayed.
DHCP Discover	Number of DHCP Discover messages.
DHCP Offer	Number of DHCP Offer messages.
DHCP Request	Number of DHCP Request messages.
DHCP Decline	Number of DHCP Decline responses.
DHCP Ack	Number of DHCP Ack responses.
DHCP NAck	Number of DHCP NAck responses.
DHCP Release	Number of DHCP Release instances.
DHCP Inform	Not used.

Table 24: Router Interface Statistics Field Definitions

Field	Definition
Packets IN/OUT	Total number of IP packets received or transmitted on a VLAN router interface.
Octets IN/OUT	Total number of octets received or transmitted on a VLAN router interface.
Mcast packets IN/OUT	Total number of multicast packets received or transmitted on a VLAN router interface.
Bcast packets IN/OUT	Total number of broadcast packets received or transmitted on a VLAN router interface.
Errors IN/OUT	Total number of IP packets with errors received or transmitted on a VLAN router interface.
Discards IN/OUT	Total number of IP packets that cannot travel up to the CPU due to lack of buffer space.
Unknown Protocols IN/OUT	Total number of IP packets with unknown upper layer protocols received by the router interface.

Example

The following command displays IP statistics for the VLAN *accounting*:

```
show ipstats vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show udp-profile

```
show udp-profile {<profile_name>}
```

Description

Displays the UDP profile information.

Syntax Description

profile_name	Specifies a UDP profile name.

Default

N/A.

Usage Guidelines

Displays the following information:

- Profile names
- Input rules of UDP port, destination IP address, or VLAN
- Source VLANs to which the profile is applied.

Example

The following command displays the UDP profile information for the UPD profile named *backbone*:

```
show udp-profile backbone
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

unconfigure icmp

```
unconfigure icmp
```

Description

Resets all ICMP settings to the default values.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command resets all ICMP settings to the default values.

```
unconfigure icmp
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

unconfigure iparp

```
unconfigure iparp
```

Description

Resets IP ARP timeout, IP ARP max-entries, and IP ARP max-pending-entries to their default values.

Syntax Description

This command has no arguments or variables.

Default

N/A

Usage Guidelines

None.

Example

The following command resets all IP ARP related settings to the default values:

```
unconfigure iparp
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

unconfigure irdp

```
unconfigure irdp
```

Description

Resets all router advertisement settings to the default values.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command resets all router advertisement settings to the default values.

```
unconfigure irdp
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

unconfigure udp-profile

```
unconfigure udp-profile vlan [<vlan name> | all]
```

Description

Removes the UDP-forwarding profile configuration for one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all UDP profiles.

Default

N/A.

Usage Guidelines

None.

Example

The following command removes the UDP profile configuration from the VLAN *accounting*:

```
unconfigure udp-profile vlan accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

17 IGP Commands

This chapter documents commands used for the following interior gateway protocols:

- OSPF
- Integrated IS-IS
- RIP

OSPF is a link-state protocol that distributes routing information between routers belonging to a single IP domain, also known as an *autonomous system* (AS). In a link-state routing protocol, each router maintains a database describing the topology of the autonomous system. Each participating router has an identical database maintained from the perspective of that router.

From the link-state database (LSDB), each router constructs a tree of shortest paths, using itself as the root. The shortest path tree provides the route to each destination in the autonomous system. When several equal-cost routes to a destination exist, traffic can distributed among them. The cost of a route is described by a single metric.

OSPF allows parts of a networks to be grouped together into *areas.* The topology within an area is hidden from the rest of the autonomous system. Hiding this information enables a significant reduction in LSA traffic, and reduces the computations needed to maintain the LSDB. Routing within the area is determined only by the topology of the area.

The three types of routers defined by OSPF are as follows:

- **Internal Router (IR**)—An internal router has all of its interfaces within the same area.
- **Area Border Router (ABR)**—An ABR has interfaces belonging to two or more areas. It is responsible for exchanging summary advertisements with other ABRs.
- **Autonomous System Border Router (ASBR)**—An ASBR acts as a gateway between OSPF and other routing protocols, or other autonomous systems.

Each switch that is configured to run OSPF must have a unique router ID. It is recommended that you manually set the router ID of the switches participating in OSPF, instead of having the switch automatically choose its router ID based on the highest interface IP address. Not performing this configuration in larger, dynamic environments could result in an older LSDB remaining in use.

NOTE

Do not set the router ID to 0.0.0.0.

The Intermediate System to Intermediate System (IS-IS) routing protocol is a link-state protocol that is very similar to OSPF. ExtremeWare Integrated IS-IS support allows switches to act as IP-only IS-IS routers.

The IS-IS routing protocol provides transport-independent routing. IS-IS partitions the network into "routing domains." Routing domain boundaries are defined by interior and exterior links. Interior links are part of the IS-IS routing domain; exterior links are not. No IS-IS routing messages are sent on exterior links.

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) first used in computer routing in the Advanced Research Projects Agency Network (ARPAnet) as early as 1969. It is primarily intended for use in homogeneous networks of moderate size.

To determine the best path to a distant network, a router using RIP always selects the path that has the least number of hops. Each router that data must traverse is considered to be one hop.

The routing table in a router using RIP contains an entry for every known destination network. Each routing table entry contains the following information:

- IP address of the destination network
- Metric (hop count) to the destination network
- IP address of the next router
- Timer that tracks the amount of time since the entry was last updated

The router exchanges an update message with each neighbor every 30 seconds (default value), or if there is a change to the overall routed topology (also called *triggered updates*). If a router does not receive an update message from its neighbor within the route timeout period (180 seconds by default), the router assumes the connection between it and its neighbor is no longer available.

A new version of RIP, called RIP version 2 (RIPv2), expands the functionality of RIP version 1 to include:

- Variable-Length Subnet Masks (VLSMs)
- Next-hop addresses
- Support for next-hop addresses allows for optimization of routes in certain environments
- Multicasting

If you are using RIP with supernetting/Classless Inter-Domain Routing (CIDR), you must use RIPv2 only, and RIP route aggregation must be turned off.

clear isis adjacency

```
clear isis adjacency {level-1 | level-2 | level-1-2 | point-to-point}
{vlan <vlan name>}
```

Description

Clear the IS-IS adjacencies currently present.

Syntax Description

level-1	Specifies IS-IS level 1 adjacencies.
level-2	Specifies IS-IS level 2 adjacencies.
level-1-2	Specifies IS-IS level 1 and level 2 adjacencies.
point-to-point	Specifies IS-IS point-to-point adjacencies.
vlan name	Specifies the name of a VLAN.

Default

N / A.

Usage Guidelines

The command clears IS-IS adjacencies. If no parameters are specified, all adjacencies, for all VLANs, are cleared

Example

The following command clears the level 1 adjacencies for VLAN *v1*:

```
clear isis adjacency level 1 vlan v1
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

clear isis lsdb

```
clear isis lsdb {level-2 | area <isis area identifier>} {system-identifier
<system identifier> | sysName <alphanumeric string>} {type [non-pseudonode
| pseudonode {circuit-identifier <number(1-255)>}]} {lsp-number
<number(0-255)>}
```

Description

Clears the IS-IS LSDB of the level 2 subdomain or a level 1 area.

Syntax Description

level-2	Specifies the level 2 subdomain.
isis area identifier	Specifies a level 1 area identifier.
system identifier	Specifies a system identifier. The format is xxxx.xxxx.xxxx, where x is a hexadecimal digit.
alphanumeric string	Specifies the system name of the switch.
type	Specifies LSDB type, non-pseudonode or pseudonode.
number(1-255)	Specifies a circuit ID from 1 to 255.
number(0-255)	Specifies an LSP number from 0 to 255.

Default

N/A.

Usage Guidelines

This command clears the IS-IS LSDB for the level 2 subdomain or a level 1 area. If no parameters are specified, all entries are cleared.

Example

The following command clears all non-pseudonode LSDB:

```
clear isis lsdb type non-pseudonode
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis add area address

```
configure isis [level-2 | area <isis area identifier>] add <area address>
```

Description

Adds an IS-IS area address for a level 2 subdomain or a level 1 area.

Syntax Description

level-2	Specifies level 2.
isis area identifier	Specifies an area identifier.
area address	Specifies an area address.

Default

N / A.

Usage Guidelines

At least one area address must be configured per area or subdomain, up to a maximum of three. Configuring multiple area addresses can be temporarily useful when multiple areas are merged, or when one area is split into multiple areas. Multiple area addresses enable you to remember an area individually as needed.

If no area address is configured, the IS-IS process will not start.

Example

The following command adds an IS-IS area address for level 2 subdomains:

```
configure isis level-2 add 02
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis add vlan

```
configure isis add vlan [<vlan name> | all] [[level-1 | level-1-2] area
<isis area identifier> | level-2-only]
```

Description

Enables IS-IS routing on a routing interface.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.
isis area identifier	Specifies an area identifier.

Default

By default, IS-IS is not enabled on an interface.

Usage Guidelines

A VLAN must have an IP address configured on it for it to become a routing interface.

The interface type is specified with the `level-1`, `level-1-2`, and `level-2-only` options. The interface type determines the adjacencies that can be established on the interface. The types are:

- level-1: A level 1 adjacency can be established if there is at least one area address in common between this system and its neighbors. Level 2 adjacencies are never established over this interface. The area identifier of the level 1 area in which the interface is present is specified with this option.
- level-1-2: Both level 1 and level 2 adjacency is established if the neighbor's interface is also configured as level-1-2 and there is at least one area in common. If there is no area in common, a level 2 adjacency is established. The area identifier of the level 1 area in which the interface is present is specified with this option.
- level 2-only: level 2 adjacency is established if the neighbors interface is configured for level 1-2 or level 2. Level 1 adjacencies will never be established over this interface.

Example

The following command adds vlan *test* as level 2 only interfaces to IS-IS:

```
configure isis add vlan test level-2-only
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis area add domain-summary

```
configure isis area <isis area identifier> add domain-summary
<ip address> /<netmask> [advertise {cost <cost(0-4261412864)>} | noadvert]
```

Description

Adds a summary address to be applied on the IP reachability information from this level 1 area, which will be included in the level 2 LSP.

Syntax Description

isis area identifier	Specifies an area identifier.
cost	Specifies the cost for the route (0-4,261,412,864).
advertise	Specifies that the summarized IP reachability information may be included in the level 2 LSP.
noadvert	Specifies that the summary IP reachability information must not be included in the level 2.

Default

N/A.

Usage Guidelines

When the `advertise` option is configured, the summarized IP reachability information should be included in the level 2 LSP. The `noadvert` option filters out the summary.

Example

The following command adds the domain summary address 10.0.0.0/8 to the level 1 area *a1*, advertises the address and sets the cost to 15:

```
configure isis area a1 add domain-summary 10.0.0.0/8 advertise cost 15
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis area delete domain-summary

```
configure isis area <isis area identifier> delete domain-summary
<ip address> /<netmask>
```

Description

Deletes a summary address to be applied on the IP reachability information from this level 1 area, which will be included in the level 2 LSP.

Syntax Description

isis area identifier	Specifies an area identifier.
ip address	Specifies an IP address.
netmask	Specifies an IP mask

Default

N/A.

Usage Guidelines

When the summary address is deleted, the summarized IP reachability information must not be included in the level 2 LSP

Example

The following command deletes one summary address 10.0.0.0/8 from the level 1 area *a1*:

```
configure isis area a1 delete domain-summary 10.0.0.0/8
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis area domain-filter

```
configure isis area <isis area identifier> domain-filter [<access profile>
| none]
```

Description

Configures an access profile to filter the IP reachability information from this level 1 area that will be included in the level 2 LSP:

Syntax Description

isis area identifier	Specifies an area identifier.
access profile	Specifies an access profile name.
none	Specifies no access profile.

Default

N / A.

Usage Guidelines

When an access profile is not configured, none of the information is filtered. By default, no access profile is present on a level 1 area.

Example

The following command configures access profile *ap1* as the domain filter for the area *a1*:

```
configure isis area a1 domain-filter ap1
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis authentication

```
configure isis [level-2 | area <isis area identifier>] authentication
[simple-password <isis simple password> {no-check} | hmac-md5 <hmac-md5>
{no-check} | none]
```

Description

Configures authentication for a level 2 subdomain or a level 1 area.

Syntax Description

level-2	Specifies to configure authentication for a level 2 subdomain.
isis area identifier	Specifies an area.
isis simple password	Specifies a text password in the transmitted packet.
no-check	Specifies not to drop received packets that cannot be authenticated.
hmac-md5	Specifies an MD5 authentication key.

Default

By default, authentication is not configured.

Usage Guidelines

Two types of authentication are supported: simple password and HMAC-MD5. Simple password authentication inserts a text password in the transmitted packet. HMAC-MD5 authentication inserts an authentication key that is generated using a cryptographic hash function, HMAC, on the data present in the packet. The no-check option prevents the system from dropping received packets that cannot be authenticated.

Example

The following command configures authentication using the simple password “extreme” with no checking for the level 2 subdomain:

```
configure isis level-2 authentication simple-password extreme no-check
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis delete area-address

```
configure isis [level-2 | area <isis area identifier>] delete <area
address>
```

Description

Deletes an IS-IS area address for a level 2 subdomain or a level 1 area.

Syntax Description

isis area identifier	Specifies the area identifier.
area address	Specifies the area address.

Default

N / A.

Usage Guidelines

At least one area address must be configured per area or subdomain, up to a maximum of three. Configuring multiple area addresses can be temporarily useful when multiple areas are merged, or when one area is split into multiple areas. Multiple area addresses enable you to remember an area individually as needed.

If no area address is configured, the IS-IS process will not start.

Example

The following command deletes an IS-IS area address 00.0001 for the level 2 subdomain:

```
configure isis level-2 delete 00.0001
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis delete vlan

```
configure isis delete vlan [<vlan name> | all]
```

Description

Disables IS-IS routing on a routing interface.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.

Default

By default, IS-IS is not enabled on an interface.

Usage Guidelines

None.

Example

The following command disables IS-IS on all VLANs.

```
configure isis delete vlan all
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis external-filter

```
configure isis [level-2 | area <isis area identifier>] external-filter
[<access profile> | none]
```

Description

Configures an access profile to filter routes being redistributed in to the level 1 area or level 2 subdomain.

Syntax Description

isis area identifier	Specifies an area identifier.
access profile	Specifies an access profile name.

Default

By default no access profile is present.

Usage Guidelines

The filter is applied on the routes from all the non-IS-IS origins. When an access profile is not configured, none of the routes are filtered.

Example

The following command configures an external filter for a level 1 area with the access profile *ap*:

```
configure isis area a1 external-filter ap
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis lsp holddown interval

```
configure isis lsp-holddown-interval <seconds>
```

Description

Configures the LSP hold down interval.

Syntax Description

seconds	Specifies the LSP hold down interval in seconds.

Default

10 seconds.

Usage Guidelines

The LSP hold down interval range is from 3 to 120 seconds.

Example

The following command configures the LSP hold down interval:

```
configure isis lsp-holddown-interval 20
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis lsp lifetime

```
configure isis lsp-lifetime <seconds>
```

Description

Configures the LSP lifetime.

Syntax Description

seconds	Specifies the LSP lifetime in seconds.

Default

1200 seconds.

Usage Guidelines

You can only use this command when IS-IS is disabled.

The LSP lifetime range is from 400 to 65,535 seconds.

Example

The following command sets the LSP lifetime to 1000:

```
configure isis lsp-lifetime 1000
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis lsp refresh interval

```
configure isis lsp-refresh-interval <seconds>
```

Description

Configures the LSP refresh interval.

Syntax Description

seconds	Specifies the LSP refresh interval in seconds.

Default

900 seconds.

Usage Guidelines

You can only use this command when IS-IS is disabled.

The LSP refresh interval range is from 100 to 65,235 seconds.

Example

The following command configures the LSP refresh interval:

```
configure isis lsp-refresh-interval 120
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis metric-size

```
configure isis [level-2 | area <isis area identifier>] metric-size [regular
| wide | both]
```

Description

Configures the size of the metric originated in the LSP for the level 2 subdomain or level 1 area.

Syntax Description

isis area identifier	Specifies an area identifier.

Default

The default setting is `regular`.

Usage Guidelines

The `regular` option indicates that the metric can have a maximum value of 63 (as specified in the basic specifications). The `wide` option indicates that the metric can have a maximum value of 4,261,412,864 (as specified in the traffic engineering draft). The `both` option indicates that the metric should be described in both formats.

You can only use this command when IS-IS is disabled.

Example

The following command configures the metric size as `both` for the level 2 subdomain:

```
confit isis level-2 metric-size both
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis spf hold time

```
configure isis spf-hold-time <seconds>
```

Description

Configures the shortest-path-first hold time.

Syntax Description

seconds	Specifies the SPF hold time in seconds.

Default

3 seconds.

Usage Guidelines

The SPF hold time range is from 1 to 300 seconds.

Example

The following command configures the IS-IS shortest-path-first hold time:

```
configure isis spf-hold-time 7
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis system-identifier

```
configure isis system-identifier <system identifier>
```

Description

Configures a 6 hex octet system identifier for IS-IS routing.

Syntax Description

system identifier	Specifies the 6 hex octet system identifier. The format is xxxx.xxxx.xxxx where x represents a hexadecimal digit.

Default

By default, the system identifier is set to the switch's MAC address. This command overrides that default.

Usage Guidelines

The system identifier can only be configured when IS-IS processing is disabled.

Example

The following command sets the system identifier:

```
configure isis system-identifier 0000.0000.001a
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis vlan

```
configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2]
[passive | non-passive]
```

Description

Configures the different IS-IS levels on a routing interface as passive or non-passive.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.
level-1	Specifies IS-IS level 1.
level-2	Specifies IS-IS level 2.
level-1-2	Specifies IS-IS level 1 and level 2.
passive	Specifies passive.
non-passive	Specifies non-passive.

Default

By default, all the routing interfaces are non-passive.

Usage Guidelines

If `all` is specified, all routing interfaces in the system are configured as passive or non-passive.

When a level on an interface is configured as passive, the corresponding Hello packets are not sent or received on that interface. Any packet that is received is ignored. As result of this no adjacency is established.

Example

The following command configures vlan *v1* as a level 2 passive interface

```
configure isis vlan v1 level-2 passive
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis vlan authentication

```
configure isis vlan <vlan name> [level-1 | level-2 | level-1-2]
authentication [simple-password <isis simple password> {no-check} |
hmac-md5 <hmac-md5> {no-check} | none]
```

Description

Configures authentication on a VLAN for the IS-IS levels on a routing interface:

Syntax Description

vlan name	Specifies the name of a VLAN.
level-1	Specifies IS-IS level 1.
level-2	Specifies IS-IS level 2.
level-1-2	Specifies IS-IS level 1 and level 2.
isis simple password	Specifies simple password authentication.
no-check	Specifies not to drop packets that cannot be authenticated.
md5 key	Specifies HMAC-MD5 authentication.

Default

An interface does not have any authentication configured on it by default.

Usage Guidelines

Two types of authentication are supported: simple password and HMAC-MD5. Simple password authentication inserts a text password in the transmitted packet. HMAC-MD5 authentication inserts an authentication key that is generated using the cryptographic hash function, HMAC, on the data present in the packet. The `no-check` option prevents the system from dropping received packets that cannot be authenticated.

The `level-1`, `level-2`, and `level-1-2` options specify the levels on which the authentication is to be configured.

Example

The following command configures authentication for level 1 and level 2 to use the simple password “extreme” for vlan *v1*, and to drop non-authenticated packets:

```
configure isis vlan v1 level-1-2 authentication simple-password extreme
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis vlan cost

```
configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2] cost
<cost>
```

Description

Configures the IS-IS metric for the different IS-IS levels of a routing interface.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.
level-1	Specifies IS-IS level 1.
level-2	Specifies IS-IS level 2.
level-1-2	Specifies IS-IS level 1 and level 2.
cost	Specifies the cost value.

Default

The default cost value is 10.

Usage Guidelines

Extreme Networks recommends that you configure metrics on all interfaces. If you do not, the IS-IS metrics are similar to hop-count metrics.

If `all` is specified, the metric is applied to all the routing interfaces in the system.

The range of `cost` is 0 to 16,777,215, where 16,777,215 is the maximum value allowed with wide metrics. If `cost` is greater than 63, a value of 63 is advertised as the regular metric of the interface. The default is 10.

The `level-1`, `level-2`, and `level-1-2` options specify the levels to which the metric is applied.

Example

The following command configures the level 1 vlan *v1* cost as 25:

```
configure isis vlan v1 level-1 cost 25
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis vlan hello-multiplier

```
configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2]
hello-multiplier <number(3-1000)>
```

Description

Configures the number of IS-IS Hello packets an IS-IS neighbor at a particular level on this routing interface must miss before the it declares that the adjacency with this system is down.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.
level-1	Specifies IS-IS level 1.
level-2	Specifies IS-IS level 2.
level-1-2	Specifies IS-IS level 1 and level 2.
hello-multiplier	Specifies the hello multiplier.

Default

The default hello multiplier number is 3.

Usage Guidelines

If `all` is specified, the hello multiplier is applied to all the routing interfaces in the system. The advertised hold time in the IS-IS hellos is the `hello multiplier` times the `hello interval`.

The `hello multiplier` range is 3 to 1000, and the default is 3.

The `level-1`, `level-2`, and `level-1-2` options specify the levels to which the timers are applied.

Example

The following command configures the hello multiplier on level 1 of all VLANs to be 100.

```
configure isis vlan all level-1 hello-multiplier 100
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis vlan priority

```
configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2]
priority <priority>
```

Description

Configures the IS-IS priority for the IS-IS levels of a routing interface.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.
level-1	Specifies IS-IS level 1.
level-2	Specifies IS-IS level 2.
level-1-2	Specifies IS-IS level 1 and level 2.
priority	Specifies the priority to apply to IS-IS levels. Range is 0 to 127. Default is 64.

Default

The default priority is 64.

Usage Guidelines

If `all` is specified, the priority is applied to all the routing interfaces in the system. The priority in applicable only for broadcast routing interfaces. The priorities are advertised in the Hello packets. The router with the higher priority at a particular level becomes the designated IS for that level on that interface. The range of `priority` is 0 to 127, and the default is 64.

The `level-1`, `level-2`, and `level-1-2` options specify the levels for which the priority is applied.

Example

The following command configures an IS-IS priority of 100 to level 1 of all VLANs.

```
configure isis vlan all level-1 priority 100
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure isis vlan timer

```
configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2]
timer [csnp <seconds>| hellotime <seconds>]
```

Description

Configures the IS-IS timer interval for the different levels of a routing interface.

Syntax Description

vlan name	Specifies the name of a VLAN.
all	Specifies all VLANs.
level-1	Specifies IS-IS level 1.
level-2	Specifies IS-IS level 2.
level-1-2	Specifies IS-IS level 1 and level 2.
csnp	Specifies the time in seconds between CSNP transmissions. Range is 1 to 3600. Default is 10.
hellotime	Specifies the time in seconds between Hello PDU transmissions. Range is 3 to 3600. Default is 10.

Default

The default for CSNP and Hello timer is 10 seconds.

Usage Guidelines

If `all` is specified, the timer intervals are applied to all the routing interfaces in the system. The command configures both the CSNP and Hello timer values.

The `csnp` interval is the time in seconds between transmission of CSNPs on multi access networks. This interval applies for the designated router. The range is 1 to 3600, and the default is 10.

The `hellotime` interval is the time in seconds between transmission of Hello PDUS on the interface. The range is 3 to 3600, and the default is 10.

The `level-1`, `level-2`, and `level-1-2` options specify the levels to which the timers are applied.

Example

The following command configures the level 1 hellotime interval to 60 seconds for all VLANs

```
configure isis vlan all level-1 timer hellotime 60
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure ospf cost

```
configure ospf [area <area identifier> | vlan [<vlan name> | all]] cost
[automatic | <cost>]
```

Description

Configures the cost metric of one or all interface(s).

Syntax Description

area identifier	Specifies an OSPF area.
vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
automatic	Determine the advertised cost from the OSPF metric table.
cost	Specifies the cost metric.

Default

The default cost is automatic.

Usage Guidelines

None.

Example

The following command configures the cost metric of the VLAN *accounting*:

```
configure ospf vlan accounting cost 10
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf priority

```
configure ospf [area <area identifier> | vlan [<vlan name> | all]] priority
<priority>
```

Description

Configures the priority used in the designated router-election algorithm for one or all OSPF interface(s) for all the interfaces within the area.

Syntax Description

area identifier	Specifies an OSPF area.
vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
priority	Specifies a priority range. The range is 0 through 255.

Default

The default setting is 1.

Usage Guidelines

The range is 0 through 255, and the default setting is 1. Setting the value to 0 ensures that the router is never selected as the designated router or backup designated router.

Example

The following command sets the switch to not be selected as the designated router:

```
configure ospf area 1.2.3.4 priority 0
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf virtual-link authentication password

```
configure ospf [vlan <vlan name> | area <area identifier> | virtual-link
<routerid> <area identifier>] authentication [simple-password <password> |
md5 <md5_key_id> <md5_key>| none | encrypted [simple-password <password> |
md5 <md5_key_id> <md5_key>]
```

Description

Specifies the authentication password (up to eight characters) or Message Digest 5 (MD5) key for one or all interfaces in an area.

Syntax Description

vlan name	Specifies a VLAN name.
area identifier	Specifies an OSPF area.
routerid	Specifies a router interface number.
password	Specifies an authentication password (up to 8 ASCII characters).
md5-key_id	Specifies a Message Digest 5 key, from 0-255.
md5_key	Specifies a numeric value from 0-65,536. Can also be alphanumeric
none	Disables authentication.

Default

N / A.

Usage Guidelines

The md5_key is a numeric value with the range 0 to 65,536 or alphanumeric. When the OSPF area is specified, authentication information is applied to all OSPF interfaces within the area.

Example

The following command configures MD5 authentication on the VLAN *subnet_26*:

```
configure ospf vlan subnet_26 authentication md5 32 test
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf timer

```
configure ospf [vlan <vlan name> | area <area identifier> | virtual-link
<routerid> <area identifier>] timer <retransmit interval> <transit delay>
<hello interval> <dead interval> {<wait timer interval>}
```

Description

Configures the timers for one interface or all interfaces in the same OSPF area.

Syntax Description

vlan name	Specifies a VLAN name.
area identifier	Specifies an OSPF area.
routerid	Specifies a router number.
retransmit interval	Specifies the length of time that the router waits before retransmitting an LSA that is not acknowledged. The range is 0 - 3,600 seconds.
transit delay	Specifies the length of time it takes to transmit an LSA packet over the interface. The range is 0 - 3,600 seconds.
hello interval	Specifies the interval at which routers send hello packets. The range is 1 - 65,535 seconds.
dead interval	Specifies the interval after which a neighboring router is declared down due to the fact that hello packets are no longer received from the neighbor. The range is 1 - 2,147,483,647 seconds.
wait timer interval	Specifies the interval between the interface coming up and the election of the DR and BDR. Usually equal to the dead timer interval.

Default

- retransmit interval—Default: 5
- transit delay—Default: 1
- hello interval—Default: 10
- dead interval—Default: 40
- wait timer interval—Default: dead interval

Usage Guidelines

Configuring OSPF timers and authentication on a per-area basis is a shorthand for applying the timers and authentication to each VLAN in the area at the time of configuration. If you add more VLANs to the area, you must configure the timers and authentication for the new VLANs explicitly.

Example

The following command sets the timers on the virtual link in area 0.0.0.2:

```
configure ospf virtual-link 6.6.6.6 0.0.0.2 timer 10 1 20 200
```

History

This command was available in ExtremeWare 2.0.

The syntax was modified in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure ospf add virtual-link

```
configure ospf add virtual-link <routerid> <area identifier>
```

Description

Adds a virtual link connected to another ABR.

Syntax Description

routerid	Specifies an IP address that identifies the router.
area identifier	Specifies an OSPF area.

Default

N / A.

Usage Guidelines

A virtual link provides a logical path between the ABR of the disconnected area and the ABR of the normal area that connects to the backbone. A virtual link must be established between two ABRs that have a common area, with one ABR connected to the backbone. Specify the following:

- routerid—Far-end router interface number.
- area identifier—Transit area used for connecting the two end-points. The transit area cannot have the IP address 0.0.0.0. the transit area cannot be a stub area or an NSSA.

Example

The following command configures a virtual link between the two interfaces:

```
configure ospf add virtual-link 10.1.2.1 10.1.0.0
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf add vlan area

```
configure ospf add vlan [<vlan name> | all] area <area identifier>
{passive}
```

Description

Enables OSPF on one or all VLANs (router interfaces).

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
area identifier	Specifies the area to which the VLAN is assigned.
passive	Specifies to stop sending and receiving hello packets on this interface.

Default

Disabled.

Usage Guidelines

None.

Using OSPF and MPLS. The following detailed information pertains to using OSPF in conjunction with MPLS. When the peer LSR is also an Extreme switch, the following options are available for ensuring that an OSPF route is advertised for the tunnel endpoint IP address:

- A route is advertised when OSPF is enabled on the VLAN to which the IP address is assigned (using the `configure ospf add vlan` command on the peer switch).
- A route is advertised when the peer switch is configured to distribute direct routes into the OSPF domain (via the `enable ospf export direct` command). The export option should be used when the tunnel LSP needs to cross OSPF area boundaries or when the Extreme Standby Routing Protocol (ESRP) is enabled on the VLAN to which the IP address is assigned.

In either case, LDP must be configured to advertise label mappings for direct routing interfaces.

In some configurations, you may want to enable loopback mode on the VLAN to which the tunnel endpoint IP address is assigned. One situation where loopback mode may be useful is when multiple physical interfaces, associated with different VLANs, are connected to the MPLS backbone. In this case, use of loopback-mode can provide redundancy by enabling TLS traffic to continue even when the physical interfaces associated with the tunnel endpoint IP address VLAN fail.

Example

The following command enables OSPF on a VLAN named *accounting*:

```
configure ospf add vlan accounting area 0.0.0.1
```

History

This command was available in ExtremeWare 2.0. This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

configure ospf add vlan area link-type

```
configure ospf add vlan [<vlan name> | all] area <area identifier>
link-type [auto | broadcast | point-to-point] {passive}
```

Description

Configures the OSPF link type.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
area identifier	Specifies the area to which the VLAN is assigned.
auto	Specifies to automatically determine the OSPF link type based on the interface type.
broadcast	Specifies a broadcast link, such as Ethernet. Routers must elect a DR and a BDR during synchronization.
point-to-point	Specifies a point-to-point link type, such as PPP.
passive	Specifies to stop sending and receiving packets on this interface.

Default

Auto.

Usage Guidelines

The passive parameter indicates that the router only synchronizes and listens, and does not originate or send any new information on the interface.

Example

The following command configures the OSPF link type as automatic on a VLAN named *accounting*:

```
configure ospf add vlan accounting area 0.0.0.1 link-type auto
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure ospf area external-filter

```
configure ospf area <area identifier> external-filter [<access profile>
|none]
```

Description

Configures an external filter policy.

Syntax Description

area identifier	Specifies the OSPF target area.
access profile	Specifies an access profile.
none	Specifies not to apply an external filter.

Default

N / A.

Usage Guidelines

For switches configured to support multiple OSPF areas (an ABR function), an access profile can be applied to an OSPF area that filters a set of OSPF external routes from being advertised into that area.

NOTE

If any of the external routes specified in the filter have already been advertised, those routes will remain until the associated LSAs in that area time-out.

Using the none mode specifies that no external filter is applied.

Example

The following command configures an external filter policy from the access profile *nosales*:

```
configure ospf area 1.2.3.4 external-filter nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure ospf area interarea-filter

```
configure ospf area <area identifier> interarea-filter [<access profile> |
none]
```

Description

Configures a global inter-area filter policy.

Syntax Description

area identifier	Specifies the OSPF target area.
access profile	Specifies an access profile.
none	Specifies not to apply an interarea filter.

Default

N/A.

Usage Guidelines

For switches configured to support multiple OSPF areas (an ABR function), an access profile can be applied to an OSPF area that filters a set of OSPF inter-area routes from being sourced from any other areas.

Example

The following command configures an inter-area filter policy from the access profile *nosales*:

```
configure ospf area 0.0.0.6 interarea-filter nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure ospf area add range

```
configure ospf area <area identifier> add range <ipaddress> <mask>
[advertise | noadvertise] {type-3 | type-7}
```

Description

Configures a range of IP addresses in an OSPF area to be aggregated.

Syntax Description

area identifier	Specifies an OSPF area.
ipaddress	Specifies an IP address
mask	Specifies a subnet mask.
advertise	Specifies to advertise the aggregated range of IP addresses.
noadvertise	Specifies not to advertise the aggregated range of IP addresses.
type-3	Specifies type 3 LSA, summary LSA.
type-7	Specifies type 7 LSA, NSSA external LSA.

Default

N/A.

Usage Guidelines

If advertised, the aggregated IP range is exported as a single LSA by the ABR.

Example

The following command is used to summarize a certain range of IP addresses within an area and export them out as a single address:

```
configure ospf area 1.2.3.4 add range 10.1.2.0/24 advertise type-3
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf area delete range

```
configure ospf area <area identifier> delete range <ipaddress> <mask>
```

Description

Deletes a range of aggregated IP addresses in an OSPF area.

Syntax Description

area identifier	Specifies an OSPF area.
ipaddress	Specifies an IP address.
mask	Specifies a subnet mask.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes an aggregated IP address range:

```
configure ospf area 1.2.3.4 delete range 10.1.2.0/24
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf area normal

```
configure ospf area <area identifier> normal
```

Description

Configures an OSFP area as a normal area.

Syntax Description

area identifier	Specifies an OSPF area.

Default

Normal.

Usage Guidelines

A normal area is an area that is not any of the following:

- Stub area
- NSSA

Virtual links can be configured through normal areas. External routes can be distributed into normal areas.

Example

The following command configures an OSPF area as a normal area:

```
configure ospf area 10.1.0.0 normal
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf area nssa stub-default-cost

```
configure ospf area <area identifier> nssa [summary | nosummary]
stub-default-cost <cost> {translate}
```

Description

Configures an OSPF area as an NSSA.

Syntax Description

area identifier	Specifies an OSPF area.
summary	Specifies that type-3 can be propagated into the area.
nosummary	Specifies that type-3 cannot be propagated into the area.
cost	Specifies a cost metric.
translate	Specifies whether type-7 LSAs are translated into type-5 LSAs.

Default

N/A.

Usage Guidelines

NSSAs are similar to the existing OSPF stub area configuration option, but have the following two additional capabilities:

- External routes originating from an ASBR connected to the NSSA can be advertised within the NSSA.
- External routes originating from the NSSA can be propagated to other areas, including the backbone area, if translated to type 5 LSAs.

When configuring an OSPF area as an NSSA, the translate option should only be used on NSSA border routers, where translation is to be enforced. If translate is not used on any NSSA border router in a NSSA, one of the ABRs for that NSSA is elected to perform translation (as indicated in the NSSA specification). The option should not be used on NSSA internal routers. Doing so inhibits correct operation of the election algorithm.

Example

The following command configures an OSPF area as an NSSA:

```
configure ospf area 10.1.1.0 nssa summary stub-default-cost 10 translate
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure ospf area stub stub-default-cost

```
configure ospf area <area identifier> stub [summary | nosummary]
stub-default-cost <cost>
```

Description

Configures an OSPF area as a stub area.

Syntax Description

area identifier	Specifies an OSPF area.
summary	Specifies that type-3 can be propagated into the area.
nosummary	Specifies that type-3 cannot be propagated into the area.
cost	Specifies a cost metric.

Default

N / A.

Usage Guidelines

A stub area is connected to only one other area. The area that connects to a stub area can be the backbone area. External route information is not distributed into stub areas. Stub areas are used to reduce memory and computation requirements on OSPF routers.

Example

The following command configures an OSPF area as a stub area:

```
configure ospf area 0.0.0.6 stub nosummary stub-default-cost 10
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf asbr-filter

```
configure ospf asbr-filter [<access profile> | none]
```

Description

Configures a route filter for all OSPF exported routes.

Syntax Description

access profile	Specifies an access profile.
none	Specifies not to apply an ASBR filter.

Default

N/A.

Usage Guidelines

For switches configured to support RIP, BGP, VIP, IS-IS, and static route re-distribution into OSPF, an access profile can be used to limit the routes that are advertised into OSPF for the switch as a whole.

Example

The following command configures a route filter for all routes OSPF exports from RIP or other sources:

```
configure ospf asbr-filter subnet25-filter
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure ospf ase-limit

```
configure ospf ase-limit <number> {timeout <seconds>}
```

Description

Configures the AS-external LSA limit and overflow duration associated with OSPF database overflow handling.

Syntax Description

number	Specifies the number of external routes that can be held on a link-state database.
seconds	Specifies a duration for which the system has to remain in the overflow state.

Default

The default for timeout is 0, which indicates that once the router goes into overflow state, it stays there until OSPF is disabled and then re-enabled.

Usage Guidelines

None.

Example

The following command configures the AS-external LSA limit and overflow duration:

```
configure ospf ase-limit 50000 timeout 1800
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure ospf ase-summary add

```
configure ospf ase-summary add <ip address> <mask> cost <cost>
{tag <number>}
```

Description

Aggregates AS-external routes in a specified address range.

Syntax Description

ipaddress	Specifies an IP address.
mask	Specifies a subnet mask.
cost	Specifies a metric that will be given to the summarized route.
tag	Specifies an OSPF external route tag.

Default

N/A.

Usage Guidelines

This command is only valid on an ASBR.

Example

The following command summarizes AS-external routes:

```
configure ospf ase-summary add 175.1.0.0/16 cost 10
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure ospf ase-summary delete

```
configure ospf ase-summary delete <ip address> <mask>
```

Description

Deletes an aggregated OSPF external route.

Syntax Description

ipaddress	Specifies an IP address.
mask	Specifies a subnet mask.

Default

N / A.

Usage Guidelines

This command is only valid on an ASBR.

Example

The following command deletes the aggregated AS-external route:

```
configure ospf ase-summary delete 175.1.0.0/16
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure ospf delete virtual-link

```
configure ospf delete virtual-link <routerid> <area identifier>
```

Description

Removes a virtual link.

Syntax Description

routerid	Specifies a router interface number.
area identifier	Specifies an OSPF area.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes a virtual link:

```
configure ospf delete virtual-link 10.1.2.1 10.1.0.0
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf delete vlan

```
configure ospf delete vlan [<vlan name> | all]
```

Description

Disables OSPF on one or all VLANs (router interfaces).

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables OSPF on VLAN *accounting*:

```
configure ospf delete vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf direct-filter

```
configure ospf direct-filter [<access profile> | none]
```

Description

Configures a route filter for direct routes.

Syntax Description

access profile	Specifies an access profile.
none	Specifies not to apply a direct filter.

Default

N/A.

Usage Guidelines

If none is specified, all direct routes are exported if ospf export direct is enabled.

In versions of ExtremeWare before release 6.0, direct routes corresponding to the interfaces on which RIP was enabled were exported into OSPF as part of RIP routes, using the command enable ospf export rip. Using ExtremeWare 6.0 and above, you must configure ExtremeWare to export these direct routes to OSPF. You can use an access profile to filter unnecessary direct routes.

For switches configured to support direct route re-distribution into OSPF, an access profile can be used to limit the routes that are advertised into OSPF for the switch as a whole.

Example

The following command configures a route filter for direct routes based on the access profile *nosales*:

```
configure ospf direct-filter nosales
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure ospf lsa-batch-interval

```
configure ospf lsa-batch-interval <seconds>
```

Description

Configures the OSPF LSA batching interval.

Syntax Description

seconds	Specifies a time in seconds.

Default

The default setting is 30 seconds.

Usage Guidelines

The range is between 0 (disabled) and 600 seconds, using multiples of 5 seconds. The LSAs added to the LSDB during the interval are batched together for refresh or timeout.

Example

The following command configures the OSPF LSA batch interval to a value of 100 seconds:

```
configure ospf lsa-batch-interval 100
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure ospf metric-table

```
configure ospf metric-table 10M <cost> 100M <cost> 1G <cost> {10G <cost>}
```

Description

Configures the automatic interface costs for 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps interfaces.

Syntax Description

cost	Specifies the interface cost for the indicated interfaces.

Default

- 10 Mbps—The default cost is 10.
- 100 Mbps—The default cost is 5.
- 1 Gbps—The default cost is 4.
- 10 Gbps—The default cost is 2.

Usage Guidelines

None.

Example

The following command configures the automatic interface costs for 10 Mbps, 100 Mbps, and 1 Gbps interfaces:

```
configure ospf metric-table 10m 20 100m 10 1g 2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure ospf routerid

```
configure ospf routerid [automatic | <routerid>]
```

Description

Configures the OSPF router ID. If automatic is specified, the switch uses the highest IP interface address as the OSPF router ID.

Syntax Description

automatic	Specifies to use automatic addressing.
routerid	Specifies a router address.

Default

Automatic.

Usage Guidelines

Each switch that is configured to run OSPF must have a unique router ID. It is recommended that you manually set the router ID of the switches participating in OSPF, instead of having the switch automatically choose its router ID based on the highest interface IP address. Not performing this configuration in larger, dynamic environments could result in an older link-state database remaining in use.

NOTE

Do not set the router ID to 0.0.0.0.

The implementation of the configure ospf routerid command has been augmented to support automatic advertisement of a label mapping for the OSPF router ID. A label is advertised for the OSPF router ID regardless of whether OSPF distributes a route for the router ID IP address in its router LSA.

To support the use of indirect LSPs, Extreme LSRs automatically advertise a label mapping for a /32 LSP to its OSPF router ID (configured using the configure ospf routerid command).

Example

The following command sets the router ID:

```
configure ospf routerid 10.1.6.1
```

History

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

configure ospf spf-hold-time

```
configure ospf spf-hold-time <seconds>
```

Description

Configures the minimum number of seconds between Shortest Path First (SPF) recalculations.

Syntax Description

seconds	Specifies a time in seconds.

Default

3 seconds.

Usage Guidelines

None.

Example

The following command configures the minimum number of seconds between Shortest Path First (SPF) recalculations:

```
configure ospf spf-hold-time 6
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure ospf vlan area

```
configure ospf [all | vlan <vlan name>] area <area identifier>
```

Description

Associates a VLAN (router interface) with an OSPF area. By default, all router interfaces are associated with area 0.0.0.0.

Syntax Description

all	Specifies all VLANs.
vlan name	Specifies a VLAN name.
area identifier	Specifies an OSPF area.

Default

Area 0.0.0.0

Usage Guidelines

Any OSPF network that contains more than one area is required to have an area configured as area 0, also called the *backbone*. All areas in an autonomous system must be connected to the backbone. When designing networks, you should start with area 0, and then expand into other areas.

The backbone allows summary information to be exchanged between ABRs. Every ABR hears the area summaries from all other ABRs. The ABR then forms a picture of the distance to all networks outside of its area by examining the collected advertisements, and adding in the backbone distance to each advertising router.

When a VLAN is configured to run OSPF, by default you must assign it to an area.

Example

The following command associates the VLAN *accounting* with an OSPF area:

```
configure ospf vlan accounting area 0.0.0.6
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure ospf vlan neighbor add

```
configure ospf vlan <vlan name> neighbor add <ipaddress>
```

Description

Configures the IP address of a point-to-point neighbor.

Syntax Description

vlan name	Specifies a VLAN name.
ipaddress	Specifies an IP address.

Default

N / A.

Usage Guidelines

None.

Example

The following command configures the IP address of a point-to-point neighbor:

```
configure ospf vlan accounting neighbor add 10.0.0.1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure ospf vlan neighbor delete

```
configure ospf vlan <vlan name> neighbor delete <ipaddress>
```

Description

Deletes the IP address of a point-to-point neighbor.

Syntax Description

vlan name	Specifies a VLAN name.
ipaddress	Specifies an IP address.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes the IP address of a point-to-point neighbor:

```
configure ospf vlan accounting neighbor delete 10.0.0.1
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure ospf vlan timer

```
configure ospf vlan <vlan name> timer <retransmit interval> <transit delay>
<hello interval [1-655191]> <dead interval> {<wait timer interval>}
```

Description

Configures the OSPF wait interval.

Syntax Description

vlan name	Specifies a VLAN name.
retransmit interval	Specifies the length of time that the router waits before retransmitting an LSA that is not acknowledged.
transit delay	Specifies the length of time it takes to transmit an LSA packet over the interface.
hello interval	Specifies the interval at which routers send hello packets.
dead interval	Specifies the interval after which a neighboring router is declared down due to the fact that hello packets are no longer received from the neighbor.
wait timer interval	Specifies the interval between the interface coming up and the election of the DR and BDR.

Default

- retransmit interval—5 seconds.
- transit delay—1 second.
- hello interval—10 seconds.
- dead interval—40 seconds.
- wait timer interval—dead interval.

Usage Guidelines

Specify the following:

- retransmit interval—If you set an interval that is too short, unnecessary retransmissions will result.
- transit delay—The transit delay must be greater than 0.
- hello interval—Smaller times allow routers to discover each other more quickly, but also increase network traffic.
- dead interval—This interval should be a multiple of the hello interval.
- wait timer interval—This interval is required by the OSPF standard to be equal to the router dead interval. Under some circumstances, setting the wait interval to smaller values can help OSPF routers on a broadcast network to synchronize more quickly at the expense of possibly electing an incorrect DR or BDR. This value should not be set to less than the hello interval. The default value is equal to the router dead interval.

Example

The following command configures the OSPF wait interval on the VLAN *accounting*:

```
configure ospf vlan accounting timer 10 15 20 60 60
```

History

This command was first available in ExtremeWare 6.2.

This command was modified in ExtremeWare 6.22.

Platform Availability

This command is available on all platforms.

configure rip add vlan

```
configure rip add vlan [<vlan name> | all]
```

Description

Configures RIP on an IP interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

All. If no VLAN is specified, then all is assumed.

Usage Guidelines

When an IP interface is created, RIP configuration is disabled on the interface by default. When the RIP interface is disabled, the parameters are not reset to default automatically.

Example

The following command configures RIP on the VLAN *finance*:

```
configure rip add finance
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip delete vlan

```
configure rip delete vlan [<vlan name> | all]
```

Description

Disables RIP on an IP interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

All. If no VLAN is specified, then all is assumed.

Usage Guidelines

When an IP interface is created, RIP configuration is disabled on the interface by default. When the RIP interface is disabled, the parameters are not reset to default automatically.

Example

The following command deletes RIP on a VLAN named *finance*:

```
configure rip delete finance
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip garbagetime

```
configure rip garbagetime {<seconds>}
```

Description

Configures the RIP garbage time.

Syntax Description

seconds	Specifies a time in seconds.

Default

120 seconds.

Usage Guidelines

None.

Example

The following command configures the RIP garbage time to have a 60-second delay:

```
configure rip garbagetime 60
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip routetimeout

```
configure rip routetimeout {<seconds>}
```

Description

Configures the route timeout period.

Syntax Description

seconds	Specifies a time in seconds.

Default

180 seconds.

Usage Guidelines

If a router does not receive an update message from its neighbor within the route timeout period (180 seconds by default), the router assumes the connection between it and its neighbor is no longer available.

Example

The following example sets the route timeout period to 120 seconds:

```
configure rip routetimeout 120
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip rxmode

```
configure rip rxmode [none | v1only | v2only | any] {vlan [<vlan name> |
all]}
```

Description

Changes the RIP receive mode for one or more VLANs.

Syntax Description

none	Specifies to drop all received RIP packets.
v1only	Specifies to accept only RIP version 1 format packets.
v2only	Specifies to accept only RIP version 2 format packets.
any	Specifies to accept RIP version 1 and RIP version 2 packets.
vlan name	Specifies to apply settings to specific VLAN name.
all	Specifies all VLANs.

Default

Any.

Usage Guidelines

If no VLAN is specified, the setting is applied to all VLANs.

Example

The following command configures the receive mode for the VLAN *finance* to accept only RIP version 1 format packets:

```
configure rip rxmode v1only finance
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip txmode

```
configure rip txmode [none | v1only | v1comp | v2only] {vlan [<vlan name> |
all]}
```

Description

Changes the RIP transmission mode for one or more VLANs.

Syntax Description

none	Specifies to not transmit any packets on this interface.
v1only	Specifies to transmit RIP version 1 format packets to the broadcast address.
v1comp	Specifies to transmit RIP version 2 format packets to the broadcast address.
v2only	Specifies to transmit RIP version 2 format packets to the RIP multicast address.
vlan name	Specifies to apply settings to a specific VLAN name.
all	Specifies all VLANs.

Default

v2only.

Usage Guidelines

If no VLAN is specified, the setting is applied to all VLANs.

Example

The following command configures the transmit mode for the VLAN *finance* to transmit version 2 format packets to the broadcast address:

```
configure rip txmode v1comp finance
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip updatetime

```
configure rip updatetime {<seconds>}
```

Description

Specifies the time interval in seconds within which RIP sends update packets.

Syntax Description

seconds	Specifies a time in seconds.

Default

30 seconds.

Usage Guidelines

The router exchanges an update message with each neighbor every 30 seconds (default value), or if there is a change to the overall routed topology (also called *triggered updates*). The timer granularity is 10 seconds.

Example

The following command sets the update timer to 60 seconds:

```
configure rip updatetime 60
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure rip vlan cost

```
configure rip vlan [<vlan name> | all] cost <cost>
```

Description

Configures the cost (metric) of the interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
cost	Specifies a cost metric.

Default

The default setting is 1.

Usage Guidelines

None.

Example

The following command configures the cost for the VLAN *finance* to a metric of 3:

```
configure rip vlan finance cost 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure rip vlan export-filter

```
configure rip vlan [<vlan name> | all] export-filter [<access profile> |
none]
```

Description

Configures RIP to suppress certain routes when performing route advertisements.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access-profile name.
none	Specifies to check the access profile for permit and deny attributes.

Default

N/A.

Usage Guidelines

Use an access profile to determine trusted RIP router neighbors for the VLAN on the switch running RIP.

Using the none mode, the access profile can contain a combination of permit and deny entries. Each entry must have a permit or deny attribute. The operation is compared with each entry in the list. When a match is found, the operation is either permitted or denied, depending on the configuration of the matched entry. If no match is found, the operation is implicitly denied.

Example

The following command uses the access profile *nosales* to determine which RIP routes are advertised into the VLAN *backbone*:

```
configure rip vlan backbone export-filter nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure rip vlan import-filter

```
configure rip vlan [<vlan name> | all] import-filter [<access profile> |
none]
```

Description

Configures RIP to ignore certain routes received from its neighbor.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access-profile name.
none	Specifies to check the access profile for permit and deny attributes.

Default

N/A.

Usage Guidelines

Configures an import filter policy, which uses an access profile to determine which RIP routes are accepted as valid routes. This policy can be combined with the trusted neighbor policy to accept selected routes only from a set of trusted neighbors.

Using the none mode, the access profile can contain a combination of permit and deny entries. Each entry must have a permit or deny attribute. The operation is compared with each entry in the list. When a match is found, the operation is either permitted or denied, depending on the configuration of the matched entry. If no match is found, the operation is implicitly denied.

Example

The following command configures the VLAN *backbone* to accept selected routes from the access profile *nosales*:

```
configure rip vlan backbone import-filter nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure rip vlan trusted-gateway

```
configure rip vlan [<vlan name> | all] trusted-gateway [<access profile> |
none]
```

Description

Configures a trusted neighbor policy, which uses an access profile to determine trusted RIP router neighbors for the VLAN on the switch running RIP.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access-profile name.
none	Specifies to check the access profile for permit and deny attributes.

Default

N/A.

Usage Guidelines

Using the none mode, the access profile can contain a combination of permit and deny entries. Each entry must have a permit or deny attribute. The operation is compared with each entry in the list. When a match is found, the operation is either permitted or denied, depending on the configuration of the matched entry. If no match is found, the operation is implicitly denied.

Example

The following command configures RIP to use the access profile *nointernet* to determine from which RIP neighbor to receive (or reject) the routes to the VLAN *backbone*:

```
configure rip vlan backbone trusted-gateway nointernet
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

create isis area

```
create isis area <name>
```

Description

Creates an IS-IS level 1 area.

Syntax Description

name	Specifies the area identifier.

Default

N/A.

Usage Guidelines

Currently, only one level 1 area can be created.

The maximum length for an area identifier is 32 characters. The identifier must begin with one alphabetic character followed by up to 31 alphabetic or numeric characters.

Example

The following command creates an IS-IS level 1 area:

```
create isis area a1000
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

create ospf area

```
create ospf area <area identifier>
```

Description

Creates an OSPF area.

Syntax Description

area identifier	Specifies an OSPF area.

Default

Area 0.0.0.0

Usage Guidelines

Area 0.0.0.0 does not need to be created. It exists by default.

Example

The following command creates an OSPF area:

```
create ospf area 1.2.3.4
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

delete isis area

```
delete isis area [<isis area identifier> | all]
```

Description

Deletes an IS-IS level 1 area.

Syntax Description

isis area identifier	Specifies the area identifier.

Default

N/A.

Usage Guidelines

Currently, only one level 1 area can be created.

The maximum length for an area identifier is 32 characters. The identifier must begin with one alphabetic character followed by up to 31 alphabetic or numeric characters.

The `all` option deletes all of the level 1 areas simultaneously.

The level 1 area can only be deleted when no interface attaches to it.

Example

The following command deletes an IS-IS level 1 area:

```
delete isis area a1000
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

delete ospf area

```
delete ospf area [<area identifier> | all]
```

Description

Deletes an OSPF area.

Syntax Description

area identifier	Specifies an OSPF area.
all	Specifies all areas.

Default

N/A.

Usage Guidelines

An OSPF area cannot be deleted if it has an associated interface.

Example

The following command deletes an OSPF area:

```
delete ospf area 1.2.3.4
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable isis

```
disable isis
```

Description

Disables IS-IS routing.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

To enable IS-IS routing, use the following command:

```
enable isis
```

Example

The following command disables IS-IS routing:

```
disable isis
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable isis export

```
disable isis [level-2 | area <isis area identifier>] export [bgp | i-bgp |
e-bgp | direct | rip | static | vip | ospf | ospf-intra | ospf-inter |
ospf-extern1 | ospf-extern2]
```

Description

Disables the redistribution of non-IS-IS routes from the kernel routing table into a IS-IS level 2 subdomain or level 1 area:

Syntax Description

level-2	Specifies a level 2 subdomain
isis area identifier	Specifies an IS-IS level 1 area
bgp	Specifies BGP routes.
i-bgp	Specifies I-BGP routes.
e-bgp	Specifies E-BGP routes.
direct	Specifies direct routes.
rip	Specifies RIP routes.
static	Specifies static routes.
vip	Specifies VIP routes.
ospf	Specifies OSPF routes.
ospf-intra	Specifies Intra OSPF routes.
ospf-inter	Specifies Inter OSPF routes.
ospf-extern1	Specifies Extern 1 OSPF routes.
ospf-extern2	Specifies Extern 2 OSPF routes.

Default

The default setting is disabled.

Usage Guidelines

All the redistributed routes are associated with the same metric and metric type.

Example

The following command disables redistribution of OSPF routes for a level 2 subdomain:

disable isis level-2 export ospf

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable isis ignore-attached-bit

```
disable isis ignore-attached-bit
```

Description

Disables ignoring the attached bit.

Syntax Description

This command has no arguments or variables.

Default

The default setting is disabled.

Usage Guidelines

This command can only be applied to a level 1 only switch. It specifies that the level 1 only switch will not ignore the attached bit (ATT bit) from level 1/2 switches.

This command has the effect of enabling the feature described in the *ExtremeWare Software User Guide, Software Version 7.0.0*, in the chapter, "Interior Gateway Protocols", in the section, "Default Routes to Nearest Level 1/2 Switch for Level 1 Only Switches". See the user guide for more information.

Example

The following command disables ignoring the attached bit:

```
disable isis ignore-attached-bit
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable isis originate-default

```
disable isis [level-2 | area <isis area identifier>] originate-default
```

Description

Disables the origination of an IS-IS default route from a system into the level 1 area or level 2 subdomain.

Syntax Description

level-2	Specifies the level 2 subdomain.
area identifier	Specifies a level 1 area identifier.

Default

The default setting is disabled.

Usage Guidelines

None.

Example

The following command disables the origination of an IS-IS default route for the level 2 subdomain:

```
disable isis level-2 originate-default
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable isis overload

```
disable isis [level-2 | area <isis area identifier>] overload {at-startup}
```

Description

Disables the setting of the overload bit in the LSP originated by the system in the level 2 subdomain or level 1 area.

Syntax Description

level-2	Specifies the level 2 subdomain.
isis area identifier	Specifies a level 1 area.
at-startup	Specifies that setting the overload bit is disabled at startup.

Default

The default setting is disabled.

Usage Guidelines

The `at-startup` option disables setting the overload bit at system startup time.

Example

The following command disables setting the overload bit for the level 1 area *a1*:

```
disable isis area a1 overload
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable ospf

```
disable ospf
```

Description

Disables the OSPF process for the router.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables the OSPF process for the router:

```
disable ospf
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable ospf capability opaque-lsa

```
disable ospf capability opaque-lsa
```

Description

Disables opaque LSAs across the entire system.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Opaque LSAs are a generic OSPF mechanism used to carry auxiliary information in the OSPF database. Opaque LSAs are most commonly used to support OSPF traffic engineering.

Normally, support for opaque LSAs is auto-negotiated between OSPF neighbors. In the event that you experience interoperability problems, you can disable opaque LSAs.

If your network uses opaque LSAs, all routers on your OSPF network should support opaque LSAs. Routers that do not support opaque LSAs do not store or flood them. At minimum a well-interconnected subsection of your OSPF network needs to support opaque LSAs to maintain reliability of their transmission.

On an OSPF broadcast network, the designated router (DR) must support opaque LSAs or none of the other routers on that broadcast network will reliably receive them. You can use the OSPF priority feature to give preference to an opaque-capable router, so that it becomes the elected DR.

For transmission to continue reliably across the network, the backup designated router (BDR) must also support opaque LSAs.

Example

The following command disables opaque LSAs across the entire system:

```
disable ospf capability opaque-lsa
```

History

This command was available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable ospf export

```
disable ospf export [bgp | direct | e-bgp | i-bgp | isis | isis-level-1 |
isis-level-1-external | isis-level-2 | isis-level-2-external | rip | static
| vip]
```

Description

Disables redistribution of routes to OSPF.

Syntax Description

bgp	Specifies BGP routes.
direct	Specifies direct routes.
i-bgp	Specifies I-BGP routes.
e-bgp	Specifies E-BGP routes.
isis	Specifies IS-IS routes.
isis-level-1	Specifies IS-IS level 1 routes.
isis-level-1-external	Specifies IS-IS level 1 external routes.
isis-level-2	Specifies IS-IS level 2 routes.
isis-level-2-external	Specifies IS-IS level 2 external routes.
rip	Specifies RIP routes.
static	Specifies static routes.
vip	Specifies VIP routes.

Default

The default setting is disabled.

Usage Guidelines

Use this command to stop OSPF from exporting routes derived from other protocols.

Example

The following command disables OSPF to export BGP-related routes to other OSPF routers:

```
disable ospf export bgp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable ospf originate-router-id

```
disable ospf originate-router-id
```

Description

Disables distribution of a route for the OSPF router ID in the router LSA.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

When this function is enabled, OSPF includes a link with the router ID IP address and a mask of 255.255.255.255 in the router LSA. The link type is stub and the metric is 0.

When disabled, OSPF does not include a link with the router ID IP address in the router LSA

Example

The following command disables the distribution of a route for the OSPF router ID in the router LSA:

```
disable ospf originate-router-id
```

History

This command was available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

Platform Availability

This command is available on the BlackDiamond switch only.

disable rip

```
disable rip
```

Description

Disables RIP for the whole router.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

RIP has a number of limitations that can cause problems in large networks, including:

- A limit of 15 hops between the source and destination networks
- A large amount of bandwidth taken up by periodic broadcasts of the entire routing table
- Slow convergence
- Routing decisions based on hop count; no concept of link costs or delay
- Flat networks; no concept of areas or boundaries

Example

The following command disables RIP for the whole router:

```
disable rip
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable rip aggregation

```
disable rip aggregation
```

Description

Disables the RIP aggregation of subnet information on a RIP version 2 (RIPv2) router.

Syntax Description

This command has no arguments or variables.

Default

RIP aggregation is disabled by default.

Usage Guidelines

The disable RIP aggregation command disables the RIP aggregation of subnet information on a switch configured to send RIPv2-compatible traffic. The switch summarizes subnet routes to the nearest class network route. The following rules apply when using RIP aggregation:

- Within a class boundary, no routes are aggregated.
- If aggregation is disabled, subnet routes are never aggregated, even when crossing a class boundary.

Example

The following command disables RIP aggregation on the interface:

```
disable rip aggregation
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable rip export

```
disable rip export [direct | isis | isis-level-1 | isis-level-1-external |
isis-level-2 | isis-level-2-external | ospf | ospf-extern1 | ospf-extern2 |
ospf-inter | ospf-intra | static | vip]
```

Description

Disables RIP from redistributing routes from other routing protocols.

Syntax Description

static	Specifies static routes.
direct	Specifies interface routes (only interfaces that have IP forwarding enabled are exported).
isis	Specifies IS-IS routes.
isis-level-1	Specifies IS-IS level 1 routes.
isis-level-1-external	Specifies IS-IS level 1 external routes.
isis-level-2	Specifies IS-IS level 2 routes.
isis-level-2-external	Specifies IS-IS level 2 external routes.
ospf	Specifies all OSPF routes.
ospf-intra	Specifies OSPF-intra area routes.
ospf-inter	Specifies OSPF-inter area routes.
ospf-extern1	Specifies OSPF external route type 1.
ospf-extern2	Specifies OSPF external route type 2.
vip	Specifies VIP routes.

Default

Disabled.

Usage Guidelines

This command disables the exporting of static, direct, IS-IS, and OSPF-learned routes into the RIP domain.

Example

The following command disables RIP from redistributing any routes learned from OSPF:

```
disable rip export ospf
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

disable rip exportstatic

```
disable rip exportstatic
```

Description

Disables the redistribution of static routes.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure 64 static unicast routes. Static routes can also be used for security reasons, to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

Example

The following command disables the redistribution of static routes:

```
disable rip exportstatic
```

History

This command was removed in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

disable rip originate-default

```
disable rip originate-default
```

Description

Disables the advertisement of a default route.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command unconfigures a default route to be advertised by RIP if no other default route is advertised:

```
disable rip originate-default cost 0
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable rip poisonreverse

```
disable rip poisonreverse
```

Description

Disables poison reverse algorithm for RIP.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Like split horizon, poison reverse is a scheme for eliminating the possibility of loops in the routed topology. In this case, a router advertises a route over the same interface that supplied the route, but the route uses a hop count of 16, defining it as unreachable.

Example

The following command disables the split horizon with poison reverse algorithm for RIP:

```
disable rip poisonreverse
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable rip splithorizon

```
disable rip splithorizon
```

Description

Disables the split horizon algorithm for RIP.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Split horizon is a scheme for avoiding problems caused by including routes in updates sent to the router from which the route was learned. Split horizon omits routes learned from a neighbor in updates sent to that neighbor.

Example

The following command disables the split horizon algorithm for RIP:

```
disable rip splithorizon
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable rip triggerupdate

```
disable rip triggerupdate
```

Description

Disables the trigger update mechanism. Triggered updates are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes or changes their metric.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Triggered updates occur whenever a router changes the metric for a route and it is required to send an update message immediately, even if it is not yet time for a regular update message to be sent. This will generally result in faster convergence, but may also result in more RIP-related traffic.

Example

The following command disables the trigger update mechanism:

```
disable rip triggerupdate
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable isis

```
enable isis
```

Description

Enables IS-IS routing.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

To enable IS-IS routing, use the following command:

```
enable isis
```

Example

The following command enables IS-IS routing:

```
enable isis
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable isis export

```
enable isis [level-2 | area <isis area identifier>] export [bgp | i-bgp |
e-bgp | direct | rip | static | vip | ospf | ospf-intra | ospf-inter |
ospf-extern1 | ospf-extern2] [cost <cost(0-4261412864)> type [internal |
external] | <route map>]
```

Description

Enables the redistribution of non-IS-IS routes from the kernel routing table into a IS-IS level 2 subdomain or level 1 area:

Syntax Description

level-2	Specifies a level 2 subdomain
isis area identifier	Specifies an IS-IS level 1 area
bgp	Specifies BGP routes.
i-bgp	Specifies I-BGP routes.
e-bgp	Specifies E-BGP routes.
direct	Specifies direct routes.
rip	Specifies RIP routes.
static	Specifies static routes.
vip	Specifies VIP routes.
ospf	Specifies OSPF routes.
ospf-intra	Specifies Intra OSPF routes.
ospf-inter	Specifies Inter OSPF routes.
ospf-extern1	Specifies Extern 1 OSPF routes.
ospf-extern2	Specifies Extern 2 OSPF routes.
cost	Specifies a cost from 0 to 4,261,412,864.
internal	Specifies an internal metric type.
external	Specifies an external metric type.
route map	Specifies a route map name.

Default

The default setting is disabled.

Usage Guidelines

All the redistributed routes are associated with the same metric and metric type, if specified. If a route map is specified, routes can be assigned different metric and metric types. Routes maps can also filter out routes.

Example

The following command enables redistribution of direct routes to the level 1 area *a1* with the route map *rm*:

```
enable isis area a1 export direct rm
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable isis ignore-attached-bit

```
enable isis ignore-attached-bit
```

Description

Enables ignoring the attached bit.

Syntax Description

This command has no arguments or variables.

Default

The default setting is disabled.

Usage Guidelines

This command can only be applied to a level 1 only switch. It specifies that the level 1 only switch will ignore the attached bit (ATT bit) from level 1/2 switches.

This command has the effect of disabling the feature described in the *ExtremeWare Software User Guide, Software Version 7.0.0*, in the chapter, "Interior Gateway Protocols", in the section, "Default Routes to Nearest Level 1/2 Switch for Level 1 Only Switches". See the user guide for more information.

Example

The following command enables ignoring the attached bit:

```
enable isis ignore-attached-bit
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable isis originate-default

```
enable isis [level-2 | area <isis area identifier>] originate-default
{always} cost <cost(0-4261412864)> type [internal | external]
```

Description

Enables the origination of a default route from a system into the level 1 area or level 2 subdomain.

Syntax Description

level-2	Specifies the level 2 subdomain.
isis area identifier	Specifies a level 1 area identifier
always	Specifies that the default route is always originated.
cost	Specifies a cost from 0 to 4,261,412,864.
internal	Specifies an internal metric type.
external	Specifies an external metric type.

Default

The default setting is disabled.

Usage Guidelines

When the `always` option is specified, the default route is originated even if there is no default route in the kernel routing table. Otherwise the default route will be originated only if the default route is available in the kernel route table.

Example

The following command enables the origination of an IS-IS default route that uses the internal metric type and a cost of 15 for the level 2 subdomain:

```
enable isis level-2 originate-default cost 15 type internal
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

enable isis overload

```
enable isis [level-2 | area <isis area identifier>] overload {at-startup}
{<seconds(1-86400)>}
```

Description

Enables the setting of the overload bit in the LSP originated by the system in the level 2 subdomain or level 1 area.

Syntax Description

level-2	Specifies the level 2 subdomain.
isis area identifier	Specifies a level 1 area.
at-startup	Specifies that setting the overload bit is enabled at startup.
seconds(1-86400)	Specifies the duration of the overload.

Default

The default setting is disabled.

Usage Guidelines

The `at-startup` option sets the overload bit at system startup time.

The `<seconds(1-186400)>` parameter sets the duration of the overload bit. If the duration is not specified, the bit is set until it is disabled. The range is 1 to 186,400 seconds.

Example

The following command enables IS-IS overload for the level 1 area *a1* with a duration of 100 seconds:

```
enable isis area a1 overload 100
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

enable ospf

```
enable ospf
```

Description

Enables the OSPF process for the router.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command enables the OSPF process for the router:

```
enable ospf
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable ospf capability opaque-lsa

```
enable ospf capability opaque-lsa
```

Description

Enables opaque LSAs across the entire system.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Opaque LSAs are a generic OSPF mechanism used to carry auxiliary information in the OSPF database. Opaque LSAs are most commonly used to support OSPF traffic engineering.

Normally, support for opaque LSAs is auto-negotiated between OSPF neighbors. In the event that you experience interoperability problems, you can disable opaque LSAs.

If your network uses opaque LSAs, all routers on your OSPF network should support opaque LSAs. Routers that do not support opaque LSAs do not store or flood them. At minimum a well-interconnected subsection of your OSPF network needs to support opaque LSAs to maintain reliability of their transmission.

On an OSPF broadcast network, the designated router (DR) must support opaque LSAs or none of the other routers on that broadcast network will reliably receive them. You can use the OSPF priority feature to give preference to an opaque-capable router, so that it becomes the elected DR.

For transmission to continue reliably across the network, the backup designated router (BDR) must also support opaque LSAs.

Example

The following command enables opaque LSAs across the entire system:

```
enable ospf capability opaque-lsa
```

History

This command was available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable ospf export

```
enable ospf export [bgp | e-bgp | i-bgp | isis | isis-level-1 |
isis-level-1-external | isis-level-2 | isis-level-2-external]
[cost <number> [ase-type-1 | ase-type-2] {tag <number>} | <route map>]
```

Description

Enables redistribution of routes to OSPF.

Syntax Description

bgp	Specifies BGP routes.
i-bgp	Specifies I-BGP routes.
e-bgp	Specifies E-BGP routes.
isis	Specifies IS-IS routes.
isis-level-1	Specifies IS-IS level 1 routes.
isis-level-1-external	Specifies IS-IS level 1 external routes.
isis-level-2	Specifies IS-IS level 2 routes.
isis-level-2-external	Specifies IS-IS level 2 external routes.
number	Specifies a cost metric.
ase-type-1	Specifies AS-external type 1 routes.
ase-type-2	Specifies AS-external type 2 routes.
number	Specifies a tag value.
route map	Specifies a route map.

Default

The default tag number is 0. The default setting is disabled.

Usage Guidelines

After it is enabled, the OSPF router is considered to be an ASBR. Interface routes that correspond to the interface that has OSPF enabled are ignored.

Exporting routes from OSPF to RIP, and from RIP to OSPF, are discrete configuration functions. To run OSPF and RIP simultaneously, you must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to RIP and the routes to export from RIP to OSPF.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

The same cost, type, and tag values can be inserted for all the export routes, or route maps can be used for selective insertion. When a route map is associated with the export command, the route map is applied on every exported route. The exported routes can also be filtered using route maps.

Example

The following command enables OSPF to export BGP-related routes using LSAs to other OSPF routers:

```
enable ospf export bgp cost 1 ase-type-1 tag 0
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable ospf export direct

```
enable ospf export direct [cost <metric> [ase-type-1 | ase-type-2] {tag
<number>} | <route map>]
```

Description

Enables the redistribution of local interface (direct) routes into the OSPF domain. This will not export the loopback address of 127.0.0.1.

Syntax Description

metric	Specifies a cost metric.
ase-type-1	Specifies AS-external type 1 routes.
ase-type-2	Specifies AS-external type 2 routes.
number	Specifies a tag value.
route map	Specifies a route map.

Default

The default tag number is 0. The default setting is disabled.

Usage Guidelines

After it is enabled, the OSPF router is considered to be an ASBR. Interface routes that correspond to the interface that has OSPF enabled are ignored.

Exporting routes from OSPF to RIP, and from RIP to OSPF, are discreet configuration functions. To run OSPF and RIP simultaneously, you must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to RIP and the routes to export from RIP to OSPF.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

The same cost, type, and tag values can be inserted for all the export routes, or route maps can be used for selective insertion. When a route map is associated with the export command, the route map is applied on every exported route. The exported routes can also be filtered using route maps.

Example

The following command enables the distribution of local interface (direct) routes into the OSPF domain:

```
enable ospf export direct cost 1 ase-type-1 tag 0
```

History

This command was first available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

Platform Availability

This command is available on all platforms.

enable ospf export rip

```
enable ospf export rip [cost <metric> [ase-type-1 | ase-type-2] {tag
<number>} | <route map>]
```

Description

Enables the redistribution of RIP to OSPF.

Syntax Description

metric	Specifies a cost metric.
ase-type-1	Specifies AS-external type 1 routes.
ase-type-2	Specifies AS-external type 2 routes.
number	Specifies a tag value.
route map	Specifies a route map name.

Default

The default tag number is 0. The default setting is disabled.

Usage Guidelines

After it is enabled, the OSPF router is considered to be an ASBR.

This command enables the exporting of RIP by way of LSA to other OSPF routers as AS-external type 1 or type 2 routes.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

When re-distributing RIP routes, you should turn off RIP aggregation unless you are expertly familiar with the possible consequences and impact. By default, new configurations of RIP using ExtremeWare 4.0 and above disable RIP aggregation. In previous ExtremeWare versions, RIP aggregation is enabled by default. This configuration is preserved when upgrading to ExtremeWare 4.0. Verify the configuration using the command `show rip`.

Example

The following command enables the exporting of RIP to OSPF:

```
enable ospf export rip cost 1 ase-type-1 tag 0
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

enable ospf export static

```
enable ospf export static [cost <metric> [ase-type-1 | ase-type-2] {tag
<number>} | <route map>]
```

Description

Enables the redistribution of static routes to OSPF.

Syntax Description

metric	Specifies a cost metric.
ase-type-1	Specifies AS-external type 1 routes.
ase-type-2	Specifies AS-external type 2 routes.
number	Specifies a tag value.
route map	Specifies a route map name.

Default

The default tag number is 0. The default setting is disabled.

Usage Guidelines

After it is enabled, the OSPF router is considered to be an ASBR.

This command enables the redistribution of static routes by way of LSA to other OSPF routers as AS-external type 1 or type 2 routes.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

Example

The following command enables the exporting of static routes to OSPF:

```
enable ospf export static cost 0 ase-type-1 tag 0
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

enable ospf export vip

```
enable ospf export vip [cost <metric> [ase-type-1 | ase-type-2] {tag
<number>} | <route map>]
```

Description

Enables the redistribution of virtual IP addresses into the OSPF domain.

Syntax Description

metric	Specifies a cost metric.
ase-type-1	Specifies AS-external type 1 routes.
ase-type-2	Specifies AS-external type 2 routes.
number	Specifies a tag value.
route map	Specifies a route map.

Default

The default tag number is 0. The default setting is disabled.

Usage Guidelines

After it is enabled, the OSPF router is considered to be an ASBR.

Exporting routes from OSPF to RIP, and from RIP to OSPF, are discreet configuration functions. To run OSPF and RIP simultaneously, you must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to RIP and the routes to export from RIP to OSPF.

These commands enable or disable the exporting of RIP, static, and direct routes by way of LSA to other OSPF routers as AS-external type 1 or type 2 routes. The default setting is disabled.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

The same cost, cost-type, and tag values can be inserted for all the export routes, or route maps can be sued for selective insertion. When a route map is associated with the export command, the route map is applied on every exported route. The exported routes can also be filtered using route maps.

Example

The following command enables the redistribution of virtual IP addresses into the OSPF domain:

```
enable ospf export vip cost 0 ase-type-1 tag 0
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable ospf originate-default

```
enable ospf originate-default {always} cost <metric> [ase-type-1 |
ase-type-2] {tag <number>}
```

Description

Enables a default external LSA to be generated by OSPF, if no other default route is originated by OSPF by way of RIP and static route re-distribution.

Syntax Description

always	Specifies for OSPF to always advertise the default route.
metric	Specifies a cost metric.
ase-type-1	Specifies AS-external type 1 routes.
ase-type-2	Specifies AS-external type 2 routes.
number	Specifies a tag value.

Default

N/A.

Usage Guidelines

If always is specified, OSPF always advertises the default route. If always is not specified, OSPF adds the default LSA if a reachable default route is in the route table.

Example

The following command generates a default external type-1 LSA:

```
enable ospf originate-default cost 1 ase-type-1 tag 0
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable ospf originate-router-id

```
enable ospf originate-router-id
```

Description

Enables distribution of a route for the OSPF router ID in the router LSA.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

When this function is enabled, OSPF includes a link with the router ID IP address and a mask of 255.255.255.255 in the router LSA. The link type is stub and the metric is 0.

When disabled, OSPF does not include a link with the router ID IP address in the router LSA

Example

The following command enables the distribution of a route for the OSPF router ID in the router LSA:

```
enable ospf originate-router-id
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

Platform Availability

This command is available on the BlackDiamond switch only.

enable rip

```
enable rip
```

Description

Enables RIP for the whole router.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

RIP has a number of limitations that can cause problems in large networks, including:

- A limit of 15 hops between the source and destination networks
- A large amount of bandwidth taken up by periodic broadcasts of the entire routing table
- Slow convergence
- Routing decisions based on hop count; no concept of link costs or delay
- Flat networks; no concept of areas or boundaries

Example

The following command enables RIP for the whole router:

```
enable rip
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable rip aggregation

```
enable rip aggregation
```

Description

Enables the RIP aggregation of subnet information on a RIP version 2 (RIPv2) interface.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

The enable (disable) rip aggregation command enables (disables) the RIP aggregation of subnet information on an interface configured to send RIPv1 or RIPv2-compatible traffic. The switch summarizes subnet routes to the nearest class network route. The following rules apply when using RIP aggregation:

- Subnet routes are aggregated to the nearest class network route when crossing a class boundary.
- Within a class boundary, no routes are aggregated.
- If aggregation is enabled, the behavior is the same as in RIPv1.
- If aggregation is disabled, subnet routes are never aggregated, even when crossing a class boundary.

Example

The following command enables RIP aggregation on the interface:

```
enable rip aggregation
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable rip export cost

```
enable rip export [direct | isis | isis-level-1 | isis-level-1-external |
isis-level-2 | isis-level-2-external | ospf | ospf-extern1 | ospf-extern2 |
ospf-inter | ospf-intra | static | vip] cost <number> {tag <number>}
```

Description

Enables RIP to redistribute routes from other routing functions.

Syntax Description

static	Specifies static routes.
direct	Specifies interface routes (only interfaces that have IP forwarding enabled are exported).
isis	Specifies IS-IS routes.
isis-level-1	Specifies IS-IS level 1 routes.
isis-level-1-external	Specifies IS-IS level 1 external routes.
isis-level-2	Specifies IS-IS level 2 routes.
isis-level-2-external	Specifies IS-IS level 2 external routes.
ospf	Specifies all OSPF routes.
ospf-intra	Specifies OSPF-intra area routes.
ospf-inter	Specifies OSPF-inter area routes.
ospf-extern1	Specifies OSPF external route type 1.
ospf-extern2	Specifies OSPF external route type 2.
vip	Specifies VIP routes.
cost <number>t	Specifies the `cost` metric, from 0-15. If set to 0, RIP uses the route metric obtained from the route origin.
tag <number>	Specifies a tag number.

Default

Disabled.

Usage Guidelines

This command enables the exporting of static, direct, IS-IS, and OSPF-learned routes into the RIP domain. You can choose which types of OSPF or IS-IS routes are injected, or you can simply choose `ospf` or `isis`, which will inject all learned OSPF or IS-IS routes regardless of type.

The cost metric is inserted for all RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag.

Example

The following command enables RIP to redistribute routes from all OSPF routes:

```
enable rip export ospf cost 0
```

History

This command was first available in ExtremeWare 4.0.

The keyword `metric` was changed to the keyword `cost`.

Platform Availability

This command is available on all platforms.

enable rip exportstatic

```
enable rip exportstatic
```

Description

Enables the redistribution of static routes.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure 64 static unicast routes. Static routes can also be used for security reasons, to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

Example

The following command enables the redistribution of static routes:

```
enable rip exportstatic
```

History

This command was removed in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

enable rip originate-default cost

```
enable rip originate-default {always} cost <number> {tag<number>}
```

Description

Configures a default route to be advertised by RIP if no other default route is advertised.

Syntax Description

always	Specifies to always advertise the default route.
cost <number>	Specifies a cost metric.
tag <number>	Specifies a tag number.

Default

Disabled.

Usage Guidelines

If always is specified, RIP always advertises the default route to its neighbors. If always is not specified, RIP adds a default route if a reachable default route is not in the route table.

The cost metric is inserted for all RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag.

Example

The following command configures a default route to be advertised by RIP if no other default route is advertised:

```
enable rip originate-default cost 0
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable rip poisonreverse

```
enable rip poisonreverse
```

Description

Enables poison reverse algorithm for RIP.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Like split horizon, poison reverse is a scheme for eliminating the possibility of loops in the routed topology. In this case, a router advertises a route over the same interface that supplied the route, but the route uses a hop count of 16, defining it as unreachable.

Example

The following command enables the split horizon with poison reverse algorithm for RIP:

```
enable rip poisonreverse
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable rip splithorizon

```
enable rip splithorizon
```

Description

Enables the split horizon algorithm for RIP.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Split horizon is a scheme for avoiding problems caused by including routes in updates sent to the router from which the route was learned. Split horizon omits routes learned from a neighbor in updates sent to that neighbor.

Example

The following command enables the split horizon algorithm for RIP:

```
enable rip splithorizon
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable rip triggerupdate

```
enable rip triggerupdate
```

Description

Enables the trigger update mechanism. Triggered updates are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes or changes their metric.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

Triggered updates occur whenever a router changes the metric for a route and it is required to send an update message immediately, even if it is not yet time for a regular update message to be sent. This will generally result in faster convergence, but may also result in more RIP-related traffic.

Example

The following command enables the trigger update mechanism:

```
enable rip triggerupdate
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show isis

```
show isis
```

Description

Displays the system parameters that are configured for the system and other system runtime information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

show isis adjacency

```
show isis adjacency {level-2 | area <isis area identifier> | vlan <vlan
name>} {detail}
```

Description

Displays the runtime information for all the adjacencies currently present on a VLAN.

Syntax Description

level-2	Specifies IS-IS level 2.
vlan name	Specifies the name of a VLAN.
isis area identifier	Specifies the level 1 are identifier.
detail	Specifies display of more detailed information.

Default

N / A.

Usage Guidelines

If `isis area identifier` is specified, the adjacency information for all the VLANs in the area is displayed.

Example

The following command shows the adjacency information of VLAN *v1* in detail:

```
show isis adjacency vlan v1 detail
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

show isis interface

```
show isis interface {vlan <vlan name> | area <isis area identifier>}
{detail}
```

Description

Displays the interface parameters that are configured and other interface related runtime information.

Syntax Description

vlan name	Specifies the name of a VLAN.
isis area identifier	Specifies the level 1 are identifier.
detail	Specifies display of more detailed information.

Default

N / A.

Usage Guidelines

None.

Example

The following command shows the IS-IS VLAN *v1* interface information in detail:

```
show isis interface vlan v1 detail
```

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

show isis lsdb

```
show isis lsdb {level-2 | area <isis area identifier>} {system-identifier
<system identifier> | sysName <alphanumeric string>} {type [non-pseudonode
| pseudonode {circuit-identifier <number(1-255)>}]} {lsp-number
<number(0-255)>}
```

Description

Displays the contents of the LSDB of the level 2 subdomain or a level 1 area.

Syntax Description

level-2	Specifies the level 2 subdomain.
isis area identifier	Specifies a level 1 area identifier.
system identifier	Specifies a system identifier. The format is xxxx.xxxx.xxxx, where x is a hexadecimal digit.
alphanumeric string	Specifies the system name of the switch.
type	Specifies LSDB type, non-pseudonode or pseudonode.
number(1-255)	Specifies a circuit ID from 1 to 255.
number(0-255)	Specifies an LSP number from 0 to 255.

Default

N/A.

Usage Guidelines

None.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

show ospf

```
show ospf
```

Description

Displays global OSPF information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays global OSPF information:

```
show ospf
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ospf area

```
show ospf area <area identifier>
```

Description

Displays information about a particular OSPF area.

Syntax Description

area identifier	Specifies an OSPF area.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays information about OSPF area 1.2.3.4:

```
show ospf area 1.2.3.4
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ospf area detail

```
show ospf area detail
```

Description

Displays information about all OSPF areas.

Syntax Description

detail	Specifies to display the information in detailed format.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays information about all OSPF areas:

```
show ospf area detail
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show ospf ase-summary

```
show ospf ase-summary
```

Description

Displays the OSPF external route aggregation configuration.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the OSPF external route aggregation configuration:

```
show ospf ase-summary
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show ospf interfaces detail

```
show ospf interfaces detail
```

Description

Displays detailed information about all OSPF interfaces.

Syntax Description

detail	Specifies to display the information in detailed format.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays information about all OSPF interfaces:

```
show ospf interfaces detail
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

show ospf interfaces

```
show ospf interfaces {vlan <vlan name> | area <area identifier>}
```

Description

Displays information about one or all OSPF interfaces.

Syntax Description

vlan name	Specifies a VLAN name.
area identifier	Specifies an OSPF area.

Default

If no argument is specified, all OSPF interfaces are displayed.

Usage Guidelines

None.

Example

The following command displays information about one or all OSPF interfaces on the VLAN *accounting*:

```
show ospf interfaces vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ospf lsdb area lstype

```
show ospf lsdb area [all | <area identifier>[/<len>] | detail | interface |
lsid <id>[/<len>] | lstype [all | as-external | external-type7 | network |
opaque-area | opaque-global | opaque-local | router | summary-asb
|summary-net| routerid <id>[/<len>] | stats | summary | vlan <vlan name>]
```

Description

Displays a table of the current LSDB.

Syntax Description

all	Specifies all OSPF areas.
area identifier	Specifies an OSPF area.
detail	Specifies to display all fields of matching LSAs in a multi-line format.
interface	Specifies to display interface types.
id	Specifies an LS ID.
id	Specifies a router ID.
stats	Specifies to display the number of matching LSAs, but not any of their contents.
summary	Specifies to display several important fields of matching LSAs, one line per LSA.
vlan name	Specifies a VLAN name.

Default

Display in summary format.

Usage Guidelines

ExtremeWare provides several filtering criteria for the show ospf lsdb command. You can specify multiple search criteria and only results matching all of the criteria are displayed. This allows you to control the displayed entries in large routing tables.

A common use of this command is to omit all optional parameters, resulting in the following shortened form:

```
show ospf lsdb
```

The shortened form displays all areas and all types in a summary format.

You can filter the display using either the area ID, the remote router ID, or the link-state ID. The default setting is `all` with no detail. If detail is specified, each entry includes complete LSA information.

Example

The following command displays all areas and all types in a summary format:

```
show ospf lsdb
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ospf virtual-link

```
show ospf virtual-link {routerid <routerid> <area identifier>}
```

Description

Displays virtual link information about a particular router or all routers.

Syntax Description

routerid	Specifies a router interface number.
area identifier	Specifies an OSPF area.

Default

N / A.

Usage Guidelines

area identifier—Transit area used for connecting the two end-points. The transit area cannot have the IP address 0.0.0.0.

Example

The following command displays virtual link information about a particular router:

```
show ospf virtual-link routerid 1.2.3.4 10.1.6.1
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show rip

```
show rip {detail}
```

Description

Displays RIP specific configuration and statistics for all VLANs.

Syntax Description

detail	Specifies to display the information in detailed format.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays RIP specific configuration and statistics for all VLANs:

```
show rip
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show rip stats

```
show rip stats {detail}
```

Description

Displays RIP-specific statistics for all VLANs.

Syntax Description

detail	Specifies to display the information in detailed format.

Default

All.

Usage Guidelines

Statistics include the following per interface:

- Packets transmitted
- Packets received
- Bad packets received
- Bad routes received
- Number of RIP peers
- Peer information

Example

The following command displays RIP-specific statistics for all VLANs:

```
show rip stat
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show rip stats vlan

```
show rip stats vlan <vlan name>
```

Description

Displays RIP specific statistics for a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays RIP specific statistics for the VLAN *accounting*:

```
show rip stat accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

show rip vlan

```
show rip vlan <vlan name>
```

Description

Displays RIP configuration and statistics for a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

All.

Usage Guidelines

None.

Example

The following command displays RIP configuration and statistics for the VLAN *accounting*:

```
show rip vlan accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

unconfigure ospf

```
unconfigure ospf {vlan <vlan name> | area <area identifier>}
```

Description

Resets one or all OSPF interfaces to the default settings.

Syntax Description

vlan name	Specifies a VLAN name.
area identifier	Specifies an OSPF area.

Default

N/A.

Usage Guidelines

None.

Example

The following command resets the OSPF interface to the default settings on the VLAN *accounting*:

```
unconfigure ospf accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

unconfigure rip

```
unconfigure rip {vlan <vlan name>}
```

Description

Resets all RIP parameters to the default VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

All.

Usage Guidelines

Does not change the enable/disable state of the RIP settings.

Example

The following command deletes RIP configuration from the VLAN *finance*:

```
unconfigure rip finance
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

18 BGP Commands

Border Gateway Protocol (BGP) is an exterior routing protocol that was developed for use in TCP/IP networks. The primary function of BGP is to allow different autonomous systems (ASs) to exchange network reachability information.

An autonomous system is a set of routers that are under a single technical administration. This set of routers uses a different routing protocol (such as OSPF) for intra-AS routing. One or more routers in the AS are configured to be border routers, exchanging information with other border routers (in different autonomous systems) on behalf of all of the intra-AS routers.

BGP can be used as an exterior gateway protocol (E-BGP), or it can be used within an AS as an interior gateway protocol (I-BGP).

BGP Attributes

The following well-known BGP attributes are supported by the switch:

- Origin – Defines the origin of the route. Possible values are IGP, EGP, and incomplete.
- AS_Path – The list of ASs that are traversed for this route.
- Next_hop – The IP address of the next hop BGP router to reach the destination listed in the NLRI field.
- Multi_Exist_Discriminator – Used to select a particular border router in another AS when multiple border routers exist.
- Local_Preference – Used to advertise this router's degree of preference to other routers within the AS.
- Atomic_aggregate – Indicates that the sending border router is used a route aggregate prefix in the route update.
- Aggregator – Identifies the BGP router AS number and IP address that performed route aggregation.
- Community – Identifies a group of destinations that share one or more common attributes.
- Cluster_ID – Specifies a 4 byte field used by a route reflector to recognize updates from other route reflectors in the same cluster.

BGP Communities

A BGP community is a group of BGP destinations that require common handling. ExtremeWare supports the following well-known BGP community attributes:

- no-export
- no-advertise
- no-export-subconfed

BGP Features

This section lists BGP features supported by ExtremeWare:

- Route Reflectors
- Route Confederations
- Route Aggregation
- IGP Synchronization
- Using the Loopback Interface
- BGP Peer Groups
- BGP Route Flap Dampening
- Route Redistribution
- Policy Filtering
- Maximum Prefix Limit
- MD5 TCP Authentication

clear bgp neighbor counters

```
clear bgp neighbor [<ip address> | all] counters
```

Description

Resets the BGP counters for one or all BGP neighbor sessions to zero.

Syntax Description

ip address	Specifies the IP address of a specific BGP neighbor.
all	Specifies that counters for all BGP neighbors should be reset.

Default

N/A.

Usage Guidelines

This command resets the following counters:

- In-total-msgs
- Out-total-msgs
- In-updates
- Out-updates
- Last-error
- FsmTransitions

Example

The following command resets the counters for the BGP neighbor at 10.20.30.55:

```
clear bgp neighbor 10.20.30.55 counters
```

History

This command was first available in ExtremeWare 6.2.1

This command was modified in ExtremeWare 6.2.2 to add the FsmTransitions counter.

Platform Availability

This command is available on all platforms.

clear bgp neighbor flap-statistics

```
clear bgp neighbor <ip address> flap-statistics
[community [access-profile <access profile> | no-advertise | no-export |
no-export-subconfed | number <community number> |
<autonomous system id (0 - 65535)>:<bgp community (0 - 65535)>]
| as-path [<path expression> | access-profile <access profile>]
| route-map <route map>
| network <ip address>/<mask> {exact}
| all]
```

Description

Clears flap statistics for routes to specified neighbors.

Syntax Description

ip address	Specifies an IP address that identifies a BGP neighbor.
access profile	Specifies an access profile used as a community attribute.
no-advertise	Specifies the no-advertise community attribute.
no-export	Specifies the no-export community attribute.
no-export-subconfed	Specifies the no-export-subconfed community attribute.
community number	Specifies a community number.
autonomous system id	Specifies an autonomous system ID (0-65535).
access profile	Specifies an access profile.
route map	Specifies a route map.
ip address	Specifies an IP address.
mask	Specifies a subnet mask (number of bits).
exact	Specifies an exact match with the IP address and subnet mask.
all	Specifies all routes.

Default

N / A.

Usage Guidelines

Use this command to clear flap statistics for a specified BGP neighbor.

Example

The following command clears the flap statistics for a specified neighbor:

```
clear bgp neighbor 10.10.10.10 flap-statistics
```

History

This command was introduced in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure bgp add aggregate-address

```
configure bgp add aggregate-address <ip address>/<mask length> {as-set |
as-match} {summary-only} {advertise-route-map <route-map>}
{attribute-route-map <route-map>}
```

Description

Configures a BGP aggregate route.

Syntax Description

ip address	Specifies an IP address.
mask length	Specifies a netmask length.
as-set	Specifies to aggregate only the path attributes of the aggregate routes.
summary-only	Specifies to send only aggregated routes to the neighbors.
advertise-route-map	Specifies the route map used to select routes for this aggregated route.
attribute-route-map	Specifies the route map used to set the attributes of the aggregated route.

Default

N / A.

Usage Guidelines

Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

To use BGP route aggregation, follow these steps:

1. Enable aggregation using the following command:

   ```
   enable bgp aggregation
   ```

2. Create an aggregate route using the following commands:

   ```
   configure bgp add aggregate-address <ip address>/<mask length> {as-set | as-match}
   {summary-only} {advertise-route-map <route-map>} {attribute-route-map <route-map>}
   ```

Example

The following command configures a BGP aggregate route:

```
configure bgp add aggregate-address 192.1.1.4/30
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp add confederation-peer sub-AS-number

```
configure bgp add confederation-peer sub-AS-number <number>
```

Description

Adds a sub-AS to a confederation.

Syntax Description

number	Specifies a sub-AS number.

Default

N/A.

Usage Guidelines

Invoke this command multiple times to add multiple sub-ASs.

IBGP requires networks to use a fully-meshed router configuration. This requirement does not scale well, especially when BGP is used as an interior gateway protocol. One way to reduce the size of a fully-meshed AS is to divide the AS into multiple sub-autonomous systems and group them into a *routing confederation*. Within the confederation, all BGP speakers in each sub-AS must be fully-meshed. The confederation is advertised to other networks as a single AS.

Example

The following command adds one sub-AS to a confederation:

```
configure bgp add confederation-peer sub-AS-number 65002
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp add network

```
configure bgp add network <ip address>/<mask length> {<route map>}
```

Description

Adds a network to be originated from this router.

Syntax Description

ip address	Specifies an IP address.
mask length	Specifies a netmask length.
route map	Specifies a route map.

Default

N/A.

Usage Guidelines

The network must be present in the routing table.

Using the `export` command to redistribute routes complements the redistribution of routes using the `configure bgp add network` command. The `configure bgp add network` command adds the route to BGP only if the route is present in the routing table. The `enable bgp export` command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the `network` command take precedence over routes redistributed using the `export` command.

Example

The following command adds a network to be originated from this router:

```
configure bgp add network 192.1.1.16/12
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp AS-number

```
configure bgp AS-number <number>
```

Description

Changes the local AS number used by BGP.

Syntax Description

number	Specifies a local AS number.

Default

N/A.

Usage Guidelines

BGP must be disabled before the as number can be changed.

Example

The following command changes the local AS number used by BGP:

```
configure bgp AS-number 65001
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp cluster-id

```
configure bgp cluster-id <bgp cluster id (0 - 4294967295)>
```

Description

Configures the local cluster ID.

Syntax Description

bgp cluster id	Specifies a 4 byte field used by a route reflector to recognize updates from other route reflectors in the same cluster.

Default

N/A.

Usage Guidelines

Used when multiple route reflectors are used within the same cluster of clients.

Extreme Networks recommends disabling BGP before configuring the cluster ID.

Example

The following command appends a BGP route reflector cluster ID to the cluster list of a route:

```
configure bgp cluster-id 40000
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp confederation-id

```
configure bgp confederation-id <number>
```

Description

Specifies a BGP routing confederation ID.

Syntax Description

confederation-id	Specifies a routing confederation identifier.

Default

N / A.

Usage Guidelines

IBGP requires networks to use a fully-meshed router configuration. This requirement does not scale well, especially when BGP is used as an interior gateway protocol. One way to reduce the size of a fully-meshed AS is to divide the AS into multiple sub-autonomous systems and group them into a *routing confederation*. Within the confederation, each sub-AS must be fully-meshed. The confederation is advertised to other networks as a single AS.

Use a confederation ID of 0 to indicate no confederation.

Example

The following command specifies the BGP routing confederation ID as *200*:

```
configure bgp confederation-id 200
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp delete aggregate-address

```
configure bgp delete aggregate-address [<ip address/masklength> | all]
```

Description

Deletes one or all BGP aggregated route.

Syntax Description

ip address/mask length	Specifies an IP address and netmask length.
all	Specifies all aggregated routes.

Default

N/A.

Usage Guidelines

Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

Example

The following command deletes a BGP aggregate route:

```
configure bgp delete aggregate-address 192.1.1.4/30
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp delete confederation-peer sub-AS-number

```
configure bgp delete confederation-peer sub-AS-number <number>
```

Description

Specifies a sub-AS that should be deleted from a confederation.

Syntax Description

sub-AS-number	Specifies a sub-AS.

Default

N/A.

Usage Guidelines

IBGP requires networks to use a fully-meshed router configuration. This requirement does not scale well, especially when BGP is used as an interior gateway protocol. One way to reduce the size of a fully-meshed AS is to divide the AS into multiple sub-autonomous systems and group them into a *routing confederation*. Within the confederation, each sub-AS must be fully-meshed. The confederation is advertised to other networks as a single AS.

Example

The following command deletes a sub-AS from a confederation:

```
configure bgp delete confederation-peer sub-AS-number 65002
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp delete network

```
configure bgp delete network [all | <ip address>/<masklength>]
```

Description

Deletes a network to be originated from this router.

Syntax Description

all	Specifies all networks.
ip address/mask length	Specifies an IP address and a netmask length.

Default

N/A.

Usage Guidelines

None.

Example

The following command deletes a network to be originated from this router:

```
configure bgp delete network 192.1.1.12/30
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure bgp local-preference

```
configure bgp local-preference <number>
```

Description

Changes the default local preference attribute.

Syntax Description

number	Specifies a value used to advertise this router's degree of preference to other routers within the AS.

Default

100.

Usage Guidelines

The range is 0 to 2,147,483,647.

BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example

The following command changes the default local preference attribute to *500*:

```
configure bgp local-preference 500
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp med

```
configure bgp med [none | <bgp med (0-2147483647)>]
```

Description

Configures the metric to be included in the Multi-Exit-Discriminator (MED) path attribute. The MED path attribute is included in route updates sent to external peers if a value is configured.

Syntax Description

none	Specifies not to use a multi-exist-discriminator number.
number	Specifies a multi-exist-discriminator number.

Default

N/A.

Usage Guidelines

BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example

The following command configures the metric to be included in the MED path attribute:

```
configure bgp med 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor as-path-filter

```
configure bgp neighbor [<ip address> | all] as-path-filter [in | out] [none
| <access profile>]
```

Description

Configures the AS path filter for a neighbor.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
in	Specifies to install the filter on the input side.
out	Specifies to install the filter on the output side.
none	Specifies to remove the filter.
access profile	Specifies an access profile.

Default

N/A.

Usage Guidelines

The filter is defined using the access-profile mechanism and can be installed on the input side and/or the output side of the router.

Example

The following command configures the AS path filter for a neighbor based on the access profile *nosales:*

```
configure bgp neighbor 192.1.1.22 as-path-filter in nosales
```

History

This command was available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor dampening

```
configure bgp neighbor [<ip address> | all] dampening {{<half-life>
{<reuse> <suppress> <max-suppress> }} | {route-map <route map>}}
```

Description

Configures route flap dampening over BGP peer sessions.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
half-life	Specifies the dampening half life.
reuse	Specifies the reuse limit.
suppress	Specifies the suppress limit.
max-suppress	Specifies the maximum hold down time.
route map	Specifies a route map

Default

This feature is disabled by default.

Usage Guidelines

The half life is the period of time, in minutes, during which the accumulated penalty of a route is reduced by half. The range is 1 to 45 minutes, and the default is 15 minutes.

The reuse limit is the penalty value below which a route will be used again. The range is 1-20,000, and the default is 750.

The suppress limit is the penalty value above which a route will be suppressed. The range is 1-20,000, and the default is 2,000.

The maximum hold down time is the maximum time a route can be suppressed, no matter how unstable it has been, as long as it no longer flaps. The range is 1-255 minutes, and the default is 4 * the half life.

Use the following command to disable route flap dampening for BGP neighbors:

```
configure bgp neighbor [<ip address> | all] no-dampening
```

Example

The following command configures route flap dampening to the BGP neighbor at 192.168.1.22:

```
configure bgp neighbor 192.168.1.22 dampening
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure bgp neighbor maximum-prefix

```
configure bgp neighbor [<ip address> | all] maximum-prefix <number>
{{threshold <percent>} {teardown {holddown-interval <seconds>}}
{send-traps}
```

Description

Configures the maximum number of IP prefixes accepted from a BGP neighbor.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
number	Specifies the maximum number of prefixes accepted. The range is 0 to 4294967294. A value of 0 disables prefix limit feature.
percent	Specifies the percentage of the maximum prefix (threshold) at which a warning message is printed in the log (and console), and/or a trap will be sent to the SNMP manager.
teardown	Specifies that the peer session is torn down when the maximum is exceeded.
seconds	Specifies the length of time before the session is re-established. If the session is torn down due to maximum prefix exceeded, it is kept down until the peer is enabled. The range is 30 to 86400 seconds.
send-traps	Specifies sending “number of prefix reached threshold” and “number of prefix exceed the max-prefix limit” SNMP traps.

Default

This feature is disabled by default.

The default threshold is 75%.

By default, `teardown` is not specified.

By default, `send-traps` is not specified.

Usage Guidelines

Configure the peer group before configuring the neighbors. To configure the peer group, use the following command:

`configure bgp peer-group maximum-prefix`

Example

The following command configures the maximum number of IP prefixes accepted from all neighbors to 5000, sets the threshold for warning messages to 60%, and specifies SNMP traps:

```
configure bgp neighbor all maximum-prefix 5000 threshold 60 send-traps
```

History

This command was introduced in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure bgp neighbor next-hop-self

```
configure bgp neighbor [<ip address> | all] [next-hop-self |
no-next-hop-self]
```

Description

Configures the next hop address used in the outgoing updates to be the address of the BGP connection originating the update.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
next-hop-self	Specifies that the next hop address used in the updates be the address of the BGP connection originating it.
no-next-hop-self	Specifies that the next hop address used in the updates not be the address of the BGP connection originating it (lets BGP decide what would be the next hop).

Default

N/A.

Usage Guidelines

These settings apply to the peer group and all neighbors of the peer group.

Example

The following command configures the next hop address used in the updates to be the address of the BGP connection originating it:

```
configure bgp neighbor 172.16.5.25 next-hop-self
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp neighbor nlri-filter

```
configure bgp neighbor [<ip address> | all] nlri-filter [in | out] [none |
<access profile>]
```

Description

Configures an NLRI filter for a neighbor.

Syntax Description

ip address	Specifies a BGP neighbor IP address.
all	Specifies all neighbors.
in	Specifies to install the filter on the input side.
out	Specifies to install the filter on the output side.
none	Specifies to remove the filter.
access profile	Specifies an access profile.

Default

N/A.

Usage Guidelines

The NLRI filter is defined using the access-profile mechanism and can be installed on the input side and/or the output side of the router.

Example

The following command configures the NLRI filter for a neighbor based on the access profile *nosales:*

```
configure bgp neighbor 192.1.1.22 nlri-filter in nosales
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor no-dampening

```
configure bgp neighbor [<ip address> | all] no-dampening
```

Description

Configures no route flap dampening over BGP peer sessions (disables route flap dampening).

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.

Default

This feature is disabled by default.

Usage Guidelines

Use the following command to enable route flap dampening for BGP neighbors:

```
configure bgp neighbor [<ip address> | all] dampening {{<half-life> {<reuse>
<suppress> <max-suppress> }} | {route-map <route map>}}
```

Example

The following command disables route flap dampening to the BGP neighbor at 192.168.1.22:

```
configure bgp neighbor 192.168.1.22 no-dampening
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure bgp neighbor password

```
configure bgp neighbor [all | <ip address>] password [none | {encrypted}
<password>]
```

Description

Configures a password for a neighbor.

Syntax Description

all	Specifies all neighbors.
ip address	Specifies an IP address.
none	Specifies not to use a password
encrypted	This option is for use only by the switch when generating an ASCII configuration file. Specifies that the password should be encrypted when the configuration is uploaded to a file. Do not use this option.
password	Specifies a password string.

Default

N/A.

Usage Guidelines

When a password is configured, TCP MD5 authentication is enabled on the TCP connection that is established with the neighbor.

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

To change any one of the following parameters you must disable and re-enable the peer session:

- timer
- source-interface
- soft-in-reset
- password

Changing a route reflector client will automatically disable and enable the peer session.

NOTE

Do not select the encrypted *option in the CLI.*

The `encrypted` option is used by the switch when generating an ASCII configuration file (using the `upload configuration` command), and parsing a switch-generated configuration file (using the `download configuration` command). Do not select the encrypted option in the CLI.

Example

The following command configures the password for a neighbor as *Extreme*:

```
configure bgp neighbor 192.168.1.5 password extreme
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure bgp neighbor peer-group

```
configure bgp neighbor [all | <ip address>] peer-group [<peer group> |
none] {acquire-all}
```

Description

Configures an existing neighbor as the member of a peer group.

Syntax Description

all	Specifies all neighbors.
ip address	Specifies an IP address.
peer group	Specifies a peer group name.
none	Removes the neighbor from the peer group.
acquire-all	Specifies that all parameters should be inherited by the neighbor from the peer group.

Default

By default, remote AS (if configured for the peer group), source-interface, out-NLRI-filter, out-ASpath-filter, out-route-map, send-community and next-hop-self settings are inherited.

Usage Guidelines

If `acquire-all` is not specified, only the default parameters are inherited by the peer group.

When you remove a neighbor from a peer group, it retains the parameter settings of the group. The parameter values are not reset to those the neighbor had before it inherited the peer group values.

To create a new neighbor and add it to a BGP peer group, use the following command:

```
create bgp neighbor <ip address> peer-group <peer group> {multi-hop}
```

The new neighbor is created as part of the peer group and inherits all of the existing parameters of the peer group. The peer group must have remote AS configured.

Example

The following command configures an existing neighbor as the member of the peer group *outer*:

```
configure bgp neighbor 192.1.1.22 peer-group outer
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp neighbor route-map-filter

```
configure bgp neighbor [<ip address> | all] route-map-filter [in | out]
[none | <route map>]
```

Description

Configures a route map filter for a neighbor.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
in	Specifies to install the filter on the input side.
out	Specifies to install the filter on the output side.
none	Specifies to remove the filter.
route map	Specifies a route map.

Default

N/A.

Usage Guidelines

The route map filter can be installed on the input or output side of the router. The route map is used to modify or filter the NLRI information and the path attributes associated with it when exchanging updates with the neighbor.

Example

The following command configures the route-map-filter filter for a neighbor based on the access profile *nosales:*

```
configure bgp neighbor 192.168.1.22 route-map-filter in nosales
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor route-reflector-client

```
configure bgp neighbor [<ip address> | all] [route-reflector-client |
no-route-reflector-client]
```

Description

Configures a BGP neighbor to be a route reflector client.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
route-reflector-client	Specifies for the BGP neighbor to be a route reflector client.
no-route-reflector-client	Specifies for the BGP neighbor not to be a route reflector client.

Default

N/A.

Usage Guidelines

Another way to overcome the difficulties of creating a fully-meshed AS is to use *route reflectors*. Route reflectors allow a single router to serve as a central routing point for the AS or sub-AS.

Use this command to implicitly define the router to be a route reflector. The neighbor must be in the same AS as the router.

When changing the route reflector status of a peer, the peer will automatically be disabled and re-enabled and a warning message will appear on the console and in the log.

A *cluster* is formed by the route reflector and its client routers. Peer routers that are not part of the cluster must be fully meshed according to the rules of BGP.

Example

The following command configures a BGP neighbor to be a route reflector client:

```
configure bgp neighbor 192.168.1.5 route-reflector-client
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor send-community

```
configure bgp neighbor [<ip address> | all] [send-community |
dont-send-community]
```

Description

Configures whether the community path attribute associated with a BGP NLRI should be included in the route updates sent to the BGP neighbor.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
send-community	Specifies to include the community path attribute.
dont-send-community	Specifies not to include the community path attribute.

Default

N / A.

Usage Guidelines

A BGP community is a group of BGP destinations that require common handling. ExtremeWare supports the following well-known BGP community attributes:

- no-export
- no-advertise
- no-export-subconfed

Example

The following command includes the community path attribute associated with a BGP NLRI in the route updates sent to all BGP neighbors:

```
configure bgp neighbor all send-community
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor soft-reset

```
configure bgp neighbor [<ip address> | all] soft-reset {in | out}
```

Description

Applies the current input or output routing policy to the routing information already exchanged with the neighbor.

Syntax Description

ip address	Specifies an IP address
all	Specifies all neighbors.
in	Specifies to apply the input routing policy.
out	Specifies to apply the output routing policy.

Default

N/A.

Usage Guidelines

The input/output policy is determined by the NLRI-filter, AS-path-filter, and the route map configured for the neighbor on the input and/or output side of the router. This command does not affect the switch configuration.

Example

The following command applies the current input routing policy to the routing information already exchanged with the neighbor:

```
configure bgp neighbor 192.168.1.5 soft-reset in
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor source-interface

```
configure bgp neighbor [<ip address> | all] source-interface [any | vlan
<vlan name>]
```

Description

Changes the BGP source interface for TCP connections.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
any	Specifies any source interface.
vlan name	Specifies a VLAN name as a source interface for TCP.

Default

Any.

Usage Guidelines

None.

Example

The following command changes the BGP source interface on the VLAN *accounting*:

```
configure bgp neighbor 192.168.1.5 source-interface vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor timer

```
configure bgp neighbor [<ip address> | all] timer keep-alive <keepalive>
hold-time <holdtime>
```

Description

Configures the BGP neighbor timers.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
keepalive	Specifies a BGP neighbor timer keepalive time in seconds. The range is 0 to 21,845 seconds.
holdtime	Specifies a BGP neighbor timer hold time in seconds. The range is 3 to 65,535 seconds.

Default

The default keepalive setting is 60 seconds. The default hold time is 180 seconds.

Usage Guidelines

None.

Example

The following command configures the BGP neighbor timers:

```
configure bgp neighbor 192.168.1.5 timer keep-alive 120 hold-time 360
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp neighbor weight

```
configure bgp neighbor [<ip address> | all] weight <weight>
```

Description

Assigns a locally-used weight to a neighbor connection for the route selection algorithm.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.
weight	Specifies a BGP neighbor weight.

Default

0.

Usage Guidelines

All routes learned from this peer are assigned the same weight. The route with the highest weight is more preferable when multiple routes are available to the same network. The range is 0 to 4294967295.

BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example

The following command assigns a locally used weight of 10 to a neighbor connection:

```
configure bgp neighbor 192.168.1.5 weight 10
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp peer-group as-path-filter

```
configure bgp peer-group <peer group> as-path-filter [in | out] [none |
<access profile>]
```

Description

Configures the AS-path filters for a peer group and all neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
in	Specifies to install the filter on the input side.
out	Specifies to install the filter on the output side.
none	Specifies to remove the filter.
access profile	Specifies an access profile.

Default

N/A.

Usage Guidelines

None.

Example

The following command configures the as-path filters for the peer group *outer* and its neighbors using the access profile *nosales*:

```
configure bgp peer-group outer as-path-filter in nosales
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group dampening

```
configure bgp peer group <name> dampening {{<half-life> {<reuse> <suppress>
<max-suppress> }} | {route-map <route map>}}
```

Description

Configures route flap dampening for a BGP peer group.

Syntax Description

name	Specifies a peer group
half-life	Specifies the dampening half life.
reuse	Specifies the reuse limit.
suppress	Specifies the suppress limit.
max-suppress	Specifies the maximum hold down time.
route map	Specifies a route map

Default

This feature is disabled by default.

Usage Guidelines

The half life is the period of time, in minutes, during which the accumulated penalty of a route is reduced by half. The range is 1 to 45 minutes, and the default is 15 minutes.

The reuse limit is the penalty value below which a route will be used again. The range is 1-20,000, and the default is 750.

The suppress limit is the penalty value above which a route will be suppressed. The range is 1-20,000, and the default is 2,000.

The maximum hold down time is the maximum time a route can be suppressed, no matter how unstable it has been, as long as it no longer flaps. The range is 1-255 minutes, and the default is 4 * the half life.

Use the following command to disable route flap dampening for a BGP peer-group:

```
configure bgp peer-group <name> no-dampening
```

Example

The following command configures route flap dampening for the BGP peer group *outer*:

```
configure bgp peer-group outer dampening
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure bgp peer-group maximum-prefix

```
configure bgp peer-group <name> maximum-prefix <number> {{threshold
<percent>} {teardown {holddown-interval <seconds>}} {send-traps}
```

Description

Configures the maximum number of IP prefixes accepted for all neighbors in the peer group.

Syntax Description

name	Specifies a peer group.
number	Specifies the maximum number of prefixes accepted. The range is 0 to 4294967294. A value of 0 disables prefix limit feature.
percent	Specifies the percentage of the maximum prefix (threshold) at which a warning message is printed in the log (and on the console). An SNMP trap can also be sent.
teardown	Specifies that the peer session is torn down when the maximum is exceeded.
seconds	Specifies the length of time before the session is re-established. If the session has been torn down due to exceeding the max limit, it is kept down until the peer is enabled. The range is 30 to 86400 seconds.
send-traps	Specifies sending “number of prefix reached threshold” and “number of prefix exceed the max-prefix limit” SNMP traps.

Default

This feature is disabled by default.

The default threshold is 75%.

By default, `teardown` is not specified.

By default, `send-traps` is not specified.

Usage Guidelines

Configure the peer group before configuring the neighbors. To configure the neighbors, use the following command:

`configure bgp neighbor 192.168.1.1 maximum-prefix`

Example

The following command configures the maximum number of IP prefixes accepted from the peer group *outer* to 5000, sets the threshold for warning messages to 60%, and specifies SNMP traps:

```
configure bgp peer-group outer maximum-prefix 5000 threshold 60 send-traps
```

History

This command was introduced in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure bgp peer-group next-hop-self

```
configure bgp peer-group <peer group> [next-hop-self | no-next-hop-self]
```

Description

Configures the next hop address used in the updates to be the address of the BGP connection originating the update.

Syntax Description

peer group	Specifies a peer group.
next-hop-self	Specifies that the next hop address used in the updates be the address of the BGP connection originating it.
no-next-hop-self	Specifies that the next hop address used in the updates not be the address of the BGP connection originating it.

Default

N/A.

Usage Guidelines

These settings apply to the peer group and all neighbors of the peer group.

Example

The following command configures the next hop address used in the updates to be the address of the BGP connection originating it:

```
configure bgp peer-group outer next-hop-self
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group nlri-filter

```
configure bgp peer-group <peer group> nlri-filter [in | out] [none |
<access profile>]
```

Description

Configures the NLRI filter for a peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
in	Specifies to install the filter on the input side.
out	Specifies to install the filter on the output side.
none	Specifies to remove the filter.
access profile	Specifies an access profile.

Default

N/A.

Usage Guidelines

None.

Example

The following command configures the NLRI filter for the peer group *outer* and its neighbors using the access profile *nosales*:

```
configure bgp peer-group outer nlri-filter in nosales
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group no-dampening

```
configure bgp peer-group <name> no-dampening
```

Description

Configures no route flap dampening for a BGP peer group (disables route flap dampening).

Syntax Description

name	Specifies a BGP peer group.

Default

This feature is disabled by default.

Usage Guidelines

Use the following command to enable route flap dampening for a BGP peer-group:

```
configure bgp peer-group <name> dampening {{<half-life> {<reuse> <suppress>
<max-suppress> }} | {route-map <route map>}}
```

Example

The following command disables route flap dampening to the BGP peer group *outer*:

```
configure bgp peer-group no-dampening
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure bgp peer-group route-reflector-client

```
configure bgp peer-group <peer group> [route-reflector-client |
no-route-reflector-client]
```

Description

Configures all the peers in a peer group to be a route reflector client.

Syntax Description

peer group	Specifies a peer group.
route-reflector-client	Specifies that all the neighbors in the peer group be a route reflector client.
no-route-reflector-client	Specifies that all the neighbors in the peer group not be a route reflector client.

Default

N/A.

Usage Guidelines

This command implicitly defines this router to be a route reflector.

The peer group must be in the same AS of this router.

Example

The following command configures the peer group *outer* as a route reflector client:

```
configure bgp peer-group outer route-reflector-client
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group send-community

```
configure bgp peer-group <peer group> [send-community |
dont-send-community]
```

Description

Configures whether communities should be sent to neighbors as part of route updates.

Syntax Description

peer group	Specifies a peer group.
send-community	Specifies that communities are sent to neighbors as part of route updates.
dont-send-community	Specifies that communities are not sent to neighbors as part of route updates.

Default

N/A.

Usage Guidelines

These settings apply to the peer group and all neighbors of the peer group.

Example

The following command configures communities to be sent to neighbors as part of route updates:

```
configure bgp peer-group outer send-community
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group password

```
configure bgp peer-group <peer group> password {encrypted} [none |
<password>]
```

Description

Configures the password for a peer group and all neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
encrypted	Specifies an encrypted password.
none	Specifies no password.
password	Specifies a password.

Default

N/A.

Usage Guidelines

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:

- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example

The following command configures the password as *Extreme* for the peer group *outer* and its neighbors:

```
configure bgp peer-group outer password extreme
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group remote-AS-number

```
configure bgp peer-group <peer group> remote-AS-number <number>
```

Description

Configures the remote AS number for a peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
number	Specifies a remote AS number.

Default

N/A.

Usage Guidelines

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:

- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example

The following command configures the remote AS number for the peer group *outer* and its neighbors:

```
configure bgp peer-group outer remote-AS-number 65001
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group route-map-filter

```
configure bgp peer-group <peer group> route-map-filter [in | out] [none |
<routemap>
```

Description

Configures the route maps for a peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
in	Specifies to install the filter on the input side.
out	Specifies to install the filter on the output side.
none	Specifies to remove the filter.
route map	Specifies a route map.

Default

N/A.

Usage Guidelines

None.

Example

The following command configures the route map filter for the peer group *outer* and its neighbors using the access profile *nosales*:

```
configure bgp peer-group outer route-map-filter in nosales
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group soft-reset

```
configure bgp peer-group <peer group> soft-reset {[in | out]}
```

Description

Applies the current input/output routing policy to the neighbors in the peer group.

Syntax Description

peer group	Specifies a peer group.
in	Specifies to apply the input routing policy.
out	Specifies to apply the output routing policy.

Default

N/A.

Usage Guidelines

The input/output routing policy is determined by the NLRI-filter, AS-path-filter, and the route-map configured for the neighbors in the peer group on the input/output side of the router. This command does not affect configuration of the switch.

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:

- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example

The following command applies the current input routing policy to the neighbors in the peer group *outer*:

```
configure bgp peer-group outer soft-reset in
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group source-interface

```
configure bgp peer-group <peer group> source-interface [any | vlan <vlan
name>]
```

Description

Configures the source interface for a peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
any	Specifies any source interface.
name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:

- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example

The following command configures the source interface for the peer group *outer* and its neighbors on the VLAN *accounting*:

```
configure bgp peer-group outer source-interface accounting
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group timer

```
configure bgp peer-group <peer group> timer keep-alive <seconds> hold-time
<seconds>
```

Description

Configures the keepalive timer and hold timer values for a peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
keep-alive <seconds>	Specifies a keepalive time in seconds.
hold-time <seconds>	Specifies a hold-time in seconds.

Default

N/A.

Usage Guidelines

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:

- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example

The following command configures the keepalive timer and hold timer values for the peer group *outer* and its neighbors:

```
configure bgp peer-group outer timer keep-alive 30 hold-time 90
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp peer-group weight

```
configure bgp peer-group <peer group> weight <number>
```

Description

Configures the weight for the peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
number	Specifies a BGP peer group weight.

Default

N/A.

Usage Guidelines

BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example

The following command configures the weight for the peer group *outer* and its neighbors:

```
configure bgp peer-group outer weight 5
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure bgp routerid

```
configure bgp routerid <router identifier>
```

Description

Changes the router identifier.

Syntax Description

router identifier	Specifies a router identifier.

Default

N/A.

Usage Guidelines

BGP must be disabled before changing the router ID.

BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest router ID

Example

The following command changes the router ID:

```
configure bgp router-id 192.1.1.13
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure bgp soft-reconfiguration

```
configure bgp soft-reconfiguration
```

Description

Immediately applies the route map associated with the network command, aggregation, and redistribution.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command does not affect the switch configuration.

Example

The following command applies the route map associated with the network command, aggregation and redistribution:

```
configure bgp soft-reconfiguration
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

create bgp neighbor peer-group

```
create bgp neighbor <ip address> peer-group <peer group> {multi-hop}
```

Description

Creates a new neighbor and makes it part of the peer group.

Syntax Description

ip address	Specifies an IP address.
peer group	Specifies a peer group.
multi-hop	Specifies to allow connections to EBGP peers that are not directly connected.

Default

N / A.

Usage Guidelines

All the parameters of the neighbor are inherited from the peer group. The peer group should have the remote AS configured.

To add an existing neighbor to a peer group, use the following command:

```
configure bgp neighbor [<ip address> | all] peer-group <peer group> {acquire-all}
```

If you do not specify acquire-all, only the mandatory parameters are inherited from the peer group. If you specify acquire-all, all of the parameters of the peer group are inherited. This command disables the neighbor before adding it to the peer group.

Example

The following command creates a new neighbor and makes it part of the peer group *outer*:

```
create bgp neighbor 192.1.1.22 peer-group outer
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

create bgp neighbor remote-AS-number

```
create bgp neighbor <ip address> remote-AS-number <number> {multi-hop}
```

Description

Creates a new BGP peer.

Syntax Description

ip address	Specifies an IP address.
number	Specifies a remote AS number.
multi-hop	Specifies to allow connections to EBGP peers that are not directly connected.

Default

N / A.

Usage Guidelines

If the AS number is the same as the AS number provided in the `configure bgp as` command, then the peer is consider an IBGP peer, otherwise the neighbor is an EBGP peer. The BGP session to a newly created peer is not started until the `enable bgp neighbor` command is issued.

Example

The following command creates a new BGP peer:

```
create bgp neighbor 192.168.1.17 remote-AS-number 65001
```

History

This command was available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

create bgp peer-group

```
create bgp peer-group <name>
```

Description

Creates a new peer group.

Syntax Description

name	Specifies a peer group.

Default

N/A.

Usage Guidelines

You can use BGP peer groups to group together up to 200 BGP neighbors. All neighbors within the peer group inherit the parameters of the BGP peer group. The following mandatory parameters are shared by all neighbors in a peer group:

- remote AS
- source-interface
- out-nlri-filter
- out-aspath-filter
- out-route-map
- send-community
- next-hop-self

Each BGP peer group is assigned a unique name when the peer group is created.

Example

The following command creates a new peer group named *external*:

```
create bgp peer-group outer
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

delete bgp neighbor

```
delete bgp neighbor [<ip address> | all]
```

Description

Deletes one or all BGP neighbors.

Syntax Description

ip address	Specifies the IP address of the BGP neighbor to be deleted.
all	Specifies all neighbors.

Default

N/A.

Usage Guidelines

Use this command to delete one or all BGP neighbors.

Example

The following command deletes the specified BGP neighbor:

```
delete bgp neighbor 192.168.1.17
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

delete bgp peer-group

```
delete bgp peer-group <peer group>
```

Description

Deletes a peer group.

Syntax Description

peer group	Specifies a peer group.

Default

N/A.

Usage Guidelines

Use this command to delete a specific BGP peer group.

Example

The following command deletes the peer group named *external*:

```
delete bgp peer-group outer
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

disable bgp

```
disable bgp
```

Description

Disables BGP.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Use this command to disable BGP on the router.

Example

The following command disables BGP:

```
disable bgp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable bgp aggregation

```
disable bgp aggregation
```

Description

Disables BGP route aggregation.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

Use this command to disable BGP route aggregation.

Example

The following command disables BGP route aggregation:

```
disable bgp aggregation
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable bgp always-compare-med

```
disable bgp always-compare-med
```

Description

Disables Multi Exit Discriminator (MED) from being used in the route selection algorithm.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

MED is only used when comparing paths from the same AS. Use this command to disable the MED from being used when selecting a route.

Example

The following command disables MED from being used in the route selection algorithm:

```
disable bgp always-compare-med
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable bgp community format

```
disable bgp community format AS-number : number
```

Description

Disables the AS-number:number format of display for communities in the output of show and upload commands.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Using this command, communities are displayed as a single decimal value.

Example

The following command disables the AS-number:number format of display for communities:

```
disable bgp community format AS-number : number
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable bgp export

```
disable bgp export [direct | ospf | ospf-extern1 | ospf-extern2 |
ospf-inter | ospf-intra | isis | isis-level-1 | isis-level-1-external |
isis-level-2 | isis-level-2-external | rip | static | vip]
```

Description

Disables BGP from exporting routes from other protocols to BGP peers.

Syntax Description

direct	Specifies direct routing.
ospf	Specifies OSPF routing.
ospf-extern1	Specifies OSPF-extern1 routing.
ospf-extern2	Specifies OSPF-extern2 routing.
ospf-inter	Specifies OSPF-inter routing.
ospf-intra	Specifies OSPF-intra routing.
isis	Specifies IS-IS routing.
isis-level-1	Specifies IS-IS level 1 routing
isis-level-1-external	Specifies IS-IS level 1 external routing.
isis-level-2	Specifies IS-IS level 2 routing
isis-level-2-external	Specifies IS-IS level 2 external routing
rip	Specifies RIP routing.
static	Specifies static routing.
vip	Specifies VIP routing.

Default

Disabled.

Usage Guidelines

The exporting of routes between any two routing protocols is a discreet configuration function. For example, you must configure the switch to export routes from OSPF to BGP and, if desired, you must configure the switch to export routes from BGP to OSPF. You must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to BGP, and the routes to export from BGP to OSPF. Similarly for BGP and ISIS, or BGP and RIP.

You can use route maps to associate BGP attributes including Community, NextHop, MED, Origin, and Local Preference with the routes. Route maps can also be used to filter out exported routes.

Using the `export` command to redistribute routes complements the redistribution of routes using the `configure bgp add network` command. The `configure bgp add network` command adds the route to BGP only if the route is present in the routing table. The `enable bgp export` command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the `network` command take precedence over routes redistributed using the `export` command.

Example

The following command disables BGP from exporting routes from the OSPF protocol to BGP peers:

```
disable bgp export ospf
```

History

This command was first available in ExtremeWare 6.1.

The IS-IS options were added in ExtremeWare 7.0.0

Platform Availability

This command is available on all platforms.

disable bgp neighbor

```
disable bgp neighbor [<ip address> | all]
```

Description

Disables the BGP session.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.

Default

Disabled.

Usage Guidelines

After the session has been disabled, all the information in the route information base (RIB) for the neighbor is flushed.

Example

The following command disables the BGP session:

```
disable bgp neighbor 192.1.1.17
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable bgp neighbor remove-private-AS-numbers

```
disable bgp neighbor [<ip address> | all] remove-private-AS-numbers
```

Description

Disables the removal of private AS numbers from the AS path in route updates sent to EBGP peers.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.

Default

Disabled.

Usage Guidelines

Private AS numbers are AS numbers in the range 64512 through 65534. You can remove private AS numbers from the AS path attribute in updates that are sent to external BGP (EBGP) neighbors. Possible reasons for using private AS numbers include:

- The remote AS does not have officially allocated AS numbers.
- You want to conserve AS numbers if you are multi-homed to the local AS.

Private AS numbers should not be advertised on the Internet. Private AS numbers can only be used locally within an administrative domain. Therefore, when routes are advertised out to the Internet, the private AS number can be stripped out from the AS paths of the advertised routes using this feature.

Example

The following command disables the removal of private AS numbers from the AS path in route updates sent to the EBGP peers:

```
disable bgp neighbor 192.168.1.17 remove-private-AS-numbers
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable bgp neighbor soft-in-reset

```
disable bgp neighbor [all | <ip address>] soft-in-reset
```

Description

Disables the soft input reset feature.

Syntax Description

all	Specifies all neighbors.
ip address	Specifies an IP address.

Default

Disabled.

Usage Guidelines

Disabling the soft input reset feature can potentially limit the amount of system memory consumed by the RIB-in.

Example

The following command disables the soft input reset feature:

```
disable bgp neighbor 192.168.1.17 soft-in-reset
```

History

This command was available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable bgp peer-group

```
disable bgp peer-group <peer group> {soft-in-reset}
{remove-private-AS-numbers}
```

Description

Disables a BGP peer group and all the neighbors of the peer group.

Syntax Description

peer group	Specifies a peer group.
soft-in-reset	Specifies the soft input reset feature.
remove-private-AS-numbers	Specifies to remove private AS numbers.

Default

Disabled.

Usage Guidelines

You can use BGP peer groups to group together up to 200 BGP neighbors. All neighbors within the peer group inherit the parameters of the BGP peer group. The following mandatory parameters are shared by all neighbors in a peer group:

- remote AS
- source-interface
- out-nlri-filter
- out-aspath-filter
- out-route-map
- send-community
- next-hop-self

Example

The following command disables the BGP peer group *outer* and all of its neighbors:

```
disable bgp peer-group outer
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

disable bgp synchronization

```
disable bgp synchronization
```

Description

Disables the synchronization between BGP and IGP.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

When enabled, BGP waits for IGP to provide the exact same IP route before installing the route into the local forwarding database and advertising the route to an external neighbor.

Example

The following command disables the synchronization between BGP and IGP:

```
disable bgp synchronization
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable bgp

```
enable bgp
```

Description

Enables BGP.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command enables the Border Gateway Protocol (BGP) on the router. Before invoking this command, the local AS number and BGP router ID must be configured.

Example

The following command enables BGP:

```
enable bgp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable bgp aggregation

```
enable bgp aggregation
```

Description

Enables BGP route aggregation.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

To use BGP route aggregation, follow these steps:

1. Enable aggregation using the following command:

   ```
   enable bgp aggregation
   ```

2. Create an aggregate route using the following command:

   ```
   configure bgp add aggregate-address <ip address>/<mask length> {as-set | as-match}
   {summary-only} {advertise-route-map <route-map>} {attribute-route-map <route-map>}
   ```

Example

The following command enables BGP route aggregation:

```
enable bgp aggregation
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable bgp always-compare-med

```
enable bgp always-compare-med
```

Description

Enables BGP to use the Multi Exit Discriminator (MED) from neighbors in different autonomous systems (ASs) in the route selection algorithm.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

MED is only used when comparing paths from the same AS. A MED value of zero is treated as the lowest MED and therefore the most preferred route.

Example

The following command enables BGP to use the Multi Exit Discriminator (MED) from neighbors in different autonomous systems in the route selection algorithm:

```
enable bgp always-compare-med
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable bgp community format

```
enable bgp community format AS-number : number
```

Description

Enables the as-number:number format of display for the communities in the output of `show` and `upload` commands.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

If not enabled, the communities are displayed as a single decimal value.

Example

The following command enables the AS-number:number format of display for communities:

```
enable bgp community format AS-number : number
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable bgp export

```
enable bgp export [[direct | ospf | ospf-extern1 | ospf-extern2 |
ospf-inter | ospf-intra | isis | isis-level-1 | isis-level-1-external |
isis-level-2 | isis-level-2-external | rip | static | vip] {<route map>}
```

Description

Enables BGP to export routes from other protocols to BGP peers.

Syntax Description

direct	Specifies direct routing.
ospf	Specifies OSPF routing.
ospf-extern1	Specifies OSPF-extern1 routing.
ospf-extern2	Specifies OSPF-extern2 routing.
ospf-inter	Specifies OSPF-inter routing.
ospf-intra	Specifies OSPF-intra routing.
isis	Specifies IS-IS routing.
isis-level-1	Specifies IS-IS level 1 routing
isis-level-1-external	Specifies IS-IS level 1 external routing.
isis-level-2	Specifies IS-IS level 2 routing
isis-level-2-external	Specifies IS-IS level 2 external routing
rip	Specifies RIP routing.
static	Specifies static routing.
vip	Specifies VIP routing.
route map	Specifies a route map.

Default

Disabled.

Usage Guidelines

The exporting of routes between any two routing protocols is a discreet configuration function. For example, you must configure the switch to export routes from OSPF to BGP and, if desired, you must configure the switch to export routes from BGP to OSPF. You must first configure both protocols and then verify the independent operation of each. Then, you can configure the routes to export from OSPF to BGP, and the routes to export from BGP to OSPF. Similarly for BGP and ISIS, or BGP and RIP.

You can use route maps to associate BGP attributes including Community, NextHop, MED, Origin, and Local Preference with the routes. Route maps can also be used to filter out exported routes.

Using the `export` command to redistribute routes complements the redistribution of routes using the `configure bgp add network` command. The `configure bgp add network` command adds the route to BGP only if the route is present in the routing table. The `enable bgp export` command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the `network` command take precedence over routes redistributed using the `export` command.

Example

The following command enables BGP to export routes from the OSPF protocol to BGP peers:

```
enable bgp export ospf
```

History

This command was first available in ExtremeWare 6.1.

The IS-IS options were added in ExtremeWare 7.0.0

Platform Availability

This command is available on all platforms.

enable bgp neighbor

```
enable bgp neighbor [<ip address> | all]
```

Description

Enables the BGP session. The neighbor must be created before the BGP neighbor session can be enabled.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.

Default

Disabled.

Usage Guidelines

To create a new neighbor and add it to a BGP peer group, use the following command:

```
create bgp neighbor <ip address> peer-group <peer group> {multi-hop}
```

Example

The following command enables the BGP neighbor session:

```
enable bgp neighbor 192.168.1.17
```

History

This command was available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable bgp neighbor remove-private-AS-numbers

```
enable bgp neighbor [<ip address> | all] remove-private-AS-numbers
```

Description

Enables the removal of private AS numbers from the AS path in route updates sent to EBGP peers.

Syntax Description

ip address	Specifies an IP address.
all	Specifies all neighbors.

Default

Disabled.

Usage Guidelines

Private AS numbers are AS numbers in the range 64512 through 65534. You can remove private AS numbers from the AS path attribute in updates that are sent to external BGP (EBGP) neighbors. Possible reasons for using private AS numbers include:

- The remote AS does not have officially allocated AS numbers.
- You want to conserve AS numbers if you are multi-homed to the local AS.

Private AS numbers should not be advertised on the Internet. Private AS numbers can only be used locally within an administrative domain. Therefore, when routes are advertised out to the Internet, the routes can be stripped out from the AS paths of the advertised routes using this feature.

Example

The following command enables the removal of private AS numbers from the AS path in route updates sent to the EBGP peers:

```
enable bgp neighbor 192.168.1.17 remove-private-AS-numbers
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable bgp neighbor soft-in-reset

```
enable bgp neighbor [all | <ip address>] soft-in-reset
```

Description

Enables the soft input reset feature.

Syntax Description

all	Specifies all neighbors.
ip address	Specifies an IP address.

Default

Disabled.

Usage Guidelines

Disabling the soft input reset feature can potentially limit the amount of system memory consumed by the RIB-in.

Example

The following command enables the soft recognition feature:

```
enable bgp neighbor 192.168.1.17 soft-in-reset
```

History

This command was available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable bgp peer-group

```
enable bgp peer-group <peer group> {soft-in-reset}
{remove-private-AS-numbers}
```

Description

Enables a peer group and all the neighbors of a peer group.

Syntax Description

peer group	Specifies a peer group.
soft-in-reset	Specifies the soft recognition feature.
remove-private-AS-numbers	Specifies to remove private AS numbers.

Default

Disabled.

Usage Guidelines

You can use BGP peer groups to group together up to 200 BGP neighbors. All neighbors within the peer group inherit the parameters of the BGP peer group. The following mandatory parameters are shared by all neighbors in a peer group:

- remote AS
- source-interface
- out-nlri-filter
- out-aspath-filter
- out-route-map
- send-community
- next-hop-self

Example

The following command enables the BGP peer group *outer* and all its neighbors:

```
enable bgp peer-group outer
```

History

This command was available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

enable bgp synchronization

```
enable bgp synchronization
```

Description

Enables synchronization between BGP and IGP.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

When enabled, BGP waits for IGP to provide the exact same route before advertising the BGP route to an external neighbor.

Example

The following command enables synchronization between BGP and IGP:

```
enable bgp synchronization
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show bgp

```
show bgp
```

Description

Displays BGP configuration information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Displays information such as AS number, router ID, local preference, sync flag, route reflection, cluster ID, confederation ID, and AS redistributed networks.

Example

The following command displays BGP configuration information:

```
show bgp
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

show bgp neighbor

```
show bgp neighbor <ip address> {[accepted-routes | flap-statistics |
received-routes | rejected-routes | suppressed-routes | transmitted-routes]
{detail} [community [access-profile <access profile> | no-advertise |
no-export | no-export-subconfed | number <community number> |
<autonomous system id>:<bgp community>] | as-path [<as-path-expression> |
access-profile <access profile>] | route-map <route map> | network <ip
address>/<mask> {exact} | all]}
```

Description

Displays information about a specified neighbor.

Syntax Description

ip address	Specifies an IP address that identifies a BGP neighbor.
accepted-routes	Specifies that only accepted routes should be displayed.
flap-statistics	Specifies that only flap-statistics should be displayed (for route flap dampening enabled routes).
received-routes	Specifies that only received routes should be displayed.
rejected-routes	Specifies that only rejected routes should be displayed.
suppressed-routes	Specifies that only suppressed routes should be displayed (for route flap dampening enabled routes).
transmitted-routes	Specifies that only transmitted routes should be displayed.
detail	Specifies to display the information in detailed format.
access profile	Specifies an access profile used as a community attribute.
no-advertise	Specifies the no-advertise community attribute.
no-export	Specifies the no-export community attribute.
no-export-subconfed	Specifies the no-export-subconfed community attribute.
community number	Specifies a community number.
autonomous system id	Specifies an autonomous system ID (0-65535).
access profile	Specifies an access profile.
route map	Specifies a route map.
ip address	Specifies an IP address.
mask	Specifies a subnet mask (number of bits).
exact	Specifies an exact match with the IP address and subnet mask.
all	Specifies all routes.

Default

N/A.

Usage Guidelines

Use this command to display information about a specific BGP neighbor. If you do not specify a neighbor, information about all neighbors is displayed.

Example

The following command displays information about a specified neighbor:

```
show bgp neighbor 10.10.10.10
```

Following is the output from this command:

```
IBGP Peer: 10.10.10.10  As: 14490  Enabled: Yes  Router: Enabled  Weight: 1
ConnectRetry: 120   HoldTimeCfg: 180   KeepaliveCfg: 60   MinAsOrig:15
Source Interface: Not configured  RRClient: No  EBGP-Multihop: No
NextHopSelf: Enabled Send Communities: No Soft Input Reconfiguration: Disabled
Max-Prefix: 100000 Threshold: 75 Teardown: Yes(HoldInt: 300) SendTraps: No
Remove Private AS : No
IN NLRI Filter     : None
OUT NLRI Filter    : None
IN AS-Path Filter  : None
OUT AS-Path Filter : None
IN ROUTE-MAP       : None
OUT ROUTE-MAP      : None
State: IDLE(Reached maximum prefix limit)
RemoteAddr:10.10.10.10:179 LocalAddr:10.10.10.51:1024 PeerRtrId:0.0.0.0
InUpdates: 26549  OutUpdates(InQ): 0(0)  InTotalMsgs: 26559  OutTotalMsgs: 9
InUpdateElapsedTime: 0:0:00:20  InMsgElapsedTime: 0:0:00:20  InPrefix: 0
HoldTime: 180  KeepAlive: 60  FsmTransitions: 1  RestartAfter: 0:04:43
FSM Down since: Mon Apr 1 15:59:42 2002 (Duration: 0:0:00:17)
LastErr: 0/0
```

History

This command was available in ExtremeWare 6.1.

This command was modified in ExtremeWare 6.2.2 to include information about maximum prefix settings.

This command was modified in ExtremeWare 7.0.0 to show flap statistics and suppressed routes for BGP route flap dampening.

Platform Availability

This command is available on all platforms.

show bgp peer-group

```
show bgp peer-group {detail | <peer group> {detail}}
```

Description

Displays the peer groups configured in the system.

Syntax Description

detail	Specifies to display the information in detailed format.
peer group	Specifies a peer group.
detail	Specifies to display the information in detailed format.

Default

N / A.

Usage Guidelines

If the `detail` keyword is specified then the parameters of the neighbors in the peer group, which are different from the ones that are configured in the peer group, will be displayed.

If no peer group name is specified, all the peer group information will be displayed.

Example

The following command displays the peer groups configured in the system:

```
show bgp peer-group detail
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

show bgp routes

```
show bgp routes [all | as-path <as-path-expression> | community <number> |
detail | network <ip address>/<mask> {exact} | route-map <route map> ]
```

Description

Displays the BGP route information base (RIB).

Syntax Description

all	Specifies all routes.
as-path-expression	Specifies an AS path.
number	Specifies a community number.
detail	Specifies to display the information in detailed format.
ip address	Specifies an IP address.
mask	Specifies a subnet mask (number of bits).
exact	Specifies an exact match with the IP address and subnet mask.
route map	Specifies a route map.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the BGP route information base (RIB):

```
show bgp routes all
```

History

This command was available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

19 IP Multicast Commands

IP multicast routing is a function that allows a single IP host to send a packet to a group of IP hosts. This group of hosts can include devices that reside on the local network, within a private network, or outside of the local network.

IP multicast routing consists of the following functions:

- A router that can forward IP multicast packets
- A router-to-router multicast protocol [for example, Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM)]
- A method for the IP host to communicate its multicast group membership to a router [for example, Internet Group Management Protocol (IGMP)]

NOTE

You must configure IP unicast routing before you configure IP multicast routing.

IGMP is a protocol used by an IP host to register its IP multicast group membership with a router. Periodically, the router queries the multicast group to see if the group is still in use. If the group is still active, a single IP host responds to the query, and group registration is maintained.

IGMP is enabled by default on the switch. However, the switch can be configured to disable the generation of period IGMP query packets. IGMP query should be enabled when the switch is configured to perform IP unicast or IP multicast routing.

Distance Vector Multicast Routing Protocol (DVMRP) is a distance-vector protocol that is used to exchange routing and multicast information between routers. Like RIP, DVMRP periodically sends the entire routing table to its neighbors.

DVMRP has a mechanism (flood and prune) that allows it to prune and graft multicast trees to reduce the bandwidth consumed by IP multicast traffic.

Protocol Independent Multicast (PIM) is a multicast routing protocol with no inherent route exchange mechanism. The switch supports dense mode and sparse mode operation. You can configure dense mode or sparse mode on a per-interface basis. After they are enabled, some interfaces can run dense mode, while others run sparse mode.

PIM Dense Mode

Protocol Independent Multicast-Dense Mode (PIM-DM) is a multicast routing protocol that is similar to DVMRP. PIM-DM routers perform reverse path multicasting (RPM). However, instead of exchanging its own unicast route tables for the RPM algorithm, PIM-DM uses the existing unicast route table for the reverse path. As a result, PIM-DM requires less system memory.

PIM-DM is a broadcast and prune protocol. Using PIM-DM, multicast routes are pruned and grafted in a similar way as DVMRP.

PIM Sparse Mode (PIM-SM)

Unlike PIM-DM, PIM-SM is an explicit join and prune protocol, and it supports shared trees as well as shortest path trees (SPTs). The routers must explicitly join the group(s) in which they are interested in becoming a member, which is beneficial for large networks that have group members who are sparsely distributed.

Using PIM-SM, the router sends a join message to the rendezvous point (RP). The RP is a central multicast router that is responsible for receiving and distributing multicast packets. By default, the RP is selected dynamically (but not automatically). You can also define a static RP in your network, using the following command:

```
configure pim crp static <rp address>
```

When a router has a multicast packet to distribute, it encapsulates the packet in a unicast message and sends it to the RP. The RP decapsulates the multicast packet and distributes it among all member routers.

When a router determines that the multicast rate from of a particular group has exceeded a configured threshold, that router can send an explicit join to the originating router. When this occurs, the receiving router gets the multicast directly from the sending router, and bypasses the RP.

NOTE

You can run either PIM-DM or PIM-SM per VLAN.

PIM Mode Interoperation

An Extreme Networks switch can function as a PIM multicast border router (PMBR). A PMBR integrates PIM-SM and PIM-DM traffic.

When forwarding PIM-DM traffic into a PIM-SM network, the PMBR notifies the RP that the PIM-DM network exists. The PMBR forwards PIM-DM multicast packets to the RP, which in turn forwards the packets to those routers that have joined the multicast group.

The PMBR also forwards PIM-SM traffic to a PIM-DM network. The PMBR sends a join message to the RP and the PMBR floods traffic from the RP into the PIM-DM network.

No commands are needed to enable PIM mode interoperation. PIM mode translation is automatically enabled when a dense mode interface and a sparse mode interface are enabled on the same switch.

clear igmp group

```
clear igmp group {vlan <vlan name>}
```

Description

Removes one or all IGMP groups.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

This command can be used by network operations to manually remove IGMP group entries instantly.

Example

The following command clears IGMP groups from VLAN *accounting*:

```
clear igmp group accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

clear igmp snooping

```
clear igmp snooping {vlan <vlan name>}
```

Description

Removes one or all IGMP snooping entries.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

This command can be used by network operations to manually remove IGMP snooping entries instantly. However, removing an IGMP snooping entry can disrupt the normal forwarding of multicast traffic.

The static IGMP snooping entry will not be removed. The dynamic IGMP snooping entry will be removed, then re-created upon the next general query.

Example

The following command clears IGMP snooping from VLAN *accounting*:

```
clear igmp snooping accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

clear ipmc cache

```
clear ipmc cache {<IP multicast group> {<source IP address>/<netmask>}}
```

Description

Resets the IP multicast cache table.

Syntax Description

IP multicast group	Specifies a group address.
source IP address	Specifies a source IP address.
netmask	Specifies a subnet mask.

Default

If no options are specified, all IP multicast cache entries are flushed.

Usage Guidelines

This command can be used by network operators to manually remove IPMC hardware forwarding cache entries instantly. If the source is available, caches will be re-created, otherwise caches are removed permanently. This command can disrupt the normal forwarding of multicast traffic.

Example

The following command resets the IP multicast table for group *224.1.2.3*:

```
clear ipmc cache 224.1.2.3
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

clear ipmc fdb

```
clear ipmc fdb {group <ip address> {sender <ip address> / <netmask>}}
```

Description

Resets the IP multicast forwarding database entry.

Syntax Description

ip address	Specifies an IP address.
netmask	Specifies a netmask.

Default

N/A.

Usage Guidelines

If no options are specified, all IP multicast forwarding database entries are cleared. This command has an effect similar to the command `clear ipmc cache`, except that the targets are the forwarding database entries.

Example

The following command resets the IP multicast forwarding database entry:

```
clear ipmc fdb group 10.0.0.1 sender 10.0.0.2/24
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure dvmrp add vlan

```
configure dvmrp add vlan [<vlan name> | all]
```

Description

Enables DVMRP on one or all IP interfaces.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

Disabled.

Usage Guidelines

If `all` is specified, DVMRP is enabled on all IP interfaces. When an IP interface is created, DVMRP is disabled by default.

Example

The following command enables DVMRP on the VLAN *accounting*:

```
configure dvmrp add vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure dvmrp delete vlan

```
configure dvmrp delete vlan [<vlan name> | all]
```

Description

Disables DVMRP on one or all IP interfaces.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

Disabled.

Usage Guidelines

If `all` is specified, DVMRP is disabled on all IP interfaces.

Example

The following command disables DVMRP on the VLAN *accounting:*

```
configure dvmrp delete vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure dvmrp timer

```
configure dvmrp timer <route-report-interval> <route-replacement-time>
```

Description

Configures the global DVMRP timers.

Syntax Description

route-report-interval	Specifies the time in seconds between transmission of periodic report packets.
route-replacement-time	Specifies a time in seconds before a route becomes unreachable.

Default

- route-report-interval default—60 seconds.
- route-replacement-time default—140 seconds.

Usage Guidelines

Specify the following:

- route-report-interval—The amount of time the system waits between transmitting periodic route report packets. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 60 seconds. Because triggered update is always enabled, the route report will always be transmitted prior to the expiration of the route report interval.
- route-replacement-time—The route expiration time, commonly called route timeout. Initially it is 2 x route-report-interval +20 (2 x 60 + 20 = 140). It is the time for a particular DVMRP route to expire, while the route hold-down time is initially 2 x route-report-interval (2 x 60 = 120) which is the time before a route gets removed from advertisement after it has been expired. The range is 1 to 2,147,483,647 seconds (68 years).

Example

The following command configures the DVMRP timers:

```
configure dvmrp timer 300 620
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure dvmrp vlan cost

```
configure dvmrp vlan [<vlan name> | all] cost <cost>
```

Description

Configures the cost (metric) of the interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
cost	Specifies a cost metric.

Default

The default setting is 1.

Usage Guidelines

The cost range is 1 - 32.

Example

The following command configures the cost (metric) of the interface on the VLAN accounting:

```
configure dvmrp vlan accounting cost 5
```

History

This command was available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure dvmrp vlan export-filter

```
configure dvmrp vlan [<vlan name> | all] export-filter [<access profile> |
none]
```

Description

Configures DVMRP to filter out certain routes when performing the route advertisement.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access profile name.
none	Deletes any associated filter.

Default

None.

Usage Guidelines

Use this command to filter out certain routes when performing the route advertisement. The filtered routes are specified in an access profile.

Example

The following command configures DVMRP to filter out routes according to the *nosales* access profile:

```
configure dvmrp vlan accounting export-filter nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure dvmrp vlan import-filter

```
configure dvmrp vlan [<vlan name> | all] import-filter [<access profile> |
none]
```

Description

Configures DVMRP to filter certain routes received from its neighbor, and uses an access profile to determine which DVMRP routes are accepted as valid routes.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access profile name.
none	Deletes any associated filter.

Default

None.

Usage Guidelines

Use this command to filter out certain routes when accepting routes from its neighbors. The filtered routes are specified in an access profile.

Example

The following command configures DVMRP to use the *nosales* access profile to determine which DVMRP routes are to accept:

```
configure dvmrp vlan accounting import-filter nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure dvmrp vlan trusted-gateway

```
configure dvmrp vlan [<vlan name> | all] trusted-gateway [<access profile>
| none]
```

Description

Configures DVMRP to use the access policy to determine which DVMRP neighbor is trusted and to receive routes from.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access profile name.
none	Specifies that all neighbors are trusted (no neighbors are compared to an access profile).

Default

None (all neighbors are trusted).

Usage Guidelines

Using this command to specify trusted versus non-trusted neighbors.

Example

The following command configures DVMRP to use the *nosales* access policy to determine which DVMRP neighbor is trusted and to receive routes from:

```
configure dvmrp vlan accounting trusted-gateway nosales
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure dvmrp vlan timer

```
configure dvmrp vlan <vlan name> timer <probe interval> <neighbor timeout>
```

Description

Configures DVMRP interface timers.

Syntax Description

vlan name	Specifies a VLAN name.
probe interval	Specifies the time in seconds between probe messages.
neighbor timeout	Specifies the time in seconds before a neighbor router is declared to be down.

Default

The probe interval default setting is 10 seconds. The neighbor timeout default setting is 35 seconds.

Usage Guidelines

Specify the following:

- probe interval—The amount of time that the system waits between transmitting DVMRP probe messages. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 10 seconds.
- neighbor timeout—The amount of time before a DVMRP neighbor router is declared to be down. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 35 seconds (3.5 * probe interval).

Example

The following command configures the DVMRP timers:

```
configure dvmrp vlan accounting timer 3000 9000
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure igmp

```
configure igmp <query interval> <query response interval> <last member
query interval>
```

Description

Configures the Internet Group Management Protocol (IGMP) timers.

Syntax Description

query interval	Specifies the interval (in seconds) between general queries.
query response interval	Specifies the maximum query response time (in seconds).
last member query interval	Specifies the maximum group-specific query response time (in seconds).

Default

- query interval—125 seconds
- query response interval—10 seconds
- last member query interval—1 second

Usage Guidelines

Timers are based on RFC2236. Specify the following:

- query interval—The amount of time, in seconds, the system waits between sending out general queries. The range is 1 to 429,496,729 seconds.
- query response interval—The maximum response time inserted into the periodic general queries. The range is 1 to 25 seconds.
- last member query interval—The maximum response time inserted into a group-specific query sent in response to a leave group message. The range is 1 to 25 seconds.

Example

The following command configures the IGMP timers:

```
configure igmp 100 5 1
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure igmp snooping add static group

```
configure igmp snooping vlan <vlan name> ports <portlist> add static
group <ip address>
```

Description

Configures VLAN ports to receive the traffic from a multicast group, even if no IGMP joins have been received on the port.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
ip address	Specifies the multicast group IP address.

Default

None.

Usage Guidelines

Use this command to forward a particular multicast group to VLAN ports. In effect, this command emulates a host on the port that has joined the multicast group. As long as the port is configured with the static entry, multicast traffic for that multicast group will be forwarded to that port.

The switch sends proxy IGMP messages in place of those generated by a real host. The proxy messages use the VLAN IP address for source address of the messages. If the VLAN has no IP address assigned, the proxy IGMP message will use 0.0.0.0 as the source IP address.

The multicast group should be in the class-D multicast address space, but should not be in the multicast control subnet range (224.0.0.x/24).

If the ports also have an IGMP filter configured, the filter entries take precedence. IGMP filters are configured using the command:

```
configure igmp snooping vlan <vlan name> ports <portlist> filter <access
profile>
```

Example

The following command configures a static IGMP entry so the multicast group 224.34.15.37 will be forwarded to VLAN *marketing* on ports 2:1-2:4:

```
configure igmp snooping marketing ports 2:1-2:4 add static group 224.34.15.37
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure igmp snooping delete static group

```
configure igmp snooping vlan <vlan name> ports <portlist> delete static
group [<ip address> | all]
```

Description

Removes the port configuration that causes multicast group traffic to be forwarded, even if no IGMP leaves have been received on the port.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
ip address	Specifies the multicast group IP address.
all	Delete all the static groups.

Default

None.

Usage Guidelines

Use this command to remove an entry created by the following command:

```
configure igmp snooping vlan <vlan name> ports <portlist> add static
group <group address>
```

Example

The following command removes a static IGMP entry that forwards the multicast group 224.34.15.37 to the VLAN *marketing* on ports 2:1-2:4:

```
configure igmp marketing ports 2:1-2:4 delete static group 224.34.15.37
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure igmp snooping add static router

```
configure igmp snooping vlan <vlan name> ports <portlist> add static router
```

Description

Configures VLAN ports to forward the traffic from all multicast groups, even if no IGMP joins have been received on the port.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

None.

Usage Guidelines

Use this command to forward all multicast groups to the specified VLAN ports. In effect, this command emulates a multicast router attached to those ports. As long as the ports are configured with the static entry, all available multicast traffic will be forwarded to those ports.

Example

The following command configures a static IGMP entry so all multicast groups will be forwarded to VLAN *marketing* on ports 2:1-2:4:

```
configure igmp snooping marketing ports 2:1-2:4 add static router
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure igmp snooping delete static router

```
configure igmp snooping vlan <vlan name> ports <portlist> delete static
router
```

Description

Removes the configuration that causes VLAN ports to forward the traffic from all multicast groups, even if no IGMP joins have been received on the port.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

None.

Usage Guidelines

Use this command to remove the static IGMP entry created with the following command:

```
configure igmp snooping vlan <vlan name> ports <portlist> add static router
```

Example

The following command removes the static IGMP entry that caused all multicast groups to be forwarded to VLAN *marketing* on ports 2:1-2:4:

```
configure igmp snooping marketing ports 2:1-2:4 delete static router
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure igmp snooping filter

```
configure igmp snooping vlan <vlan name> ports <portlist> filter [<access
profile> | none]
```

Description

Configures an IGMP snooping access profile filter on VLAN ports.

Syntax Description

vlan name	Specifies a VLAN name.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
access profile	Specifies an access profile for the ports.

Default

None.

Usage Guidelines

Use this command to filter multicast groups to the specified VLAN ports.

The access profile specified in this command must only include IP address type entries, and the IP addresses included in the entries must be in the class-D multicast address space, but should not be in the multicast control subnet range (224.0.0.x/24).

To remove IGMP snooping filtering from a port, use the none keyword version of the command.

Example

The following command configures the access profile *ap_multicast* to filter multicast packets forwarded to VLAN *marketing* on ports 2:1-2:4:

```
configure igmp snooping marketing ports 2:1-2:4 filter ap_multicast
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

configure igmp snooping flood-list

```
configure igmp snooping flood-list [<access profile> | none]
```

Description

Configures certain multicast addresses to be slow path flooded within the VLAN.

Syntax Description

access profile	Specifies an access profile with a list of multicast addresses to be handled. The access profile must be type IP address.
none	Specifies no access profile is to be used.

Default

None.

Usage Guidelines

With this command, a user can configure certain multicast addresses to be slow path flooded within the VLAN, which otherwise will be fast path forwarded according to IGMP and/or layer 3 multicast protocol.

The specified access profile `<access profile>` should contain a list of addresses which will determine if certain multicast streams are to be treated specially. Typically, if the switch receives a stream with destination address which is in the `<access profile>` in 'permit' mode, that stream will be software flooded and no hardware entry would be installed.

The specified access profile must be type IP address.

When adding an IP address into the access-profile, a 32-bit host address is recommended.

This feature is meant to solve the multicast connectivity problem for unknown destination addresses within system reserved ranges. Specifically this feature was introduced to solve the problem of recognizing certain stream as control packets.

NOTE

The switch will not validate any IP address in the access profile used in this command. Therefore, slow-path flooding should be used only for streams which are very infrequent, such as control packets. It should not be used for multicast data packets. This option overrides any default mechanism of hardware forwarding (with respect to IGMP, PIM, or DVMRP) so it should be used with caution.

Slow path flooding will be done within the L2 VLAN only.

Use the none option to effectively disable slow path flooding.

You can use the `show ipconfig` command to see the configuration of slow path flooding. It will be listed in the IGMP snooping section of the display.

Example

Given access profile *access1* created as follows:

```
create access-profile access1 type ipaddress
configure access-profile access1 add ipaddress 224.1.0.1/32
```

The following command configures the multicast data stream specified in *access1* for slow path flooding:

```
configure igmp snooping flood-list access1
```

The following command specifies that no access profile is to be used, this effectively disabling slow path flooding:

```
configure igmp snooping flood-list none
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure igmp snooping leave-timeout

```
configure igmp snooping leave-timeout <leave_time ms>
```

Description

Configures the IGMP snooping leave timeout.

Syntax Description

leave_time ms	Specifies an IGMP leave timeout value in milliseconds.

Default

1000 ms.

Usage Guidelines

The range is 0 - 10000 ms (10 seconds). For timeout values of one second or less, you must set the leave-timeout to a multiple of 100 ms. For values of more than one second, you must set the leave-timeout to a multiple of 1000 ms (one second).

The specified time is the maximum leave timeout value. The switch could leave sooner if an IGMP leave message is received before the timeout occurs.

Example

The following command configures the IGMP snooping leave timeout:

```
configure igmp snooping leave-timeout 10000
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure igmp snooping timer

```
configure igmp snooping timer <router timeout> <host timeout>
```

Description

Configures the IGMP snooping timers.

Syntax Description

router timeout	Specifies the time in seconds between router discovery.
host timeout	Specifies the time in seconds between host reports

Default

The router timeout default setting is 260 seconds. The host timeout setting is 260 seconds.

Usage Guidelines

Timers should be set to approximately 2.5 times the router query interval in use on the network. Specify the following:

- router timeout—The interval, in seconds, between the last time the router was discovered and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds.
- host timeout—The interval, in seconds, between the last IGMP group report message from the host and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds.

IGMP snooping is a layer 2 function of the switch. It does not require multicast routing to be enabled. The feature reduces the flooding of IP multicast traffic. IGMP snooping optimizes the usage of network bandwidth and prevents multicast traffic from being flooded to parts of the network that do not need it. The switch does not reduce any IP multicast traffic in the local multicast domain (224.0.0.x).

IGMP snooping is enabled by default on the switch. If you are using multicast routing, IGMP snooping can be enabled or disabled (in versions of ExtremeWare previous to 7.0.0, IGMP snooping must have been enabled for multicast routing). If IGMP snooping is disabled, all IGMP and IP multicast traffic floods within a given VLAN. IGMP snooping expects at least one device on every VLAN to periodically generate IGMP query messages. Without an IGMP querier, the switch eventually stops forwarding IP multicast packets to any port, because the IGMP snooping entries will time out, based on the value specified in `host timeout`. An optional optimization for IGMP snooping is the strict recognition of routers only if the remote devices are running a multicast protocol.

Example

The following command configures the IGMP snooping timers:

```
configure igmp snooping timer 600 600
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

configure pim add vlan

```
configure pim add vlan [<vlan name> | all] {dense | sparse}
```

Description

Enables PIM on an IP interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
dense	Specifies PIM dense mode (PIM-DM).
sparse	Specifies PIM sparse mode (PIM-SM).

Default

Dense.

Usage Guidelines

When an IP interface is created, per-interface PIM configuration is disabled by default.

The switch supports both dense mode and sparse mode operation. You can configure dense mode or sparse mode on a per-interface basis. After they are enabled, some interfaces can run dense mode, while others run sparse mode.

Example

The following command enables PIM-DM multicast routing on VLAN *accounting*:

```
configure pim add vlan accounting dense
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure pim cbsr

```
configure pim cbsr [vlan <vlan name> {<priority [0-254]> | none]
```

Description

Configures a candidate bootstrap router for PIM sparse-mode operation.

Syntax Description

vlan name	Specifies a VLAN name.
priority	Specifies a priority setting. The range is 0 - 254.
none	Specifies to delete a CBSR.

Default

The default setting for priority is 0, and indicates the lowest priority.

Usage Guidelines

The VLAN specified for CBSR must have IPMC forwarding enabled for PIM sparse mode.

Example

The following command configures a candidate bootstrap router on the VLAN *accounting*:

```
configure pim cbsr vlan accounting 30
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure pim crp static

```
configure pim crp static <rp address> [none | <access profile>] {<priority
[0-254]>}
```

Description

Configures a rendezvous point and its associated groups statically, for PIM sparse mode operation.

Syntax Description

rp address	Specifies a rendezvous point address.
none	Deletes the static rendezvous point.
access profile	Specifies an access profile name.
priority	Specifies a priority setting. The range is 0 - 254.

Default

The default setting for priority is 0, which indicates highest priority.

Usage Guidelines

Using PIM-SM, the router sends a join message to the rendezvous point (RP). The RP is a central multicast router that is responsible for receiving and distributing multicast packets. If you use a static RP, all switches in your network must be configured with the same RP address for the same group (range).

The access profile contains a list of multicast group accesses served by this RP.

Example

The following command statically configures an RP and its associated groups defined in access profile *rp-list*:

```
configure pim crp static 10.0.3.1 rp-list
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all platforms.

configure pim crp timer

```
configure pim crp timer <crp advertisement interval>
```

Description

Configures the candidate rendezvous point advertising interval for PIM sparse mode operation.

Syntax Description

crp advertisement interval	Specifies a candidate rendezvous point advertising interval in seconds.

Default

The default is 60 seconds.

Usage Guidelines

None.

Example

The following command configures the candidate rendezvous point advertising interval to 120 seconds:

```
configure pim crp timer 120
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure pim crp vlan access profile

```
configure pim crp vlan <vlan name> [none | <access profile>] {<priority>}
```

Description

Configures the dynamic candidate rendezvous point for PIM sparse-mode operation.

Syntax Description

vlan name	Specifies a VLAN name.
none	Specifies no access profile.
access profile	Specifies an access profile name.
priority	Specifies a priority setting. The range is 0 - 254.

Default

The default setting is for priority is 0 and indicates the highest priority.

Usage Guidelines

The access profile contains the list of multicast group accesses serviced by this RP. To delete a CRP, use the keyword none as the access policy.

The VLAN specified for CBSR must have IPMC forwarding enabled for PIM sparse mode.

Example

The following command configures the candidate rendezvous point for PIM sparse-mode operation on the VLAN *HQ_10_0_3* with the access profile *rp-list* and priority set to 30:

```
configure pim crp HQ_10_0_3 rp-list 30
```

History

This command was available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

configure pim delete vlan

```
configure pim delete vlan [<vlan name> | all]
```

Description

Disables PIM on an interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables PIM-DM on VLAN *accounting*:

```
configure pim delete vlan accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure pim register-rate-limit-interval

```
configure pim register-rate-limit-interval <time>
```

Description

Configures the initial PIM-SM periodic register rate.

Syntax Description

time	Specifies an interval time in seconds. Range is 0 - 60. Default is 0.

Default

Default is 0.

Usage Guidelines

Configuring a non-zero interval time can reduce the CPU load on the first hop in case register stop messages are not received normally.

If a non-zero value is configured, the first hop switch would send register messages only at `time` second intervals. The default value is zero, which sends continuos register messages. This command takes effect only until the register stop message is not received, in other words, when the register suppression timer is not running.

Example

The following command configures the initial PIM register rate limit interval:

```
configure pim register-rate-limit-interval 2
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure pim register-suppress-interval register-probe-interval

```
configure pim register-suppress-interval <time> register-probe-interval
<time>
```

Description

Configures an interval for periodically sending null-registers.

Syntax Description

register-suppress-interval <time>	Specifies an interval time in seconds. Range is 30 - 200 seconds. Default is 60.
register-probe-interval <time>	Specifies an interval time in seconds. Default is 5.

Default

The following defaults apply:

- register-suppress-interval—60
- register-probe-interval—5

Usage Guidelines

The register-probe-interval time should be set less than the register-suppress-interval time. By default, a null register is sent every 55 seconds (*register-suppress-interval - register-probe-interval*). A response to the null register is expected within register probe interval. By specifying a larger interval, a CPU peak load can be avoided because the null-registers are generated less frequently. The register probe time should be less than half of the register suppress time, for best results.

Example

The following command configures the register suppress interval and register probe time:

```
configure pim register-suppress-interval 90 register-probe time 10
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure pim register-checksum-to

```
configure pim register-checksum-to [include-data | exclude-data]
```

Description

Configures the checksum computation to either include data (for compatibility with Cisco Systems products) or to exclude data (for RFC-compliant operation), in the register message.

Syntax Description

include-data	Specifies to include data.
exclude-data	Specifies to exclude data.

Default

Include data

Usage Guidelines

None.

Example

The following command configures the checksum mode to include data for compatibility with Cisco Systems products:

```
configure pim register-checksum-to include-data
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure pim spt-threshold

```
configure pim spt-threshold <last hop router threshold> {<rp threshold>}
```

Description

Configures the threshold, in kbps, for switching to SPT. On leaf routers, this setting is based on data packets. On the RP, this setting is based on register packets.

Syntax Description

last hop router threshold	Specifies a last hop router threshold.
rp threshold	Specifies an RP threshold.

Default

The default setting is 0.

Usage Guidelines

For the best performance leveraged by hardware forwarding, use default value “0,0”, or small values below 16. From release 6.2.2 onwards, since the RP learns the source address from the register message, the RP threshold has no effect.

Example

The following command sets the threshold for switching to SPT:

```
configure pim spt-threshold 4 16
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure pim timer vlan

```
configure pim timer <hello interval> <join prune interval> vlan [<vlan
name>]
```

Description

Configures the global PIM timers.

Syntax Description

hello interval	Specifies the amount of time before a hello message is sent out by the PIM router. The range is 1 to 65,519 seconds.
join prune interval	Specifies the join/prune interval. The range is 1 to 65,519 seconds.
vlan name	Specifies a VLAN name.

Default

- hello interval—30 seconds.
- join prune interval—60 seconds.

Usage Guidelines

None.

Example

The following command configures the global PIM timers on the VLAN *accounting*:

```
configure pim timer 150 300 vlan accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

configure pim vlan trusted-gateway

```
configure pim vlan [<vlan name> | all] trusted-gateway [<access profile> |
none]
```

Description

Configures a trusted neighbor policy.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
access profile	Specifies an access profile name.
none	Specifies no access profile, so all gateways are trusted.

Default

No access profile, so all gateways are trusted.

Usage Guidelines

Because PIM leverages the unicast routing capability that is already present in the switch, the access policy capabilities are, by nature, different. When the PIM protocol is used for routing IP multicast traffic, the switch can be configured to use an access profile to determine trusted PIM router neighbors for the VLAN on the switch running PIM.

Example

The following command configures a trusted neighbor policy on the VLAN *backbone*:

```
configure pim vlan backbone trusted-gateway nointernet
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

disable dvmrp

```
disable dvmrp
```

Description

Disables DVMRP on the system.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command disables DVMRP on the system:

```
disable dvmrp
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable dvmrp rxmode vlan

```
disable dvmrp rxmode vlan [<vlan name> | all]
```

Description

Disables the receive capability of DVMRP packets on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables the receive capability of DVMRP packets on the VLAN *accounting*:

```
disable dvmrp rxmode vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable dvmrp txmode vlan

```
disable dvmrp txmode vlan [vlan <vlan name> | all]
```

Description

Disables the transmit capability of DVMRP packets on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

None.

Example

The following command disables the transmit capability of DVMRP packets on the VLAN *accounting*:

```
disable dvmrp txmode vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

disable igmp

```
disable igmp {vlan <vlan name>}
```

Description

Disables IGMP on a router interface. If no VLAN is specified, IGMP is disabled on all router interfaces.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

IGMP is a protocol used by an IP host to register its IP multicast group membership with a router. Periodically, the router queries the multicast group to see if the group is still in use. If the group is still active, hosts respond to the query, and group registration is maintained.

IGMP is enabled by default on the switch. However, the switch can be configured to disable the generation and processing of IGMP packets. IGMP should be enabled when the switch is configured to perform IP unicast or IP multicast routing. IGMP must be enabled if the switch is configured for DVMRP.

Example

The following command disables IGMP on VLAN *accounting*:

```
disable igmp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable igmp snooping

```
disable igmp snooping {forward-mcrouter-only | vlan <vlan name>}
```

Description

Disables IGMP snooping.

Syntax Description

forward-mcrouter-only	Specifies that the switch forwards all multicast traffic to the multicast router only.
vlan name	Specifies a VLAN.

Default

Enabled.

Usage Guidelines

If a VLAN is specified, IGMP snooping is disabled only on that VLAN, otherwise IGMP snooping is disabled on all VLANs.

If the switch is in the `forward-mcrouter-only` mode, then the command `disable igmp snooping forward-mcrouter-only` changes the mode so that all multicast traffic is forwarded to any IP router. If not in the forward-mcrouter-mode, the command `disable igmp snooping forward-mcrouter-only` has no effect.

To change the snooping mode you must disable IP multicast forwarding. Use the command:

```
disable ipmcforwarding
```

Example

The following command disables IGMP snooping on the VLAN accounting:

```
disable igmp snooping accounting
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

disable igmp snooping with-proxy

```
disable igmp snooping with-proxy
```

Description

Disables the IGMP snooping proxy. The default setting is enabled.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

This command can be used for troubleshooting purpose. It should be enabled for normal network operation.

Enabling the proxy allows the switch to suppress the duplicate join requests on a group to forward to the connected layer 3 switch. The proxy also suppresses unnecessary IGMP leave messages so that they are forwarded only when the last member leaves the group.

Example

The following command disables the IGMP snooping proxy:

```
disable igmp snooping with-proxy
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

disable ipmcforwarding

```
disable ipmcforwarding {vlan <vlan name>}
```

Description

Disables IP multicast forwarding on an IP interface.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

If no options are specified, all configured IP interfaces are affected. When new IP interfaces are added, IP multicast forwarding is disabled by default.

IP forwarding must be enabled before enabling IP multicast forwarding, and IP multicast forwarding must be disabled before disabling IP forwarding.

Disabling IP multicast forwarding disables any layer 3 forwarding for the streams coming to the interface.

Example

The following command disables IP multicast forwarding on the VLAN *accounting*:

```
disable ipmcforwarding vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

disable pim

```
disable pim
```

Description

Disables PIM on the system.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command disables PIM on the system:

```
disable pim
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

enable dvmrp

```
enable dvmrp
```

Description

Enables DVMRP on the system.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command enables DVMRP on the system:

```
enable dvmrp
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable dvmrp rxmode vlan

```
enable dvmrp rxmode vlan [<vlan name> | all]
```

Description

Enables the receive capability of DVMRP packets on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

None.

Example

The following command enables the receive capability of DVMRP packets on the VLAN *accounting*:

```
enable dvmrp rxmode vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable dvmrp txmode vlan

```
enable dvmrp txmode vlan [vlan <vlan name> | all]
```

Description

Enables the transmit capability of DVMRP packets on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

None.

Example

The following command enables the transmit capability of DVMRP packets on the VLAN *accounting*:

```
enable dvmrp txmode vlan accounting
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

enable igmp

```
enable igmp {vlan <vlan name>}
```

Description

Enables IGMP on a router interface. If no VLAN is specified, IGMP is enabled on all router interfaces.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

IGMP is a protocol used by an IP host to register its IP multicast group membership with a router. Periodically, the router queries the multicast group to see if the group is still in use. If the group is still active, IP hosts respond to the query, and group registration is maintained.

IGMP is enabled by default on the switch. However, the switch can be configured to disable the generation and processing of IGMP packets. IGMP should be enabled when the switch is configured to perform IP unicast or IP multicast routing.

Example

The following command enables IGMP on the VLAN *accounting*:

```
enable igmp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable igmp snooping

```
enable igmp snooping {forward-mcrouter-only | vlan <vlan name>}
```

Description

Enables IGMP snooping on the switch.

Syntax Description

forward-mcrouter-only	Specifies that the switch forwards all multicast traffic to the multicast router only.
vlan name	Specifies a VLAN.

Default

Enabled.

Usage Guidelines

If a VLAN is specified, IGMP snooping is enabled only on that VLAN, otherwise IGMP snooping is enabled on all VLANs.

Two IGMP snooping modes are supported:

- The `forward-mcrouter-only` mode forwards all multicast traffic to the multicast router (that is, the router running PIM or DVMRP).
- When not in the `forward-mcrouter-only` mode, the switch forwards all multicast traffic to any IP router (multicast or not).

To change the snooping mode you must disable IP multicast forwarding. To disable IP multicast forwarding, use the command:

```
disable ipmcforwarding
```

To change the IGMP snooping mode from the `forward-mcrouter-only` mode to the non-`forward-mcrouter-only` mode, use the command:

```
disable igmp snooping forward-mcrouter-only
```

The snooping mode is not changed from the non-`forward-mcrouter-only` mode to the `forward-mcrouter-only` mode solely by enabling that mode. You must disable IGMP snooping, then enable IGMP snooping for multicast only. Disable IP multicast forwarding, then use the following commands:

```
disable igmp snooping
enable igmp snooping forward-mcrouter-only
```

Example

The following command enables IGMP snooping on the switch:

```
enable igmp snooping
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable igmp snooping with-proxy

```
enable igmp snooping with-proxy
```

Description

Enables the IGMP snooping proxy. The default setting is enabled.

Syntax Description

This command has no arguments or variables.

Default

Enabled.

Usage Guidelines

This command can be used for troubleshooting purpose. It should be enabled for normal network operation. The command does not alter the snooping setting. IP multicast forwarding should be disabled globally for this command.

Enabling the proxy allows the switch to suppress the duplicate join requests on a group to forward to the connected layer 3 switch. The proxy also suppresses unnecessary IGMP leave messages so that they are forwarded only when the last member leaves the group.

Example

The following command enables the IGMP snooping proxy:

```
enable igmp snooping with-proxy
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

enable ipmcforwarding

```
enable ipmcforwarding {vlan <vlan name>}
```

Description

Enables IP multicast forwarding on an IP interface.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Disabled.

Usage Guidelines

If no options are specified, all configured IP interfaces are affected. When new IP interfaces are added, IPMC forwarding is disabled by default.

IP forwarding must be enabled before enabling IPMC forwarding, and IPMC forwarding must be disabled before disabling IP forwarding.

Example

The following command enables IPMC forwarding on the VLAN *accounting*:

```
enable ipmcforwarding vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

enable pim

```
enable pim
```

Description

Enables PIM on the system.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

None.

Example

The following command enables PIM on the system:

```
enable pim
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

mrinfo

```
mrinfo <ip address> {from <ip address>} {timeout <seconds>}
```

Description

Initiates a request to get multicast information from a router.

Syntax Description

<ip address>	Specifies an IP address. The first <ip address> parameter specifies the unicast IP address of the router to query.
from	Specifies the unicast address of an interface in the system to use as the source address in the request.
timeout	Specifies the time to wait before indicating a failure.

Defaults

- from—outgoing interface
- timeout—three seconds

Usage Guidelines

This command queries a multicast router for information useful for tracing and troubleshooting. The command returns the following information:

- code version
- system multicast information
- interface information
  - interface IP address
  - interface multicast capabilities
  - metric configured on the interface
  - threshold configured on the interface
  - count and IP address of the neighbors discovered on the interface

Example

The following command queries the router at 10.10.34.14:

```
mrinfo 10.10.34.14
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

mtrace

```
mtrace source <ip address> {destination <ip address>} {group <ip address>}
{from <ip address>} {gateway <ip address >} {timeout <seconds>}
{maximum-hops <number>}
```

Description

Initiates a request to trace the path of multicast traffic from the source to the destination of a multicast group.

Syntax Description

<ip address>	Specifies an IP address.
source	Specifies the unicast address of the multicast source.
destination	Specifies the unicast address of the destination to which the path of the multicast traffic will be traced.
group	Specifies the multicast IP address of the group for which the traffic will be traced.
from	Specifies the unicast address of an interface in the system to use as the response address in the request.
gateway	Specifies the unicast address of a first hop router to which the query will be directed.
timeout	Specifies the time to wait before indicating a failure.
maximum-hops	Specifies the maximum number of hops the mtrace request can traverse.

Defaults

- destination—current system
- group—0.0.0.0
- from—outgoing interface to reach the source or destination
- gateway—destination 224.0.0.2
- timeout—three seconds
- maximum-hops—255

Usage Guidelines

This command relies on a feature of multicast routers that is accessed using the IGMP protocol. Since multicast uses reverse path forwarding, a multicast trace is run from the destination to the source. A query packet is sent to the last-hop multicast router. This router builds a trace response packet, fills in a report for its hop, and forwards the packet to the next upstream router. As the request is forwarded, each router in turn adds its own report to the trace response. When the request reaches the first-hop router, the filled in request is sent back to the system requesting the trace. The request will also be returned if the maximum hop limit is reached.

If a router does not support the mtrace functionality, it will silently drop the request packet and no information will be returned. For this situation, you would send the trace with a small number of maximum hops allowed, increasing the number of hops as the stream is traced.

The group IP address must be in the class-D multicast address space, but should not be in the multicast control subnet range (224.0.0.x/24).

ExtremeWare based systems do not maintain packet forwarded statistics for each source/group combination (S,G) and cannot return that information.

Example

The following command traces the multicast group 221.160.14.23 originating at 10.10.32.14 that is coming through the gateway at 172.16.255.1:

```
mtrace source 10.10.34.14 group 227.160.14.23 gateway 172.16.255.1
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

run ipmcfdb-check

```
run ipmcfdb-check [index <bucket> <entry> | <IP multicast group> <source IP
address> vlan <vlan name>] {extended} {detail}
```

Description

Checks IP multicast FDB entries for consistency.

Syntax Description

bucket	Specifies the bucket portion of the FDB hash index.
entry	Specifies the entry portion of the FDB hash index.
IP multicast group	Specifies a multicast group. FDB entries with this group will be checked.
source IP address	Specifies an IP source address.
vlan name	Specifies a VLAN name. FDB entries for this VLAN with the specified multicast group number will be checked.
extended	Enables OTP index checking in the MAC entry and VPST of the egress port.
detail	Specifies that more detailed debug information should be logged.

Default

N/A.

Usage Guidelines

The FDB error checking function logs the error count into the system log. Use the `detail` option to log more detailed debug information.

Example

The following command runs a consistency check on the FDB entries for the IP multicast group 168.192.2.4:

```
run ipmcfdb-check 168.192.2.4 195.1.1.100 vlan lab1 extended detail
```

History

This command was first available in ExtremeWare 6.1.9.

Platform Availability

This command is available on all platforms.

show dvmrp

```
show dvmrp {vlan <vlan name> | route {detail}}
```

Description

Displays the DVMRP configuration and statistics, or the unicast route table.

Syntax Description

vlan name	Specifies a VLAN name.
route	Specifies a route.
detail	Specifies to display the information in detailed format.

Default

All.

Usage Guidelines

None.

Example

The following command displays the DVMRP configuration and statistics for the VLAN *accounting*:

```
show dvmrp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show igmp group

```
show igmp group {<ip address> {sender <ip address>}} {vlan <vlan name>}
```

Description

Lists the IGMP group membership for the specified VLAN.

Syntax Description

group <ip address>	Specifies a group IP address.
sender <ip address>	Specifies a sender's IP address.
vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

If no VLAN is specified all VLANs are displayed. You can also filter the display by group address and by multicast stream sender address.

Example

The following command lists the IGMP group membership for the VLAN *accounting*:

```
show igmp group 10.0.0.1 sender 10.0.0.2 accounting
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show igmp snooping

```
show igmp snooping {vlan <vlan name> | detail}
```

Description

Displays IGMP snooping registration information and a summary of all IGMP timers and states.

Syntax Description

vlan name	Specifies a VLAN name.
detail	Specifies to display the information in detailed format.

Default

N/A.

Usage Guidelines

The two types of IGMP snooping entry are sender entry and subscribed entry.

The following information is displayed in a per-interface format:

- Group membership information
- Router entry
- Timeout information

Example

The following command displays IGMP snooping registration information on the VLAN *accounting*:

```
show igmp snooping vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show igmp snooping filter

```
show igmp snooping {vlan <vlan name>} filter
```

Description

Displays IGMP snooping filters.

Syntax Description

vlan name	Specifies a VLAN name.

Default

None.

Usage Guidelines

Use this command to display IGMP snooping filters configured on the specified VLAN. When no VLAN is specified, all the filters will be displayed.

Example

To display the IGMP snooping filter configured on VLAN *vlan101,* use the following command:

```
show igmp snooping vlan101 filter
```

The output of the command will be similar to the following:

```
VLAN vlan101 (4094)
Filter           Port
ap5              31    (-)
Total number of configured static filters = 1

Flags: (a) Active
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show igmp snooping static group

```
show igmp snooping {vlan <vlan name>} static group
```

Description

Displays static IGMP snooping entries.

Syntax Description

vlan name	Specifies a VLAN name.

Default

None.

Usage Guidelines

Use this command to display IGMP snooping filters configured on the specified VLAN. When no VLAN is specified, all the filters will be displayed.

Example

To display the IGMP snooping static groups configured on VLAN *vlan101*, use the following command:

```
show igmp snooping vlan101 static group
```

The output of the command will be similar to the following:

```
VLAN vlan101 (4094)
    Group            Port   Flags
    239.1.1.2        29      s-
    239.1.1.2        30      s-
    239.1.1.2        31      sa
    239.1.1.2        32      s-
    239.1.1.2        34      s-

Total number of configured static IGMP groups = 5
Flags: (s) Static, (a) Active
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

show ipmc cache

```
show ipmc cache {detail} | {<IP multicast group> {<source IP address>
<netmask>}}
```

Description

Displays the IP multicast forwarding cache.

Syntax Description

detail	Specifies to display the information in detailed format.
IP multicast group	Specifies an IP group address.
source IP address	Specifies an IP source address.
netmask	Specifies a subnet mask.

Default

N/A.

Usage Guidelines

Displays the following information:

- IP group address
- IP source address / source mask
- Upstream neighbor (RPF neighbor)
- Interface (VLAN-port) to upstream neighbor
- Cache expiry time
- Routing protocol

When the detail option is specified, the switch displays the egress VLAN list and the pruned VLAN list.

Example

The following command displays the IP multicast table for group *224.1.2.3*:

```
show ipmc cache 224.1.2.3
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show ipmc fdb

```
show ipmc fdb {<ip address>}
```

Description

Displays the IP multicast forwarding database.

Syntax Description

ip address	Specifies an IP group address.

Default

N/A.

Usage Guidelines

If the group address is specified, only the IP multicast FDB entries corresponding to the group address are displayed.

Example

The following command displays the IP multicast forwarding database:

```
show ipmc fdb
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show l2stats

```
show l2stats {vlan <vlan name>}
```

Description

Displays the counters for the number of packets bridged, switched, and snooped.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the counters for the number of packets bridged, switched, and snooped for the VLAN *accounting*:

```
show l2stats accounting
```

History

This command was first available in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show pim

```
show pim {detail | rp-set {<IP multicast group>}| vlan <vlan name>}
```

Description

Displays the PIM configuration and statistics.

Syntax Description

detail	Specifies to display the detailed format.
IP multicast group	Specifies an IP multicast group.
vlan name	Specifies a VLAN name.

Default

If no VLAN is specified, the configuration is displayed for all PIM interfaces.

If no multicast group is specified for the `rp-set` option (Rendezvous Point set), all groups are displayed.

Usage Guidelines

The `detail` version of this command displays the global statistics for PIM register and register-stop packets.

Example

The following command displays the PIM configuration and statistics for the VLAN *accounting*:

```
show pim accounting
```

History

This command was first available in ExtremeWare 4.0.

The `rp-set` option was added in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

unconfigure dvmrp

```
unconfigure dvmrp {vlan <vlan name>}
```

Description

Resets the DVMRP timers to their default settings.

Syntax Description

vlan name	Specifies a VLAN name.

Default

If no VLAN is specified, all interfaces are reset.

Usage Guidelines

None.

Example

The following command resets all DVMRP timers on VLAN *accounting*:

```
unconfigure dvmrp vlan accounting
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

unconfigure igmp

```
unconfigure igmp
```

Description

Resets all IGMP settings to their default values and clears the IGMP group table.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command resets all IGMP settings to their default values and clears the IGMP group table:

```
unconfigure igmp
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

unconfigure pim

```
unconfigure pim {vlan <vlan name>}
```

Description

Resets all PIM settings on one or all VLANs to their default values.

Syntax Description

vlan name	Specifies a VLAN name.

Default

If no VLAN is specified, the configuration is reset for all PIM interfaces.

Usage Guidelines

None.

Example

The following command resets all PIM settings on the VLAN *accounting*:

```
unconfigure pim vlan accounting
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

20 IPX Commands

Basic IPX Command Overview

The switch provides support for the IPX, IPX/RIP, and IPX/SAP protocols. The switch dynamically builds and maintains an IPX routing table and an IPX service table.

The routing software and hardware routes IPX traffic between IPX router interfaces. A router interface is simply a VLAN that has an IPX network identifier (NetID) and IPX encapsulation type assigned to it.

As you create VLANs with different IPX NetIDs the switch automatically routes between them. Both the VLAN switching and IPX routing function occur within the switch.

NOTE

A VLAN can be configured with either an IPX NetID or an IP address. A VLAN cannot be configured for both IPX and IP routing simultaneously.

This chapter describes the IPX commands.

configure ipxmaxhops

```
configure ipxmaxhops <number>
```

Description

Configures the IPX maximum hop count when forwarding IPX packets.

Syntax Description

number	Specifies a hop count number.

Default

The default setting is 16.

Usage Guidelines

Change the default number only if NetWare Link Services Protocol (NLSP) is running in the IPX network.

Example

The following command configures a maximum IPX hop count of 24:

```
configure ipxmaxhops 24
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip add vlan

```
configure ipxrip add vlan [<vlan name> | all]
```

Description

Configures one or all IPX VLANs to run IPX/RIP.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

IPX/RIP is enabled by default when you configure the IPX VLAN.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following command configures IPX VLAN backbone to run IPX/RP:

```
configure ipxrip add vlan backbone
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip delete vlan

```
configure ipxrip delete vlan [<vlan name> | all]
```

Description

Disables IPX/RIP on one or all interfaces.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following command disables IPX/RIP on VLAN backbone:

```
configure ipxrip delete vlan backbone
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip vlan delay

```
configure ipxrip vlan [<vlan name> | all] delay <msec>
```

Description

Configures the time between each IPX/RIP packet within an update interval.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
msec	Specifies the delay time in milliseconds.

Default

The default setting is 55 milliseconds.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following command configures a delay of 80 milliseconds:

```
configure ipxrip vlan accounting delay 80
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip vlan export-filter

```
configure ipxrip vlan [<vlan name> | all] export-filter [none |
<access_profile>]
```

Description

Assigns an export route filter to an ingress VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
none	Specifies no export filters.
access_profile	Specifies an access profile name.

Default

N / A.

Usage Guidelines

Only the network ID matching the export filter will be added to the IPX route table.

Example

The following command assigns an export route filter to ingress VLAN `accounting`:

```
configure ipxrip vlan accounting export-filter my-profile
```

History

This command was introduced in ExtremeWare 4.0; `access-profiles` modified in version 6.1.5b20.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip vlan import-filter

```
configure ipxrip vlan [<vlan name> | all] import-filter [none |
<access_profile>]
```

Description

Assigns an import route filter to an ingress VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
none	Specifies no import filters.
access_profile	Specifies an access profile name.

Default

N/A.

Usage Guidelines

Only the network ID matching the import filter will be added to the IPX route table.

Example

The following command assigns an import route filter to ingress VLAN `accounting`:

```
configure ipxrip vlan accounting import-filter my-profile
```

History

This command was introduced in ExtremeWare 4.0; `access-profiles` modified in version 6.1.5b20.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip vlan max-packet-size

```
configure ipxrip vlan [<vlan name> | all] max-packet-size <size>
```

Description

Configures the maximum transmission unit (MTU) size of the IPX/RIP packet.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
size	Specifies the maximum packet size in bytes.

Default

The default setting is 432 bytes.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following command configures an MTU size of 128 for the IPX/RIP packet:

```
configure ipxrip vlan accounting max-packet-size 128
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxrip vlan trusted-gateway

```
configure ipxrip vlan [<vlan name> | all] trusted-gateway [none |
<access_profile>]
```

Description

Assigns an export route filter to the egress VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
none	Specifies no export filters.
access_profile	Specifies an access profile name.

Default

N/A.

Usage Guidelines

Only services matching the trusted gateway are advertised on the egress VLAN.

Example

The following command assigns export route filter `smith` to VLAN `accounting`:

```
configure ipxrip vlan accounting trusted-gateway access_profile
```

History

This command was introduced in ExtremeWare 4.0; `access-profiles` modified in version 6.1.5b20.

Platform Availability

This command is available on all platforms.

configure ipxrip vlan update-interval

```
configure ipxrip vlan [<vlan name> | all] update-interval <time>
{hold-multiplier <number>}
```

Description

Configures the update interval and hold multiplier for IPX/RIP updates.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
update-interval <time>	Specifies the update interval time.
hold-multiplier <number>	Specifies the hold multiplier for IPX/RIP updates.

Default

The default update interval is 60 seconds. The default multiplier is 3.

Usage Guidelines

This setting affects both the periodic update interval of IPX/RIP and the aging interval of learned routes. The aging period is calculated using the formula (update-interval * multiplier).

Example

The following command configures the IPX/RIP updates for an update interval of `30` seconds and a hold multiplier of `2` for VLAN `accounting`:

```
configure ipxrip vlan accounting update-interval 30 hold-multiplier 30
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxroute add

```
configure ipxroute add [<dest_netid> | default] <next_hop_id>
<next_hop_node_addr> <hops> <tics>
```

Description

Adds a static IPX route entry in the IPX route table.

Syntax Description

dest_netid	Specifies the destination NetID.
next_hop_id	Specifies the NetID of the neighbor IPX network.
next_hop_node_addr	Specifies the node address of the next IPX router.
hops	Specifies the maximum hop count.
tics	Specifies the timer delay value.

Default

N/A.

Usage Guidelines

Static routes are used to reach networks not advertised by routers. You can configure up to 64 static IPX routes on the switch. Static routes are never aged out of the routing table. Static routes are advertised to the network using IPX/RIP.

Example

The following command adds a static IPX route entry to the IPX route table:

```
configure ipxroute add default 0011 00:eb:2a:0b:1e:0a
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxroute delete

```
configure ipxroute delete [<dest_netid> | default] <next_hop_netid>
<next_hop_node_addr>
```

Description

Removes a static IPX route entry from the route table.

Syntax Description

dest_netid	Specifies the destination NetID.
next_hop_id	Specifies the NetID of the neighbor IPX network.
next_hop_node_addr	Specifies the node address of the next IPX router.

Default

N/A.

Usage Guidelines

If you have defined default or static routes, those routes will remain in the configuration independent of whether the VLAN or VLAN IP address that used them remains. You should manually delete the routes if no VLAN IP address is capable of using them.

Example

The following command deletes a static IPX route entry to the IPX route table:

```
configure ipxroute delete default 0011 00:eb:2a:0b:1e:0a
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap add vlan

```
configure ipxsap add vlan [<vlan name> | all]
```

Description

Configures an IPX VLAN to run IPX/SAP routing.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following command configures the IPX VLAN accounting to run IPX/SAP routing:

```
configure ipxsap add vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap delete vlan

```
configure ipxsap delete vlan [<vlan name> | all]
```

Description

Disables IPX/SAP on an interface.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

N/A.

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following command disables IPX/SAP on VLAN accounting:

```
configure ipxsap delete vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap vlan delay

```
configure ipxsap vlan [<vlan name> | all] delay <msec>
```

Description

Configures the time between each SAP packet within an update interval.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
msec	Specifies a delay in milliseconds.

Default

The default setting is 55 milliseconds.

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following command sets the time between each SAP packet to `40` milliseconds for VLAN `accounting`:

```
configure ipxsap vlan accounting delay 40
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap vlan export-filter

```
configure ipxsap vlan [<vlan name> | all] export-filter [none |
access_profile]
```

Description

Assigns an export route filter to an ingress VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
none	Specifies no export filters
access_profile	Specifies an access profile name.

Default

N / A.

Usage Guidelines

Only the network ID matching the export filter will be added to the IPX route table.

Example

The following command assigns an export route filter to ingress VLAN `accounting`:

```
configure ipxsap vlan accounting export-filter none
```

History

This command was introduced in ExtremeWare 4.0; `access-profiles` modified in version 6.1.5b20.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap vlan import-filter

```
configure ipxsap vlan [<vlan name> | all] import-filter [none |
access_profile]
```

Description

Assigns an import route filter to an ingress VLAN.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
none	Specifies no route filters.
access_profile	Specifies an access profile name.

Default

N/A.

Usage Guidelines

Only the network ID matching the import filter will be added to the IPX route table.

Example

The following command assigns an import route filter to ingress VLAN `accounting`:

```
configure ipxsap vlan accounting import-filter none
```

History

This command was introduced in ExtremeWare 4.0; `access-profiles` modified in version 6.1.5b20.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap vlan max-packet-size

```
configure ipxsap vlan [<vlan name> | all] max-packet-size <number>
```

Description

Configures the MTU size of the IPX/SAP packets.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
max-packet-size <number>	Specifies the maximum packet size in bytes.

Default

The default setting is 432 bytes.

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following command configures an MTU size of 356 bytes for the IPX/SAP packets on VLAN accounting:

```
configure ipxsap vlan accounting max-packet-size 356
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap vlan trusted-gateway

```
configure ipxsap vlan [<vlan name> | all] trusted-gateway [none |
<access_profile>]
```

Description

Assigns an export SAP service filter to the egress VLAN.

Syntax Description

vlan name>	Specifies a VLAN name.
al	Specifies all VLANs.
none	Specifies no service filters.
access_profile	Specifies an access profile name.

Default

N/A.

Usage Guidelines

Only the services matching the trusted-gateway are advertised on the egress VLAN.

Example

The following command assigns an export SAP service filter named `smith` to VLAN `accounting`:

```
configure ipxsap vlan accounting trusted-gateway smith
```

History

This command was introduced in ExtremeWare 4.0; `access-profiles` modified in version 6.1.5b20.

Platform Availability

This command is available on all platforms.

configure ipxsap vlan update-interval

```
configure ipxsap vlan [<vlan name> | all] update-interval <time>
{hold-multiplier <number>}
```

Description

Configures the update interval and hold multiplier for IPX/SAP updates.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
update-interval <time>	Specifies the update interval time.
hold-multiplier <number>	Specifies the hold multiplier for IPX/RIP updates.

Default

The default update interval is 60 seconds. The default multiplier is 3.

Usage Guidelines

This setting affects both the periodic update interval of SAP and the aging interval of learned routes. The default update interval is 60 seconds. The aging period is calculated using the formula (update-interval * multiplier). The default multiplier is 3. Triggered update is always enabled; therefore, new information is processed and propagated immediately.

Example

The following command configures an update interval of `30` seconds and a hold multiplier of 2 for the IPX/SAP updates for VLAN `accounting`:

```
configure ipxsap vlan accounting update-interval 30 hold-multiplier 2
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxsap vlan gns-delay

```
configure ipxsap vlan <vlan name> gns-delay <msec>
```

Description

Configures the amount of time the switch waits before answering a GNS request.

Syntax Description

vlan name	Specifies a VLAN name.
msec	Specifies a delay in milliseconds.

Default

The switch answers a GNS request as soon as possible (0 milliseconds).

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following command sets a GNS delay time of `20` milliseconds on VLAN `accounting`:

```
configure ipxsap vlan accounting gns-delay 20
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxservice add

```
configure ipxservice add <service_type> <service_name> <netid>
<mac_address> <socket> <hops>
```

Description

Adds a static entry to the IPX service table.

Syntax Description

service_type	Specifies a service type.
service_name	Specifies a service name.
netid	Specifies the IPX network identifier of the server.
mac_address	Specifies the MAC address of the server.
socket	Specifies the IPX port number on the server.
hops	Specifies the number of hops (for SAP routing purposes).

Default

N/A.

Usage Guidelines

Service information may also be entered into the IPX Service Table dynamically, by way of SAP.

The `socket` provides you with access to a particular function on the server.

Example

The following command adds non-advertising server `chalk` to the IPX service table, with `0004` as SAP for a file server, `00:AO:C9:17:22:F5` as the MAC address, `0451` as the socket number for a connection request, and `3` as the number of hops to the server:

```
configure ipxservice add chalk 0004 00:AO:C9:17:22:F5 0451 3
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure ipxservice delete

```
configure ipxservice delete <service_type> <service_name> <netid>
<mac_address> <socket>
```

Description

Deletes an IPX service from the service table.

Syntax Description

service_type	Specifies a service type.
service_name	Specifies a service name.
netid	Specifies the IPX network identifier of the server.
mac_address	Specifies the MAC address of the server.
socket	Specifies the IPX port number on the server.

Default

N / A.

Usage Guidelines

The service information is entered into the IPX Service Table in one of the following two ways:

- Dynamically, by way of SAP
- Statically, using the `configure ipxservice add` command

The `socket` provides you with access to a particular function on the server.

Example

The following command deletes non-advertising server `chalk` from the IPX service table, with `0004` as SAP for a file server, `00:AO:C9:17:22:F5` as the MAC address, `0451` as the socket number for a connection request, and `3` as the number of hops to the server.

```
configure ipxservice delete chalk 0004 00:AO:C9:17:22:F5 0451
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

configure vlan xnetid

```
configure vlan <vlan name> xnetid <netid> [enet_ii | enet_8023 | enet_8022
| enet_snap]
```

Description

Configures a VLAN to use a particular encapsulation type.

Syntax Description

vlan name	Specifies a VLAN name.
netid	Specifies the IPX network identifier of the server.
enet_ii	Specifies an Ethernet 2 header.
enet_8023	Specifies the IEEE 802.3 length field.
enet_8022	Specifies and IEEE format and includes the IEEE 802.2 LLC header.
enet_snap	Specifies to add SNAP header to the IEEE 802.2 LLC header.

Default

N/A.

Usage Guidelines

Novell NetWare supports four types of frame encapsulation. The ExtremeWare term for each type is shown in the following list:

Table 25:

ENET_II	The frame uses the standard Ethernet 2 header.
ENET_8023	The frame includes the IEEE 802.3 length field, but does not include the IEEE 802.2 Logical Link Control (LLC) header. This encapsulation is used by NetWare version 2.x and the original NetWare 3.x version.
ENET_8022	The frame uses the standard IEEE format and includes the IEEE 802.2 LLC header. This encapsulation is used by NetWare version 3.12 and 4.x.
ENET_SNAP	The frame adds a Subnetwork Access Protocol (SNAP) header to the IEEE 802.2 LLC header.

Example

The following command configures VLAN `Support` to use encapsulation `enet_8022`:

```
configure vlan Support xnetid A2B5 enet_8022
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

disable ipxrip

```
disable ipxrip
```

Description

Disables IPX/RIP on the router.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following disables IPX/RIP on the router:

```
disable ipxrip
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

disable ipxsap

```
disable ipxsap
```

Description

Disables IPX/SAP on the router.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following disables IPX/SAP on the router:

```
disable ipxsap
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

disable ipxsap gns-reply

```
disable ipxsap gns-reply {vlan <vlan name>}
```

Description

Disables Get Nearest Server (GNS) reply on one or all IPX interfaces.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

ExtremeWare supports the GNS reply function. When a NetID is assigned to the switch, the GNS reply service is automatically enabled. When a station requests a particular service on the network (for example, locating a print server), the station sends a GNS request and the switch responds to the request. If GNS-reply is disabled, the switch drops the request.

Example

The following command disables GNS reply on IPX VLAN `accounting`:

```
disable ipxsap gns-reply vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

disable type20 forwarding

```
disable type20 forwarding {vlan <vlan name>}
```

Description

Disables the forwarding of IPX type 20 packets.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Type 20 packets are NetBIOS inside IPX.

Example

The following command disables the forwarding of IPX type 20 packets for VLAN accounting:

```
disable type20 forwarding vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all “*i*” series systems.

enable ipxrip

```
enable ipxrip
```

Description

Enables IPX/RIP on the router.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following command enables IPX/RIP on the router:

```
enable ipxrip
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

enable ipxsap

```
enable ipxsap
```

Description

Enables IPX/SAP on the router.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example

The following command enables IPX/SAP on the router:

```
enable ipxsap
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

enable ipxsap gns-reply

```
enable ipxsap gns-reply {vlan <vlan name>}
```

Description

Enables GNS reply on one or all IPX interfaces.

Syntax Description

vlan name	Specifies a VLAN name.

Default

The default setting is enabled.

Usage Guidelines

If no VLAN is specified, GNS reply is enabled on all IPX interfaces.

Example

The following command enables GNS reply for IPX VLAN accounting:

```
enable ipxsap gns-reply vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

enable type20 forwarding

```
enable type20 forwarding {vlan <vlan name>}
```

Description

Enables the forwarding of IPX type 20 packets.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Enabled.

Usage Guidelines

Type 20 packets are NetBIOS inside IPX.

Example

The following command enables the forwarding of IPX type 20 packets for VLAN accounting:

```
enable type20 forwarding vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all “*i*” series systems.

show ipxconfig

```
show ipxconfig {vlan <vlan name>}
```

Description

Displays IPX configuration information for one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

This command is analogous to the `show ipconfig` command for the IP protocol. It displays summary global IPX configuration information followed by per-VLAN information. Information includes enable/disable status for IPX/RIP, IPX/SAP, IPX route sharing, IPX service sharing, and so on.

Example

The following command displays the IPX configuration information for VLAN `accounting`:

```
show ipxconfig vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

show ipxfdb

```
show ipxfdb {vlan <vlan name> | xnetid <netid>}
```

Description

Displays the hardware IPX FDB information.

Syntax Description

vlan name	Specifies a VLAN name.
netid	Specifies an IPX network number.

Default

N / A.

Usage Guidelines

The switch maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in the FDB to decide whether a frame should be forwarded or filtered.

Example

The following command displays the hardware IPX FDB information for VLAN `accounting`:

```
show ipxfdb vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

show ipxrip

```
show ipxrip {vlan <vlan name>}
```

Description

Displays IPX/RIP configuration and statistics for one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

The enable status of IPX/RIP displayed includes operational and administrative status. It also lists any identified IPX/RIP neighbors, RIP packet statistics, and several other timer settings.

Example

The following command displays the IPX/RIP configuration information and statistics for VLAN `accounting`:

```
show ipxrip vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

show ipxroute

```
show ipxroute {vlan <vlan name> | xnetid <netid> | origin [static | rip |
local]}
```

Description

Displays the IPX routes in the route table.

Syntax Description

vlan name	Specifies a VLAN name.
netid	Specifies an IPX network number.
static	Specifies a statically defined route.
rip	Specifies a RIP learned route.
local	Specifies a local interface.

Default

N/A.

Usage Guidelines

Route information is entered into the IPX route table in one of the following two ways:

- Dynamically, by way of RIP
- Statically, using the `configure ipxroute add` command

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN. To remove the advertisement of an IPX VLAN, use the `configure ipxrip delete` command.

Example

The following command displays the IPX routes in the route table for VLAN `accounting`:

```
show ipxroute vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

show ipxsap

```
show ipxsap {vlan <vlan name>}
```

Description

Displays the enable status of IPX/SAP for the VLAN, and its operational and administrative status (including the GNS reply service). It also lists any identified IPX/SAP neighbors, SAP packet statistics, and several other timer settings.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

None.

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

show ipxservice

```
show ipxservice {vlan <vlan name> | xnetid <netid> _ origin [static | sap |
local]}
```

Description

Displays IPX services learned by way of SAP.

Syntax Description

vlan name	Specifies a VLAN name.
netid	Specifies an IPX network number.

Default

N/A.

Usage Guidelines

The service information is entered into the IPX Service Table in one of the following two ways:

- Dynamically, by way of SAP
- Statically, using the `configure ipxservice add` command

Example

The following command displays IPX/SAP service information for VLAN `accounting`:

```
show ipxservice vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

show ipxstats

```
show ipxstats {vlan <vlan name>}
```

Description

Displays IPX packet statistics for the IPX router, and one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.

Default

All VLANs.

Usage Guidelines

Displays both RIP and SAP packet statistics.

Example

The following command displays IPX packet statistics for VLAN accounting:

```
show ipxstats vlan accounting
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

unconfigure ipxrip

```
unconfigure ipxrip {vlan <vlan name>}
```

Description

Resets the IPX/RIP settings on one or all VLANs to the default.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

Removes import and export filters, and resets the MTU size, update interval, and inter-packet delay.

Example

The following command

```
unconfigure ipxrip vlan backbone
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

unconfigure ipxsap

```
unconfigure ipxsap {vlan <vlan name>}
```

Description

Resets the IPX/SAP settings on one or all VLANs to the default.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

Removes import and export filters, and resets the MTU size, update interval, and inter-packet delay.

Example

The following command resets the IPX/SAP settings on VLAN backbone to the defaults:

```
unconfigure ipxsap vlan backbone
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

unconfigure vlan xnetid

```
unconfigure vlan <vlan name> xnetid
```

Description

Removes the IPX NetID of a VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example

The following command removes the IPX NetID of VLAN accounting:

```
unconfigure vlan accounting xnetid
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

xping

```
xping {continuous} {size <n>} <netid> <node_address>
```

Description

Pings an IPX node specified by the network ID and the node address.

Syntax Description

continuous	Specifies that pings are to be sent continuously.
size <n>	Specifies the ping packet size in bytes.
netid	Specifies an IPX network number.

Default

N / A.

Usage Guidelines

If `continuous` is not specified, four pings are sent. The default ping packet size is 256 data bytes. The size range is between 1 and 1,484 bytes.

Example

The following command pings IPX node `0010460` with a node address of `00:2b:2a:00:1c:0a`:

```
xping 0010460 00:2b:2a:00:1c:0a
```

History

This command was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on the all "*i*" series systems.

21 ARM Commands

The Accounting and Routing Module (ARM) is a self-contained module for the BlackDiamond switch. Unlike other BlackDiamond modules, there are no external network interfaces on the ARM. Instead, the ARM provides advanced IP services for the other input/output (I/O) modules installed in the chassis. The ARM contains a powerful set of packet processing resources that operate in a one-armed fashion: receiving frames from the switch fabric, processing the frames, and transmitting the frames back into the switch fabric.

The two main features of the ARM are: IP unicast forwarding with selective longest prefix match and destination-sensitive accounting.

IP unicast packets are routed in the ARM hardware using a longest prefix match algorithm. This differs from the BlackDiamond's switch fabric, which uses an exact match algorithm. The BlackDiamond's switch fabric has greater forwarding capacity, but the ARM module has better handling of large numbers (hundreds of thousands) of IP routes to match each packet's destination IP address. To take advantage of the BlackDiamond switch fabric's forwarding capacity and the ARM module's scalability, the ARM module can be configured to use the BlackDiamond switch fabric for some routes, and the ARM's longest prefix match for others. This feature is called Selective-LPM.

The second feature, destination-sensitive accounting collects statistics that are maintained for forwarded IP traffic to support billing on a destination basis. To configure destination-sensitive accounting, a bin number can be assigned to one or more IP route entries using the ExtremeWare `route-map` command.

Bin numbers are integers that range from 0-7 and their only intrinsic meaning is to identify a particular set of accounting statistics. Each bin contains a 64-bit count of the number of packets that have been forwarded and a 64-bit count of the number of bytes that have been forwarded. When the ARM or MPLS module forwards an IP packet, the bin number from the forwarding database entry for the IP destination is used to identify the set of counters to be updated.

Eight unique bins are maintained for each of the possible 4096 VLAN IDs. Logically, the bins are organized as a two-dimensional array, with the row index being a VLAN ID and the column index being a bin number. Thus, when an IP frame is forwarded, the input VLAN ID selects the row and the bin number from the forwarding database entry selects the column. The use of input VLAN ID enables billing statistics to be maintained on a per customer basis where the VLAN ID identifies the customer.

This chapter documents the ARM command set. Some commands are new for the ARM; other commands have been enhanced to support the ARM.

Basic Accounting Configuration Information

This section uses several typical usage and configuration schemes to provide a brief overview of the destination-sensitive accounting configuration process as a general context for the detailed command description sections that follow.

In the most basic terms, to enable the accounting function, you must enable the accounting feature, create a customer VLAN ID, enable IP forwarding, and configure the accounting bin using the route map feature.

You use a special set of commands to configure the ARM module to initiate the accounting function.

clear accounting counters

```
clear accounting counters
```

Description

Clears (zeroes out) all of the accounting statistics.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command clears (zeroes out) all of the accounting statistics.:

```
clear accounting counters
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure route-map set accounting-index 1 value

```
configure route-map <route-map> <sequence_number> [add | delete] set
accounting-index 1 value <bin_number>
```

Description

Configures the accounting bin number to be associated with the specified route map entry.

Syntax Description

route-map	Specifies a route map.
sequence number	Specifies a specific entry in the route map.
add	Specifies to add the statement to the route map.
delete	Specifies to delete the statement from the route map.
bin_number	Specifies an accounting bin number.

Default

N / A.

Usage Guidelines

- The accounting-index value is always set to 1 for destination-sensitive accounting.
- The `route-map` parameter identifies a particular route map.
- The `sequence_number` parameter identifies a specific entry in that route map. The sequence number must be associated with a match statement.
- The `set accounting-index 1 value` keyword phrase indicates that the following parameter is an accounting bin number.
- The `bin_number` parameter is an integer between 0—7, and allows you to define the accounting bin number.

Table 26: Set Operation Keywords

Command	Description of Change
accounting-index <index> value <value>	Sets the accounting bin number for the route-mapped accounting index. The accounting index value is always set to 1 for destination-sensitive accounting.

Example

The following command configures the accounting bin number to be associated with the specified route map entry:

```
configure route-map rt40 11 add set accounting-index 1 value 5
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure route-map set iphost-routing

```
configure route-map <route-map> <sequence-number> [add | delete ] set
iphost-routing
```

Description

Enables or disables Selective-LPM for a specified route-map when the LPM feature is enabled.

Syntax Description

route-map	Specifies a route map name.
sequence-number	Specifies a sequence number.
add	Specifies to add the statement to the route map.
delete	Specifies to delete the statement from the route map.

Default

N / A.

Usage Guidelines

This command optionally enables or disables Longest Prefix Match (LPM) for the specified route-map. This command may be used to override the VLAN lpm-routing configuration for specific routes. The `iphost-routing` keyword specifies how packets are to be routed for route-map matched IP prefixes.

If the `iphost-routing` property is added to a route-map, packets are forwarded to the IP prefixes' next hop using the hardware host-based IP FDB. The `iphost-routing` keyword is only significant for routes learned on VLANs that are lpm-routing enabled.

Example

This command enables Selective-LPM and specifies IP-host routing on the route map *lpm_map*:

```
configure lpm_map 20 add set iphost-routing
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure route-map set lpm-routing

```
configure route-map <route-map> <sequence-number> [add | delete ] set
lpm-routing
```

Description

Enables or disables Selective-LPM for a specified route-map when the LPM feature is enabled.

Syntax Description

route-map	Specifies a route map name.
sequence-number	Specifies a sequence number.
add	Specifies to add the statement to the route map.
delete	Specifies to delete the statement from the route map.

Default

N/A.

Usage Guidelines

This command optionally enables or disables Longest Prefix Match (LPM) for the specified route-map. This command may be used to override the VLAN lpm-routing configuration for specific routes. The `lpm-routing` keyword specifies how packets are to be routed for route-map matched IP prefixes. If the `lpm-routing` property is added to a route-map, packets are forwarded to the IP prefixes' next hop by the ARM/MPLS module using LPM routing.

The `lpm-routing` keyword is only significant for routes learned on VLANs that are not lpm-routing enabled.

Example

This command enables Selective-LPM and specifies lpm-routing on the route map *lpm_map*:

```
configure lpm_map 10 add set lpm-routing
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

disable accounting

```
disable accounting
```

Description

Disables the destination-sensitive accounting function.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Destination-sensitive accounting collects statistics that are maintained for forwarded IP traffic to support billing on a destination basis. To configure destination-sensitive accounting, a bin number can be assigned to one or more IP route entries using the ExtremeWare `route-map` command.

Example

The following command disables the destination-sensitive accounting function:

```
disable accounting
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

disable ipforwarding lpm-routing

```
disable ipforwarding lpm-routing {vlan <vlan name>}
```

Description

Disables Longest Prefix Match (LPM) routing for the specified VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N/A.

Usage Guidelines

When either an ARM or MPLS module is installed in a BlackDiamond switch, the module may be configured to forward IP packets for specified VLANs using LPM routing. If the `vlan name` parameter is omitted, lpm-routing is enabled for all configured VLANs, except the management VLAN.

Specifying the `lpm-routing` keyword for the disable command only disables LPM routing; it does not disable IP forwarding. By default, lpm-routing is not enabled on the VLAN when IP forwarding is enabled (for example, all VLANs perform host-based IP routing by default).

Example

This command configures LPM and IP-host routing for the *hop1* VLAN:

```
disable ipforwarding lpm-routing hop1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

disable lpm

```
disable lpm
```

Description

Disables Selective-LPM.

Syntax Description

This command has no arguments or variables.

Default

Default is disabled.

Usage Guidelines

None.

Example

The following command disables the Selective-LPM feature:

```
disable lpm
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

enable accounting

```
enable accounting
```

Description

Enables the destination-sensitive accounting function.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Destination-sensitive accounting collects statistics that are maintained for forwarded IP traffic to support billing on a destination basis. To configure destination-sensitive accounting, a bin number can be assigned to one or more IP route entries using the ExtremeWare `route-map` command.

Destination-sensitive accounting, LPM, and SLB are mutually exclusive functions and cannot be simultaneously enabled.

Example

The following command enables the destination-sensitive accounting function:

```
enable accounting
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

enable ipforwarding lpm-routing

```
enable ipforwarding lpm-routing {vlan <vlan name>}
```

Description

Enables Longest Prefix Match (LPM) routing for the specified VLAN.

Syntax Description

vlan name	Specifies a VLAN name.

Default

Default is disabled.

Usage Guidelines

When either an ARM or MPLS module is installed in a BlackDiamond switch, the module may be configured to forward IP packets for specified VLANs using LPM routing. If the `vlan name` parameter is omitted, lpm-routing is enabled for all configured VLANs, except the management VLAN.

By default, lpm-routing is not enabled on the VLAN when IP forwarding is enabled (for example, all VLANs perform host-based IP routing by default).

Example

This command configures LPM and IP-host routing for the *hop2* VLAN:

```
enable ipforwarding lpm-routing hop2
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

enable lpm

```
enable lpm
```

Description

Enables Selective-LPM routing.

Syntax Description

This command has no arguments or variables.

Default

Default is disabled.

Usage Guidelines

This command alters the state of the Selective-LPM routing feature (which is disabled by default). If Accounting is disabled, non-MPLS traffic to known routes is forwarded by hardware and the MSM CPU is used for slow-path traffic. When LPM is enabled, slow-path traffic is forwarded by the MPLS/ARM module at a faster rate. Also, if LPM is enabled, fast-path traffic to specified vlans or route-maps can be forwarded using longest prefix match on the module without installing IP FDB entries.

Example

The following command enables the Selective-LPM feature:

```
enable lpm
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show accounting

```
show accounting {vlan <vlan name>}
```

Description

Displays accounting statistics for the specified VLAN. If no VLAN is specified, statistics for all VLANs are displayed.

Syntax Description

vlan name	Specifies a VLAN name.

Default

N / A.

Usage Guidelines

You can display the accounting statistics for a single VLAN or all VLANs by issuing the `show accounting <vlan name>` command. The `show accounting <vlan name>` command lists the packet and octet counts for each bin number per VLAN. Omitting the VLAN name displays the accounting statistics for all the VLANs.

Example

The following command displays accounting statistics for the *vlan1* VLAN:

```
show accounting vlan1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show lpm

```
show lpm
```

Description

Shows the status of the LPM feature.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Example

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

22 ATM Commands

The Asynchronous Transfer Mode (ATM) module is an I/O module for the BlackDiamond 6800 series chassis-based system. The ATM module connects a BlackDiamond 6800 series switch to the ATM infrastructure used by service providers or enterprise customers.

Key applications for the ATM module are: interconnecting metropolitan area networks across an ATM network infrastructure, interconnecting server co-location network sites directly using ATM links, and providing connectivity between a legacy Enterprise ATM network and an Ethernet backbone.

In the first application, the metropolitan area network service provider can build service network sites in various cities, then use ATM modules in a BlackDiamond 6800 series switch to connect those cities to a carrier's ATM infrastructure.

In the second application, operators of server co-location networks can use ATM modules in BlackDiamond 6800 series switches to create an ATM-based connection between server co-location sites. The result is that their network is simpler to manage, and problems can be isolated and resolved more expediently.

In the third application, a service provider can provide Ethernet-based services by using ATM modules in a BlackDiamond 6800 series switch to connect their Enterprise ATM network to an Ethernet backbone.

Extreme Networks offers the ATM module in the following configuration:

- A3cSi: four OC-3c/STM-1 single-mode, intermediate-reach optical interfaces

This chapter documents the ATM command set. Some commands are new for the PoS modules; other commands have been enhanced to support the ATM modules.

configure atm add pvc

```
configure atm add pvc <vpi/vci> encap [l2 | ip peer-ipaddress <ipaddress>]
vlan <vlan name> ports <portlist>
```

Description

This command configures PVC on an ATM port.

Syntax Description

vpi	Specifies the VPI parameter as an integer.
	The valid VPI range is from 0 to 15.
vci	Specifies the VCI parameter as an integer.
	The valid VCI range is from 17 to 4095
encap	Specifies the type of encapsulation to be used.
l2	Specifies Layer-2 encapsulation.
ip peer-ipaddress	Specifies that the VLAN will carry only routed IP traffic and that LLC encapsulation should be used.
vlan name	Specifies a VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

None.

Usage Guidelines

Before packets can be forwarded over ATM ports, at least one PVC must be configured on the port and mapped to a VLAN. Each PVC must be mapped to one or more VLANs and each mapping must be designated to use the bridged protocol encapsulation or the routed protocol encapsulation. Both encapsulations can be simultaneously used on a PVC as long as they are associated with different VLANs.

The PVC is identified by the specified `vpi` and `vci` parameters. The `vpi` parameter is an integer in the range of 0 through 15. The `vci` parameter is an integer in the range of 17 through 4095. Both parameters are defined in RFC 2648/1483.

The `encap` parameter indicates the type of encapsulation that is to be used on the PVC for traffic from the associated VLAN. The `l2` keyword is an abbreviation for Layer-2 and indicates the LLC Encapsulation for Bridged Protocols (defined in RFC 2684). The `ip` keyword indicates that the VLAN will carry only routed IP traffic and that the LLC Encapsulation for Routed Protocols (defined in RFC 2684) should be used.

Example

The following command configures PVC 5/101 on ATM port 1:1 on a VLAN named `accounting`.

```
configure atm add pvc 5/102 encap l2 vlan accounting port 1:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure atm delete pvc

```
configure atm delete pvc [<vpi / vci> | all] {vlan <vlan name>} ports
<portlist>
```

Description

This command is used to delete a PVC configuration on an ATM port.

Syntax Description

vpi	Specifies the VPI parameter as an integer.
	The valid VPI range is from 0 to 15.
vci	Specifies the VCI parameter as an integer.
	The valid VCI range is from 17 to 4095
all	Specifies all ATM ports or all PVCs.
vlan name	Specifies a VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

None.

Usage Guidelines

This command deletes the specified PVC configuration on the specified ATM port(s). The optional `vlan` parameter may be used to limit the scope of the command to the specified VLAN. The PVC may still exist following command execution if multiple VLANs have been configured to use the PVC. If the `vlan` parameter is omitted, the PVC configuration is deleted for all VLANs on the specified ATM port(s).

The command can be used to delete configuration information for the PVC identified via the `vpi` and `vci` parameters for all PVCs defined for the specified VLAN(s) or port(s). The `all` keyword may be used as either a portlist parameter to indicate that the command should be applied to all ATM ports or all PVCs. A PVC is completely deleted when there are no longer any VLANs configured for the PVC on a given ATM port.

NOTE

All associated PVCs must be deleted before an ATM port can be removed from a VLAN.

Example

The following command deletes the specified PVC configuration on ATM port 1:1 on a VLAN named `accounting`.

```
configure atm delete pvc 5/102 encap l2 vlan accounting port 1:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure atm scrambling

```
configure atm scrambling [on | off] ports <portlist>
```

Description

This command configures an ATM port to scramble the cell payload on a specified ATM port(s).

Syntax Description

on	Enables payload data scrambling. Default is on.
off	Disables payload data scrambling.
portlist	Specifies list of ports or slots and ports. May be in the form 2:5, 2:6-2:8.

Default

Enabled.

Usage Guidelines

Scrambling is used to improve signal synchronization and the performance of the ATM cell delineation process.

Choose either on or off. Scrambling is enabled by default.

Example

The following command example turns off the scrambling function for port 1 of the ATM module installed in slot 8 of a BlackDiamond switch.

```
configure atm scrambling off ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show atm

```
show atm {<portlist>}
```

Description

This command displays ATM port status.

Syntax Description

portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

None.

Usage Guidelines

You can use the optional `portlist` parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all ports.

By default, the command displays a summary of status information for the specified ports.

The summary of status information includes the following information for each port:

- Values of all port configuration parameters
- Port state
- ATM statistics

The detailed status information includes the summary information plus any ATM statistics. Table 27 describes the ATM receive statistics, and Table 28 describes the ATM transmit statistics.

Table 27: Summary of ATM Receive Statistics

Receive Statistics	Description
Cells Received	Number of cells received.
Cells OAM	Number of Operations, Administration, and Maintenance (OAM) cells received.
Cells Dropped (Congestion)	Number of cells dropped due to insufficient buffers.
Cells Dropped (Invalid VCC)	Number of cells dropped due to invalid VPI/VCI or AAL-5 header.
Cells Dropped (HEC)	Number of cells dropped with Header Error Control (HEC) errors. HEC is an 8 bit cyclic redundancy check (CRC) computed on all fields in an ATM header and capable of detecting bit errors. HEC is used for cell delineation.
PDUs Received	Number of PDUs received.
PDUs Dropped (CRC)	Number of PDUs discarded due to CRC-32 errors.

Table 27: Summary of ATM Receive Statistics (continued)

Receive Statistics	Description
PDUs Dropped (Oversized)	Number of PDUs discarded because they were too large.
PDUs Dropped (Other)	PDUs dropped due to an invalid VLAN ID, Spanning Tree Protocol (STP) state, or invalid encapsulation.

Table 28: Summary of ATM Transmit Statistics

Receive Statistics	Description
Cells Transmitted	Number of cells transmitted.
Cells Dropped (Congestion)	Number of cells dropped due to insufficient buffers.
PDUs Transmitted	Number of PDUs transmitted.

Example

The following command displays ATM port status for all ports:

```
show atm
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show atm pvc

```
show atm [<vpi / vci> | all] {vlan <vlan name>} ports <portlist>
```

Description

This command display status information for a PVC.

Syntax Description

vpi	Specifies the VPI parameter as an integer. The valid VPI range is from 0 to 15.
vci	Specifies the VCI parameter as an integer. The valid VCI range is from 17 to 4095
vlan name	Specifies a VLAN name.
portlist	Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

None.

Usage Guidelines

You can specify a particular PVC to display information for, or you can specify that information for all PVCs be displayed.

Use the optional `vlan` parameter to narrow the range of status information the command displays; otherwise, the command displays status information for all VLANs.

You can use the optional `portlist` parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all PVCs associated with all ATM ports.

By default, the command displays a summary of status information for the specified PVC.

The summary of status information includes the following information for each PVC:

- Port number
- VPI/VCI
- VLAN IDs on this PVC
- Type of PVC (L2 or IP)
- Peer IP address (for IP PVCs)
- Received octets
- Received packets
- Transmitted octets
- Transmitted packets

Example

The following command example displays all of the PVC status information for a PVC configured on an ATM port in a BlackDiamond switch:

```
show atm pvc 5/101 port 1:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

PoS Commands

The Packet over SONET (PoS) modules are I/O modules for the BlackDiamond switch. These modules connect a BlackDiamond 6800 series switch to the SONET infrastructure used by metropolitan area service providers and operators of server co-location networks. (The BlackDiamond 6800 series switch is a chassis-based switch designed to be placed in the core of your network.)

Two key applications for the PoS modules are: interconnecting metropolitan area networks across the SONET network infrastructure, and interconnecting server co-location network sites directly using SONET links.

In the first application, the metropolitan area network service provider can build service network sites in various cities, then use PoS modules in a BlackDiamond switch to connect those cities to a carrier's SONET infrastructure.

In the second application, operators of server co-location networks can use PoS modules in BlackDiamond switches to create a SONET-based connection between server co-location sites. The result is that their network is simpler to manage, and problems can be isolated and resolved more expediently.

This chapter documents the PoS command set. Some commands are new for the PoS modules; other commands have been enhanced to support the PoS modules.

configure aps

```
configure aps <group#> [nonrevert | revert <minutes>]
```

Description

Configures APS operation in either nonrevertive or revertive switching mode.

Syntax Description

group#	Specifies the APS group# to which the command applies.
nonrevert	Specifies nonrevertive switching mode when traffic is active on the protection line and the working line becomes operational.
revert	Specifies revertive switching mode when traffic is active on the protection line and the working line becomes operational.
minutes	Specifies the wait-to-restore (WTR) period in minutes.

Default

The default mode is nonrevertive switching.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the configuration command applies to. The default mode is nonrevertive switching. This parameter determines what action should be taken when traffic is active on the protection line and the working line becomes operational. In revertive mode, traffic will automatically be switched from the protection line to the working line, after the user-defined wait-to-restore (WTR) period, which may be specified via the minutes parameter. The WTR period is intended to prevent frequent switches due to intermittent errors on the working line; service is restored only if no errors are detected on the working line during the WTR period. The minutes parameter is an integer in the range [0-12]. Conversely, in nonrevertive mode, traffic will remain on the protection line (until either manual intervention or a failure on the protection line forces a switch back to the working line). This parameter is only applicable to SONET ports performing the protection line function.

Example

The following command configures an APS operation on group 1001 in revertive switching mode for 5 minutes:

```
configure APS 1001 revert 5
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps add

```
configure aps <group#> add <port> [working | protection <ip address>]
```

Description

Adds a SONET port to an APS group.

Syntax Description

group#	Specifies the APS group# to which the command applies.
port	Specifies the SONET port number to be added to the APS group.
working	Specifies that the port is the working line.
protection	Specifies that the port is the protection line.
ip address	Specifies the IP address of the BlackDiamond switch where working line resides.

Default

By default, no ports are added to an APS group. Ports must be explicitly added using this command for proper APS operation.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the port is to be added to. You also specify the port parameter, which identifies the SONET port that is to be added to the APS group. Additionally, you specify whether the port is designated as the working or protection line. Only one working line and one protection line can be added to an APS group. If the port is designated as the protection line, then you must also specify an IP address (ip address) of the BlackDiamond switch where the working line resides. This IP address is used to send APS control messages to the BlackDiamond switch containing the working line. It is recommended that the configured ip address be associated with an Ethernet VLAN that has loopback mode enabled (to minimize the impact of network outages on APS functionality). It is important that the network connecting working and protection switches always has sufficient bandwidth to support APS control transfers.

In routing configurations, the working line and the protection line should represent the same IP address from a neighboring PPP router's perspective. When the working line and protection line reside in the same BlackDiamond switch, this implies that both ports should be members of the same VLAN. The case where both the working line and the protection line for an APS group reside in the same BlackDiamond switch is the only situation where PPP's IP control protocol (IPCP) can be enabled on multiple SONET ports that are members of the same VLAN. In general, if IPCP is enabled on a SONET, then the port can only be a member of one VLAN, and no others ports can be members of that VLAN.

Example

The following command example adds port 1 of the module installed in slot 8 of the BlackDiamond switch to APS group 1001 as the working line:

```
config aps 1001 add 8:1 working
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps authenticate

```
configure aps <group#> authenticate [off | on <string>]
```

Description

Configures authentication of APS control messages.

Syntax Description

group#	Specifies the APS group# to which the command applies.
off	Specifies that authentication is turned off.
on	Specifies authentication is turned on.
string	Specifies the authentication string used to validate the APS control frames received over an Ethernet link.

Default

The default setting is off.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the authentication command applies to. You also specify whether authentication is to be turned off or turned on. If authentication is being enabled, a text authentication string must also be specified. This string can contain up to eight alphanumeric characters. If the working line and the protection line for an APS group reside in different BlackDiamond switches, then the same string must be configured at both BlackDiamond switches for authentication to work properly. The authentication string is used to validate APS control frames received over an Ethernet link. If authentication fails, the associated APS control frame is discarded.

Example

The following command example enables APS authentication for group 1001, with seer5dog as the authentication string:

```
config aps 1001 authenticate on seer5dog
```

History

This command was first available in ExtremeWare 6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps delete

```
configure aps <group#> delete <port>
```

Description

Deletes a SONET port from an APS group.

Syntax Description

group#	Specifies the APS group# to which the command applies.
port	Specifies the port number.

Default

N/A.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the port is to be deleted from. You also specify the port parameter, which identifies the SONET port that is to be deleted from the APS group. If you delete the working line from a group, it causes a switch to the protection line; however, if you delete an active protection line from a group, it does not initiate a switch to the working line.

Example

The following command example deletes port 1 of the module installed in slot 8 of the BlackDiamond switch from APS group 1001:

```
config aps 1001 delete 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps force

```
configure aps <group#> force [off | working | protection]
```

Description

Requests that an APS group be forced to use a specified line as the active line.

Syntax Description

group#	Specifies the APS group# to which the command applies.
off	Specifies that force is disabled.
working	Specifies that the APS group uses the working line as the active line.
protection	Specifies that the APS group uses the protection line as the active line.

Default

The default is `force off`.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the force command applies to. When `force working` is specified, the command requests that the APS group uses the working line as the active line. Conversely, when `force protection` is specified, the command requests that the APS group uses the protection line as the active line. A forced switch is a high priority request. Only three events can override a forced switch request: (1) a `force off` command, (2) a `lockout on` command (that was either in effect before the force command or issued after the force command), or (3) a signal-fail condition on the protection line. This command is only applicable to SONET ports performing the protection line function. Additionally, the effects of this command are not preserved across a switch reboot.

Example

The following command example forces APS group `1001` to use the protection line as the active line:

```
config aps 1001 force protection
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps lockout

```
configure aps <group#> lockout [off | on]
```

Description

Controls whether a switch to the protection line is locked out.

Syntax Description

group#	Specifies the APS group# to which the command applies.
off	Specifies that switches from the working line to the protection line are allowed.
on	Specifies that switches from the working line to the protection line are prohibited.

Default

The default is off.

Usage Guidelines

The group# identifies the APS group that the lockout command applies to. When lockout on is specified, switches from the working line to the protection line are prohibited, until you subsequently issue a **lockout off** command. The default is lockout off. This command is only applicable to SONET ports performing the protection line function. Additionally, the effects of this command are not preserved across a switch reboot.

Example

The following command example turns on lockout mode for APS group 1001:

```
config aps 1001 lockout on
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps manual

```
configure aps <group#> manual [off | working | protection]
```

Description

Manually determines whether an APS group uses its working line or its protection line as the active line.

Syntax Description

group#	Specifies the APS group# to which the command applies.
off	Specifies that manual switching is disabled, and can be overridden.
working	Specifies that the APS group uses the working line as the active line.
protection	Specifies that the APS group uses the protection line as the active line.

Default

The default is `manual off`.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the command applies to. When `manual working` is specified, the command requests that the APS group uses the working line as the active line. Conversely, when `manual protection` is specified, the command requests that the APS group uses the protection line as the active line. One potential use of the `manual working` command is to switch back to the working line after an error condition has cleared without waiting for the full wait-to-restore period to elapse. A manual switch is a lower priority request than a forced switch. events that can override a manual switch include: (1) a `manual off` command, (2) a `force working` or a force protection command, (3) a `lockout on` command, or (4) a signal-fail or signal degrade line condition. This command is only applicable to SONET ports performing the protection line function. Additionally, the effects of this command are not preserved across a switch reboot.

Example

The following command example configures APS group `1001` to use its working line as the active line:

```
config aps 1001 manual working
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure aps timers

```
configure aps <group#> timers <seconds> <consecutive_misses>
```

Description

Sets the values of the timers used in the APS hello protocol that is exchanged between the working and protection switches for an APS group.

Syntax Description

group#	Specifies the APS group# to which the command applies.
seconds	Specifies the amount of time in seconds the protection switch waits between transmissions of hello packets to the working switch.
consecutive_misses	Specifies the time interval the protection switch will wait before assuming the working switch has failed.

Default

The default values are seconds = 1 and consecutive_misses = 5. These parameters are only applicable to SONET ports performing the protection line function.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the configuration command applies to. The seconds parameter is an integer in the range [1-300] that specifies the amount of time the protection switch waits between transmissions of hello packets to the working switch. The consecutive_misses parameter is an integer in the range [1-100] that controls the time interval the protection switch will wait before assuming that the working switch has failed. If the working switch does not respond within consecutive_misses hello intervals, or (consecutive_misses * seconds) seconds, then the protection switch assumes that the working switch has failed and initiates a line switch.

Example

The following command example configures the timers for APS group 1001 to 1 second and 3 consecutive misses:

```
config aps 1001 timers 1 3
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure diffserv dscp-mapping ports

```
configure diffserv dscp-mapping <input_codepoint>/<output_codepoint> ports
<portlist> {egress {no-congestion | congestion} | ingress}
```

Description

Configures a mapping between an input DiffServ code point (DSCP) and an associated output DSCP for the specified PoS or ATM ports.

Syntax Description

input_codepoint	Specifies one of the 64 possible DiffServ code point values as the input code point.
output_codepoint	Specifies one of the 64 possible DiffServ code point values as the output code point.
portlist	Specifies the port number(s).
egress	Applies the DSCP mapping to the egress direction.
no-congestion	Applies the DSCP mapping to the egress mapping table for the non-congested state.
congestion	Applies the DSCP mapping to the egress mapping table for the congested state.
ingress	Applies the DSCP mapping to the ingress direction.

Default

By default, all the tables are initialized such that DSCPs are not altered by the mapping operations; for example, an input DSCP value of n is always mapped to an output DSCP value of n. Additionally, `dscp-mapping` is performed without regard to whether `diffserv examination` is enabled on the port.

Usage Guidelines

Three DSCP mapping tables are supported per SONET port. One of the tables is used in the ingress direction and two are used for egress flows (onto the SONET link). The two egress tables are for the congested and non-congested states, as determined by the RED algorithm (in other words, the congested state is when the average queue length is greater than the minimum RED threshold). If RED is not enabled on the SONET port, then the egress congested-state mapping table is not used.

The tables are very simple. In the ingress direction, the input DSCP of a packet received from the SONET link is replaced with an output DSCP before the packet is forwarded. The replacement is straightforward; the input DSCP is used as an index into a 64-entry table that contains the output DSCPs associated with each of the input DSCP values. The operation is similar in the egress direction, with the DSCP mapping occurring before the packet is transmitted onto the SONET link(s). The mapping operation is performed after the packet has been assigned to a QoS profile. One potential use of the DSCP mapping capability is reconciliation of varying DiffServ policies at the boundary between autonomous systems (for example, at the boundary between two ISPs). The availability of different tables for the congested / non-congested states is useful for marking operations that increase the drop probability of packets during times of congestion, as discussed in the DiffServ assured forwarding (AF) RFC.

This command is currently only applicable to SONET ports. If the `no-congestion/congestion` keywords are omitted, the mapping is applied to the egress tables for both states. If the `egress/ingress` keywords are omitted, the mapping is assumed to apply to the egress direction, and a symmetrical mapping (with the `input_codepoint` and `output_codepoint` reversed) is automatically configured in the `ingress` direction.

Example

The following command example configures the congested-state mappings for DSCPs 10 (AF11):

```
configure diffserv dscp-mapping 10/12 egress congestion
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure dot1q tagmapping ports

```
configure dot1q tagmapping <input_vlanid/output_vlanid> ports <portlist>
{egress {priority <priority>} | ingress {priority <priority>}}
```

Description

Configures the VLAN tag mapping attributes for a PoS or ATM port.

Syntax Description

input_vlanid	Specifies VLAN ID of the input to be mapped.
output_vlanid	Specifies the VLAN ID of the output to be mapped.
portlist	Specifies the port number(s).
ingress	Indicates that the mapping is to be applied to input frames received from the PPP link.
egress	Indicates that the mapping is to be applied to input frames going to the PPP link.
priority	Allows you to set the 802.1p priority value.

Default

The default is to initialize the tables so the VLAN IDs are not altered by the mapping operations (for example, an input VLAN ID of n is always mapped to an output VLAN ID of n), and the frame priority is preserved.

Usage Guidelines

This command is only applicable when BCP is enabled on the port. Currently, the command is only supported for PoS ports. Two mapping tables are supported per PoS port. One of the tables is used in the egress direction and the other table is used in the ingress direction. Each of the tables enable an input VLAN ID to be mapped to an output VLAN ID, which can be useful in reconciling policy differences at customer/service provider boundaries. The egress keyword indicates that the mapping is to be applied to frames received from the switch backplane before transmission onto the PoS link(s). Conversely, the ingress keyword indicates that the mapping is to be applied to input frames received from the PoS link. The mappings are applied following classification to a QoS profile.

Frames containing the specified input_vlanid are altered such that the VLAN ID is set to the specified output_vlanid before the frame is forwarded. The tables also allow the option of preserving the 802.1p priority or overwriting the priority field with a configured value. The priority keyword indicates that the 802.1p priority field is to be set to the value of the priority parameter. Omission of the priority keyword indicates that the 802.1p priority of the frame is to be preserved. If the egress/ingress keywords are omitted, the specified mapping is applied to the egress direction, and a symmetrical mapping (with the input_vlanid and output_vlanid reversed) is automatically configured in the ingress direction. The input_vlanid and output_vlanid parameters are integers in the range [1-4095]. The priority parameter is an integer in the range [0-7].

Example

The following command configures the tagmapping attributes for input VLAN ID 30 and output VLAN ID 130 for port 1 of the module installed in slot 8 for the input frames from the PPP link:

```
configure dot1q tagmapping 30/130 port 8:1 ingress
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure dot1q tagnesting ports

```
configure dot1q tagnesting {<vlanid> | <vlanid_range>} [off | pop | push
<new_vlanid> {priority <priority>}] ports <portlist> {egress | ingress}
```

Description

Configures the VLAN tag nesting attributes for a PoS or ATM port. Currently, the command is only supported for PoS and ATM ports.

Syntax Description

vlanid	Specifies that the tag nesting will be performed on the frames containing the VLAN ID given.
vlanid_range	Specifies that the tag nesting will be performed on the frames containing VLAN ID values in the given range.
off	Disables tag nesting.
pop	Deletes a tag from the frame.
push	Adds a tag to the frame.
new_vlanid	Specifies the VLAN ID of the tag to be added or deleted from the frame.
priority	Allows you to set the 802.1p priority value.
portlist	Specifies the port number(s).
egress	Specifies that the tag operations are to be performed to the PPP link.
ingress	Specifies that the tag operations are to be performed from the PPP link.

Default

By default, tag nesting is off for all VLAN IDs. If the `egress/ingress` keywords are omitted, the direction defaults to `egress`. Additionally, if the `egress/ingress` keywords are omitted and a tag push operation is configured, a corresponding tag pop operation is automatically configured for the `ingress` direction. Similarly, if the `egress/ingress` keywords are omitted and tag nesting is configured off, it is disabled in both directions.

Usage Guidelines

The command provides support for nested 802.1Q tags by allowing a tag push/pop attribute to be associated with a VLAN ID. The push attribute indicates that a new tag is to be added to the frame, while the pop attribute indicates that the top-level tag is to be removed from the frame. The `push` keyword indicates that a new tag is to be added to frames containing the specified `vlanid` or one of the VLAN IDs in the specified `vlanid_range`. The syntax of the `vlanid_range` parameter is `start_vlanid-end_vlanid`. Omission of the `vlanid/vlanid_range` parameter indicates that the command settings should be applied to all VLAN IDs. For push operations, the new tag added to frames contains the specified `new_vlanid`.

The `pop` keyword indicates that the top-level tag is to be removed from frames when the tag contains any of the specified VLAN IDs. Tag operations may be performed in either `egress` (to the PoS link) or `ingress` directions.

When a new tag is pushed, an option is available to allow the 802.1p priority of the frame to be either preserved or set to a configured value. The priority keyword indicates that the 802.1p priority field is to

be set to the value of the priority parameter. Omission of the `priority` keyword indicates that the 802.1p priority of the frame is to be preserved. The `vlanid` parameters are integers in the range [1-4095]. The `priority` parameter is an integer in the range [0-7].

This command is only applicable when BCP is enabled on the port. Furthermore, tag push operations are applicable to egress frames only when the port is configured to transmit tagged frames for the associated VLAN. The tag-nesting operations are only applicable to `ingress` frames that contain a VLAN tag. The tag-nesting operations are applied after classification to a QoS profile. The default PPP MRU is sufficient for a single level of tag nesting (where the frame contains two VLAN tags) between two Extreme switches; jumbo frame support must be enabled if higher levels of VLAN tag nesting are needed.

The DiffServ/RED functions are not performed by PoS ports when frames contain nested tags (in other words, more than one tag).

Example

The following command adds VLAN `140` to the frame for port 1 of the module installed in slot 8 for input frames from the PPP link:

```
configure dot1q tagnesting push 140 port 8:1 ingress
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure flowstats export add

```
configure flowstats export {<group#>} add [<ip address> | <hostname>]
<udp_port>
```

Description

Configures the flow-collector devices to which NetFlow datagrams are exported.

Syntax Description

export <group#>	Specifies a particular export distribution group on a per-filter basis. Identifies the set of flow collector devices to which records for flows matching the filter are to be exported.
ip address	Specifies the IP address of the flow-collector destination.
hostname	Specifies the host name of the flow-collector destination.
udp_port	Specifies the UDP port number of the flow-collector destination.

Default

By default, no flow-collector destinations are configured.

Usage Guidelines

A flow-collector destination is identified by either an IP address and UDP port #, or by a hostname and UDP port #, to which NetFlow export datagrams are transmitted. The command allows flow-collector destinations to be added. Up to 8 flow-collector destinations can be configured for each group, and up to 32 groups can be defined per switch. The optional group# parameter, which identifies the specific group the destination is being configured for, is an integer in the range [1..32]. The group# defaults to 1 if the parameter is omitted. At least one flow-collector destination must be configured for NetFlow datagrams to be exported to a group.

When multiple flow-collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations. This NetFlow-distribution feature enables a scalable collection architecture that is able to accommodate high volumes of exported data. The distribution algorithm ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that flow records for both the ingress and egress directions of a TCP or UDP connection are exported to the same collector (when both flows traverse the same SONET link and both filters are configured to export to the same group).

Example

The following command adds a flow-collector destination of 10.1.1.88 for group 5 using UDP port 2025 to which NetFlow datagrams are exported:

```
configure flowstat export 5 add 10.1.1.88 2025
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure flowstats export delete

```
configure flowstats export {<group#>} delete [<ip address> | <hostname>]
<udp_port>
```

Description

Configures the flow-collector devices to which NetFlow datagrams are exported.

Syntax Description

export <group#>	Specifies a particular export distribution group on a per-filter basis. Identifies the set of flow collector devices to which records for flows matching the filter are to be exported.
ip address	Specifies the IP address of the flow-collector destination.
hostname	Specifies the host name of the flow-collector destination.
udp_port	Specifies the UDP port number of the flow-collector destination.

Default

N / A.

Usage Guidelines

A flow-collector destination is identified by either an IP address and UDP port #, or by a hostname and UDP port #, to which NetFlow export datagrams are transmitted. The command allows flow-collector destinations to be `deleted`. Up to 8 flow-collector destinations can be configured for each group, and up to 32 groups can be defined per switch. The optional `group#` parameter, which identifies the specific group the destination is being configured for, is an integer in the range [1..32]. The `group#` defaults to 1 if the parameter is omitted. At least one flow-collector destination must be configured for NetFlow datagrams to be exported to a group.

When multiple flow-collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations. This NetFlow-distribution feature enables a scalable collection architecture that is able to accommodate high volumes of exported data. The distribution algorithm ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that flow records for both the ingress and egress directions of a TCP or UDP connection are exported to the same collector (when both flows traverse the same SONET link and both filters are configured to export to the same group).

Example

The following command deletes a flow-collector destination of `10.1.1.88` for group `5` to which NetFlow datagrams are exported:

```
configure flowstat export 5 delete 10.1.1.88 2025
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure flowstats filter ports

```
configure flowstats filter <filter#> {aggregation} {export <group#>} ports
<portlist> [ingress | egress] <filterspec>
```

Description

Configures a flow record filter for the specified SONET ports.

Syntax Description

filter#	The `filter#` parameter is an integer in the range from 1 to 8 that operates with either the `ingress` or `egress` keyword to identify the filter that is being defined.
aggregation	Reduces the volume of exported data, use this optional keyword to maintain a single set of statistics for all the flows that match the specified filter.
export <group# tn	Specifies a particular export distribution group on a per-filter basis. Identifies the set of flow collector devices to which records for flows matching the filter are to be exported.
portlist	Specifies the port number(s).
ingress	Use this keyword to specify that the filter being defined in the command is one of the eight filters to be applied to ingress flows.
egress	Use this keyword to specify that the filter being defined in the command is one of the eight filters to be applied to egress flows.

filterspec	Each filter is defined using a *value/filtermask* pair for each of the five components in the following sequence:
	{des tination IP address, source IP address,
	destination port number, source port number, protocol}
	in the form:
	`[{dest-ip <ipaddress_value/ipaddress_filtermask>}`
	`{source-ip <ipaddress_value/ipaddress_filtermask>}`
	`{dest-port <port_value/port_filtermask>}`
	`{source-port <port_value/port_filtermask>}`
	`{protocol <protocol_value/protocol_filtermask>} |`
	`match-all-flows | match-no-flows]`
	The `ipaddress_filtermask`, `port_filtermask`, and `protocol_filtermask` parameters are configured using hexadecimal notation.
	You can also use either the `match-all-flows` keyword or the `match-no-flows` keyword in place of settings for the five components. The `match-all-flows` keyword adjusts the *value/filtermask* settings for all the components to 0/0 such that the filter matches any flow. The `match-no-flows` keyword adjusts the *value/filtermask* settings for all the components such that the filter does not match any flow.

Default

By default, filter#1 is configured to `match-all-flows`, and the remaining filters are configured to `match-no-flows`. The `group#` defaults to 1 if the parameter is omitted.

Usage Guidelines

The command allows a port to be configured to selectively maintain statistics for only those flows that match the specified filters. Sixteen filters are supported for each port, eight filters for ingress flows and another eight filters for egress flows. The `filter#` parameter and either the `ingress` or `egress` keyword are specified to identify the filter that is being configured. The `filter#` parameter is an integer in the range [1..8]. The filters are comprised of a value/filtermask pair for each component of the {destination IP address, source IP address, destination port number, source port number, protocol} 5-tuple. Conceptually, the filters work by ANDing the contents of each 5-tuple component of a forwarded flow with the associated masks from filter#1. Statistics are maintained if the results of the AND operations match the configured filter values for all fields of the 5-tuple. If there is no match, then the operation is repeated for filter#2, and so on. If there is no match for any of the filters, then statistics are not maintained for the flow. Filters for any/all of the 5-tuple components can be configured with a single command.

The `filterspec` parameter also supports the `match-all-flows` and `match-no-flows` keywords. The `match-all-flows` keyword adjusts the settings such that the filter matches any flow (that is, the value/filtermask pairs are set to 0/0 for all the 5-tuple components), while the `match-no-flows` keyword adjusts the settings such that the filter does not match any flow.

The optional `aggregation` keyword may be used to indicate that a single set of statistics is to be maintained for all the flows that match the filter, which can substantially reduce the volume of exported data. A particular export distribution group may also be specified on a filter-basis. The `group#` parameter identifies the set of collector devices that records for flows matching the filter are to be exported to.

Example

The following command example configures a filter to collect statistics on ingress flows destined for `192.168.1.1` from the `192.169.0.0/16` subnet with a destination port of `80` using protocol `6`:

```
config flowstats filter 1 export 1 ports all ingress
   dest-ip 192.168.1.1/FFFFFFFF source-ip 192.169.0.0/FFFF0000
   dest-port 80/FFFF source-port 0/0 protocol 6/FF
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure flowstats source ipaddress

```
configure flowstats source ipaddress <ip address>
```

Description

Configures the IP address that is to be used as the source IP address for NetFlow datagrams to be exported.

Syntax Description

ip address	Specifies the source IP address to be used as the source for NetFlow datagrams to be exported.

Default

Normal.

Usage Guidelines

No NetFlow datagrams will be exported until the source `ip address` is configured. Flow-collector devices may use the source IP address of received NetFlow datagrams to identify the switch that sent the information. It is recommended that the configured `ip address` be associated with a VLAN that has loopback mode enabled.

Example

The following command example specifies that the IP address `192.168.100.1` is to be used as the source IP address for exported NetFlow datagrams:

```
configure flowstats source ipaddress 192.168.100.1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20 for the PoS module only.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ports tunnel hdlc

```
configure ports <portlist> tunnel hdlc [off | mpls]
```

Description

Enables tunneling for HDLC encapsulated frames from a SONET port through an MPLS network.

Syntax Description

portlist	Specifies the SONET port number(s).
off	Disables HDLC tunneling.
mpls	Enables an MPLS TLS-tunnel.

Default

The default is `off`.

Usage Guidelines

The ingress SONET port encapsulates the entire HDLC frame (including the HDLC header and FCS) inside an Ethernet/MPLS header. The egress SONET port strips the Ethernet/MPLS header and forwards the HDLC frame. HDLC idle bytes (x7E) are not tunneled, but runts and aborted frames are. HDLC control bytes are destuffed on ingress and stuffed on egress.

When a SONET port is configured for HDLC tunneling, PPP should not be configured on the port (BCP and IPCP should be off). Furthermore, the port should be the only port in a VLAN and a MPLS TLS-tunnel should be configured for this VLAN. The payload inside HDLC could be PPP or some other HDLC-encapsulated protocol. SONET APS (automatic protection switching) is supported between tunneled PoS ports on the same module or different modules in the same switch. APS for tunneled ports is not supported for ports on different switches.

Example

The following command example configures an HDLC tunnel, and applies to a PoS module installed in slot 1 of a BlackDiamond switch:

```
configure ports 1:4 tunnel hdlc mpls
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ppp ports

```
configure ppp [bcp [on | off] | ipcp [on {peer-ipaddress <ip address>} |
off]] ports <portlist>
```

Description

Configures the network control protocol that will run on the specified PPP ports.

Syntax Description

bcp	Specifies bridging control protocol for the port.
ipcp	Specifies IP control protocol for the port.
on	Enables the designated protocol on the port.
off	Disables the designated protocol on the port.
peer-ipaddress	Allows you to configure IP address of the peer router.
ip address	Specifies IP address of the peer router.
portlist	Specifies the port number(s).

Default

By default, BCP is enabled on all PoS ports. (However, ports 2 and 4 of OC-3c modules are not members of any VLANs by default; all other ports are members of the default VLAN by default.)

Usage Guidelines

The `bcp` keyword represents the bridging control protocol (BCP), and the `ipcp` keyword represents the IP control protocol. IPCP and BCP are mutually exclusive configuration options for a given port (that is, they cannot both be enabled simultaneously on the same port). Generally, when IPCP is enabled on a port, the port must be a member of one and only one VLAN. Furthermore, no other ports can be members of this VLAN, and IP routing is the only protocol supported on the VLAN. The one exception to this rule occurs when SONET automatic protection switching (APS) is enabled. A single VLAN can contain two IPCP-enabled ports if they are members of the same APS group.

The `peer-ipaddress` keyword provides an option to configure the IP address of the peer router. This can be useful with peer routers that do not advertise their IP address using the IPCP IP address configuration option (for example, Juniper routers). If the peer router does advertise an IP address via IPCP, the configured `peer-ipaddress` is ignored.

BCP enables Ethernet MAC frames to be transported across a PPP link. Thus, any protocol can be transported across a BCP connection. Essentially, BCP enables the PPP link to appear as an Ethernet LAN segment to the rest of the switch. Therefore, the port may be a member of multiple VLANs, and frames can be either bridged or routed onto the link. There are restrictions regarding which ports can be bridged together (in other words, they may be members of the same VLAN) on the OC-3 PoS Module. Ports 1 and 2 on the same OC-3 module cannot be bridged together (unless they are members of the same APS group). Additionally, ports 3 and 4 on the same OC-3 module cannot be bridged together (unless they are members of the same APS group). There are no similar restrictions regarding bridging ports together on the OC-12 PoS Module.

PoS operation requires at least one Ethernet I/O module be operational in the chassis. IPCP cannot be enabled on a port unless BCP is off, and vice versa. IPCP is recommended when a PoS port only carries

routed IP traffic (because IPCP imposes less header overhead, the maximum link throughput is higher than with BCP).

Example

The following command example configures BCP on the PPP port, and applies to a PoS module installed in slot 1 of a BlackDiamond switch:

```
configure ppp bcp off port 1:4
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.

configure ppp authentication ports

```
configure ppp authentication [off | chap | pap | chap-pap] ports <portlist>
```

Description

Configures authentication on the specified PPP ports.

Syntax Description

off	Disables authentication
chap	Authenticates the peer using the challenge handshake authentication protocol (CHAP).
pap	Authenticates the peer using the password authentication protocol.
chap-pap	Specifies that either CHAP or PAP may be used to authenticate the peer.
portlist	Specifies the port number(s).

Default

The default is authentication `off`.

Usage Guidelines

When `off` is specified, the peer is not authenticated. When `chap` is specified, the peer is authenticated using the challenge handshake authentication protocol (CHAP). When `pap` is specified, the peer is authenticated via the password authentication protocol (PAP). Specification of `chap-pap` indicates that either CHAP or PAP may be used to authenticate the peer.

Example

The following command example turns on CHAP authentication for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp authentication chap ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.

configure ppp delayed-down-time ports

```
configure ppp delayed-down-time <seconds> ports <portlist>
```

Description

Configures the delayed-down-time interval used by PPP for the specified ports.

Syntax Description

seconds	Specifies interval for delayed-down-time in seconds.
portlist	Specifies the port number(s).

Default

The default value is 1 second.

Usage Guidelines

The delayed-down-time interval is the amount of time that PPP waits before declaring a port down after a physical link failure has been detected. A non-zero value is useful when recovery from the link failure is fast (for example, when APS is enabled on a SONET port). In this case, APS may be able to recover from the link failure fast enough that there is no need to perturb the logical connection with the peer PPP entity, which minimizes network down time. A non-zero value is desirable when APS is configured at either end of the link. The delayed-down-time parameter is configured in seconds, with a valid range of [0..20].

Example

The following command example sets the delayed-down-time interval to 2 seconds for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp delayed-down-time 2 ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ppp echo ports

```
configure ppp echo [<seconds> <consecutive_misses> | off] ports <portlist>
```

Description

Configures the link maintenance protocol on the specified ports.

Syntax Description

seconds	Specifies the amount of time in seconds between transmissions of echo-request packets.
consecutive_ misses	Controls the amount of time that PPP waits for a reply.
off	Disables the link maintenance protocol.
portlist	Specifies the port number(s).

Default

The link maintenance protocol is `off` by default.

Usage Guidelines

When link maintenance is enabled and the port is receiving no packets, echo-request packets are transmitted over the link on a periodic basis. The `seconds` parameter in an integer in the range [1..300] that specifies the amount of time between transmissions of echo-request packets. The `consecutive_misses` parameter is an integer in the range [1..100] that controls the amount of time that PPP waits for a reply. If an echo-reply is not received within an interval of duration (`consecutive_misses` * `seconds`) seconds, the link is brought down. The link maintenance protocol may be disabled using the `off` keyword.

Example

The following example enables link maintenance on port 1 of a PoS module in slot 8 and sets `seconds` to 3 and `consecutive misses` to 10:

```
config ppp echo 3 10 ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ppp pos checksum ports

```
configure ppp pos checksum [32 | 16] ports <portlist>
```

Description

Configures the size of the HDLC Frame Check Sequence (FCS) to be used on the specified SONET ports.

Syntax Description

16 or 32	Specifies the size of the HDLC frame check sequence (either 32 bits or 16 bits).
portlist	Specifies the port number(s).

Default

The default is a 32-bit FCS.

Usage Guidelines

The two choices are a 32-bit FCS or a 16-bit FCS. RFC 2615 recommends that a 32-bit FCS be used.

Example

The following command example sets the FCS to 16 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp pos checksum 16 ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ppp pos scrambling ports

```
configure ppp pos scrambling [on | off] ports <portlist>
```

Description

Specifies whether the payload data should be scrambled on the specified ports. RFC 2615 recommends that the SONET payload be scrambled.

Syntax Description

on	Enables scrambling.
off	Disables scrambling.
portlist	Specifies the port number(s).

Default

The default is scrambling on.

Usage Guidelines

The option of disabling scrambling is provided for backward compatibility with an earlier (now obsoleted) PoS standard specified in RFC 1619. Scrambling was introduced in RFC 2615 to alleviate potential security problems where malicious users might generate packets with bit patterns that create SONET synchronization problems.

Example

The following command example turns off the scrambling function for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp pos scrambling off ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ppp quality ports

```
configure ppp quality [off | <required_percent> {<seconds>}]
ports <portlist>
```

Description

Configures the Link Quality Monitoring (LQM) protocol on the specified ports.

Syntax Description

off	Disables link quality monitoring protocol.
required_percent	Specifies required link drop percentage for link quality management (LQM).
seconds	Specifies how often (in seconds) the quality reports are to be received from the peer LQM entity.
portlist	Specifies the port number(s).

Default

The default value of `seconds` is 30. By default, LQM is `off`.

Usage Guidelines

LQM periodically transmits counts of packets/octets that were transmitted, along with counts of packets/octets that were successfully received. This information enables LQM to determine the percentage of data that is being dropped due to poor link quality. If the drop percentage is greater than (100 - `required_percent`), all network-layer protocols running over the link are brought down. You may want to bring a poor-quality link down when an alternate network path exists, or when billing is based on the amount of data transmitted. The `required_percent` parameter is an integer in the range [1..99]. The `seconds` parameter is an integer in the range [1..300] that determines how often quality reports are to be received from the peer LQM entity (that is, the reporting interval). Specifying the `seconds` parameter is optional. It can take up to seven reporting intervals for LCP to bring a link down. If the link quality subsequently improves, LCP will automatically bring the link back up; this type of service restoration will take a minimum of 7 reporting intervals.

Example

The following example enables the LQM protocol on port 1 of a PoS module in slot 3 and sets `required_percent` to 95. Because no value is specified for the optional `seconds` parameter, the command uses the default of 30 seconds:

```
config ppp quality 95 ports 3:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure ppp user ports

```
configure ppp user <name> {encrypted} {<password>} ports <portlist>
```

Description

Configures the user name and password that the specified PPP port uses in the event the PPP peer requests authentication.

Syntax Description

name	Specifies user name for PPP peer authentication requests.
encrypted	This parameter option should not be entered.
password	Specifies the password for PPP peer authentication requests.
portlist	Specifies the port number(s).

Default

The default value of both name and password is **extreme**.

Usage Guidelines

The name is also sent when a port transmits a CHAP authentication request. The implementation responds to either CHAP or PAP authentication requests issued by the peer regardless of whether the port is configured to authenticate the peer. The name parameter is a string with a length in the range of [1..32] characters. The password parameter is also a character string, with a maximum length of 32 characters. If no password is provided on the command line, then you are prompted to enter the password twice (with the second time serving as a confirmation). You should not enter the encrypted parameter option (it is used by the switch when generating an ASCII configuration).

Example

The following command example sets the name to titus and sets the password to 1Afortune for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp user "titus" "1Afortune" ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the on the BlackDiamond switch. A similar command is available on the Alpine switch.

configure qosprofile

```
configure qosprofile <qosprofile> {minbw <percent>} {maxbw <percent>}
{priority <level>} {minbuf <percent>} {maxbuf <percent>} {<portlist>}
{egress | ingress}
```

Description

Configures a QoS profile.

Syntax Description

qosprofile	Specifies the QoS profile to be configured.
minbw	Specifies the minimum percentage of the bandwidth available for transmissions from the profile.
maxbw	Specifies the maximum percentage of the bandwidth that can be used for transmissions from the profile.
priority	Specifies which traffic is scheduled when bandwidth is still available after the minimum requirements of all profiles have been satisfied.
level	Specifies the priority level (low, lowHi, normal, normalHi, medium, mediumHi, high, or highHi).
minbuf	This keyword is not applicable to SONET ports.
maxbuf	This keyword is not applicable to SONET ports.
portlist	Specifies the port number(s).
egress	Specifies that the flow is from the SONET port.
ingress	Specifies that the flow is to the SONET port.

Default

Normal.

Usage Guidelines

The optional `egress` and `ingress` keywords have been added to support the PoS module. These new keywords are currently only applicable to PoS ports. The PoS modules support eight egress queues and eight ingress queues per port, and the scheduling parameters for these queues are controlled by QoS profiles `qp1-qp8` (in other words, queue #0 is controlled by `qp1`, queue #1 by `qp2`, and so on). The `portlist` parameter allows QoS profiles to be customized on a SONET-port basis, while the `egress` and `ingress` keywords enable even finer customization (down to a particular `egress` or `ingress` queue on a given port). If the `egress` and `ingress` keywords are omitted, then the configured parameters apply to the `egress` queue associated with the specified `qosprofile`.

The `minbw` parameter is an integer in the range [0..100] that specifies the minimum percentage of the bandwidth that must be available for transmissions from the profile. The sum of the `minbw` parameters across all eight profiles cannot exceed 90%.

The maxbw parameter is also an integer in the range [1..100] that specifies the maximum percentage of the bandwidth that can be used for transmissions from the profile. The priority level may be set to low, lowHi, normal, normalHi, medium, mediumHi, high, or highHi. The priority determines which traffic is scheduled when bandwidth is still available after the minimum requirements of all profiles have been satisfied.

The `minbuf` and `maxbuf` keywords are not applicable to PoS ports.

Example

The following command configures the QoS profile in the egress direction, with a minimum bandwidth of 10 percent and a maximum of 20 percent:

```
config qosprofile qp8 minbw 10 maxbw 20 2:1-2:2 egress
```

History

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support the PoS module.

Platform Availability

This command is available on the BlackDiamond switch only.

configure red

```
configure red [drop-probability | low-drop-probability |
high-drop-probability] <percent> {ports <portlist>}
```

Description

Configures the RED drop probability for a specified port.

Syntax Description

drop-probability	Specifies both the high and low drop probability rates.
low-drop-probability	Sets the low drop probability rate.
high-drop-probability	Sets the high drop probability rate.
percent	Specifies the percentage for the drop probability.
portlist	Specifies the port number(s).

Default

For PoS ports, both the low and high drop-probabilities default to 10%.

Usage Guidelines

The optional `low-drop-probability`, `high-drop-probability`, and `ports` keywords have been added to support the PoS module. Currently, these new keywords are only supported for SONET ports. Omission of the `ports` keyword indicates that the setting is to be applied to all ports.

The drop probability is specified as a percentage, where the `percent` parameter is an integer in the range [1..100]. The implementation provides weighted RED (WRED) functionality via support for two different drop probabilities: a `low-drop-probability` and a `high-drop-probability`. The DSCPs of IP packets indicate whether the packet should be dropped with low probability or high probability, and the appropriate percentage is then applied if WRED is active. WRED is only applied to IP packets, and the `configure diffserv examination code-point` command supports complete flexibility in assigning DSCPs to the two different drop-probability levels. The configured mapping of DSCPs to drop-probability levels is used by WRED even if `diffserv examination` is disabled on the port.

The `drop-probability` keyword indicates that the specified percentage should be used for both the low and high drop-probabilities, which effectively disables WRED and reverts to standard RED operation. RED is active when the average queue length is between the minimum and maximum thresholds. In this region, the probability that a given packet is dropped increases linearly up to the configured drop probability at the maximum threshold. All packets are dropped when the average queue length exceeds the maximum threshold.

Example

The following command configure a RED high drop-probability of 20% on the SONET ports:

```
config red high-drop-probability 20 ports 2:1-2:2
```

History

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

Platform Availability

This command is available on the BlackDiamond switch only.

configure red min-threshold ports

```
configure red min-threshold <percent> ports <portlist>
```

Description

Configures the minimum queue length threshold for RED operation on the specified PoS ports.

Syntax Description

percent	Specifies the percentage for the minimum queue length threshold for RED operation.
portlist	Specifies the port number(s).

Default

By default, `min-threshold` is 10% for PoS ports.

Usage Guidelines

When this threshold is exceeded, the RED algorithm is activated. Currently, the command is only applicable to PoS ports. The `ports` keyword allows the threshold parameter to be configured on a PoS-port basis. The *min-threshold* is specified as a percentage, where the `percent` parameter is an integer in the range [1..100]. For PoS ports, the minimum threshold is a percentage of 1000 packet buffers, and the maximum threshold is set to minimum ((3 * minimum threshold buffers), maximum available buffers). The settings for both the minimum and maximum thresholds, in terms of number of buffers, are displayed by the `show ports info detail` command.

Example

The following command configures minimum queue length threshold of 50 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
configure red min-threshold 50 port 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet clocking ports

```
configure sonet clocking [line | internal] ports <portlist>
```

Description

Configures the clocking source for the specified SONET ports.

Syntax Description

line	Sets the line clocking on the specified port.
internal	Sets internal clocking on the specified port.
portlist	Specifies the port number(s).

Default

The default setting is `internal`.

Usage Guidelines

The clock is recovered from the received bitstream when `line` clocking is configured.

Example

The following command example selects line clocking for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet clocking line ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet framing ports

```
configure sonet framing [sonet | sdh] ports <portlist>
```

Description

Configures the framing type for the specified SONET ports.

Syntax Description

sonet	Sets the framing type to SONET.
sdh	Sets the framing type to SDH.
portlist	Specifies the port number(s).

Default

The default setting is sonet.

Usage Guidelines

You can configure each port for framing that complies with either the SONET standard or the SDH standard. SONET is primarily an American standard; SDH is the international version.

Example

The following command example selects SDH framing for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet framing sdh ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet loop

```
configure sonet loop [internal | line | off] ports <portlist>
```

Description

Configures loopback options for the specified SONET port(s).

Syntax Description

internal	Sets the signal to be looped back onto the receive interface.
line	Sets the signal to be looped back onto the transmit interface.
off	Disables the loopback setting. Default is `off`.
portlist	Specifies the port number(s).

Default

The default setting is `off`.

Usage Guidelines

SONET loopback is only available on OC-12 ports. Configuring loopback on a SONET port may be useful for diagnostics or network troubleshooting. When internal loopback is configured, the transmitted signal is looped back onto the receive interface. When line loopback is configured, the received signal is looped back onto the transmit interface.

Example

The following command configures loopback on SONET port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet loop internal ports 8:1
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet signal label ports

```
configure sonet signal label [auto | <hex_octet>] ports <portlist>
```

Description

Configures the signal label value for the specified SONET ports.

Syntax Description

auto	Enables the signal label field to be automatically set.
hex_octet	Allows you to set the signal label field to a particular hex octet value.
portlist	Specifies the port number(s).

Default

The default is `auto`, where the value of the signal Label field is automatically set based on standard conventions for the given payload type.

Usage Guidelines

The signal label field occupies one byte of the path overhead associated with each SONET frame. It is used to indicate the type of contents carried in the SPE. For example, 0x16 indicates scrambled PPP/HDLC, while 0xCF indicates unscrambled PPP/HDLC. The default may be overridden by specifying a particular `hex octet` that is to be used instead, where `hex octet` is a hexadecimal integer in the range [0..xFF]. It may be necessary to specify a particular `hex octet` in order to interoperate with implementations that do not follow the standard conventions for the signal label field.

Example

The following command example sets the Signal Label to the hexadecimal value `CF` for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet signal label CF ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet threshold signal degrade ports

```
configure sonet threshold signal degrade <error_rate> ports <portlist>
```

Description

Configures the signal degrade threshold for the specified SONET ports.

Syntax Description

error_rate	Sets the threshold for the bit error rate for the SONET line.
portlist	Specifies the port number(s).

Default

The default is 10^{-6}.

Usage Guidelines

A signal degrade (SD) event is generated if the bit error rate (BER) for the SONET line exceeds the configured threshold. If automatic protection switching (APS) is enabled on the port, a SD event will initiate a line switch. The `error_rate` parameter is an integer in the range [5-9], where the SD BER is 10-`error_rate`. The default value of the `error_rate` parameter is 6, which equates to a SD BER of 10^{-6}, or 1 per million.

Example

The following command example sets the Signal Degrade threshold value to `8` for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet threshold signal degrade 8 ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet threshold signal fail ports

```
configure sonet threshold signal fail <error_rate> ports <portlist>
```

Description

Configures the signal failure threshold for the specified SONET ports.

Syntax Description

error_rate	Sets the signal failure threshold for the SONET ports.
portlist	Specifies the port number(s).

Default

The default is 10^{-5}.

Usage Guidelines

A signal failure (SF) event is generated if the bit error rate (BER) for the SONET line exceeds the configured threshold. A SF event brings the port down. If automatic protection switching (APS) is enabled on the port, a SF event will initiate a line switch. The `error_rate` parameter is an integer in the range [3-5], where the SF BER is 10^{-error_rate}. The default value of the `error_rate` parameter is 5, which equates to a SF BER of 10^{-5}, or 1 per hundred thousand.

Example

The following command example sets the signal fail threshold value to 3 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet threshold signal fail 3 ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet trace path ports

```
configure sonet trace path <id_string> ports <portlist>
```

Description

Configures the path trace identifier string for the specified SONET ports.

Syntax Description

id_string	Specifies the path trace identifier string for the SONET ports.
portlist	Specifies the port number(s).

Default

The default is null.

Usage Guidelines

Path trace is a maintenance feature of SONET. One byte of the path overhead associated with each SONET frame is used to carry information identifying the originating path terminating equipment (PTE). The `id_string` parameter is a string that may contain up to 64 characters (which always includes a carriage return and a line feed character at the end). By default, `id_string` contains an IP address assigned to the VLAN that the port is a member of. This IP address is represented in dotted-decimal notation. If no IP address is assigned to the port's VLAN, `id_string` defaults to a string of 64 NULL characters. When SONET framing is configured, a 64-character string is repetitively transmitted, one character per frame. If the configured string is less than 64 characters, it is padded with NULL characters. Operation is similar when SDH framing is configured, except that the maximum string length is 15 characters. If necessary, the configured `id_string` is truncated to 15 characters.

Example

The following command example sets the path trace identifier to the string `parador` for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet trace path parador ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

configure sonet trace section ports

```
configure sonet trace section [<id_byte> | string <id_string>]
ports <portlist>
```

Description

Configures the section trace identifier for the specified SONET ports.

Syntax Description

id_byte	Configures the ID byte section trace identifier for the specified SONET port.
id_string	Configures the ID string section trace identifier for the specified SONET port.
portlist	Specifies the port number(s).

Default

The default is 1 for SONET, null for SDH.

Usage Guidelines

Section trace is a maintenance feature of SONET. One byte of the section overhead associated with each SONET frame is used to carry information identifying the transmitting equipment. The section trace identifier has two forms: an `id_byte` and an `id_string`. The `id_byte` parameter is an integer in the range [0-255], with a default value of 1. The `id_string` parameter is a string that may contain up to 15 characters. By default, `id_string` contains 15 NULL characters. The `id_byte` parameter is only applicable when SONET framing is configured. In this case, the configured `id_byte` value is transmitted in each SONET frame. Analogously, the `id_string` parameter is only applicable when SDH framing is configured. SDH framing repetitively cycles through a 15-character string, sending one character per frame. If the configured string is less than 15 characters, it is padded with NULL characters.

Example

The following command example sets the section trace identifier to the string `1800wombat` for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet trace section string 1800wombat ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

create account pppuser

```
create account pppuser <username> {encrypted} {<password>}
```

Description

Creates a local database entry that can be used to authenticate a PPP peer.

Syntax Description

username	Specifies the user name used for authentication.
encrypted	This parameter should not be used with SONET ports.
password	Specifies the password used for authentication.

Default

N / A.

Usage Guidelines

Authentication responses include a username. When a response is received, the database is searched for an entry with the specified username. The associated password is then used to validate the authentication response. This is a new application of the existing `create account` command. The `pppuser` keyword is new. The `username` parameter is a string with a length in the range [1-32] characters. The `password` parameter is also a character string, with a maximum length of 32 characters. If no password is provided on the command line, then you are prompted to enter the password twice (with the second time serving as a confirmation). You should not enter the `encrypted` parameter option (it is used by the switch when generating an ASCII configuration).

Example

The following command example sets the authentication database name to `stretch` and sets the password to `baserunner` for the BlackDiamond switch:

```
create account pppuser stretch baserunner
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the on the BlackDiamond switch. A similar command is available on the Alpine switch.

create aps

```
create aps <group#>
```

Description

Creates an APS group with the specified group number.

Syntax Description

group#	Specifies the APS group# to which the command applies.

Default

N/A.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# is used to identify the APS group. An APS group includes one working line and one protection line. The working line and protection line can reside on the same BlackDiamond switch or two different BlackDiamond switches. The group numbers must be unique across all BlackDiamond switches that are cooperating to provide the APS function. The group numbers must also be used in a consistent manner across BlackDiamond switches. For example, if the working line is assigned to group# 1 on BlackDiamond #1, and the associated protection line resides on BlackDiamond #2, then the protection line must also be assigned to group #1 on BlackDiamond #2. The group# is used to identify the partner (in other words, working or protection) line in Ethernet messages exchanged by BlackDiamond switches that are cooperating to provide the APS function.

Example

The following command example creates APS group 1001 on the BlackDiamond switch:

```
create aps 1001
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

delete account pppuser

```
delete account pppuser <username>
```

Description

Deletes an entry in the local PPP authentication database.

Syntax Description

username	Specifies the user name used for authentication.

Default

N/A.

Usage Guidelines

Deletes a user from the PPP authentication database. Existing links already authenticated are not affected by this command.

Example

The following command example removes the entry for `stretch` from the authentication database:

```
delete account pppuser stretch
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the on the BlackDiamond switch. A similar command is available on the Alpine switch.

delete aps

```
delete aps <group#>
```

Description

Deletes the specified APS group.

Syntax Description

group#	Specifies the APS group# to which the command applies.

Default

N/A.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group to delete.

Example

The following command example deletes APS group 1001:

```
delete aps 1001
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

disable aps

```
disable aps
```

Description

Disables the APS function for an entire switch.

Syntax Description

This command has no arguments or variables.

Default

APS is disabled by default.

Usage Guidelines

If APS is disabled, interfaces configured as protection lines will not carry any traffic.

Example

To disable the APS function for the entire switch, use the following command:

```
disable aps
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

disable red ports queue

```
disable red ports <portlist> queue <queue#>
```

Description

Disables RED on the specified ports.

Syntax Description

portlist	Specifies the port number(s). May be in the form 1, 2, 3-5, 2:5, 2:6-8.
queue#	Specifies the queue for which the RED function is disabled. This parameter is supported for the PoS module only.

Default

Disabled.

Usage Guidelines

The queue keyword has been added to support the PoS module. Currently, this new keyword is only applicable to PoS ports. The keyword allows the RED function to be selectively enabled on an individual queue basis. The queue# parameter is an integer in the range [0-7]. If the queue keyword is omitted, then the command applies to all egress queue numbers for the PoS port(s). RED is not supported on the ingress queues.

Example

The following command disables RED for all PHBs except the EF PHB:

```
disable red ports 2:1-2:2 queue 8
```

History

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

Platform Availability

The general form of this command is available on all platforms. The optional queue parameter is available only on the PoS module on a BlackDiamond switch.

enable aps

```
enable aps
```

Description

Enables the APS function for an entire switch.

Syntax Description

This command has no arguments or variables.

Default

APS is disabled by default.

Usage Guidelines

If APS is enabled, interfaces configured as protection lines can carry traffic.

Example

To enable the APS function for the entire switch, use the following command:

```
enable aps
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

enable red ports queue

```
enable red ports <portlist> queue <queue#>
```

Description

Enables RED on the specified PoS ports.

Syntax Description

portlist	Specifies the port number(s).
queue#	Specifies the queue for which the RED function is enabled.

Default

By default, RED is disabled.

Usage Guidelines

The queue keyword has been added to support the PoS module. Currently, this new keyword is only applicable to PoS ports. The keyword allows the RED function to be selectively enabled on an individual queue basis. The queue# parameter is an integer in the range [0-7]. If the queue keyword is omitted, then the command applies to all egress queue numbers for the PoS port(s). (RED is not supported on the ingress queues.)

Example

The following command enables RED for all PHBs except the EF PHB:

```
enable red ports 2:1-2:2
```

History

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

Platform Availability

The general form of this command is available on all platforms. The optional queue parameter is available only on the PoS module on a BlackDiamond switch.

show accounts pppuser

```
show accounts pppuser
```

Description

Display the PPP user accounts database.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to examine the entries in the PPP user accounts database, used for authentication when a link is initiated from a remote peer.

Example

The following command displays the PPP accounts database:

```
show accounts pppuser
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.

show aps

```
show aps {<group#>} {detail}
```

Description

Displays APS group status information.

Syntax Description

group#	Specifies the APS group# to which the command applies.
detail	Displays more detailed status information for the APS groups.

Default

By default, the command shows summarized status for the APS group(s).

Usage Guidelines

The user can optionally specify a group# parameter, which is an integer in the range [1-65535]. The group# identifies a particular APS group for which status is to be shown. Alternatively, you can enter **show aps** with no parameters to obtain status for all configured APS groups. More detailed status information can be obtained for the APS group(s) by specifying the detail parameter.

Summary status includes the following information for each APS group:

- Provisioned values of all APS configuration parameters, including SONET port numbers and whether the ports are performing the working or protection line function.
- An indication of whether the line associated with each configured port is active or inactive from an APS perspective, along with a timestamp indicating when the last APS state change occurred.
- An indication of whether a signal fail (SF) or signal degrade (SD) event due to an excessive bit error rate (BER) currently exists on the line associated with each configured port, along with a timestamp indicating when the last such error occurred. (Note that the BER thresholds that cause SF and SD events may be specified as part of configuring a SONET port.)
- Counts of the number of SF and SD events initiated by each configured port due to an excessive BER.
- Count of the number of APS authentication failures (that is, a count of the number of received APS control packets that have been discarded due to authentication failures).

Detailed status includes the information reported in the summary status along with additional status and management counters. Detailed status only applies to ports performing the protection line function.

Detailed management counters reported for each protection-line port include:

- Automatic line switches initiated by working-line switch
- Automatic line switches initiated by protection-line switch
- Automatic line switches initiated by ADM
- Line switches initiated due to external commands (for example, force or manual switch command)
- Line switches completed successfully

- Hello protocol failures (this count is included as a component of the automatic line switches initiated by protection-line switch counter)
- APS mode mismatch failures (occurs when the ADM indicates that it is provisioned for the 1:n APS architecture, or when the ADM indicates that it is provisioned for unidirectional-switching mode)
- Protection switching byte failures (occurs when the received K1 byte is either inconsistent or contains an invalid request code)
- Channel mismatch failures (occurs when the channel number in the transmitted K1 byte does not match the channel number in the received K2 byte)
- Far-end protection line failures (occurs when a signal fail request code is received on the protection line)

Additional detailed status information reported for each protection-line port includes:

- Current contents of received K1 and K2 bytes
- Contents of K1 and K2 bytes that are currently being transmitted
- An indication of whether an APS mode mismatch failure is currently active
- An indication of whether a protection switching byte failure is currently active
- An indication of whether a channel mismatch failure is currently active
- An indication of whether a Far-end protection line failure is currently active

Example

The following command displays APS group status information:

```
show aps
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

show flowstats

```
show flowstats {<portlist> | export {<group#>} {detail}}
```

Description

Displays status information for the flow statistics function.

Syntax Description

portlist	Specifies the port number(s).
export	Displays status information for export groups, which are configured on a switch-wide basis.
group#	Use this optional parameter with the `export` keyword to display status information for a specific export group. If you do not specify a value for the `group#` parameter, the `export` keyword by itself displays status information for all export groups.
detail	Displays detailed export group status information.

Default

By default, the command shows summarized status.

Usage Guidelines

The `portlist` parameter can be used to specify the SONET port(s) for which status is to be shown. Alternatively, you can specify the `export` keyword to obtain status for export groups, which are configured on a switch-wide basis. Status can be obtained for a specific export group, identified by the `group#` parameter, or for all export groups by omitting the `group#` parameter. Status can be obtained for all ports by omitting both the `portlist` parameter and the `export` keyword (in other words, by simply entering `show flowstats` with no parameters). More detailed export group status information may be obtained by specifying the detail parameter.

Summary status for a port includes the following information:

- Values of all flow statistics configuration parameters
- Count of flow records that have been exported
- Counts of the number of packets/bytes for which flow statistics were not maintained due to insufficient resources

Summary status for an export group port includes the following information:

- Values of all configuration parameters
- State of each export destination device

Detailed status for an export group includes the information reported in the summary status along with the following additional management counters:

- Counts of flow records that have been exported to each flow-collector destination
- Counts of the number of times each flow-collector destination has been taken out of service due to health-check failures

Example

The following command displays status information for the flow statistics function:

```
show flowstats
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

show ppp

```
show ppp {<portlist>} {detail}
```

Description

Displays status information for PPP ports.

Syntax Description

portlist	Specifies the port number(s).
detail	Displayed more detailed status information for the PPP ports.

Default

By default, the command shows summarized status for the PPP port(s).

Usage Guidelines

The `portlist` parameter can be used to specify the port(s) for which status is to be shown. Alternatively, you can enter `show ppp` with no parameters to obtain status for all PPP ports. More detailed status information can be obtained for the PPP port(s) by specifying the detail parameter.

Summary status includes the following information for each PPP port:

- Values of all PPP configuration parameters
- Physical link status
  - operational
  - down
  - LCP state
  - IPCP/BCP state
  - EDPCP state
  - MPLSCP state
  - OSINLCP state
  - link packet and octet counters

Detailed status includes the information reported in the summary status along with the following additional status and management counters:

- Detailed link status
  - PPP link phase
- Detailed LCP status
  - LCP options negotiated (local and remote)
  - LCP packet counters
  - number of link-down events due to PPP maintenance
- Detailed authentication status

  - remote username (if applicable)
  - CHAP/PAP packet counters
- Detailed IPCP/BCP status
  - options negotiated (local and remote)
  - packet counters
  - MPLSCP/OSINLCP status
- Detailed LQM status
  - statistics from last received LQR (Link Quality Report)
  - time since last received LQR
  - LQR packet counters
  - number of link-down events due to LQM
  - MPLSCP
  - OSINLCP

Example

The following command displays status information for the PPP ports:

```
show ppp
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.

show sonet

```
show sonet {<portlist>} {detail}
```

Description

Displays SONET port status.

Syntax Description

portlist	Specifies the port number(s).
detail	Displays more detailed status information for the ports.

Default

By default, the command shows summarized status for the port(s).

Usage Guidelines

You can use the `portlist` parameter to specify which SONET port(s) you want to display the status for. You can also omit the `portlist` parameter to obtain status for all SONET ports. More detailed status information can be obtained for the port(s) by specifying the detail parameter. Summary status includes the following information for each port:

- Values of all port configuration parameters
- State of the port
- Identification of all currently active events

Example

The following command displays the SONET port status:

```
show sonet
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

unconfigure aps

```
unconfigure aps <group#>
```

Description

Resets the APS group configuration parameters to their default values.

Syntax Description

group#	Specifies the APS group# to which the command applies.

Default

N/A.

Usage Guidelines

You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the command applies to. The command does not affect the ports that have been added to the APS group. The command does cancel any outstanding lockout, force, or manual switch requests.

Example

The following command example resets the configuration parameters of APS group 1001 to their default values:

```
unconfig aps 1001
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

unconfigure diffserv dscp-mapping ports

```
unconfigure diffserv dscp-mapping ports <portlist>
```

Description

Resets the DSCP mapping tables for the specified PoS ports to their default values.

Syntax Description

portlist	Specifies the port number(s).

Default

N/A.

Usage Guidelines

Three DSCP mapping tables are supported per SONET port. One of the tables is used in the ingress direction and two are used for egress flows (onto the SONET link). The two egress tables are for the congested and non-congested states, as determined by the RED algorithm (in other words, the congested state is when the average queue length is greater than the minimum RED threshold). If RED is not enabled on the SONET port, then the egress congested-state mapping table is not used.

The tables are very simple. In the ingress direction, the input DSCP of a packet received from the SONET link is replaced with an output DSCP before the packet is forwarded. The replacement is straightforward; the input DSCP is used as an index into a 64-entry table that contains the output DSCPs associated with each of the input DSCP values. The operation is similar in the egress direction, with the DSCP mapping occurring before the packet is transmitted onto the SONET link(s). The mapping operation is performed after the packet has been assigned to a QoS profile. One potential use of the DSCP mapping capability is reconciliation of varying DiffServ policies at the boundary between autonomous systems (for example, at the boundary between two ISPs). The availability of different tables for the congested/non-congested states is useful for marking operations that increase the drop probability of packets during times of congestion, as discussed in the DiffServ assured forwarding (AF) RFC.

This command is currently only applicable to SONET ports.

Example

The following command resets the DSCP mapping tables for port 1, slot 8 of a BlackDiamond switch to their default values:

```
unconfigure diffserv dscp-mapping port 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

unconfigure ppp ports

```
unconfigure ppp ports <portlist>
```

Description

Resets the PPP configuration parameters for the specified ports to their default values.

Syntax Description

portlist	Specifies the port number(s).

Default

N/A.

Usage Guidelines

By default, BCP is enabled on all PoS ports. (However, ports 2 and 4 of OC-3c modules are not members of any VLANs by default; all other ports are members of the default VLAN by default.)

Example

The following command resets the PPP configuration parameters for port 1, slot 8 of a BlackDiamond switch to the default values:

```
unconfigure ppp ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch. A similar command is available on the Alpine switch.

unconfigure sonet ports

```
unconfigure sonet ports <portlist>
```

Description

Resets the configuration parameters of the specified SONET port to their default values.

Syntax Description

portlist	Specifies the port number(s).

Default

N/A.

Usage Guidelines

The following are the SONET port default values:

clock setting	internal
Framing	sonet
signal label	auto, where the value of the signal Label field is automatically set based on standard conventions for the given payload type.
threshold signal degrade	10^{-6}
threshold signal fail	10^{-5}
trace path	null
trace section	1 for SONET, null for SDH

Example

The following command resets the configuration parameters for port 1, slot 8 of a BlackDiamond switch to the default values:

```
unconfigure sonet ports 8:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.

24 T1, E1, and T3 WAN Commands

This chapter describes the following commands:

- Commands for configuring T1, E1, and T3 WAN links.
- Point-to-Point Protocol (PPP) and Multilink PPP (MLPPP) commands for WAN links.
- Commands to display and monitor WAN links.

Extreme Networks WAN modules allow you to pass Ethernet traffic over technologies originally developed for telecommunications. T1, E1, and T3 links have all been used to pass voice traffic over telecommunications networks for many years. Now you can pass data traffic with these modules developed specifically for the Extreme Networks Alpine 3800 family of switches.

To pass data traffic over these modules, the traditional T1, E1, or T3 parameters are configured, and then PPP is used to pass the Ethernet data across the link.

configure multilink add

```
configure multilink <groupname> add ports <portlist>
```

Description

Adds ports to a multilink group.

Syntax Description

groupname	Specifies a previously created multilink group.
portlist	A list of ports.

Default

N/A.

Usage Guidelines

Use this command to add ports to a previously created multilink group. All ports added to a multilink group must be added as tagged ports. If the first port added to a multilink group is already configured for PPP, the multilink group will inherit the configuration of the first port. Any other ports added to the link will be configured to match the multilink configuration.

Only T1 or E1 ports can be added to multilink groups.

Example

The following command add ports the previously created multilink group “example_1”:

```
configure multilink example_1 add ports 2:1-2:4
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure multilink delete

```
configure multilink <groupname> delete ports <portlist>
```

Description

Deletes ports from a multilink group.

Syntax Description

groupname	Specifies a previously created multilink group.
portlist	A list of ports.

Default

N/A.

Usage Guidelines

Use this command to delete ports from a previously created multilink group.

Example

The following command deletes a port from the multilink group example_1:

```
configure example_1 delete ports 2:3
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports clock source

```
configure ports <portlist> [t1 | e1 | t3] clock source [internal | line]
```

Description

Configures the clock source for WAN links.

Syntax Description

portlist	A list of ports.
internal	Specifies the internal clock.
line	Specifies clock derived from line signal.

Default

By default the clock source is derived from the line.

Usage Guidelines

The clock is used to synchronize data transmission across a WAN link. Generally, one end of the link provides the master clock, and the other end of the link recovers the clock from the signal on the line. If needed, an internal clock is available.

If the clock source is configured as “line”, but the clock cannot be recovered from the signal on the line, the hardware will use the internal clock instead.

Example

The following command sets the clock source to internal:

```
configure ports 4:2 t1 clock source internal
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports e1 framing

```
configure ports <portlist> e1 framing [crc4 | no-crc4]
```

Description

Configure framing for E1 links.

Syntax Description

portlist	A list of ports.
crc4	Specifies CRC4 framing.
no-crc4	Specifies No-CRC4 framing.

Default

CRC4 framing is enabled by default.

Usage Guidelines

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. The two choices for E1 framing are CRC4 and No-CRC4.

Example

The following command sets framing to CRC4 for the E1 ports:

```
configure ports 3:1-3:4 e1 framing crc4
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports e1 receivergain

```
configure ports <portlist> e1 receivergain [-12 | -43] db
```

Description

Configures E1 receiver gain to improve link performance.

Syntax Description

portlist	A list of ports.
db	Specifies the receiver gain in decibels. Only the values above are allowed.

Default

The default value is -12 db.

Usage Guidelines

The receiver gain for E1 links can be configured to improve performances of the link. Changing the receiver gain can help to receive the E1 signal or to reduce crosstalk. Receiver gain is only configurable for E1 links. For T1 links see “configure multilink add” on page 1500 and for T3 links see “configure ports t1 framing” on page 1509.

Example

The following command configures the receiver gain:

```
configure ports 2:2 e1 receivergain -43 db
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports e1 timeslots

```
configure ports <portlist> e1 timeslots <timeslots>
```

Description

Select the E1 timeslots to use for transmitting data.

Syntax Description

portlist	A list of ports.
timeslots	Specifies the data timeslots. Timeslot numbers range from 1 to 31.

Default

All timeslots are used by default.

Usage Guidelines

The E1 signal is divided into thirty-two timeslots, numbered 0 through 31. The first timeslot (0) is reserved and cannot be used to transmit data. The timeslot numbered 16 is often used for voice phone calls in installations that combine voice and data. For installations that use the full E1 bandwidth for data communications, you will not need to configure which timeslots are used. For installations that do not use the total E1 bandwidth, your E1 provider will tell you which timeslots to use.

A timeslot list uses a dash to represent a range of numbers and a comma to separate single numbers or ranges. Valid timeslots range from 1 to 31.

Example

The following command specifies timeslots 1 through 15 and 17 through 31 for the E1 port 1 on slot 4:

```
configure ports 4:1 e1 timeslots 1-15,17-31
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports snmp alert

```
configure ports <portlist> [t1 | e1 | t3] snmp alert [enable | disable]
```

Description

Enable and disable the sending of SNMP alerts for WAN links to the SMMi.

Syntax Description

portlist	A list of ports.

Default

SNMP alerts are enabled by default.

Usage Guidelines

If the WAN module hardware detects a red, yellow, or blue alarm, the alarms are displayed by using a show command. See the command “show ports alarms” on page 1545. Additionally, the module can be configured to send an SNMP alert to the SMMi in the switch when red, yellow, or blue alarms are detected. If the module is configured to send SNMP alerts, and the switch is configured to send SNMP trap messages, then the switch will send a message to any SNMP trap receivers that have been configured. To configure SNMP trap receivers, and for more information about configuring SNMP in ExtremeWare, see the *ExtremeWare Software User Guide.*

The module can also be configured not to send an SNMP alert to the SMMi. Any red, yellow, or blue alarms will not be reported to the SNMP trap receivers.

Example

The following command disables snmp alerts from a port:

```
configure ports 4:1 t1 snmp alert disable
```

History

This command was originally available as “configure ports t1 alarms” in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added and the command was changed to “configure ports snmp alert” in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports t1 cablelength

```
configure ports <portlist> t1 cablelength [[0 | -7.5 | -15 | -22.5] db |
[133 | 266 | 399 | 533 | 655] feet]
```

Description

Control T1 transmitter signal level for different cable lengths.

Syntax Description

portlist	A list of ports.
feet	Specifies the cable length in feet. Only the values above are allowed.
db	Specifies the transmitter attenuation in decibels. Only the values above are allowed.

Default

The default setting is 133 feet.

Usage Guidelines

For short haul connections (less than 1000 feet) the transmitter level for T1 is set by selecting a cable length in feet, from the following values: 133, 266, 399, 533 or 655. Choose the next higher value if the cable length provided by your service provider does not match one of these values. For example, choose 133 for a 50 foot cable and 533 for a 450 foot cable. The default value is 133, which corresponds to cables in the range of 0-133 feet.

For longer distances (up to 6000 feet) T1 equipment uses more sensitive receivers, and crosstalk is more likely to occur. Under these conditions, the transmitter level is set by selecting a transmitter attenuation level in dB from the following values: -22.5, -15, -7.5, or 0.

From lowest to highest transmitter level, use the following values for the `configure port t1 cablelength` command: -22.5 db, -15 db, -7.5 db, 0 db, 133 feet, 266 feet, 399 feet, 533 feet, and 655 feet.

Example

The following command sets the cablelength for all T1 ports:

```
configure ports 2:1-2:4 t1 cablelength 533 feet
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when the applicable WAN module is available.

configure ports t1 fdl

```
configure ports <portlist> t1 fdl [off | att | ansi]
```

Description

Configures facility data link (FDL) for T1 links.

Syntax Description

portlist	A list of ports.
att	Specifies ATT 54016 FDL.
ansi	Specifies T1.403 FDL.

Default

FDL is off.

Usage Guidelines

Facility data link (FDL) for T1 links uses twelve bits in the ESF frame to signal information about line and connection status. Since FDL is only meaningful for ESF framing, FDL settings are ignored when a port is configured for SF framing.

The two T1 standards supported for FDL are ATT, described by the ATT 54016 specification, and ANSI, described by the T1.403 standard.

Example

The following command enables ATT FDL on four T1 links:

```
configure ports 4:1-4:4 t1 fdl att
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports t1 framing

```
configure ports <portlist> t1 framing [esf | sf]
```

Description

Configure framing for T1 links.

Syntax Description

portlist	A list of ports.
esf	Specifies ESF framing.
sf	Specifies SF framing.

Default

ESF framing is enabled by default.

Usage Guidelines

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. The two choices for T1 framing are Super Frame (SF), also known as D4, and Extended Super Frame (ESF). The ESF scheme is a newer standard and is enabled by default. To choose the T1 framing scheme, use the following command:

If you choose to use SF framing, you should disable yellow alarm detection for the T1 line. SF framing may generate false yellow alarms. See the command “configure ports snmp alert” on page 1506 to disable yellow alarms.

Example

The following command sets framing to SF for the T1 ports:

```
configure ports 3:1-3:4 t1 framing sf
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports t1 lbdetect

```
configure ports <portlist> t1 lbdetect [off | inband]
```

Description

Configures inband loopback detection on T1 links.

Syntax Description

portlist	A list of ports.
inband	Specifies inband loopback detection.

Default

By default, loopback detection is off.

Usage Guidelines

When inband loopback detection is enabled, a specific sequence of data in the signal payload from the remote end of the T1 link will cause the local end to enter network line loopback mode and send any received signal back to the remote end.

Inband loopback detection is only possible if facility data link (FDL) is enabled and configured as "ATT". See the command "configure ports t1 fdl" on page 1508 for more information.

Example

The following command enables inband loopback detection:

```
configure ports 4:1-4:2 t1 lbdetect inband
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports t1 linecoding

```
configure ports <portlist> t1 linecoding [b8zs | ami]
```

Description

Configures the linecoding convention for T1 links.

Syntax Description

portlist	A list of ports.
b8zs	Specifies B8ZS linecoding.
ami	Specifies AMI linecoding.

Default

The default linecoding is B8ZS.

Usage Guidelines

The two choices for linecoding standards are bipolar eight zero suppression (B8ZS) or alternate mark inversion (AMI).

Example

The following command sets the linecoding to AMI:

```
configure ports 2:3,2:4 t1 linecoding ami
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports t1 yellow

```
configure ports <portlist> t1 yellow [detection | generation | both | off]
```

Description

Configure detection and generation of yellow alarms.

Syntax Description

portlist	A list of ports.

Default

Both detection and generation of yellow alarms is enabled by default.

Usage Guidelines

A yellow alarm occurs on a device when its signal is not received at the remote end. It is also called a Remote Alarm Indication (RAI). You can disable detection and generation of yellow alarms for a T1 port. When SF framing is used, yellow alarm detection and generation should be set to off, because detection of yellow alarms is not reliable when data traffic is transmitted with SF framing (data traffic often contains bit combinations that do not occur for encoded voice traffic).

Example

The following command enables only the detection of yellow alarms:

```
configure ports 3:1-3:4 t1 yellow detection
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ports t3 cablelength

```
configure ports <portlist> t3 cablelength [349 | 900] feet
```

Description

Control T3 transmitter signal level for different cable lengths.

Syntax Description

portlist	A list of ports.
feet	Specifies the cable length in feet. Only the values above are allowed.

Default

The default setting is 349 feet.

Usage Guidelines

The transmitter level for T3 is set by selecting a cable length in feet, from the following values: 349 or 900. Choose the next higher value if the cable length provided by your service provider does not match one of these values. For example, choose 349 for a 50 foot cable and 900 for a 450 foot cable. The default value is 349, which corresponds to cables in the range of 0-349 feet.

Example

The following command sets the cablelength for the T3 port:

```
configure ports 2:1 t3 cablelength 900 feet
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when the applicable WAN module is available.

configure ports t3 framing

```
configure ports <portlist> t3 framing [c-bit | m13]
```

Description

Configure framing for a T3 link.

Syntax Description

portlist	A list of ports.
c-bit	Specifies C-Bit framing.
m13	Specifies M13 framing.

Default

C-Bit framing is enabled by default.

Usage Guidelines

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. The two choices for T3 framing are C-Bit and M13.

Example

The following command sets framing to M13 for the T3 port:

```
configure ports 3:1 t3 framing m13
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure ppp

```
configure ppp [bcp [on | off] | ipcp [on | off]] [ports <portlist> |
multilink <groupname>]
```

Description

Configures the network control protocol (encapsulation) that will run on the specified PPP/MLPPP WAN ports.

Syntax Description

bcp	Specifies bridging control protocol for the port.
ipcp	Specifies IP control protocol for the port.
on	Enables the designated protocol on the port.
off	Disables the designated protocol on the port.
portlist	Specifies the port number(s).
groupname	Specifies a previously created multilink group.

Default

By default, BCP is enabled on all WAN ports.

Usage Guidelines

The packets passed over the PPP/MLPPP link can use either bridged or routed encapsulation. You would use bridged packets if you plan to have more than one VLANs span the link. You would use routed packets if the link connects two different routed networks or separate VLANs.

Using bridged packets allows the VLAN tags to be carried across the PPP/MLPPP link. Bridged packets are transported using the PPP Bridging Control Protocol (BCP), described in RFC 2878, except in the case of Legacy BCP, described below. When the encapsulation is set to BCP, 802.1Q and 802.1p information is preserved and transported across the link.

Routed packets are transported across a PPP/MLPPP link using IP Control Protocol (IPCP), described in RFC 1332. This is the encapsulation that is familiar to most users of PPP. The routed packets do not contain Ethernet headers so cannot preserve VLAN tags. However, the WAN ports still must be added as tagged ports to the VLAN that contains them. The module uses the tags internally and strips them off before the packets are transmitted. The IP addresses used for the PPP/MLPPP link are taken from the IP address assigned to the VLAN at each end of the link. The VLAN that contains the IPCP encapsulated PPP/MLPPP ports cannot contain other ports. In other words, the only ports allowed in the VLAN are those that make up the IPCP encapsulated link. There can only be one VLAN spanning an IPCP-encapsulated link.

You must have one and only one encapsulation type configured on a PPP/MLPPP link. Setting BCP encapsulation off implies that IPCP encapsulation is on. The default setting is BCP encapsulation on and IPCP encapsulation off.

Legacy BCP. Some routers supported by other vendors implemented BCP using an older standard, RFC 1638. For interoperability, the Extreme Networks implementation supports both standards. The limitation with RFC 1638-based BCP is that 802.1Q tags are not supported. So Legacy BCP cannot

support multiple VLANs or preserve 802.1p priority across the PPP link. Both types of BCP can operate over single and multilink PPP.

When BCP is negotiated over a link, RFC 2878 BCP is initially proposed. If the peer only supports Legacy BCP (RFC 1638), then the link is made using Legacy BCP. Since the WAN module ports are always configured as tagged ports, the VLAN tag is removed in the egress direction and inserted in the egress direction when BCP is operating in Legacy mode.

There is no Legacy BCP specific configuration, and the display for the command `show ppp info` is identical for BCP and Legacy BCP. To determine if the link is using Legacy BCP, use the following command:

```
show log warning
```

and look for the message:

```
BCP: Legacy BCP UP;Only a single VLAN over BCP is supported
```

Example

The following command example configures IPCP on a PPP port, and applies to a WAN module installed in slot 1 of an Alpine switch:

```
configure ppp ipcp on port 1:4
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

configure ppp authentication

```
configure ppp authentication [off | chap | pap | chap-pap] [ports
<portlist> | multilink <groupname>]
```

Description

Configures authentication on the specified PPP ports or MLPPP multilink group.

Syntax Description

off	Disables authentication.
chap	Authenticates the peer using the challenge handshake authentication protocol (CHAP).
pap	Authenticates the peer using the password authentication protocol.
chap-pap	Specifies that first CHAP is used, then PAP, if CHAP fails to authenticate the peer.
portlist	Specifies the port number(s).
groupname	Specifies the multilink group.

Default

The default is authentication `off`.

Usage Guidelines

When `off` is specified, the peer is not authenticated. When `chap` is specified, the peer is authenticated using the challenge handshake authentication protocol (CHAP). When `pap` is specified, the peer is authenticated via the password authentication protocol (PAP). Specification of `chap-pap` indicates that CHAP is first used, then PAP, if CHAP fails to authenticate the peer.

Example

The following command example turns on CHAP authentication for the multilink group *m1_remote*:

```
configure ppp authentication chap multilink m1_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

configure ppp user

```
configure ppp user <name> {encrypted} {<password>} [ports <portlist> |
multilink <groupname>]
```

Description

Configures the user name and password that the specified PPP/MLPPP link uses if the peer requests authentication.

Syntax Description

name	Specifies user name for PPP peer authentication requests.
encrypted	This parameter option should not be entered.
password	Specifies the password for PPP peer authentication requests.
portlist	Specifies the port number(s).
groupname	Specifies a previously created multilink group.

Default

By default, there is no value set for name or password.

Usage Guidelines

The name is also sent when a port transmits a CHAP authentication request. The implementation responds to either CHAP or PAP authentication requests issued by the peer regardless of whether the port is configured to authenticate the peer. The name parameter is a string with a length in the range of [1..32] characters. The password parameter is also a character string, with a maximum length of 32 characters. If no password is provided on the command line, then you are prompted to enter the password twice (with the second time serving as a confirmation). You should not enter the encrypted parameter option (it is used by the switch when generating an ASCII configuration).

Example

The following command example sets the name to titus and sets the password to 1Afortune for the multilink group m_link1:

```
configure ppp user "titus" "1Afortune" multilink m_link1
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

configure qosprofile min-bps

```
configure qosprofile <qosprofile> min-bps <bps> [k | m]
max-bps <bps> [k | m] {priority <level>} [ports <portlist> |
multilink <multilink name>]
```

Description

Modifies the default QoS profile parameters for T1 and E1 modules.

Syntax Description

qosprofile	Specifies a QoS profile name.
min-bps	Specifies a minimum bandwidth for this queue. The default setting is 0.
k	Specifies Kbps.
m	Specifies Mbps.
max-bps	Specifies the maximum bandwidth this queue is permitted to use. The default setting is 1536 Kbps.
level	Specifies a service priority setting. Settings are low and high. The default setting is low. Available in egress mode only.
portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
multilink name	Specifies a multilink.

Default

- Minimum bandwidth—0 Kbps
- Maximum bandwidth—1536 Kbps
- Priority—low

Usage Guidelines

This command sets the software egress QoS for T1 and E1 modules, using units of bps of bandwidth, instead of percentages of bandwidth.

For WAN QoS only two priority levels are available, low and high. Software queues are scheduled based on priority, minimum bandwidth, and maximum bandwidth. Only one queue can have high priority.

The high priority queue is flushed on every scheduling round. Minimum bandwidth is ignored for this queue. Throughput is policed based on the maximum bandwidth value. Policing prevents packets from entering a queue that is receiving traffic from the backplane too fast. The remaining bandwidth is shared by all other queues based on the minimum bandwidth setting of each queue. In other words, the high priority queue takes up all the bandwidth up to its `max-bps` setting, while the low priority queues share all the remaining bandwidth.

Example

The following command configures the QoS profile parameters of QoS profile *qp5* for specific ports on a T1 or E1 module:

```
configure qosprofile qp5 min-bps 64 k max-bps 512 k priority high ports 2:1,2:3
```

History

This command was available in ExtremeWare 7.1.0.

Platform Availability

This command is available for T1 and E1 modules.

configure qosprofile wanqos maxbuf

```
configure qosprofile <qosprofile> wanqos maxbuf <count> [ports <portlist> |
multilink <multilink name>]
```

Description

Sets the maximum queue depth for for T1 and E1 modules.

Syntax Description

qosprofile	Specifies a QoS profile name.
count	Specifies a maximum buffer size this queue. The default setting is 0.
portlist	Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.
multilink name	Specifies a multilink.

Default

By default, 256 packet buffers are assigned to the high priority queue.

Usage Guidelines

This command sets the software egress queue buffers for T1 and E1 modules.

For WAN QoS, each port has 256 packet buffers of 1900 bytes. The buffers are shared among the eight queues. Use a small number for low latency. Use a large number for best effort on bursty traffic

Example

The following command configures the QoS maximum buffer of QoS profile *qp5* to 128 for ports 2:1 and 2:3:

```
configure qosprofile qp5 wanqos maxbuf 128 ports 2:1,2:3
```

History

This command was available in ExtremeWare 7.1.0.

Platform Availability

This command is available for T1 and E1 modules.

configure vlan add multilink

```
configure vlan <vlan name> add multilink <groupname>
```

Description

Adds an MLPPP multilink group to a VLAN.

Syntax Description

vlan	Specifies a previously created VLAN.
groupname	Specifies a previously created multilink group.

Default

N / A.

Usage Guidelines

Add an MLPPP group to a VLAN to transport traffic across the link. A multilink group configured for BCP encapsulation can transport more than one VLAN's traffic (see "configure ppp user" on page 1518 for details).

Example

The following command adds the multilink group *marmots* to the VLAN *corporate*:

```
configure corporate add ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure vlan delete multilink

```
configure vlan <vlan name> delete multilink <groupname>
```

Description

Deletes an MLPPP multilink group from a VLAN.

Syntax Description

vlan	Specifies a previously created VLAN.
groupname	Specifies a previously added multilink group.

Default

N/A.

Usage Guidelines

Remove an MLPPP group from a VLAN to stop transporting that VLAN's traffic across the link.

Example

The following command deletes the multilink group *ml_remote* from the VLAN *corporate*:

```
configure corporate delete ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

configure wanqos egress map dot1p_priority

```
configure wanqos egress map dot1p_priority <priority> to qosprofile <QoS
profile>
```

Description

Change the default mapping of dot1p values to software egress queues.

Syntax Description

priority	Specifies a dot1p priority.
qosprofile	Specifies a QoS profile name.

Default

N / A.

Usage Guidelines

WAN QoS uses dot1p value to map directly to software egress queues. Use this command to change the default mapping and map several dot1p values to the same software queue. This can simplify configuration (two to three classes of service instead of eight) and improve egress burst tolerance because each queue can have a larger number of buffers. Set the maximum buffer size to one for unused queues.

To set the maximum buffer size on queues, use the following command:

```
configure qosprofile <qosprofile> wanqos maxbuf <count> [ports <portlist> |
multilink <multilink name>]
```

Example

The following command maps dot1p priority 5 to QoS profile *qp7*:

```
configure wanqos egress map dot1p_priority 5 to qosprofile qp7
```

History

This command was available in ExtremeWare 7.1.0.

Platform Availability

This command is available for T1 and E1 modules.

create account pppuser

```
create account pppuser <username> {encrypted} {<password>}
```

Description

Creates a local database entry that can be used to authenticate a PPP peer.

Syntax Description

username	Specifies the user name used for authentication.
encrypted	This parameter should not be used (see below).
password	Specifies the password used for authentication.

Default

N / A.

Usage Guidelines

When the remote end initiates the link, the local end must verify the authentication information. The local end maintains a database of authorized user accounts and passwords. Use this command to add a user to the database. You should not enter the `encrypted` parameter option (it is used by the switch when generating an ASCII configuration).

Example

The following command example adds an entry to the authentication database. A username `stretch` with password `baserunner` is added to the database:

```
create account pppuser stretch baserunner
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

create multilink

```
create multilink <groupname>
```

Description

Creates an MLPPP multilink group.

Syntax Description

groupname	Specifies the multilink group name.

Default

N / A.

Usage Guidelines

Use this command to create a multilink group. Like the `create vlan` command, the `multilink` keyword must be used when creating the multilink group. Once the group is created, ExtremeWare recognizes the group name as a multilink group, so the `multilink` keyword is not needed in other commands that manipulate multilink groups.

Example

The following command creates the multilink group *ml_remote*:

```
create multilink ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

delete account pppuser

```
delete account pppuser <username>
```

Description

Deletes an entry in the local PPP authentication database.

Syntax Description

username	Specifies the user name used for authentication.

Default

N/A.

Usage Guidelines

Deletes a user from the PPP authentication database. Existing links already authenticated are not affected by this command.

Example

The following command example removes the entry for `stretch` from the authentication database:

```
delete account pppuser stretch
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

delete multilink

```
delete multilink <groupname>
```

Description

Deletes an MLPPP multilink group.

Syntax Description

groupname	Specifies the multilink group name.

Default

N/A.

Usage Guidelines

Use this command to delete a multilink group.

Example

The following command deletes the multilink group *ml_remote*:

```
delete multilink ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

disable multilink

```
disable multilink <groupname>
```

Description

Disables an MLPPP multilink group.

Syntax Description

groupname	Specifies the multilink group name.

Default

N/A.

Usage Guidelines

Use this command to disable a multilink group. The multilink group will stop transporting traffic across the link.

Example

The following command disables the multilink group *ml_remote*:

```
disable multilink ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

disable ports loopback

```
disable ports <portlist> [t1 | e1 | t3] loopback
```

Description

Disables the current loopback mode and returns port to normal function.

Syntax Description

portlist	A list of ports.

Default

Loopback is disabled by default.

Usage Guidelines

Use this command to return the near and remote side of a T1, E1, or T3 link form loopback mode to normal mode.

You can also use the following command to return the remote T1 or T3 port to normal mode from loopback mode:

```
enable ports <portlist> [t1 | t3] loopback remote loopdown
```

Example

The following command blah:

```
disable ports 2:1-2:4 t1 loopback
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

disable wanqos

```
disable wanqos {ports <portlist> | multilink <groupname>}
```

Description

Disables WAN QoS for T1 and E1 ports.

Syntax Description

portlist	A list of ports.
groupname	A multilink group name.

Default

WAN QoS is disabled by default.

Usage Guidelines

This command disables WAN QoS for T1 and E1 links. There is no equivalent command for T3 links.

Example

The following command disables WAN QoS on ports 1:1 and 1:3:

```
disable wanqos ports 1:1,1:3
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

enable multilink

```
enable multilink <groupname>
```

Description

Enables an MLPPP multilink group.

Syntax Description

groupname	Specifies the multilink group name.

Default

N/A.

Usage Guidelines

Use this command to enable a multilink group.

Example

The following command enables the multilink group *ml_remote*:

```
enable multilink ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

enable ports loopback

```
enable ports <portlist> [t1 | e1 | t3] loopback [local | network line]
```

Description

Enables the near-end local and network line loopback modes.

Syntax Description

portlist	A list of ports.
local	Specifies local loopback.
network line	Specifies network line loopback.

Default

Loopback is disabled by default.

Usage Guidelines

Use this command to enable local and network line loopback modes on the local port for T1, E1, and T3 links.

T1 links also support an additional mode, network payload loopback. Use the following command for network payload loopback mode:

```
enable ports <portlist> t1 loopback network payload
```

For remote loopback modes, use the command:

```
enable ports <portlist> [t1 | t3] loopback remote [line | payload | loopdown]
```

Example

The following command enables network line loopback mode on all the ports of an E1 module:

```
enable ports 4:1-4:4 e1 loopback network line
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

enable ports loopback remote

```
enable ports <portlist> [t1 | t3] loopback remote [line | payload |
loopdown]
```

Description

Enables and disables remote loopback modes for T1 and T3 ports.

Syntax Description

portlist	A list of ports.

Default

Loopback is disabled by default.

Usage Guidelines

This command enables and disables remote loopback for T1 and T3 links. There is no equivalent command for E1 links.

The “loopdown” keyword is used to disable loopback at the remote end.

Example

The following command causes the remote end of a T3 link to enter payload loopback mode:

```
enable ports 3:1 t3 loopback remote payload
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

enable ports t1 loopback network payload

```
enable ports <portlist> t1 loopback network payload
```

Description

Enables network payload loopback mode on T1 links.

Syntax Description

portlist	A list of ports.

Default

Loopback is disabled by default.

Usage Guidelines

Use this command to enable network payload loopback modes on the local port for T1 links. This mode is not available for E1 and T3 links.

WAN links also support additional modes, local and network line loopback. Use the following command for these modes:

```
enable ports <portlist> [t1 | e1 | t3] loopback [local | network line]
```

For remote loopback modes, use the command:

```
enable ports <portlist> [t1 | t3] loopback remote [line | payload | loopdown]
```

Example

The following command enables network payload loopback mode on a T1 link:

```
enable ports 4:3 t1 loopback network payload
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

enable vman termination

```
enable vman termination {ports <portlist> | multilink <groupname>}
```

Description

Enables VMAN termination for T1 and E1 ports.

Syntax Description

portlist	A list of ports.
groupname	A multilink group name.

Default

VMAN termination is disabled by default.

Usage Guidelines

This command enables VMAN termination for T1 and E1 links. There is no equivalent command for T3 links.

Example

The following command enables VMAN termination on ports 1:1 and 1:3:

```
enable vman termination ports 1:1,1:3
```

History

This command was first available in ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

enable wanqos

```
enable wanqos {ports <portlist> | multilink <groupname>}
```

Description

Enables WAN QoS for T1 and E1 ports.

Syntax Description

portlist	A list of ports.
groupname	A multilink group name.

Default

WAN QoS is disabled by default.

Usage Guidelines

This command enables WAN QoS for T1 and E1 links. There is no equivalent command for T3 links.

When WAN QoS is enabled, egress traffic is sorted into eight software egress queues for each T1 or E1 port.

Example

The following command enables WAN QoS on ports 1:1 and 1:3:

```
enable wanqos ports 1:1,1:3
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

restart multilink

```
restart multilink <groupname>
```

Description

Restarts an MLPPP multilink group.

Syntax Description

groupname	Specifies the multilink group name.

Default

N / A.

Usage Guidelines

Use this command to restart a multilink group. This command is the equivalent of disabling and then enabling a multilink group. You would use this command if you have changed any configuration parameters of the MLPPP group. The changed configuration does not take effect until you disable then enable the link, or until you restart the link.

Example

The following command restarts the multilink group *ml_remote*:

```
restart multilink ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show accounts pppuser

```
show accounts pppuser
```

Description

Display the PPP user accounts database.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to examine the entries in the PPP user accounts database, used for authentication when a link is initiated from a remote peer.

Example

The following command displays the PPP accounts database:

```
show accounts pppuser
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show multilink

```
show multilink <groupname>
```

Description

Displays the configuration of the multilink group.

Syntax Description

groupname	Specifies a previously created multilink group.

Default

N/A.

Usage Guidelines

Use this command to display the ports in a multilink group, and the PPP configuration of the group.

Example

The following command displays the configuration for the multilink group *m_remote1*:

```
show multilink m_remote1
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show multilink alarms

```
show multilink <groupname> [t1 | e1] alarms {detail}
```

Description

Displays alarms for a multilink group.

Syntax Description

groupname	Specifies a previously created multilink group.

Default

N/A.

Usage Guidelines

Use this command to display alarms that may have been received on any of the ports that make up a multilink group. To display alarms on a T3 link, use the command:

```
show ports <portlist> t3 alarms
```

Example

The following command displays the alarms for T1 ports in the multilink group *ml_example*:

```
show multilink ml_example t1 alarms
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show multilink e1 errors

```
show multilink <groupname> e1 errors near-end [totals | intervals |
current]
```

Description

Displays the current and past port error statistics for E1 multilink groups.

Syntax Description

groupname	Specifies a previously created multilink group.

Default

N / A.

Usage Guidelines

For an E1 multilink group, you can display errors from the near-end only.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For T1 multilink group errors, use the following command:

```
show multilink <groupname> t1 errors [near-end | far-end] [totals | intervals |
current]
```

Example

The following command displays the E1 multilink group errors detected on the near-end during the current interval for the multilink group *m_example1*:

```
show multilink m_example1 e1 errors near-end current
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show multilink stats

```
show multilink <groupname> stats {detail}
```

Description

Displays multilink statistics.

Syntax Description

groupname	Specifies a previously created multilink group.

Default

N/A.

Usage Guidelines

Display the statistics of a multilink group.

Example

The following command displays the detailed statistics for the multilink group *m_remote1*:

```
show multilink m_remote1 stats detail
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show multilink t1 errors

```
show multilink <groupname> t1 errors [near-end | far-end] [totals |
intervals | current]
```

Description

Displays the current and past error statistics for T1 multilink groups.

Syntax Description

groupname	Specifies a previously created multilink group.

Default

N/A.

Usage Guidelines

For T1 multilink groups, you can display errors from the near-end or the far-end.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For errors on E1 multilink groups, use the following command:

```
show multilink <groupname> e1 errors near-end [totals | intervals | current]
```

Example

The following command displays the T1 errors detected on the near-end during the current interval:

```
show ports t1 errors near-end current
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ports alarms

```
show ports {mgmt | <portlist>} {t1 | e1 | t3} alarms
```

Description

Displays real-time port alarms.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, alarms are displayed for all ports.

Example

The following command displays the alarms for T1 ports in:

```
show ports 2:1-2:4 t1 stats
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ports configuration

```
show ports {mgmt | <portlist>} [t1 | e1 | t3] configuration
```

Description

Displays the port configuration and status.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, configuration and status are displayed for all ports.

Example

The following command displays the T1 configuration and status of one port:

```
show ports 4:1 t1 configuration
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ports errors

```
show ports {mgmt | <portlist>} [t1 | t3] errors [near-end | far-end]
[totals | intervals | current]
```

Description

Displays the current and past port errors for T1 and T3 links.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, errors are displayed for all ports.

For the T1 and T3 ports, you can display errors from the near-end or the far-end.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For E1 errors, use the following command:

```
show ports <portlist> e1 errors near-end [totals | intervals | current]
```

Example

The following command displays the T1 errors detected on the near-end during the current interval:

```
show ports t1 errors near-end current
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ports e1 errors

```
show ports {mgmt | <portlist>} e1 errors near-end [totals | intervals |
current]
```

Description

Displays the current and past port errors for E1 links.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, errors are displayed for all ports.

For an E1 port, you can display errors from the near-end only.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For T1 and T3 errors, use the following command:

```
show ports <portlist> [t1 | t3] errors [near-end | far-end] [totals | intervals |
current]
```

Example

The following command displays the E1 errors detected on the near-end during the current interval:

```
show ports e1 errors near-end current
```

History

This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ports info

```
show ports {mgmt | <portlist>} [t1 | e1 | t3] info
```

Description

Displays the port configuration and status.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, information is displayed for all ports.

Example

The following command displays the T1 information for a single port:

```
show ports 4:2 t1 info
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ports stats

```
show ports {mgmt | <portlist>} {t1 | e1 | t3} stats
```

Description

Displays real-time port statistics.

Syntax Description

mgmt	Specifies the management port. Supported only for switches that provide a management port.
portlist	Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify a port number or range of ports, statistics are displayed for all ports.

Example

The following command displays the statistics for the T1 ports in slot 2:

```
show ports 2:1-2:4 t1 stats
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.

show ppp

```
show ppp {<portlist>} {detail}
```

Description

Displays status information for PPP ports.

Syntax Description

portlist	Specifies the port number(s).
detail	Displayed more detailed status information for the PPP ports.

Default

By default, the command shows summarized status for the PPP port(s).

Usage Guidelines

The `portlist` parameter can be used to specify the port(s) for which status is to be shown. Alternatively, you can enter `show ppp` with no parameters to obtain status for all PPP ports. More detailed status information can be obtained for the PPP port(s) by specifying the detail parameter.

Example

The following command displays status information for the PPP ports:

```
show ppp
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

unconfigure ppp

```
unconfigure ppp [ports <portlist> | multilink <groupname>]
```

Description

Resets the configuration on the specified WAN ports or multilink group.

Syntax Description

portlist	Specifies the port number(s).
groupname	Specifies a previously created multilink group.

Default

N / A.

Usage Guidelines

The ports or multilink group PPP configuration is reset to the default, BCP encapsulation with no authentication required.

Example

The following command example resets the PPP parameters of all the ports in the multilink group *m_remote1* to BCP and no authentication:

```
unconfigure ppp m_remote1
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.

25 MPLS Commands

The MultiProtocol Label Switching (MPLS) module is a self-contained module for the BlackDiamond switch. Unlike other BlackDiamond modules, there are no external network interfaces on the MPLS module. Instead, the MPLS module provides advanced IP services for the other input/output (I/O) modules installed in the chassis. The MPLS module contains a powerful set of packet processing resources that operate in a one-armed fashion: receiving frames from the switch fabric, processing the frames, and transmitting the frames back into the switch fabric.

MPLS encompasses a growing set of protocols defined by the IETF. True to its name, MPLS is based on a label-switching forwarding algorithm. ATM and Frame Relay are examples of other protocols that use label-switching forwarding algorithms.

Conceptually, label switching is straightforward. A label is a relatively short, fixed-length identifier that is used to forward packets received from a given link. The label value is locally significant to a particular link and is assigned by the receiving entity.

Because labels are relatively short (for example, 20 bits in a MPLS shim header), the label of a received packet can be used as an index into a linear array containing the forwarding database. Forwarding database entries indicate the outgoing port and any label(s) to be applied to forwarded frames. Thus, forwarding may consist of a simple lookup and replacement of the incoming label with the appropriate outgoing label (otherwise known as *label swapping*).

The MPLS module includes the following features:

- **MultiProtocol label switching (MPLS)**—MultiProtocol Label Switching (MPLS) is a forwarding algorithm that uses short, fixed-length labels to make next-hop forwarding decisions for each packet in a stream.
- **IP unicast forwarding (longest prefix match)**—IP unicast packets are forwarded in the hardware using the longest prefix match algorithm. IP unicast forwarding is required to switch packets at ingress or upon egressing an MPLS network domain.
- **Destination-sensitive accounting**—Counts of IP packets and bytes are maintained based on the IP routes used to forward packets. Destination-sensitive accounting gives you the flexibility to bill your customers at predetermined and different rates. The rates are based on the customers' IP unicast packet destinations.

  The accounting feature categorizes IP unicast packets using two parameters, input VLAN ID and accounting bin number. The VLAN ID is used to identify from which customer the packet is received. The accounting bin number is associated with the route used to forward the packet. External billing application servers can correlate the accounting bin number to a specific billing rate.

This chapter documents the MPLS command set. Some commands are new for the MPLS module; other commands have been enhanced to support the MPLS module.

configure mpls

```
configure mpls [ldp | targeted-ldp] [hello | keep-alive] <hold_time>
<interval_time>
```

Description

Configures LDP session timers.

Syntax Description

ldp	Specifies an LDP session.
targeted-ldp	Specifies a targeted LDP session.
hello <hold_time> <interval_time>	The amount of time (in seconds) that a hello message received from a neighboring LSR remains valid. If a hello message is not received from a particular neighboring LSR within the specified `hello <hold_time>`, the hello-adjacency is not maintained with that neighboring LSR. The range is 6 to 65,534.
keep-alive <hold_time> <interval_time>	The time (in seconds) during which an LDP message must be received for the LDP session with a particular peer LSR to be maintained. If an LDP PDU is not received within the specified session `keep-alive <interval_time>`, the corresponding LDP session is torn down.The `<hold_time>` range is 6 to 65,534. The `<interval_time>` range is 1 to 21844.

Default

ldp hello <hold_time> – 15 seconds

targeted-ldp hello <hold_time> – 45 seconds

ldp hello <interval_time> – 5 seconds

targeted-ldp hello <interval_time> – 15 seconds

ldp keep-alive <hold_time> – 40 seconds

targeted-ldp keep-alive <hold_time> – 60 seconds

ldp keep-alive <interval_time> – 13 seconds

targeted-ldp keep-alive <interval_time> – 20 seconds

Usage Guidelines

LDP session timers are separately configurable for LDP and targeted LDP sessions. The `hello <hold_time> <interval_time>` parameter specifies the amount of time (in seconds) that a hello message received from a neighboring LSR remains valid. If a hello message is not received from a particular neighboring LSR within the specified `hello <hold_time>`, the hello-adjacency is not maintained with that neighboring LSR.

The session `keep-alive <hold_time> <interval_time>` parameter specifies the time (in seconds) during which an LDP message must be received for the LDP session with a particular peer LSR to be

maintained. If an LDP PDU is not received within the specified session `keep-alive <interval_time>`, the corresponding LDP session is torn down.

The minimum and maximum values for both the `hello <hold_time> <interval_time>` and `keep-alive <hold_time> <interval_time>` are 6 and 65,534, respectively.

This command can only be executed when MPLS is disabled.

Example

The following command configures LDP session hello hold time to 30 seconds and the interval time to 5 seconds:

```
configure mpls ldp hello 30 5
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls add tls-tunnel

```
configure mpls add tls-tunnel <tunnel_name> [lsp <lsp_name> | <ipaddress> |
<host_name>] <local_vlan_name> [tls-labels <ingress_label> <egress_label> |
vcid <vcid> {<groupid>} {from [<local_endpoint_ipaddress> |
<local_endpoint_vlan>]}]
```

Description

Adds a TLS tunnel.

Syntax Description

tunnel_name	Specifies a name used to identify the TLS tunnel within the switch.
[lsp <lsp_name> | <ipaddress> | <host_name>]	Identifies the peer LSR that is the tunnel endpoint. The DNS client must be configured to use the <host_name>.
local_vlan_name	Specifies a VLAN name that identifies the layer 2 traffic that is to be transported.
tls-labels <ingress_label> <egress_label>	Identifies the innermost labels of the tunnel stack.
vcid	Identifies the virtual circuit identifier. The vcid value is a non-zero, 32-bit number.
groupid	Identifies the logical VCID group number. The groupid is a 32-bit number. All TLS tunnels that are members of the same TLS group ID can be withdrawn simultaneously by specifying the groupid.
from <local_endpoint_ipaddress> | <local_endpoint_vlan>	Identifies the local endpoint of the TLS tunnel.

Default

N/A.

Usage Guidelines

To add a static labeled TLS tunnel, use the following command:

```
configure mpls add tls-tunnel <tunnel_name> [lsp <lsp_name> | <ipaddress> |
<host_name>] <local_vlan_name> tls-labels <ingress_label> <egress_label>
```

To add a dynamic labeled TLS tunnel (martini-draft compliant), use the following command:

```
configure mpls add tls-tunnel <tunnel_name> [lsp <lsp_name> | <ipaddress> |
<host_name>] <local_vlan_name> vcid <vcid> <groupid>
```

The <tunnel_name> parameter is a character string that is to be used to identify the TLS tunnel within the switch. It must begin with an alphabetic character and can contain up to 31 additional alphanumeric characters.

The <ipaddress> parameter identifies the peer LSR that is the endpoint of the tunnel. This IP address should be configured with a 32-bit prefix on the peer LSR. When the peer LSR is also an Extreme switch, either OSPF must also be enabled on the VLAN to which the IP address is assigned (using the configure ospf add vlan command on the peer switch), or the peer switch must be configured to distribute direct routes into the OSPF domain (using the enable ospf export direct command). The

`ospf export` command should be used when the tunnel LSP needs to cross OSPF area boundaries or when ESRP is enabled on the VLAN to which the IP address is assigned.

The `<vcid>` parameters are used to configure dynamic TLS tunnels when full martini-draft TLS tunnel compliance is desired. The `vcid` and `groupid` values are advertised on a targeted LDP session to the specified tunnel endpoint ipaddress in a martini-draft defined FEC-TLV. Each LER advertises the vcid, groupid, and VLAN label in the Label Mapping message across an LDP session. This three-tuple TLS tunnel information allows each egress LER to dynamically bind the TLS tunnel to a local VLAN. The vcid is a non-zero 32-bit ID that defines the tunnel connection and the optionally specified groupid is a 32-bit value that defines logical virtual tunnel connection group. The groupid value defaults to zero if not explicitly configured.

The `<local_vlan_name>` parameter identifies the Layer-2 traffic that is to be transported. All of the local traffic received by the switch for this VLAN is transported across the tunnel.

The `tls-labels` parameters specify the innermost labels of the tunnel label stack and are used to configure static TLS label tunnels. The `<egress_label>` is inserted into the MPLS header of Layer-2 frames forwarded onto the tunnel LSP by this switch, and must be meaningful to the peer TLS node.

All traffic received from the tunnel LSP that contains the `<ingress_label>` is forwarded to the local VLAN identified by the `<local_vlan_name>` parameter.

When ingress traffic is forwarded to the local VLAN, the VLAN ID is set to the VLAN ID of the local VLAN, without regard to the VLAN ID in the MAC header of the frame received from the tunnel LSP. Thus, there is no requirement that all sites of an extended VLAN be configured to use the same VLAN ID. This can simplify network management in some situations.

The `tls-labels` parameters are specified using hexadecimal notation. The value of the `<ingress_label>` parameter must be unique within the switch (the same `<ingress_label>` value cannot be used for two different tunnels). The valid range of the ingress label parameter is [8C000..8FFFF].

The valid range of the `<egress_label>` parameter is [00010..FFFFF]. If the peer LSR is also an Extreme switch, then the `<egress_label>` must be in the range [8C000..8FFFF].

Because LSPs are unidirectional in nature, coordinated configuration is required at both tunnel endpoint switches. The `<egress_label>` at one tunnel endpoint switch must match the `<ingress_label>` at the other tunnel endpoint switch, and vice versa.

Example

The following command creates a TLS tunnel to 11.0.4.11 for traffic originating from VLAN unc:

```
configure mpls add tls-tunnel rt40 11.0.4.11 unc tls-labels 8f001 8f004
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls add vlan

```
configure mpls add vlan [<vlan name> | all] {ldp | rsvp-te}
```

Description

Enables LDP or RSVP-TE for one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
ldp	Enables LDP.
rsvp-te	Enables RSVP-TE.

Default

N/A.

Usage Guidelines

MPLS must be enabled on all VLANs that transmit or receive MPLS-encapsulated frames. Using the `configure mpls add vlan` command causes the LDP neighbor discovery process to begin on the specified VLAN.

NOTE

The specified VLAN must be configured with an IP address and must have IP forwarding enabled. IGMP snooping must also be enabled on the switch.

If all VLANs are selected, MPLS is enabled on all VLANs that have an IP address and IP forwarding enabled.

If you have enabled MPLS on an OSPF interface that is used to reach a particular destination, make sure that you enable MPLS on all additional OSPF interfaces that can reach that same destination (for example, enable MPLS on all VLANs that are connected to the backbone network).

Example

The following command enables RSVP-TE on vlan1:

```
configure mpls add vlan vlan1 rsvp-te
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls delete tls-tunnel

```
configure mpls delete tls-tunnel [<tunnel_name> | group <groupid> | all]
```

Description

Deletes one or all TLS tunnels.

Syntax Description

tunnel_name	Specifies a TLS tunnel name.
group <groupid>	Specifies a group identifier
all	Specifies all TLS tunnels.

Default

N / A.

Usage Guidelines

This command deletes the TLS tunnel with the specified tunnel name. Specify the `<groupid>` if you want to delete all TLS tunnels belonging to a specific group. Specify the `<groupid>` if you want to delete all TLS tunnels belonging to a specific group. Use the `all` keyword to delete all TLS tunnels.

Example

The following command deletes the TLS tunnel *rt40*:

```
configure mpls delete tls-tunnel rt40
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls delete vlan

```
configure mpls delete vlan [<vlan name> | all] {ldp | rsvp-te}
```

Description

Disables LDP or RSVP-TE on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
ldp	Disables LDP.
rsvp-te	Disables RSVP-TE.

Default

N/A.

Usage Guidelines

Disables LDP or RSVP-TE on one or all VLANs. If not specified, both are disabled for the specified VLAN.

Example

The following command disables RSVP-TE on vlan1:

```
configure mpls delete vlan vlan1 rsvp-te
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls ldp advertise

```
configure mpls ldp advertise [direct | rip | static] [all | none |
route-map <route_map>]
```

Description

Configures a filter to be used by LDP when originating unsolicited label mapping advertisements to LDP neighbors.

Syntax Description

direct	Specifies that the advertisement filter is applied to the associated FECs with directly-attached routing interfaces.
rip	Specifies that the advertisement filter is applied to FECs associated with RIP routes exported by OSPF.
static	Specifies that the advertisement filter is applied to FECs associated with static routes.
all	Specifies that unsolicited label mapping advertisements are originated for all routes of the specified type.
none	Specifies that no unsolicited label mapping advertisements are originated for the specified route type.
route-map	Specifies a route map is used to filter the origination of unsolicited label mapping advertisements for the specified route type.

Default

All—the default setting for the direct routing method.

None—the default setting for the RIP and static routing methods.

Usage Guidelines

Only the nlri-list route-map match operation keyword is supported for filtering origination of MPLS label advertisements.

You can configure how the advertisement filter is applied, as follows:

- `direct`—The advertisement filter is applied to the FECs associated with directly-attached routing interfaces.
- `rip`—The advertisement filter is applied to the FECs associated with RIP routes exported by OSPF.
- `static`—The advertisement filter is applied to the FECs associated with static routes.

You can configure the advertisement filter, as follows:

- `all`—All unsolicited label mappings are originated for all routes of the specified type (direct, RIP, or static). This is the default setting for direct routes.
- none—No unsolicited label mappings are originated for all routes of the specified type. This is the default setting for RIP and static routes.

- `route-map <route_map>`—The specified route map is used to permit or deny the origination of unsolicited label mappings for all routes of the specified type.

  The only supported route map match operation keyword is `nlri-list`. If selected, the `access_profile` parameter of the `nlri-list` keyword is compared to the FEC that is associated with each route.

NOTE

For more information on route maps, see the ExtremeWare Software Users Guide.

RIP routes are advertised with the Implicit NULL label and direct routes are advertised with an MPLS label, unless PHP is enabled.

Advertising labels for a large number of routes may increase the required number of labels that must be allocated by LSRs. Take care to ensure that the number of labels advertised by LERs does not overwhelm the label capacity of the LSRs.

Example

The following command configures a filter to be used by LDP when originating unsolicited label mapping advertisements for RIP routes:

```
configure mpls ldp advertise rip all
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls ldp advertise vlan

```
configure mpls ldp advertise [add | delete] vlan <vlan name>
```

Description

Configures LDP to originate an unsolicited label for the FECs associated with the directly attached routing interface of the specified VLAN.

Syntax Description

add	Originates an unsolicited label for the FECs associated with the directly attached routing interface of the specified VLAN
delete	Removes label origination of the direct route for the specified VLAN
vlan name	Specifies the name of the VLAN.

Default

N / A.

Usage Guidelines

Configures LDP to originate an unsolicited label for the FECs associated with the directly attached routing interface of the specified VLAN. The `delete` keyword removes label origination of the direct route for the specified VLAN. The LDP label origination configuration for directly attached routing interfaces can also be set using the `configure mpls ldp advertise direct` command.

Example

The following command configures LDP to advertise a label for the direct route configured for VLAN vlan1:

```
configure mpls advertise add vlan vlan1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls php

```
configure mpls php [enabled | disabled]
```

Description

Enables and disables penultimate hop popping (PHP) at the egress LSR. When enabled, PHP is requested on all LSPs for which the switch is the egress LSR.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command enables or disables whether PHP is requested by the egress LER.

When PHP is enabled, PHP is requested on all LSPs for which the switch is the egress LER.

PHP is requested by assigning the Implicit Null Label in an advertised mapping. PHP is always performed when requested by an egress LSR (for example, when the switch is acting as an intermediate LSR). The Implicit Null Label is always used in conjunction with routes exported by OSPF, regardless of the PHP configuration.

This command can only be executed when MPLS is disabled.

Example

The following command enables penultimate hop popping (PHP) at the egress LSR:

```
configure mpls php enabled
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls propagate-ip-ttl

```
configure mpls propagate-ip-ttl [enabled | disabled]
```

Description

Enables or disables the propagation of the IP time-to-live (TTL) field for routed IP packets. When propagation is enabled, each LSR is viewed as a router hop from an IP TTL perspective. When propagation is disabled, the LSP is viewed as a point-to-point link between the ingress LSR and the egress LSR.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command enables and disables the propagation of the IP TTL value for routed IP packets. The default setting is enabled.

NOTE

You must maintain identical `propagate-ip-ttl` *settings on all LERs in the MPLS domain. Not doing so may cause packets to loop endlessly and not be purged from the network if a routing loop is inadvertently introduced.*

When `propagate-ip-ttl` is disabled, the LSP is viewed as a point-to-point link between the ingress LSR and the egress LSR. Intermediate LSRs in the MPLS network are not viewed as router hops (from an IP TTL perspective). In this case, the IP TTL is decremented once by the ingress LSR and once by the egress LSR. When disabled, the MPLS TTL is set to 255 by the ingress LSR and is independent of the IP TTL.

When `propagate-ip-ttl` is enabled, each LSR is viewed as a router hop (from an IP TTL perspective). When a packet traverses an LSP, it emerges with the same TTL value that it would have had if it had traversed the same sequence of routers without being label-switched. When enabled, the MPLS TTL field is initially set to the IP TTL field at the ingress LSR, and the IP TTL field is set to the MPLS TTL by the egress LSR.

Example

The following command enables the propagation of the IP time-to-live (TTL) field for routed IP packets:

```
configure mpls propagate-ip-ttl enabled
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls qos-mapping

```
configure mpls qos-mapping [dot1p-to-exp | exp-to-dot1p] [all |
<input_value>]/<output_value>
```

Description

Configures MPLS-specific QoS mappings.

Syntax Description

dot1p-to-exp	Specifies that mappings are used in performing the ingress LSR function. The value in this priority field is set based on the QoS classification performed by the ingress I/O module.
exp-to-dot1p	Specifies that mappings are used when performing label swapping as an intermediate LSR and when performing the egress LSR function.
all	Specifies to map all input values to the specified output value.
input_value	Specifies an input value.
output_value	Specifies an output value.

Default

Mapping tables are initialized such than an <input_value> of *n* is mapped to an <output_value> of *n*.

Usage Guidelines

The valid range of integers for the <input_value> and the <output_value> is 0 to 7. Two mappings are supported:

- dot1p-to-exp
- exp-to-dot1p

Dot1p-to-exp Mappings

The dot1p-to-exp mappings are used by the ingress LSR. When a non-MPLS ingress frame arrives at the MPLS module, the frame always contains an IEEE 802.1p priority field.

The value of the priority field is set based on the QoS classification performed by the ingress I/O module. The ingress I/O modules assign each packet to a hardware queue, based on the configured ExtremeWare QoS policies. There is a one-to-one mapping between the hardware queue and the 802.1p priority values that are inserted into frames forwarded to the MPLS module. For example, the 802.1p priority value is set to 0 for frames forwarded from hardware queue 0, set to 1 for frames forwarded from hardware queue 1, and so on.

The dot1p-to-exp table maps 802.1 priority values to MPLS EXP values. The table is completely flexible, such that any 802.1p priority <input_value> can be mapped to any EXP <output_value>. The EXP output_value is set in the MPLS header of the packet as it is forwarded to the MPLS network.

Exp-to-dot1p Mappings

The exp-to-dot1p mappings are used when the switch performs label swapping as an intermediate LSR and when the switch is the egress LSR. In both of these cases, the MPLS module receives an MPLS-encapsulated frame.

The EXP field in the frame is used as an <input_value> to the exp-to-dot1p table. The corresponding <output_value> is an 802.1p priority value. The 802.1p priority value is inserted into the frame before the frame is forwarded by the MPLS module.

The exp-to-dot1p table is completely flexible, such that any EXP <input_value> can be mapped to any 802.1p priority <output_value>.

The exp-to-dot1p table is also used by Packet over SONET (PoS) ports when classifying MPLS-encapsulated packets received from the SONET link. When a PoS port receives an MPLS-encapsulated packet from the SONET link, the packet is classified based on the EXP value in the MPLS shim header. The EXP value from the received frame is used as an index into the exp-to-dot1p mapping table to retrieve and 802.1p priority value. The frame is then assigned to a QoS profile, based on the retrieved 802.1p priority value. The mappings between 802.1p priority values and QoS profiles are configured using the following command:

```
configure dot1p type
```

Example

The following command configures the dot1p-to-exp MPLS-specific QoS mappings:

```
configure mpls qos-mapping dot1p-to-exp 0/1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te add lsp

```
configure mpls rsvp-te add lsp <lsp_name> path <path_name> {<profile_name>}
{primary | secondary}
```

Description

Adds an RSVP-TE LSP.

Syntax Description

lsp_name	Specifies the LSP name.
path_name	Specifies the path name
profile_name	Specifies the profile name.
primary	Specifies the primary LSP.
secondary	Specifies a secondary LSP.

Default

N / A.

Usage Guidelines

Both the <lsp_name> and <path_name> must be specified. The <lsp_name> parameter is a character string that is to be used to identify the LSP within the switch. The <lsp_name> string must begin with an alphabetic character and can contain up to 31 additional alphanumeric characters. The <profile_name> is optional. If omitted, the default profile is applied to the LSP. If no explicitly specified, the <path_name> defaults to the primary path. The LSP is immediately signaled as soon as it is configured. The maximum number of configurable LSPs is 1024.

Example

The following command adds a primary RSVP-TE LSP that takes the routed path named paththroughdenver:

```
configure mpls rsvp-te add lsp lsptonyc path paththroughdenver
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te add path

```
configure mpls rsvp-te add path <path_name> [<ipaddress> | <host_name>]
{from <local_endpoint_vlan>}
```

Description

Adds a path to an RSVT-TE LSP.

Syntax Description

path_name	Specifies the path name.
ipaddress	Specifies the IP address.
hostname	Specifies the hostname.
local_endpoint_value	Specifies the local endpoint from which the path is signaled.

Default

N / A.

Usage Guidelines

The <path_name> and <ipaddress> or <host_name> must be specified for the path. The <path_name> parameter is a character string that is to used to identify the path within the switch. The <path_name> string must begin with an alphabetic character, and may contain up to 31 additional alphanumeric characters. Each <path_name> represents a routed path to a single IP destination.

If the <host_name> is specified, the DNS client on the switch must be configured so that the <host_name> can first be resolved to an IP address. Alternate routed paths to the same IP destination may be configured by adding additional <path_names> and specifying the same <ipaddress> or <host_name> as the path endpoint.

The RSVP-TE path is not signaled until an LSP is added with the specified <path_name>. If no explicit route objects are configured, the path will follow the best-routed path to the configured <ipaddress> (or IP address obtained from DNS name resolution). Optionally, the from keyword can be used to specify the <local_endpoint_vlan> from which the path is signaled. The maximum number of configurable paths is 255.

Example

The following command adds a path to 76.42.10.1 called paththroughdenver:

```
configure mpls rsvp-te add path paththroughdenver 76.42.10.1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te add profile

```
configure mpls rsvp-te add profile <profile_name> {bandwidth <bps>}
{setup-priority <priority>} {hold-priority <priority>} {retry-timeout
<seconds>} {hop-count <number>} {ping-interval <seconds>} {metric [<metric>
| igp-tracking} {record [enabled | disabled]}
```

Description

Adds an RSVP-TE profile.

Syntax Description

profile_name	Specifies the profile name.
bandwidth	Specifies the reserved bandwidth for the LSP.
setup-priority	A value that is compared to the hold-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.
hold-priority	A value that is compared to the setup-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.
retry-timeout	Specifies the maximum number of seconds the switch allows for LSP setup.
ping-interval	Specifies how frequently an ICMP echo request is transmitted to the egress LSR IP address on the established LSP.
metric	Specifies a route metric used to determine if an established RSVP-TE LSP will actually be used to send data.
record	Specifies hop-by-hop path recording.

Default

N/A.

Usage Guidelines

A profile is a set of attributes that are applied to the LSP when the LSP is configured using the `configure mpls rsvp-te add lsp` command. A default profile is provided which cannot be deleted, but can be applied to any configured LSP. The profile name for the default profile is *default*. The default profile parameter values are initially set to their respective default values. The maximum number of configurable profiles is 255 (one of which is reserved for the default profile).

The `bandwidth` parameter specifies the desired reserved bandwidth for the LSP. Any positive integer bps value is valid. Optionally, you can append the characters, k for kilobits, m for megabits, or g for gigabits, to the bps value to specify the unit of measure. If the k, m, or g, character is omitted, the unit of measure is assumed to be kilobits. The default bandwidth bps value is zero, which indicates that the QoS for the LSP is best effort. ExtremeWare does not support bandwidth reservation.

The `setup-priority` and `hold-priority` are optional parameters indicating the LSP priority. During path set up, if the requested bandwidth cannot be reserved through the LSR, the `setup-priority` parameter is compared to the `hold-priority` of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established. Lower numerical values represent higher priorities. The `setup-priority` range is 0 to 7 and the default value is 7. The

hold-priority range is also 0 to 7 and is set equal to the setup-priority by default. ExtremeWare does not support LSP preemption.

The retry-timeout keyword specifies the maximum number of seconds the switch allows for LSP setup. If the LSP cannot be established within retry-timeout seconds, the LSP is resignaled. The default value for retry-timeout is 30 seconds with a configurable range of 5 to 600 seconds. The hop-count parameter limits the number of LSRs the path can traverse, including the ingress and egress router. The default hop-count value is 255 with a configurable range of two to 255.

After an LSP has established, the egress LSR may be optionally pinged to determine end-to-end path connectivity. If a ping response is not received within [2 * ping-interval – 1] seconds, the LSP is considered unavailable. The ping-interval keyword specifies how frequently an ICMP echo request is transmitted to the egress LSR IP address on the established LSP. The default ping-interval is zero, which indicates no end-to-end LSP health checking is performed. You can set the ping-interval value to any interval between 0 and 60 seconds.

The route metric is used to determine if an established RSVP-TE LSP will actually be used to send data. Whenever the configured metric is less than, or equal, to the calculated IGP metric, the LSP is used for sending routed IP traffic. In this case, the LSP is also used to send TLS data when the TLS tunnel is configured by specifying the tunnel LSP endpoint IP address. Traffic is distributed across up to four equal-cost LSPs. The valid metric values range from 1 to 65535. Specifying the igp-tracking keyword forces the route metric to track the underlying IGP metrics. If no IGP metric exists for the LSP (for example, the LSP traverses a RIP network), the metric is ignored. Tracking IGP metrics is the default behavior.

The record keyword is used to enable hop-by-hop path recording. The enabled keyword causes the record route object (RRO) to be inserted into the path message. The RRO is returned in the reserve message and contains a list of IPv4 subobjects that describe the RSVP-TE path. Path recording by default is disabled. When disabled, no RRO is inserted into the path message.

Example

The following command adds a profile with the configured attributes:

- Reserved bandwidth signaled is 100 Mbps
- Tunnel LSP setup priority is 1
- Tunnel LSP hold priority is 0
- Route recording is enabled

```
configure mpls rsvp-te add profile customer1 bandwidth 100m setup-priority 1
hold-priority 0 record enabled
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te delete lsp

```
configure mpls rsvp-te delete lsp [<lsp_name> | all]
```

Description

Deletes an RSVP-TE LSP.

Syntax Description

lsp_name	Specifies the name of the LSP.

Default

N / A.

Usage Guidelines

Deleting an LSP name disassociates all configured paths with this LSP and all configuration information for the LSP name is deleted. LSPs cannot be deleted if the specified `<lsp_name>` has been configured as the LSP for a TLS tunnel. If you specify the `all` keyword, all LSPs not associated with a TLS tunnel are deleted.

Example

The following command deletes all RSVP-TE LSPs:

```
configure mpls rsvp-te delete lsp all
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te delete path

```
configure mpls rsvp-te delete path [<path_name> | all]
```

Description

Deletes an RSVP-TE path.

Syntax Description

path_name	Specifies the name of the path.

Default

N/A.

Usage Guidelines

This command deletes a configured MPLS RSVP-TE routed path with the specified <path_name>. All associated configuration information for <path_name> is deleted. A path cannot be deleted as long as the <path_name> is associated with an LSP. If the all keyword is specified, all paths not associated with an LSP are deleted.

Example

The following command deletes all RSVP-TE paths:

```
configure mpls rsvp-te delete path all
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te delete profile

```
configure mpls rsvp-te delete profile [<profile_name> | all]
```

Description

Deletes an RSVP-TE path profile.

Syntax Description

profile_name	Specifies the name of the profile.

Default

N/A.

Usage Guidelines

This command deletes a configured RSVP-TE profile with the specified profile name. The default profile cannot be deleted. If a profile is associated with a configured LSP, the profile cannot be deleted. If you specify the `all` keyword, all profiles not associated with an LSP are deleted (except for the default profile).

Example

The following command deletes all RSVP-TE path profiles:

```
configure mpls rsvp-te delete profile all
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te lsp add path

```
configure mpls rsvp-te lsp <lsp_name> add path <path_name> {<profile_name>}
{secondary | primary}
```

Description

Adds a path to an RSVP-TE LSP.

Syntax Description

lsp_name	Specifies the name of a configured LSP.
path_name	Specifies the path name.
profile_name	Specifies the profile name.
primary	Specifies the primary path.
secondary	Specifies a secondary path.

Default

N/A.

Usage Guidelines

The <lsp_name> must represent a configured LSP. Only one primary path and up to two secondary paths can be added per <lsp_name>. The <path_name> specified defaults to primary when no primary path has been configured for <lsp_name> and defaults to secondary if the primary path has been previously configured for <lsp_name>.

You do not need to configure the primary path for an LSP. Each <path_name> added to an <lsp_name> must be unique, but a <path_name> can be associated with multiple LSP names.

All configured primary and secondary paths for the <lsp_name> must have the same endpoint IP address. For example, three paths can be configured for the <lsp_name>, but all paths should represent different topological paths through the network to the same LSP endpoint.

Adding a secondary <path_name> designates a path as a hot-standby redundant path, used in the event that the primary or secondary path cannot be established or fails. Provided the <path_name> has not already been established, all path names are signaled as soon as they are associated with an <lsp_name>. If the primary <path_name> fails, is not configured, or cannot be established after the specified LSP retry-timeout, one of the configured secondary paths may become the active path for <lsp_name>. All of the secondary paths have equal preference; the first one available is chosen. If at any time the primary path is established, <lsp_name> immediately switches to using the primary path. If a secondary path fails while in use, the remaining configured secondary paths can become the active path for <lsp_name>.

Example

The following command adds a secondary path named paththroughdc for the specified LSP:

```
configure mpls rsvp-te lsp lsptonyc add path paththroughdc secondary
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te delete path

```
configure mpls rsvp-te delete path [<path_name> | all]
```

Description

Deletes an RSVP-TE path.

Syntax Description

path_name	Specifies the name of the path.

Default

N/A.

Usage Guidelines

This command deletes a configured MPLS RSVP-TE routed path with the specified <path_name>. All associated configuration information for <path_name> is deleted. A path cannot be deleted as long as the <path_name> is associated with an LSP. If the all keyword is specified, all paths not associated with an LSP are deleted.

Example

The following command deletes all RSVP-TE paths.

```
configure mpls rsvp-te delete path all
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te add ero

```
configure mpls rsvp-te path <path_name> add ero [ipaddress
<ipaddress/masklength> | <host_name>] {strict | loose} {order <number>}
```

Description

Adds an RSVP-TE explicit route.

Syntax Description

path_name	Specifies the path name.
ipaddress/masklength	Specifies an LSR using either a /32 address, which may represent an LSR router ID, loopback address, or direct router interface, or an IP prefix, which represents a directly connected subnet.
strict	Specifies a strict subobject.
loose	Specifies a loose subobject.
order <number>	Specifies the LSR path order.

Default

N/A.

Usage Guidelines

This command adds an IP address to the explicit route object (ERO) for the specified path name. The RSVP-TE routed path may be described by a configured sequence of the LSRs and/or subnets traversed by the path. Each defined LSR or subnet represents an ERO subobject. Up to 64 subobjects can be added to each path name.

When specifying an LSR using the `<host_name>` parameter, the DNS client on the switch must be configured so that the `<host_name>` can first be resolved to an IP address. The `ipaddress` keyword identifies an LSR using either a /32 address, which may represent an LSR router ID, loopback address, or direct router interface, or an IP prefix, which represents a directly connected subnet. Each IP address or prefix is included in the ERO as an IPv4 subobject. Each specified subobject must be topologically adjacent to the next subobject, as listed in the ERO. If the subobject matches a direct router interface or a directly attached subnet, the switch verifies that the path message is received on the matching router interface. If the LSR specified matches the OSPF router ID or a configured loopback IP address, the router interface on which the packet is received is ignored.

If the IP address is specified as `strict`, the strict subobject must be topologically[1] adjacent to the previous subobject as listed in the ERO. If the IP address is specified as `loose`, the loose subobject is not required to be topologically adjacent to the previous subobject as listed in the ERO. If omitted, the default subobject attribute is `strict`. Each IP address or prefix is included in the ERO as an IPv4 subobject.

If the subobject matches a direct router interface or a directly attached subnet, the switch verifies that the path message is received on the matching router interface. If the LSR specified matches the OSPF

1. The LSP next hop matches either the interface IP address or the OSPF router-id of the immediate neighbor LSR.

router ID or a configured loopback IP address, the router interface which the packet is received is ignored.

The LSR path order is optionally specified using the `order` keyword. The `order number` parameter is an integer value from 1 to 65535. IP prefixes with a lower number are sequenced before IP prefixes with a higher number. You can specify multiple paths and assign them an order number. The order number determines the path that the LSP follows. Thus, the LSP path follows the configured path of the IP prefix with the order value from low to high. If the `order` keyword is not specified, the number value for the LSR defaults to a value 100 higher than the current highest number value.

If the list of IP prefixes, added to the path, does not reflect an actual path through the network topology, the path message is returned with an error from a downstream LSR and the LSP is not established.

The order of a configured subobject can not be changed. The ERO subobject must be deleted and re-added using a different order. If a subobject is added to or deleted from the ERO while the associated LSP is established, the path is torn down and is resignaled using the new ERO.

Duplicate ERO subobjects are not allowed. Defining an ERO for the path is optional. If you do not configure an ERO, the path is signaled along the best-routed path and the ERO is not included in the path message. When the last subobject in the ERO of the path message is reached and the egress IP node of the path has not been reached, the remaining path to the egress node is signaled along the best-routed path. Specification of an ERO could lead to undesirable routed paths, so you should be careful when terminating the ERO routed-path definition prior to the configured path egress node.

Example

The following command adds a strict ERO subobject of 192.18.32.5 to the specified path:

```
configure mpls rsvp-te path paththroughdenver add ero ipaddress 192.18.32.5
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te delete ero

```
configure mpls rsvp-te path <path_name> delete ero [all | ipaddress
<ipaddress/masklength> | <host_name> | order <number>]
```

Description

Deletes an RSVP-TE explicit route.

Syntax Description

path_name	Specifies the path name.
ipaddress/masklength	Specifies an LSR using either a /32 address, which may represent an LSR router ID, loopback address, or direct router interface, or an IP prefix, which represents a directly connected subnet.
strict	Specifies a strict subobject.
loose	Specifies a loose subobject.
order <number>	Specifies the LSR path order.

Default

N/A.

Usage Guidelines

This command deletes an LSR or subnet from the ERO for the specified path name. The LSR is specified using the `ipaddress`, `<host_name>`, or `order` parameter. If an LSR is deleted from an ERO while the associated LSP is established, the path is torn down and is resignaled using a new ERO. Use the `all` keyword to delete the entire ERO from the path name. When there is no configured ERO, the path is no longer required to take an explicit routed path. The path is then signaled along the best-routed path and no ERO is included in the path message.

Example

The following command deletes all configured ERO subobjects from the specified path:

```
configure mpls rsvp-te path paththroughdc delete ero all
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te profile

```
configure mpls rsvp-te profile <profile_name> {bandwidth <bps>} {hop-count
<number>} {setup-priority <priority>} {hold-priority <priority>}
{retry-timeout <seconds>} {ping-interval <seconds>} {metric [<metric> |
igp-tracking]} {record [enabled | disabled]}
```

Description

Configures an existing RSVP-TE profile.

Syntax Description

profile_name	Specifies the profile name.
bandwidth	Specifies the reserved bandwidth for the LSP.
setup-priority	A value that is compared to the hold-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.
hold-priority	A value that is compared to the setup-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.
retry-timeout	Specifies the maximum number of seconds the switch allows for LSP setup.
ping-interval	Specifies how frequently an ICMP echo request is transmitted to the egress LSR IP address on the established LSP.
metric	Specifies a route metric used to determine if an established RSVP-TE LSP will actually be used to send data.
record	Specifies hop-by-hop path recording.

Default

N / A.

Usage Guidelines

This command configures RSVP-TE attributes for the specified profile. The `<profile_name>` must have been previously added. All of the LSP profile values are updated dynamically. For LSPs configured with this profile, the LSP parameters are updated automatically with the sending of the next refresh path message. If the metric is changed, all LSPs using this profile are rechecked against the calculated IGP metric. In some cases, the LSP may be torn down because of a profile configuration change. For example, if the bandwidth value is increased, the LSRs along the existing path may not be able to accommodate the additional reserved bandwidth. In this scenario, the LSP is torn down and resignaled.

Example

The following command configures the attributes for the specified profile:

```
configure mpls rsvp-te profile customer1 ping-interval 2
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls rsvp-te vlan

```
configure mpls rsvp-te vlan [<vlan name> | all] {hello-interval <seconds>}
{refresh-time <seconds>} {summary-refresh-time <tenth-seconds>}
{bundle-time <tenth-seconds>} {keep-multiplier <number>}
```

Description

Configures RSVP-TE protocol parameters

Syntax Description

vlan name	Specifies the VLAN name.
hello-interval	Specifies the RSVP hello packet transmission interval.
refresh-time	Specifies the interval for sending refresh path messages.
bundle-time	Specified the maximum amount of time a transmit buffer is held so that multiple RSVP messages can be bundled into a single PDU.
summary-refresh-time	Specifies the time interval for sending summary refresh RSVP messages.

Default

N/A.

Usage Guidelines

This command configures the RSVP-TE protocol parameters for the specified VLAN. The RSVP-TE keyword `all` indicates that the configuration changes apply to all RSVP-TE enabled VLANs.

The `hello-interval` time specifies the RSVP hello packet transmission interval. The RSVP hello packet is used by the switch to detect when a RSVP-TE peer is no longer reachable. If an RSVP hello packet is not received from a peer with [hello-interval * `keep-multiplier`] seconds, the peer is declared down and all RSVP sessions to and from that peer are torn down. The default `hello-interval` time is three seconds with a valid range from one to 60 seconds.

The `refresh-time` specifies the interval for sending refresh path messages. RSVP refresh messages provide “soft state” link-level keep-alive information for previously established paths and enables the switch to detect when an LSP is no longer active. RSVP sessions are torn down if an RSVP refresh message is not received from a neighbor within [(`keep-multiplier` + 0.5) * 1.5 * `refresh-time`] seconds. The default `refresh-time` is 30 seconds and the default `keep-multiplier` value is three. The minimum and maximum `refresh-time` values are one and 36,000 seconds (or one hour) respectively. The minimum and maximum `keep-multiplier` values are one and 255 respectively.

The `bundle-time`, specified in tenths of a second, indicates the maximum amount of time a transmit buffer is held so that multiple RSVP messages can be bundled into a single PDU. The default `bundle-time` is zero, indicating that RSVP message bundling is not enabled. The `bundle-time` value may be set to any value between zero and 30 (or 3 seconds).

The `summary-refresh-time`, specified in tenths of a second, indicates the time interval for sending summary refresh RSVP messages. The `summary-refresh-time` must be less than the configured `refresh-time`. The default `summary-refresh-time` is zero, indicating that no summary refresh RSVP

messages are sent. The `summary-refresh-time` value may be set to any value between zero to 100 (or 10 seconds).

If configured, the bundled and summary refresh RSVP messages are only sent to RSVP-TE peers supporting RSVP refresh reduction.

Example

The following command configures the rsvp-te interface parameters for VLAN vlan1.

```
configure mpls rsvp-te vlan vlan1 hello-interval 2 refresh-time 5
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls vlan ip-mtu

```
configure mpls vlan [<vlan name> | all] ip-mtu <number>
```

Description

Configures the IP MTU for frames transmitted onto MPLS LSPs via the specified egress VLAN. The range is 42 to 9190(using jumbo frame sizes).

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
number	Specifies an IP MTU size.

Default

1500 bytes.

Usage Guidelines

This command configures the IP MTU for frames transmitted onto MPLS LSPs via the specified egress VLAN. The default settings is 1500 bytes. If `all` is selected, the configuring MTU applies to all MPLS-enabled VLANs.

This command applies to the ingress LSR only when a received IP packet is destined for an MPLS LSP. In this case, if the length of the IP packet exceeds the configured MTU size for the egress VLAN and the Don't Fragment (DF) bit is *not* set in the IP header of the packet, the packet is fragmented before it is forwarded onto an MPLS LSP. If the DF bit is set in the packet header, Path MTU Discovery starts.

Fragmentation is based on either the minimum value of the configured MPLS IP MTU size or the configured IP MTU size for the egress VLAN. (The IP MTU size is configured using the `configure ip-mtu <number> vlan <vlan name>` command.)

Configure the MPLS IP MTU so that the addition of the MPLS label stack the link layer header does not cause the packet to be too large to be transmitted on the egress ports. To avoid potential problems, enable jumbo frame support on all ports that are members of an MPLS VLAN.

Example

The following command configures the IP MTU for frames transmitted onto MPLS LSPs:

```
configure mpls vlan vlan1 ip-mtu 1550
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure mpls vlan ldp propagate

```
configure mpls vlan [<vlan name> | all] ldp propagate [all | none |
route-map <route_map>]
```

Description

Configures a filter to be used by LDP when propagating unsolicited label mappings to all LDP neighbors on one or all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
all	Specifies all VLANs.
all	Specifies that all unsolicited label mappings are propagated to the VLAN.
none	Specifies that no unsolicited label mappings are propagated to the VLAN.
route_map	Specifies the route map used to permit or deny the propagation of unsolicited label mappings to the VLAN.

Default

All unsolicited label mappings are propagated to the VLAN.

Usage Guidelines

This command configures a filter to be used by LDP when propagating unsolicited label mappings to all LDP neighbors on the specified VLAN. If all VLANs are selected, the settings of this command apply to all MPLS-enabled VLANs.

Example

The following command configures a filter to be used by LDP when propagating unsolicited label mappings to *vlan1*:

```
configure mpls vlan vlan1 ldp propagate route-map bgp_out
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure vlan add track-lsp

```
configure vlan <vlan name> add track-lsp [<lsp_name> | ipaddress
<ipaddress>/<masklength>]
```

Description

Configures the LSPs tracked by ESRP in order to determine the ESRP state of the specified VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
lsp_name	Specifies a LSP name.
ipaddress	Specifies the IP address of the route entry to be tracked.

Default

No diagnostic tracking.

Usage Guidelines

LSP tracking provides MPLS with specific ESRP selection criteria for determining the ESRP status of a VLAN. LSP tracking is similar to route tracking and ping tracking in ESRP. ESRP can be configured to protect the user VLAN from disruptions in the MPLS network core.

This type of LSP protection is especially useful when providing ESRP redundant TLS L2 VPN services using Traffic Engineered LSPs that take completely different paths.

Using ESRP domains, LSP tracking can be easily scaled to support several TLS VLANs that are tunneled across an L2 VPN using a single LSP. Instead of each TLS VLAN tracking the same LSP, all of the TLS VLANs are placed into an ESRP domain for which there is one non-TLS VLAN, configured to track the state of the LSP. When ESRP detects that the LSP has failed, all of the VLANs in the configured ESRP domain transition to neutral state and the backup LSR becomes the master switch for all of the TLS VLANs.

The `add track-lsp` command configures ESRP to track up to eight LSPs. Fail over to the slave switch is based on the total number of established tracked LSPs. The switch with the greatest number of established tracked LSPs is elected the master switch for the specified VLAN. Specifying the parameter `<lsp_name>` instructs ESRP to track the status of an RSVP-TE LSP. Specifying the `ipaddress` keyword instructs ESRP to track the LSP status for the IP prefix as defined by the `<ipaddress/masklength>` parameter. Both types of LSPs can be tracked simultaneously.

Example

The following command enables LSP route failure tracking for routes to the specified subnet:

```
configure vlan esrp-1 add track-lsp 192.168.46.0/24
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

configure vlan delete track-lsp

```
configure vlan <vlan name> delete track-lsp [<lsp_name> | ipaddress
<ipaddress>/<masklength> | all]
```

Description

Disables LSP route tracking for an ESRP-enabled VLAN.

Syntax Description

vlan name	Specifies an ESRP-enabled VLAN name.
lsp_name	Specifies a LSP name.
ipaddress	Specifies the IP address of the route entry to be tracked.
all	Specifies all LSPs.

Default

N / A.

Usage Guidelines

The `delete track-lsp` command removes an LSP from ESRP tracking for the specified VLAN. If you specify the `all` keyword, all configured LSPs are removed from ESRP tracking for the specified VLAN.

Example

The following command disables diagnostic failure tracking for VLAN esrp-1:

```
configure vlan esrp-1 delete track-lsp
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

disable mpls

```
disable mpls
```

Description

Disables MPLS on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Disabling MPLS causes all LSPs to be released and all LDP neighbor sessions to be terminated.

Example

The following command globally disables MPLS on the switch:

```
disable mpls
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

enable mpls

```
enable mpls
```

Description

Enables MPLS on the switch.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

Disabling MPLS causes all LSPs to be released and all LDP neighbor sessions to be terminated.

Example

The following command globally enables MPLS on the switch:

```
enable mpls
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls

```
show mpls {vlan <vlan name>} {detail}
```

Description

Displays MPLS configuration information for one or all VLANs. Omitting the vlan keyword displays information for all VLANs.

Syntax Description

vlan name	Specifies a VLAN name.
detail	Specifies to display the information in detailed format.

Default

N / A.

Usage Guidelines

When the `vlan` parameter is omitted, this command displays the values of all MPLS configuration parameters that apply to the entire switch, the current status of peer LSRs, and a list of the VLANs for which MPLS is enabled.

When the `vlan` parameter is specified, this command displays the current values of the MPLS configuration parameters that are specific to the VLAN.

If the optional `detail` keyword is specified, additional detailed VLAN information is displayed.

Example

The following command displays MPLS configuration information for the VLAN *accounting*:

```
show mpls vlan accounting
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls forwarding

```
show mpls forwarding {summary | detail | inactive | host <ipaddress>
{detail | inactive} | prefix <ipaddress/masklength> {detail | inactive} |
rsvp-te <ipaddress> {detail}}
```

Description

Displays information from the FEC-to-NHLFE database, used when forwarding non-MPLS packets onto an LSP. Also displays information for RSVP-TE LSPs.

Syntax Description

summary	Displays only the summary route information associated with labeled paths.
host	Displays information for a single FEC.
prefix	Displays information for a single FEC.
rsvp-te	Displays only the RSVP-TE forwarding label mapping
inactive	Causes inactive mappings to be displayed. This keyword does not apply to the `rsvp-te` keyword, because RSVP-TE operates in DoD mode.

Default

N/A.

Usage Guidelines

This command displays information from the Forwarding Equivalence Class (FEC)-to-Next Hop Label Forwarding Entry (NHLFE) database. This command also displays information for RSVP-TE LSPs.

If the `host` or `prefix` keywords are specified, summary information is displayed for a single FEC. Use the `summary` keyword to display summary route information associated with labeled paths.

By default, the information displayed includes:

- Next hop IP address
- Outgoing label
- Interface number of the outgoing VLAN

If the `detail` keyword is specified, the following additional information is displayed:

- Outgoing port number
- Counts of packets and bytes that have been transmitted using the database entry

By default, information is displayed for active mappings. To display information for liberally-retained inactive mappings, use the inactive keyword. An inactive mapping is a mapping that was received from an LDP peer, but is not being used to reach the associated FEC. Using the `inactive` keyword causes inactive mappings to be displayed. The inactive keyword does not apply to RSVP-TE LSPs, because RSVP-TE operates in downstream-on-demand mode.

Example

The following command displays information from the FEC-to-NHLFE database:

```
show mpls forwarding prefix 10.1.1.1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls interface

```
show mpls interface {ldp | targeted-ldp | rsvp-te}
```

Description

Displays targeted LDP and RSVP-TE interface information.

Syntax Description

ldp	Specifies LDP interfaces.
targeted-ldp	Specifies targeted LDP interfaces.
RSVP-TE	Specifies RSVP-TE interfaces.

Default

N / A.

Usage Guidelines

Displays targeted LDP and RSVP-TE interface information, including targeted LDP and RSVP-TE peer IP address and peer state. Specifying the keyword `ldp`, `targeted-ldp`, or `rsvp-te` limits the information displayed to only those interface types.

Example

The following command displays interface information for RSVP-TE interfaces:

```
show mpls interface rsvp-te
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls label

```
show mpls label {summary {detail} | <label_number> {detail} | host
<ipaddress> {detail} | prefix <ipaddress/masklength> {detail} | rsvp-te
<ipaddress> {detail}}
```

Description

Displays information from the Incoming Label Map (ILM), used when forwarding packets that arrive as labeled MPLS packets.

Syntax Description

summary	Specifies the number of labels allocated form each label range partition.
detail	Specifies to display the information in detailed format.
label_number	Specifies an MPLS label number.
host <ipaddress>	Specifies a particular host FEC type.
prefix	Specifies a particular prefix FEC type.
rsvp-te	Specifies only RSVP-TE assigned labels

Default

N / A.

Usage Guidelines

This command displays information from the Incoming Label Map (ILM), which is used when forwarding packets that arrive labeled as MPLS packets.

When the `label_number` parameter is omitted, summary information is displayed for all incoming label assignments that have been made by the switch. When the `label_number` is specified, summary information is displayed for the label.

Use the `fec` keyword to display the label associated with an FEC. You can specify both host and prefix FEC types. The `summary` keyword displays the number of labels allocated from each label range partition.

By default, the information displayed includes:

- Next hop IP address
- Outgoing and incoming labels
- Interface number of the outgoing VLAN
- FEC associated with the incoming label

If the detail keyword is specified, the following additional information is displayed:

- Outgoing port number
- Counts of packets and bytes that have been received with the incoming label

- Counts of packets and bytes that have been transmitted with the outgoing label
- LSP type

This command also displays information from the Incoming Label Map (ILM) for RSVP-TE LSPs.

Example

The following command displays the summary information from the Incoming Label Map:

```
show mpls label summary
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls ldp

```
show mpls ldp {<ipaddress>} {detail}
```

Description

Displays MPLS LDP session information for one or all LSP sessions.

Syntax Description

ipaddress	Specifies an IP address.
detail	Specifies to display the information in detailed format.

Default

N/A.

Usage Guidelines

Omitting the ipaddress parameter displays LDP session information for all LDP sessions.

This command displays information about the status of LDP peers. Summary information is displayed for all known LDP peers and LDP peer sessions. If you specify the `<ipaddress>` of the LDP peer, information for a single LDP peer is displayed. To display additional information in the comprehensive detailed format, use the `detail` keyword.

Displayed summary information includes:

- Peer type (targeted or not targeted)
- Peer status
- Peer sessions
- Peer session state

If you specify the `detail` keyword, the following additional information is displayed:

- LDP error counts
- LDP status timers
- Maximum PDU length

Example

The following command displays MPLS LDP session information for the LDP entity 10.1.1.1:

```
show mpls ldp 10.1.1.1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls qos-mapping

```
show mpls qos-mappings
```

Description

Displays MPLS-specified QoS mappings for dot1p-to-exp and exp-to-dot1p.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Configured mappings for both dot1p-to-exp and exp-to-dot1p are displayed.

Example

The following command displays MPLS QoS mapping information:

```
show mpls qos-mappings
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls rsvp-te

```
show mpls rsvp-te {<ipaddress>} {detail}
```

Description

Displays RSVP-TE LSP configuration information.

Syntax Description

ipaddress	Specifies the IP address of the RSVP-TE interface.
detail	Specifies to display the information in detailed format.

Default

N / A.

Usage Guidelines

This command displays information about the status of RSVP-TE enabled interfaces. Summary information is displayed for all known RSVP-TE peers including the peer IP address and peer status. If you specify the `ipaddress` of the RSVP-TE interface, the information for a single RSVP-TE interface is displayed. Additional information is displayed in the detailed format if you specify the optional `detail` keyword. The more detailed RSVP-TE information includes the number and type of RSVP messages transmitted through the local RSVP-TE interface.

Example

The following displays detailed information about all configured RSVP-TE LSPs:

```
show mpls rsvp-te detail
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls rsvp-te lsp

```
show mpls rsvp-te lsp {<lsp_name>} {detail}
```

Description

Displays the RSVP-TE LSP.

Syntax Description

lsp_name	Specifies the name of the LSP.
detail	Specifies to display the information in detailed format.

Default

N / A.

Usage Guidelines

This command displays the configuration and status information for RSVP-TE LSPs. Information is listed in tabular format and includes the LSP name, LSP state, active path name, bandwidth requested, bandwidth actually reserved, ERO flag, egress LSR, LSP up-time, and RSVP error codes (if LSP setup failed). If you specify a specific LSP name, only information for the specified LSP is displayed. If you specify the optional `detail` keyword, additional information is displayed for each LSP. The detailed information includes a list of all configured paths, including the path state, error codes for the LSP associated with each path, up-time for each LSP, the bound profile name, and a list of TLS tunnels configured to use the LSP.

Example

The following displays the configuration and status information for all configured RSVP-TE LSPs in detailed format:

```
show mpls rsvp-te lsp detail
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls rsvp-te path

```
show mpls rsvp-te path {<path_name>} {detail}
```

Description

Displays the RSVP-TE routed path.

Syntax Description

path_name	Specifies the name of the path.
detail	Specifies to display the information in detailed format.

Default

N / A.

Usage Guidelines

This command displays the configuration and status information for MPLS RSVP-TE routed paths. Information is listed in tabular format and includes the path name, path endpoint LSR IP address, and local VLAN (if configured). If the path endpoint is specified as a host name, the host name and the DNS resolved IP address are both displayed. If a specific path name is specified, only information for the specified path is displayed. If you specify the optional `detail` keyword, the list of subobjects specified for the explicit route object and any LSPs that are configured to use the path are displayed.

Example

The following displays information about all RSVP-TE routed paths in detailed format:

```
show mpls rsvp-te path detail
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls rsvp-te profile

```
show mpls rsvp-te profile {<profile_name>}
```

Description

Displays the RSVP-TE path profile.

Syntax Description

profile_name	Specifies the name of the profile.

Default

N/A.

Usage Guidelines

By default, this command displays all configured profile parameters for the specified profile. If the profile name is omitted, the profile parameter values for all configured LSP profiles are displayed.

Example

The following command displays the profile parameter values for all configured LSP profiles:

```
show mpls rsvp-te profile
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show mpls tls-tunnel

```
show mpls tls-tunnel {summary | detail | <tunnel_name> {detail} | vlan
<vlan_name> {detail}}
```

Description

Displays configuration and status information for TLS tunnels.

Syntax Description

summary	Specifies to display summary TLS tunnel counts.
detail	Specifies to display the information in detailed format.
tunnel_name	Specifies a TLS tunnel name.
vlan_name	Specifies a VLAN name.

Default

N / A.

Usage Guidelines

This command displays configuration and status information for one or all TLS tunnels. The information displayed for each tunnel includes:

- The values of all configuration parameters for the tunnel.
- The current status of the tunnel LSP.
- Transmit and receive counts in terms of packets and bytes.

If the optional `detail` keyword is specified, TLS tunnel information is displayed using the comprehensive detail format.

If the optional `summary` keyword is specified, summary TLS tunnel counts are displayed. The summary counters displayed include the total number of active static and dynamic TLS tunnels.

Example

The following command displays configuration and status information for the TLS tunnel *rt40*:

```
show mpls tls-tunnel rt40
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

unconfigure mpls

```
unconfigure mpls
```

Description

Resets MPLS configuration parameters to the default settings.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command resets the following configuration parameters:

- IP-MTU
- LDP propagation filter settings on all VLANs
- LDP advertisement filter settings
- LDP session timers
- RSVP-TE interface parameters
- RSVP-TE profile parameters
- Settings for propagate-ip-ttl
- QoS mapping tables

Example

The following command resets MPLS configuration parameters to the default settings:

```
unconfigure mpls
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

unconfigure mpls

```
unconfigure mpls [hello-hold-time | session-keep-alive-time]
```

Description

Restores the default values for hello-hold-time or session-keep-alive-time.

Syntax Description

hello-hold-time	Specifies a hello hold time.
session-keep-alive-time	Specifies a session keep alive time.

Default

The default hello-hold-time is 15 seconds.

The default session-keep-alive-time is 40 seconds.

Usage Guidelines

This command can only be executed when MPLS is disabled.

The hello-hold-time is the amount of time, in seconds, an LSR maintains a record of the label space requested by potential LDP peers. An LSR must receive an LDP hello packet at least hello-hold-time seconds after the last hello packet was received, or the LSR concludes that the LDP peer has failed or no longer wishes to label switch using the previously advertised label space.

The session-keep-alive-time specifies the minimum amount of time, in seconds, that an LSR must receive an LDP PDU from an LDP peer to which it has an established LDP session. If an LDP PDU is not received within the specified session-keep-alive-time since the reception of the last LDP PDU, the LDP session is torn down.

Example

The following command restores the default values for hello-hold-time:

```
unconfigure mpls hello-hold-time
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

unconfigure mpls qos-mapping

```
unconfigure mpls qos-mapping [dotp-to-exp | exp-to-dot1p | lsp <lsp_name>]
```

Description

Restores the default values for the specified QoS mapping table.

Syntax Description

dot1p-to-exp	Specifies dot1p-to-exp mapping.
exp-to-dot1p	Specifies exp-to-dot1p mapping.
lsp_name	Specifies the name of an LSP.

Default

N / A.

Usage Guidelines

The default contents of either QoS mapping table maps an input value of *n* to an output value of *n*.

Example

The following command restores the default values for the dot1p-to-exp QoS mapping table:

```
unconfigure mpls qos-mapping dot1p-to-exp
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

26 High Density Gigabit Ethernet Commands

The High Density Gigabit Ethernet modules (also known as "3" series modules and Triumph modules) are I/O modules for both the Alpine 3800 series and the BlackDiamond 6800 series chassis-based systems. These modules support bi-directional traffic management to control the rate of information that flows into (ingress) or out of (egress) a switched network from one individual network port.

The "3" series modules are designed for metro service providers and enterprise environments. In a service provider environment, service providers can control the flow of data on a per customer basis. In an enterprise environment, businesses can use these modules to control user access or where desktop or server interfaces require high-density Gigabit Ethernet capability.

The "3" series modules also support the QoS functions, commands, and configurations described in Chapter 7.

This chapter documents the "3" series I/O module command set.

configure diffserv ingress replacement ports

```
configure diffserv ingress replacement low-priority code-point <number>
high-priority code-point <number> ports [<portlist> | all] {<Ingress QOS
profile>}
```

Description

Configures the optional overwriting of the DiffServ code point portion of the IP TOS field for ingress traffic.

Syntax Description

low priority code-point number	Specifies the low-priority DiffServ code point (IP TOS) value to use to overwrite low-priority ingress traffic. The default is 0. The range is 0 to 63.
high priority code-point number	Specifies the high-priority DiffServ code point (IP TOS) value to use to overwrite high-priority ingress traffic. The default is 0. The range is 0 to 63.
portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.
Ingress QOS profile	Specifies an ingress QoS profile: IQP1 through IQP8.

Default

The default values for both the low-priority and high-priority code points are 0.

Usage Guidelines

This command allows the overwriting of the upper 6 bits of the IP TOS field. The lower 2 bits of the TOS field passes through unchanged.

You can specify different code point values for both high-priority (below the committed-rate) and low-priority (above the committed-rate) traffic on each port or each ingress QoS profile on each port.

DiffServ ingress replacement is only done on IP Ethernet II (Ethertype) encapsulated frames. Frames that are IPX, LLC, or SNAP encapsulated are passed through with no DiffServ code point alterations.

You must enable low-priority and high-priority DiffServ ingress replacement on the specified ports before you can overwrite low-priority or high priority traffic. To enable low-priority and high-priority DiffServ ingress replacement, use the command:

```
enable diffserv ingress replacement [low-priority | high-priority] ports [<portlist> |
all] {<Ingress QOS profile>}
```

The "3" series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

If you do not specify an ingress QoS profile, all ingress QoS profiles for the indicated ports are affected.

Example

The following command configures the low-priority to 5 and the high-priority to 10 on all ports for all ingress QoS profiles:

```
configure diffserv ingress replacement low-priority code-point 5 high-priority
code-point 10 ports all
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

configure ports egress-rate-limit

```
configure ports <portlist> egress-rate-limit [percent <percent> | rate
<bps> [k | m]]
```

Description

Configures a maximum egress rate limit on the specified "3" series ports.

Syntax Description

portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
percent	Specifies the maximum percentage of bandwidth allowed for all egress traffic for each selected port. The default is 100. The range is 0 to 100.
bps	Specifies the maximum kilobits per second (kbps) or megabits per second (mbps) allowed for all egress traffic for each selected port. • k—kbps (the range is 0-1000000) • m—mbps (the range is 0-1000)

Default

100 percent.

Usage Guidelines

If you use the `percent` parameter to configure the egress rate limit, you must use an integer.

The `rate <bps>` range is:

- kbps—0 to 1000000
- mbps—0 to 1000

This setting is independent of any "*i*" series egress rate-limiting configurations that you have on the switch and is applied to the aggregate bandwidth after the "*i*" series per-queue egress rate-limiting.

Example

The following command sets the maximum egress rate limit on slot 1, port 1 to 100 mbps:

```
configure ports 1:1 egress-rate-limit rate 100 m
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

configure qosprofile ingress

```
configure qosprofile ingress <Ingress QOS profile> [minbw <percent> % maxbw
<percent> % | committed-rate <bps> [k | m] peak-rate <bps> [k | m]]
red-threshold <percent> % maxbuf <percent> % ports [<portlist> | all]
```

Description

Modifies the default ingress QoS profile parameters.

Syntax Description

Ingress QOS profile	Specifies an ingress QoS profile: IQP1 through IQP8.
minbw	Specifies the minimum bandwidth percentage for this queue. The default setting is 0. The range is 0 to 100.
maxbw	Specifies the maximum bandwidth percentage for this queue. The default setting is 100.
committed-rate	Specifies the minimum bandwidth for this queue in either kilobits per second (kbps) or megabits per second (mbps).
peak-rate	Specifies the maximum bandwidth for this queue in either kilobits per second (kbps) or megabits per second (mbps). • k—kbps (the range is 0-1000000) • m—mbps (the range is 0-1000)
red-threshold	Random Early Drop (RED) specifies the ingress queue fill percentage when the "3" series module begins to randomly discard packets as the queue fill percentage approaches the maximum queue size. The default setting is 100. The range is 0 to 100.
maxbuf	Specifies the ingress queue size as a percentage of the maximum size available. The range is 0 to 100. The default is 100.
portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.

Default

- Minimum bandwidth—0%
- Maximum bandwidth—100%
- RED threshold—100%
- Maximum buffer percent—100%

Usage Guidelines

The sum of the committed rate and the equivalent rate for the configured minbw percent for all ingress queues on a port must not exceed the following:

- 250 mpbs for 4:1 oversubscribed platforms (GM-16T3, GM-16X3, and G24T3)
- 500 mbps for 2:1 oversubscribed platforms (G16X3)

Example

The following command configures the ingress QoS profile parameters of ingress QoS profile *IQP1* for slot 1, port 1:

```
configure qosprofile ingress iqp1 committed-rate 250 m peak-rate 1000 m red-threshold
100 % maxbuf 100 % ports 1:1
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

configure qostype ingress priority

```
configure qostype ingress priority [diffserv | dot1p | vlan] <qos-priority
(0-15)>
```

Description

Configures the relative priority among the different ingress queue selection criteria.

Syntax Description

diffserv	Specifies the priority of the ingress queue based on DiffServ information. The default is 3.
dot1p	Specifies the priority of the ingress queue based on dot1p information. The default is 1.
vlan	Specifies the priority of the ingress queue based on VLAN information. The default is 2.
qos-priority (0-15)	Specifies a priority value in the range of 0-15 (15 is the highest priority).

Default

- diffserv—3
- dot1p—1
- vlan—2

Usage Guidelines

Ingress QoS types with a greater value take higher precedence.

The queue selection criteria with the highest priority, if enabled in the received packet, is used first, followed by the remaining criteria in descending order.

The priority range is 0-15 (15 is the highest priority). Each queue selection criteria must have a unique priority; no two selection criteria can have the same priority range.

All VLANs are set to the default ingress QoS profile *none*.

Congestion can cause ingress traffic to be dropped on oversubscribed "3" series I/O modules. Ingress QoS allows received traffic with different VLAN priority values, different DiffServ code points (IP TOS), or from different VLANS to be classified to up to eight different ingress queues. This allows for specified traffic types to be queued separately so they remain unaffected by congestion in other ingress queues.

To configure which DiffServ code points map to which ingress QoS profiles, use the command:

```
configure diffserv examination code-point <code-point> qosprofile <qosprofile> ports
[<portlist> | all]
```

By default, DiffServ mapping is enabled on "3" series ports.

To disable the DiffServ mapping of an ingress IP packet to be examined to select a QoS profile, use the command:

```
disable diffserv examination [<portlist> | all]
```

Example

The following command forces dot1p QoS to take a higher precedence over VLAN QoS (with a default priority of 2):

```
configure qostype ingress priority dot1p 4
```

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.

configure vlan qosprofile ingress

```
configure vlan <vlan name> qosprofile ingress [<Ingress QOS profile> |
none]
```

Description

Configures a VLAN to use a specific ingress QoS profile.

Syntax Description

vlan name	Specifies a VLAN name.
Ingress QOS profile	Specifies an ingress QoS profile: IQP1 through IQP8.
none	Specifies that traffic from this VLAN is not associated with any ingress queue based on VLAN ID.

Default

None.

Usage Guidelines

Use this command when the ingress QoS type priority is VLAN-based for a given received packet.

The none keyword allows VLAN priority ingress queue selection to put higher priority frames into a different queue so they do not get discarded during ingress port congestion.

All VLANs are set to the default ingress QoS profile *none*.

To display the ingress QoS profile mapping for a VLAN, use the command:

`show vlan`

The "3" series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

Example

The following command configures the VLAN *sales* to use ingress QoS profile *iqp2*:

`configure vlan sales qosprofile ingress iqp2`

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.

disable diffserv ingress replacement ports

```
disable diffserv ingress replacement [high-priority | low-priority |
low-and-high-priority] ports [<portlist> | all] {<Ingress QOS profile>}
```

Description

Disables the optional overwriting of the DiffServ code point portion of the (IP TOS) field for ingress traffic.

Syntax Description

high-priority	Specifies DiffServ replacement for high-priority traffic (traffic received below the committed-rate configured for the Ingress QoS profile).
low-priority	Specifies DiffServ replacement for low-priority traffic (traffic received above the committed-rate configured for the Ingress QoS profile).
low-and-high-priority	Specifies DiffServ replacement for both high-priority and low-priority traffic.
portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.
Ingress QOS profile	Specifies an optional ingress QoS profile: IQP1 through IQP8

Default

Disabled.

Usage Guidelines

The "3" series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

You can disable replacement for high-priority, low-priority, or low- and high-priority traffic for all ingress QoS profiles on the specified ports or a selected ingress QoS profile on the specified ports.

Example

The following command disables low-priority DiffServ replacement for all "3" series ports in all ingress QoS profiles:

```
disable diffserv ingress replacement low-priority ports all
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

disable flow-control ports

```
disable flow-control ports [<portlist> | all]
```

Description

Disables 802.3x flow control on "3" series ports.

Syntax Description

portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.

Default

Disabled.

Usage Guidelines

If you disable flow control, use the:

- `portlist` keyword to specify an individual "3" series port or a group of "3" series ports
- `all` keyword to specify all "3" series ports

If you disable flow control on a "3" series port, the port does not advertise flow control support during auto-negotiation. Flow control is auto-negotiated and is disabled if both ports do not support it.

Example

The following command disables flow control on slot 2, ports 1 through 4:

```
disable flow-control ports 2:1-2:4
```

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.

enable diffserv ingress replacement ports

```
enable diffserv ingress replacement [high-priority | low-priority |
low-and-high-priority] ports [<portlist> | all] {<Ingress QOS profile>}
```

Description

Enables the optional overwriting of the DiffServ code point portion of the (IP TOS) field for ingress traffic.

Syntax Description

high-priority	Specifies DiffServ replacement for high-priority traffic (traffic received below the committed-rate configured for the Ingress QoS profile).
low-priority	Specifies DiffServ replacement for low-priority traffic (traffic received above the committed-rate configured for the Ingress QoS profile).
low-and-high-priority	Specifies DiffServ replacement for both high-priority and low-priority traffic.
portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.
Ingress QOS profile	Specifies an optional ingress QoS profile: IQP1 through IQP8

Default

Disabled.

Usage Guidelines

If you enable DiffServ ingress replacement before you configure a code point, the default code point is 0. To configure a code point for both the low-priority and high-priority traffic, use the command:

```
configure diffserv ingress replacement low-priority code-point <number> high-priority
code-point <number> ports [<portlist> | all] {<Ingress QOS profile>}
```

You can enable DiffServ ingress replacement for:

- Both high-priority and low-priority traffic on the specified ports or each ingress QoS profile on the specified ports.
- Either high-priority or low-priority traffic for all ingress QoS profiles on the specified ports or a selected ingress QoS profile on the specified ports.

The "3" series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

Example

The following command enables low-priority DiffServ replacement for all "3" series ports in all ingress QoS profiles:

```
enable diffserv ingress replacement low-priority ports all
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

enable flow-control ports

```
enable flow-control ports [<portlist> | all]
```

Description

Enables 802.3x flow control on "3" series ports.

Syntax Description

portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.

Default

Disabled.

Usage Guidelines

Since "3" series modules are oversubscribed to the module switch fabric, traffic can congest. Flow control allows you to stop incoming traffic when too much congestion occurs.

Flow control sends a PAUSE frame to the transmitter when traffic approaches the congestion threshold for a specific queue. The PAUSE frame is sent *before* the queue overflows, so throughput is slightly reduced when flow control is enabled. Flow control is auto-negotiated and is disabled if both ports do not support it.

If you enable flow control, use the:

- `portlist` keyword to specify an individual port or a group of ports
- `all` keyword to specify all "3" series ports

Example

The following command enables flow control on slot 2, ports 1 through 4:

```
enable flow-control ports 2:1-2:4
```

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.

show ports egress-rate-limit

```
show ports {<portlist>} egress-rate-limit
```

Description

Displays the maximum egress rate limit on the specified "3" series ports.

Syntax Description

portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

Depending on the port egress rate limit configuration, the maximum port bandwidth is displayed in the numeric rate (kbps or mbps) or the percentage rate.

This command applies only to "3" series I/O modules; the rate you configure is applicable to the aggregate of all outgoing traffic on a port.

This display is independent of any "*i*" series egress rate-limiting configurations that you have on the switch.

Example

The following command displays the maximum egress rate limit:

```
show ports egress-rate-limit
```

Following is sample output from this command:

```
PORT     Egress-Rate
====================
  2:1           100 %
  2:2           100 %
  2:3           100 %
  2:4          1000 k
  2:5           100 %
  2:6            10 m
  2:7           100 %
  2:8           100 %
  2:9           100 %
 2:10           100 %
 2:11           100 %
 2:12           100 %
 2:13           100 %
 2:14           100 %
 2:15           100 %
 2:16           100 %
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

show ports ingress stats

```
show ports {<portlist>} ingress stats {detail}
```

Description

Displays real-time ingress statistics for one or more "3" series ports.

Syntax Description

portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
detail	Specifies more detailed information per ingress queue.

Default

N/A.

Usage Guidelines

The "3" series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

High-priority packets are packets received below the configured ingress committed rate, and low-priority packets are packets received above the committed-rate.

View these statistics to analyze usage trends and to maximize network efficiency.

If you do not specify the `detail` keyword, the output indicates the following:

- Port Number
- Link Status—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- High Priority Bytes—Sum, per port, of the bytes forwarded for received high-priority packets (traffic received below the committed rate configured for the ingress QoS profile).
- Low Priority Bytes—Sum, per port, of the bytes forwarded for received low-priority packets (traffic received above the committed rate configured for the ingress QoS profile).
- Received Total Bytes—The total number of bytes that were received by the port.
- Receive Bytes Dropped—Total number of bytes dropped for this port.
- Total Percent Dropped—Percentage of incoming bytes dropped due to oversubscription congestion or ingress rate limiting. Displayed with a precision of 1/100 of a percent.
- Transmit XOFF—Total number of XOFF flow control packets sent from this port.

If you specify the `detail` keyword, the following additional information is displayed per ingress queue:

- Queue—One of eight ingress queue names for this port.

- High Priority Bytes—Sum, per ingress queue, of the bytes forwarded for received high-priority packets.
- Low Priority Bytes—Sum, per ingress queue, of the bytes forwarded for received low-priority packets.
- Total Percent Dropped—Percentage of incoming bytes on this queue dropped due to oversubscription congestion. This is determined using cumulative counters, so is not a rate. This will be displayed with a precision of 1%.
- Byte Rates—The following three rate values will always either add up to 0% or 100%:
  - High Priority Percentage—The ratio of high priority traffic forwarded on this queue to the total bytes received on this queue.
  - Low Priority Percentage—The ratio of low priority traffic forwarded on this queue to the total bytes received on this queue.
  - Dropped Percentage—Percentage of receive bytes dropped by this queue relative to the total number of bytes input to this queue.

Example

The following command displays real-time ingress statistics for slot 1, port 1:

```
show ports 1:1 ingress stats
```

Following is sample output from this command:

```
Port Statistics                                        Thu Jul 10 08:24:50 2003
 Port   Link     High Pri      Low Pri     Rx Total     Rx Drop      %       Tx
      Status        Bytes        Bytes        Bytes       Bytes   Drop     Xoff
================================================================================
  1:1      R          500          400         1000         100  10.00        5
```

The following command displays real-time ingress statistics for slot 1, port 1 and per ingress queue:

```
show ports 1:1 ingress stats detail
```

Following is sample output from this command:

```
Port Statistics                                        Thu Jul 10 08:24:50 2003
 Port   Link     High Pri      Low Pri     Rx Total     Rx Drop      %       Tx
      Status        Bytes        Bytes        Bytes       Bytes   Drop     Xoff
================================================================================
  1:1      R          500          400         1000         100  10.00        5

Queue     High Pri     Low Pri   Total % |---------- RATES -----------|
             Bytes       Bytes   Dropped  High Pri   Low Pri   Dropped
================================================================================
 IQP1          500           0       0 %     100 %       0 %       0 %
 IQP2            0         400      20 %       0 %      80 %      20 %
 IQP3            0           0       0 %       0 %       0 %       0 %
 IQP4            0           0       0 %       0 %       0 %       0 %
 IQP5            0           0       0 %       0 %       0 %       0 %
 IQP6            0           0       0 %       0 %       0 %       0 %
 IQP7            0           0       0 %       0 %       0 %       0 %
 IQP8            0           0       0 %       0 %       0 %       0 %
```

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.

show qosprofile ingress

```
show qosprofile ingress {<Ingress QOS profile>} {<portlist>}
```

Description

Displays ingress QoS profiles.

Syntax Description

Ingress QOS profile	Specifies an ingress QoS profile: IQP1 through IQP8.
portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.

Default

N/A.

Usage Guidelines

If you do not specify an ingress QoS profile, all ingress QoS profiles for the specified ports are displayed.

The units displayed are the same units that you used when you configured the ingress QoS profile.

Example

The following command displays ingress QoS profile information for all ingress QoS profiles on slot 1:

```
show qosprofile ingress 1:*
```

Following is sample output from this command:

```
                  MinBw %/        MaxBw %/
 Port Queue  Committed-Rate       Peak-Rate   RED %  MaxBuf %
=============================================================
  1:1  IQP1          1000 k          1000 m   100 %     100 %
       IQP2             0 %           100 %   100 %     100 %
       IQP3             0 %           100 %   100 %     100 %
       IQP4             0 %           100 %   100 %     100 %
       IQP5             0 %           100 %   100 %     100 %
       IQP6             0 %           100 %   100 %     100 %
       IQP7             0 %           100 %   100 %     100 %
       IQP8             0 %           100 %   100 %     100 %
  1:2  IQP1             0 %           100 %   100 %     100 %
       IQP2             0 %           100 %   100 %     100 %
       IQP3             0 %           100 %   100 %     100 %
       IQP4             0 %           100 %   100 %     100 %
       IQP5             0 %           100 %   100 %     100 %
       IQP6             0 %           100 %   100 %     100 %
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

show qostype ingress priority

```
show qostype ingress priority
```

Description

Displays ingress QoS priority settings.

Syntax Description

This command has no syntax or values.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays the ingress QoS traffic grouping priority settings for this switch:

```
show qostype ingress priority
```

Following is sample output from this command:

```
Ingress Qos Type             Priority
Diffserv                        3
Vlan                            2
Dot1p                           1
```

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.

unconfigure diffserv ingress replacement ports

```
unconfigure diffserv ingress replacement ports [<portlist> | all]
```

Description

Resets the optional overwriting of the DiffServ code point portion of the IP TOS field for ingress traffic to its defaults.

Syntax Description

portlist	Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all	Specifies all "3" series ports.

Default

N/A.

Usage Guidelines

Use this command to reset the low-priority and high-priority code point values to 0 and to disable DiffServ ingress replacement.

Example

The following command resets the DiffServ code points to their defaults:

```
unconfigure diffserv ingress replacement ports all
```

History

This command was first available in ExtremeWare 7.1.

Platform Availability

This command is available on "3" series I/O modules only.

unconfigure qostype ingress priority

```
unconfigure qostype ingress priority
```

Description

Restores all ingress QoS settings to their defaults.

Syntax Description

This command has no syntax or values.

Default

N/A.

Usage Guidelines

Resets the ingress traffic groupings to the following:

- diffserv—3
- dot1p—1
- vlan—2

Example

The following command resets the Ingress QoS traffic grouping priorities:

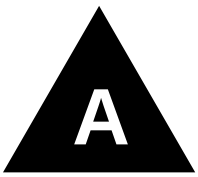
```
unconfigure qostype ingress priority
```

History

This command was first available in ExtremeWare 7.0.1.

Platform Availability

This command is available on "3" series I/O modules only.



Configuration and Image Commands

This appendix describes the following commands:

- Commands related to downloading and using a new switch software image
- Commands related to saving, uploading, and downloading switch configuration information
- Commands related to the BootROM and switch rebooting

The switch software *image* contains the executable code that runs on the switch. An image comes preinstalled from the factory. The image can be upgraded by downloading a new version from a Trivial File Transfer Protocol (TFTP) server on the network.

A switch can store up to two images; a primary and a secondary image. You can download a new image into either one of these, and you can select which image will load on the next switch reboot.

The *configuration* is the customized set of parameters that you have selected to run on the switch. As you make configuration changes, the new settings are stored in run-time memory. To retain the settings, and have them load when you reboot the switch, you must save the configuration to nonvolatile storage.

A switch can store two different configurations: a primary and a secondary configuration. You can select to which configuration you want the changes saved, and which configuration will be used on the next switch reboot.

The BootROM initializes certain important switch variables during the switch boot process. In specific situations, the BootROM can be upgraded by download from a TFTP server on the network.

configure download server

```
configure download server [primary | secondary] [<ip address> | <hostname>]
<filename>
```

Description

Configures the TFTP server(s) used by a scheduled incremental configuration download.

Syntax Description

primary	Specifies that the following parameters refer to the primary TFTP server.
secondary	Specifies that the following parameters refer to the secondary TFTP server.
ip address	Specifies the IP address of the TFTP server from which the configuration should be obtained.
hostname	Specifies the hostname of the TFTP server from which the configuration should be obtained.
filename	Specifies the filename on the server that contains the configuration to be downloaded.

Default

N/A.

Usage Guidelines

This command must be executed before scheduled configuration downloads can be performed.

Use of the <hostname> parameter requires that DNS be enabled.

Example

The following command specifies that scheduled incremental downloads into the primary configuration space be done from the server named *tftphost*, from the ASCII file *primeconfig.txt* (residing in directory *\configs\archive* on the server).

```
configure download server primary tftphost \configs\archive\prime_config.txt
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

configure switch

```
configure switch {auto | extended | standard}
```

Description

Configures the mode of switch operation for the Alpine 3802.

Syntax Description

auto	Specifies the mode of switch operation to be auto mode.
extended	Specifies the mode of switch operation to be extended mode.
standard	Specifies the mode of switch operation to be standard mode

Default

Auto mode.

Usage Guidelines

The Alpine 3802 supports all existing Alpine I/O modules; however, there are limitations to the number and type of I/O modules supported based upon the mode of switch operation.

The Alpine 3802 has three modes of switch operation:

- Extended—In extended mode, all slots (slots 1, 2, and 3) are enabled. Slot 1 supports all existing Alpine I/O modules: Alpine Ethernet I/O modules (modules with a green stripe on the front of the module) and Alpine Access I/O modules (modules with a silver stripe on the front of the module). Slots 2 and 3 support only Alpine Access I/O modules (silver stripe).

  The Extended mode LED lights when the switch is in extended mode.

- Standard—In standard mode, only slots 1 and 2 are enabled. Slot 3 is disabled. Slots 1 and 2 support all existing Alpine I/O modules: Alpine Ethernet I/O modules (green stripe) and Alpine Access I/O modules (silver stripe).

  The Standard mode LED lights when the switch is in extended mode.

- Auto—In auto mode, the switch determines if it is in standard or extended mode depending upon the type of modules installed in the chassis or the slot preconfigurations. If an Alpine I/O module with a green stripe (for example, an FM-32Ti module) is installed or preconfigured in slot 2, the switch operates in standard mode. If an Alpine I/O module with a silver stripe (for example, a WM-4Ti module) is installed or preconfigured in slots 2 or 3, the switch operates in extended mode.

Slot 3 can accept only Alpine Access I/O modules (silver stripe). You cannot insert an Alpine Ethernet I/O module (green stripe) into slot 3.

If you insert a module into the Alpine 3802 that is not allowed in a particular slot, the switch logs an error to the syslog. For example, if you insert a GM-WDMi module into slot 3, a module type not supported in slot 3, the switch logs an error.

Example

The following command specifies that the Alpine 3802 operates in standard mode.

```
configure switch standard
```

History

This command was first available in ExtremeWare 6.1.8.

Platform Availability

This command is available on the Alpine 3802 switch.

download bootrom

```
download bootrom [<ip address> | <hostname>] <filename> {slot <slot>}
```

Description

Downloads a BootROM image from a TFTP server after the switch has booted. The downloaded image replaces the BootROM in the onboard FLASH memory.

Syntax Description

ip address	Specifies the IP address of the TFTP server.
hostname	Specifies the hostname of the TFTP server.
filename	Specifies name of the file on the server that contains the bootROM image.
slot	Specifies the slot where a PoS or MPLS module is installed.

Default

N/A.

Usage Guidelines

Upgrade the BootROM only when asked to do so by an Extreme Networks technical representative.

If this command does not complete successfully it could prevent the switch from booting. In the event the switch does not boot properly, some boot option functions can be accessed through a special BootROM menu (see the ExtremeWare Software User Guide).

Use of the <hostname> parameter requires that DNS be enabled.

Example

The following command downloads a bootROM image from the tftp server *tftphost* from the file *bootimages* (residing in directory *\images* on the server):

```
download bootrom tftphost \images\bootimage
```

History

This command was first available in ExtremeWare 4.0.

This command was modified in the ExtremeWare IP Services Technology Release based on 6.1.8b12 to support download to a PoS or MPLS module.

Platform Availability

This command is available on all platforms.

download configuration

```
download configuration [<ip address> | <hostname>] <filename> {incremental}
```

Description

Downloads a previously saved ASCII configuration file from a specific TFTP server host.

Syntax Description

ip address	Specifies the IP address of the TFTP server from which the configuration should be obtained.
hostname	Specifies the hostname of the TFTP server from which the configuration should be obtained.
filename	Specifies the path and filename of a saved ASCII configuration.
incremental	Specifies an incremental configuration download (v 6.0 or later).

Default

N/A.

Usage Guidelines

Unless you specify the incremental keyword, this command does a complete download, resetting the current switch configuration and replacing it with the new downloaded configuration. You will be prompted to reboot the switch after the download is complete. If you do not reboot when prompted, the switch views the configuration file as corrupted and the next time you reboot the switch prompts you to reset to the factory defaults.

Use the `incremental` keyword to specify an incremental or partial configuration download. In this case, the commands specified in the incremental download file are executed, but configuration settings not specified in the file are left intact. No reboot is required.

The new configuration information is stored in switch runtime memory, and is not retained if the switch has a power failure. After the switch has rebooted, you should save the configuration to the primary or secondary configuration area to retain it through a power cycle. You can include a save command at the end of the configuration file to have the save done at the end of the download.

The file on the server is assumed to be located relative to the TFTP server base directory. You can specify a path as part of the file name.

Use of the <hostname> parameter requires that DNS be enabled.

Example

The following command clears the current switch configuration, and downloads a new full configuration from the tftp server *tftphost*. It uses the configuration from the file *stdconfigs.txt* residing in the subdirectory *configs\archive* of the TFTP server base directory on the server:

```
download configuration tftphost configs\archive\stdconfig.txt
```

The following command downloads a partial configuration from the tftp server *tftphost* from the file *modifyconfig.txt* (residing in the subdirectory *configs\archive* on the server):

```
download configuration tftphost configs\archive\modifyconfig.txt incremental
```

History

This command was first available in ExtremeWare 2.0.

Support for the <hostname> parameter was introduced in ExtremeWare 4.0.

Support for incremental downloads was introduced in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms. The incremental download option is available on the *"i"* series platforms.

download configuration cancel

```
download configuration cancel
```

Description

Cancels a scheduled incremental configuration download.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command cancels the scheduled download command completely, not just the next scheduled daily download. The `download configuration every <hour>` command must be issued again to resume automatic downloads.

If there are no downloads scheduled, this command has no effect.

Example

The following command cancels a previously scheduled download:

```
download configuration cancel
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

download configuration every

```
download configuration every <time>
```

Description

Automatically does an incremental configuration download every day at the specified time, or immediately after switch bootup, based on the parameters specified in the `configure download server` command.

Syntax Description

time	The time of day in the format <hour (0-23)>:<minutes (0-59)>.

Default

N / A.

Usage Guidelines

You must run the `configure download server` command prior to using this command, to specify:

- The TFTP server and the configuration file from which the downloaded configuration will be obtained.
- Whether this TFTP server is the primary server or the secondary (backup) TFTP server.

Example

The following commands set up a scheduled incremental download of the file *config_info.txt*, to be done from the TFTP server named *tftphost* into the primary configuration area, every day at 10:00 pm:

```
configure download server primary tftphost config_info.txt
download configuration every 22:00
```

History

This command was first available in ExtremeWare 6.0.

Platform Availability

This command is available on all platforms.

download image

```
download image [<hostname> | <ipaddress>] [<filename> | all-images
<filename_prefix> {image-type [non-ssh | ssh]}] {primary | secondary}
{slot <slot>}
```

Description

Downloads a new version of the ExtremeWare software image.

Syntax Description

hostname	Specifies the hostname of the TFTP server from which the image should be obtained.
ipaddress	Specifies the IP address of TFTP server from which the image should be obtained.
filename	Specifies the filename of the new image.
filename_prefix	Specifies that filename prefix of the new image.
non-ssh	Specifies that the new image be downloaded without export-restricted security features.
ssh	Specifies that the new image be downloaded with export-restricted security features.
primary	Specifies that the new image should be stored as the primary image.
secondary	Specifies that the new image should be stored as the secondary image.
slot	Specifies that the new image should be downloaded to the module in the specified slot.

Default

Stores the downloaded image in the current location (the location used for the last reboot).

Usage Guidelines

Prior to downloading an image, you must place the new image in a file on a TFTP server on your network. Unless you include a path with the filename, this command assumes that the file resides in the same directory as the TFTP server itself.

The switch can store up to two images: a primary image and a secondary image. When you download a new image, you must select into which image space (primary or secondary) you want the new image to be placed. If no parameters are specified, the software image is saved to the current image.

Use of the `<hostname>` parameter requires that DNS be enabled.

For ExtremeWare 7.1.0 and higher, the following features are available on the Alpine and BlackDiamond chassis:

- You can update the operational images for all installed modules that run a software image. All of the operational images files must be located in the same directory on the TFTP server and they must have the same filename prefix.
- To update all of the images on the installed modules, use the `all-images` keyword.

Enter the filename prefix (the filename without the image extension), not the complete software filename, to successfully download the software.

— For example, if you enter `v700b68.xtr`, the command fails because the file extension (.xtr) is included, and `v700b68.xtr.xtr` is not found.

— If you enter `v700b68`, without the file extension, the command executes.

- By default, if the ExtremeWare version currently running contains security features that are subject to export restrictions (for example, SSH2), the image downloaded contains the security features.
- To download an image type different from the type currently running, specify the optional `image-type` keyword followed by either `non-ssh` or `ssh`.

  — `non-ssh` specifies an ExtremeWare image without security features

  — `ssh` specifies an ExtremeWare image containing security features
- The main ExtremeWare image always downloads first.

  The download image process proceeds with each slot starting at slot 1.

  — If the main ExtremeWare image cannot be found, the download image process is discontinued.

  — If a specific image file is not found for a specific module, an error is displayed and the download process continues to the next module.
- Slots with modules that do not support separate operational images (for example, the G8Xi or the GM-4Ti module) are skipped.

Table 29 lists the modules and operational images supported in ExtremeWare 7.1.0:

Table 29: Supported modules and operational images

Module Name	Image Extension	Image Description
MSM64i, SMMi	xtr	ExtremeWare image
MSM64i	Gxtr	6816 ExtremeWare image
MSM64i, SMMi	Sxtr	SSH ExtremeWare image
MSM64i	SGxtr	SSH 6816 ExtremeWare image
ARM	arm	ARM image
A3cSi	atm3	ATM OC-3 image
P3cSi, P3cMi	oc3	PoS OC-3 image
P12cSi, P12cMi	oc12	PoS OC-12 image
MPLS	mpls	MPLS image
WM-4E1i	e1	E1 WAN image
WM-4T1i	t1	T1 WAN image
WM-1T3i	t3	T3 WAN image

Example

The following command downloads the switch software image from the TFTP server named *tftphost*, from the file named *s4119b2.xtr*, to the secondary image store:

```
download image tftphost s4119b2.xtr secondary
```

This example assumes that you have a modular chassis with modules installed. The following command downloads the switch and module software images from the TFTP server named *tftphost* from the filename prefix named *v710b35*, to the primary image store:

```
download image tftphost all-images v710b35 primary
```

The following sample log is displayed:

```
MSM  A  Primary   bank:  Downloading image v710b35.xtr
.................................................................
.........................................................
Verifying the image...
Done!

Slot 2  Primary   bank:  Downloading image v710b35.oc3
.................................................................
.....................................
Download to slot 1 successful.

Slot 3  Primary   bank:  Downloading image v710b35.mpls
.................................................................
.............................................
Download to slot 2 successful.

Slot 4  Primary   bank:  Downloading image v710b35.oc3
.................................................................
.....................................
Download to slot 2 successful.

Slot 7  Primary   bank:  Downloading image v710b35.atm3
.................................................................
.................................
Download to slot 4 successful.
```

This example assumes that you have a modular chassis with modules installed. The following command downloads the security switch and module software images from the TFTP server named *tftphost* from the filename prefix named *v700b68*, to the secondary image store:

```
download image tftphost all-images v700b68 image-type ssh secondary
```

The following sample log is displayed:

```
MSM  A  Secondary bank:  Downloading image v700b68.xxx
.................................................................................
.............................................
Verifying the image...
Done!

Slot 2  Secondary bank:  Downloading image v700b68.xxx
.................................................................
.....................................
Download to slot 1 successful.

Slot 3  Primary   bank:  Downloading image v700b68.xxx
.................................................................
.............................................
Download to slot 2 successful.
```

```
Slot 4  Secondary bank:  Downloading image v700b68.xxx
..................................................................
.....................................
Download to slot 2 successful.

Slot 7  Secondary bank:  Downloading image v700b68.xxx
..................................................................
.................................
Download to slot 4 successful.
```

History

This command was available in ExtremeWare 2.0.

Support for the `<hostname>` parameter was introduced in ExtremeWare 4.0.

Support for the `<slot>` parameter was introduced in ExtremeWare 7.0.0.

Support for the `<filename_prefix>` parameter was introduced in ExtremeWare 7.1.0.

Support for the `non-ssh` and `ssh` keywords was introduced in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

save configuration

```
save configuration {primary | secondary}
```

Description

Saves the current configuration from the switch's runtime memory to non-volatile memory.

Syntax Description

primary	Specifies the primary saved configuration.
secondary	Specifies the secondary saved configuration.

Default

Saves the current configuration to the location used on the last reboot.

Usage Guidelines

The configuration takes effect on the next reboot.

Example

The following command save the current switch configuration in the secondary configuration area:

```
save configuration secondary
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

show configuration

```
show configuration [detail]
```

Description

Displays the currently active configuration to the terminal.

Syntax Description

detail	Specifies to show all configuration statements including default commands.

Usage Guidelines

If the output scrolls off the top of the screen, you can use the `enable clipaging` command to pause the display when the output fills the screen. The default for clipaging is enabled.

Example

This command shows the current configuration active in the switch:

```
show configuration detail
```

History

This command was available in ExtremeWare 2.0.

This command was modified to show the auto-negotiation status of Gigabit Ethernet ports in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

synchronize

```
synchronize
```

Description

Replicates all saved images and configurations from the master MSM to the slave MSM on the BlackDiamond.

Syntax Description

This command has no arguments or variables.

Usage Guidelines

This command does the following:

1. Copy both the primary and secondary software images
2. Copy both the primary and secondary configurations
3. Copy the BootROM
4. Reboot the slave MSM64i

When you install a slave MSM64i, you are not prompted to synchronize the images and the configurations from the master. If not synchronized, the slave uses its image and the master's configuration. This image/configuration mismatch will likely cause the switch to operate differently after failover. Use the `synchronize` command to replicate all saved images and configurations from the master to the slave. However, if one of the configurations on the master MSM64i is empty, the sync process will not overwrite the corresponding configuration on the slave. If the configuration on the slave MSM64i is an older configuration, this can cause problems if the switch is rebooted using the outdated configuration.

This command does not replicate the run-time configuration. You must use the `save` command to store the run-time configuration first.

Example

The following command replicates all saved images and configurations from the master MSM64i to the slave MSM64i:

```
synchronize
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on the BlackDiamond switch.

unconfigure switch

```
unconfigure switch {all}
```

Description

Returns the switch configuration to its factory default settings.

Syntax Description

all	Specifies that the entire current configuration should be erased, and the switch rebooted.

Default

Resets configuration to factory defaults without reboot.

Usage Guidelines

Use unconfigure switch to reset the configuration to factory defaults, but without erasing the configuration and rebooting. This preserves users account information, date and time settings, and so on.

Include the parameter `all` to clear the entire current configuration, including all switch parameters, and reboot using the last used image and configuration.

Example

The following command erases the entire current configuration, resets to factory defaults, and reboots the switch using the last specified saved image and saved configuration:

```
unconfigure switch all
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

upload configuration

```
upload configuration [<ip address> | <hostname>] <filename> {every <time>}
```

Description

Uploads the current configuration to a TFTP server on your network.

Syntax Description

ip address	Specifies the IP address of the TFTP server.
hostname	Specifies the hostname of the TFTP server.
filename	Specifies a name for the file where the configuration is to be saved.
time	The time of day in the format <hour (0-23)>:<minutes (0-59)>.

Default

Uploads the current configuration immediately.

Usage Guidelines

The filename can be up to 255 characters long, and cannot include any spaces, commas, quotation marks, or special characters. Unless you include a path with the filename, this command places the file in the same directory as the TFTP server itself.

The uploaded ASCII file retains the command-line interface (CLI) format. This allows you to do the following:

- Modify the configuration using a text editor, and later download a copy of the file to the same switch, or to one or more different switches.
- Send a copy of the configuration file to Extreme Networks Technical Support for problem-solving purposes.

If `every <time>` is specified, the switch automatically saves the configuration to the server once per day, at the specified time. Because the filename is not changed, the configured file stored in the TFTP server is overwritten every day.

For version 4.0:

- The keyword `every` is not supported. Specify the time immediately after the filename.

For version 6.0 or later:

- The keyword `every` is required if a time is specified.

To cancel automatic upload, use the `cancel` option. If no options are specified, the current configuration is uploaded immediately.

Use of the `<hostname>` parameter requires that DNS be enabled.

Example

The following command uploads the current configuration to the file *configbackup.txt* on the TFTP server named *tftphost*, every night at 10:15 p.m.:

```
upload configuration tftphost configbackup.txt every 22:15
```

History

This command was available in ExtremeWare 2.0.

Support for the <hostname> parameter was introduced in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

upload configuration cancel

```
upload configuration cancel
```

Description

Cancels a previously scheduled configuration upload.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

This command cancels the scheduled upload command completely, not just the next scheduled daily upload. You must re-issue the `upload configuration every <hour>` command to resume automatic uploads.

If there are no uploads scheduled, this command has no effect.

Example

The following command cancels the current automatic upload schedule:

```
upload configuration cancel
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on all platforms.

use configuration

```
use configuration [primary | secondary] [slot <slot_number> | all]
```

Description

Configures the switch to use a previously saved configuration on the next reboot.

Syntax Description

primary	Specifies the primary saved configuration.
secondary	Specifies the secondary saved configuration.
slot_number	Specifies the management module or another I/O module in the specified slot to use the saved configuration.
all	Specifies the management module and all I/O modules that run software to use the saved configuration.

Default

N/A.

Usage Guidelines

The keyword “configuration” can be abbreviated to “config.”

Example

The following command specifies that the next reboot should use the primary saved configuration:

```
use configuration primary
```

History

This command was available in ExtremeWare 2.0.

Support for the `<slot>` parameter was introduced in ExtremeWare 7.0.0. The `<slot>` parameter is applicable to the Alpine and BlackDiamond chassis.

Support for the `all` keyword was introduced in ExtremeWare 7.1.0. The `all` keyword is applicable to the Alpine and BlackDiamond chassis.

Platform Availability

This command is available on all platforms.

use image

```
use image [primary | secondary] {slot <slot>}
```

Description

Configures the switch to use a saved image on the next reboot.

Syntax Description

primary	Specifies the primary saved software image.
secondary	Specifies the secondary saved software image.
slot	Specifies a saved image in the module in the specified slot.

Default

Primary.

Usage Guidelines

None.

Example

The following command configures the switch to use the primary image on the next reboot:

```
use image primary
```

History

This command was first available in ExtremeWare 2.0.

Support for the <slot> parameter was introduced in ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

B Troubleshooting Commands

If you encounter problems when using your switch, ExtremeWare provides troubleshooting commands. Use these commands only under the guidance of Extreme Networks technical personnel.

You can contact Extreme Networks technical support at (800) 998-2408 or (408) 579-2826.

The Event Management System (EMS), introduced in ExtremeWare 7.1.0, provides enhanced features to filter and capture information generated on a switch. The various systems in ExtremeWare are being converted to EMS components. As a system is converted, the corresponding debug trace command is no longer available. Details of using EMS are discussed in the *ExtremeWare User Guide*, in the chapter, "Status Monitoring and Statistics", and the commands used for EMS are detailed in this document in Chapter 10,"Commands for Status Monitoring and Statistics".

Until all the systems in ExtremeWare are converted, you may need to use a mix of EMS and debug trace commands under the guidance of Extreme Networks technical personnel.

Included in this chapter, as well as in Chapter 10, are the EMS commands to enable and disable debug mode for EMS components.

If CPU utilization is high, use the debug trace commands sparingly, as they require the CPU. Disable any external syslog before you configure a debug trace, because the debug trace utility can send large amounts of information to the syslog, and if your syslog is external, that information travels over your network. Alternatively, you can configure a filter to select only the most necessary information.

Configure a debug trace at lower levels first, and look for obvious problems. Higher levels typically record so much information that they record enough information within a few seconds.

clear debug-trace

```
clear debug-trace
```

Description

Resets the debug-trace levels to the factory settings of level 0.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command resets the debug-trace levels to level 0:

```
clear debug-trace
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace accounting

```
configure debug-trace accounting <debug level>
```

Description

This command provides system-level debug tracing for the accounting subsystem.

Syntax Description

debug level	Specifies a debug level: 0 — Records critical error messages, such as memory allocation errors. Indicates a severe event that can terminate or corrupt accounting. 1 — Records warning messages for various non-critical error conditions. 2 — Records various informational messages. 3 — Records debug information, such as message and event processing. Provides additional information to support engineers for the purpose of diagnosing network problems. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for accounting to 3:

```
configure debug-trace accounting 3
```

Following is the log output at this level:

```
<DBUG:NPAPI> Slot6 NP_KRT_GET_DSB_COUNTS responses from both NPs
<DBUG:NPAPI> Slot6 genpipe: received DSA message GET_COUNTS
<DBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DBUG:DSA> Vlan vlan1 Vlan ID 4091
<DBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DBUG:DSA> Vlan vlan0 Vlan ID 4092
<DBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DBUG:DSA> Vlan Mgmt Vlan ID 4094
<DBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
```

```
<DBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DBUG:DSA> Vlan MacVlanDiscover Vlan ID 4095
<DBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DBUG:DSA> Vlan Default Vlan ID 1
<DBUG:DSA> All Vlan
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the ARM and MPLS modules.

configure debug-trace bootprelay

```
configure debug-trace bootprelay <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — Records error messages and tracks BOOTP messages relayed. 2 — No additional information recorded. 3 — No additional information recorded. 4 — Displays a dump of each packet. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for BOOTP relay errors to 3:

```
configure debug-trace bootprelay 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace card-state-change

```
configure debug-trace card-state-change <debug level>
```

Description

This command is not currently supported.

Syntax Description

debug level	Specifies a debug level: 0 — Not currently supported. 1 — Not currently supported. 2 — Not currently supported. 3 — Not currently supported. 4 — Not currently supported. 5 — Not currently supported.

Default

The default level is 0.

Usage Guidelines

This command is not currently supported.

Example

This command is not currently supported.

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace debug-link

```
configure debug-trace debug-link <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Disables debug tracing for debug link and stops recording information to the syslog. 1 — Enables debug tracing for debug link and records information to the syslog. 2 — No additional information recorded. 3 — No additional information recorded. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Level 0 disables the debug-trace for link detection, and level 1 enables debug-trace for link detection.

For levels 2 through 5, no additional information recorded.

Example

The following command enables debug-trace for link detection:

```
configure debug-trace debug-link 1
```

The following command disables debug-trace for link detection:

```
configure debug-trace debug-link 0
```

History

This command was first available in ExtremeWare 6.2.2b108.

Platform Availability

This command is available on all platforms.

configure debug-trace dvmrp-cache

```
configure debug-trace dvmrp-cache <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Use this command to trace the detailed process of adding, deleting, and modifying a multicast cache. The IP multicast cache is a hardware forwarding entry identified by a ptag index number. The following command displays the cache entries:

```
show ipmc cache [detail] <IP multicast group>
```

The trace is based on the ingress VLAN of a cache. Use this tool if the egress list of a cache is incorrect, if there are missing cache entries, or if the DVMRP task has been intermittently suspended.

Example

The following command sets the reporting level for DVMRP cache errors to 3:

```
configure debug-trace dvmrp-cache 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-cache 4 vlan v49
<DBUG:DVMR> dvcareq.c 698: Remove Cache for (192.168.3.0,224.2.127.254)
<DBUG:DVMR> dvcareq.c 698: Remove Cache for (192.168.3.0,239.1.1.1)
<DBUG:DVMR> dvcareq.c 213: Build Cache for (192.168.3.10,239.1.1.1)
<DBUG:DVMR> dvcareq.c 213: Build Cache for (192.168.3.10,224.2.127.254)
<DBUG:DVMR> dvcareq.c 596: dvmrp mask del interface 6 in
239.1.1.1/192.168.3.0/255.255.255.0
```

```
<DBUG:DVMR> dvcareq.c 213: Build Cache for (192.168.3.10,224.10.253.4)
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace dvmrp-hello

```
configure debug-trace dvmrp-hello <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all DVMRP probe messages coming into a VLAN. Use this command if switches connected to a common network have problems establishing or maintaining normal neighbor relationships.

Example

The following command sets the reporting level for DVMRP hello errors to 3:

```
configure debug-trace dvmrp-hello 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-hello 4 vlan v49
<DBUG:DVMR> dvrx.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49).  Len=16, nbr=1.
<DBUG:DVMR> dvrx.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49).  Len=16, nbr=1.
<DBUG:DVMR> dvrx.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49).  Len=16, nbr=1.
<DBUG:DVMR> dvrx.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49).  Len=16, nbr=1.
<DBUG:DVMR> dvrx.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace dvmrp-message

```
configure debug-trace dvmrp-message <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the DVMRP system messages (prune, graft, and graft acknowledgement) coming into a VLAN. Use this command if a multicast stream cannot be stopped, or does not come down to the receiver after the IGMP snooping entry is verified.

Example

The following command sets the reporting level for DVMRP message errors to 3:

```
configure debug-trace dvmrp-message 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> last message repeated 2 times
<INFO:SYST> serial admin: disable dvmrp
<DBUG:DVMR> DVMRP task stopped.
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace dvmrp-neighbor

```
configure debug-trace dvmrp-neighbor <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the state of all DVMRP neighbors on a common VLAN to monitor when a neighbor is added or deleted.

Example

The following command sets the reporting level for DVMRP neighbor errors to 3:

```
configure debug-trace dvmrp-neighbor 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: enable dvmrp
<DBUG:DVMR> dvnbr.c 149: Add new Nbr 192.168.200.2 on Vlan (v49).  Len=16
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace dvmrp-route

```
configure debug-trace dvmrp-route <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command records all DVMRP route report messages coming into a VLAN. Use this command if the DVMRP routing table is incorrect or unstable.

Example

The following command sets the reporting level for DVMRP route errors to 3:

```
configure debug-trace dvmrp-route 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-route 3 vlan v49
<DBUG:DVMR> dvrx.c 159: Rx Report from 192.168.200.2 in VLAN(v49)
<DBUG:DVMR> dvrx.c 298: Rx route 10.1.2.0/24 Metric 0.1 from 192.168.200.2
<DBUG:DVMR> dvrtrx.c 330: Replace RT (10.1.2.0/24 Metrix=1).  Flag=01/4
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.3.0/24 Metric 1.1 from 192.168.200.2
<DBUG:DVMR> dvrtrx.c 330: Replace RT (192.168.3.0/24 Metrix=1).  Flag=01/4
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.1.3/32 Metric 1.1 from 192.168.200.2
<DBUG:DVMR> dvrtrx.c 330: Replace RT (192.168.1.3/32 Metrix=1).  Flag=01/4
<DBUG:DVMR> dvrttx.c 339: Trigger RT(10.1.2.0/24 metric=34) to Vlan(v49).
<DBUG:DVMR> dvrttx.c 339: Trigger RT(192.168.3.0/24 metric=34) to Vlan(v49).
<DBUG:DVMR> dvrttx.c 339: Trigger RT(192.168.1.3/32 metric=34) to Vlan(v49).
<DBUG:DVMR> dvrttx.c 496: Tx trigger report on VLAN(v49).  Len=27
<DBUG:DVMR> dvrx.c 159: Rx Report from 192.168.200.2 in VLAN(v49)
```

```
<DBUG:DVMR> dvrx.c 298: Rx route 10.1.2.0/24 Metric 0.1 from 192.168.200.2
<DBUG:DVMR> dvrtrx.c 330: Replace RT (10.1.2.0/24 Metrix=1).  Flag=00/0
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.3.0/24 Metric 1.1 from 192.168.200.2
<DBUG:DVMR> dvrtrx.c 330: Replace RT (192.168.3.0/24 Metrix=1).  Flag=00/0
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.1.3/32 Metric 1.1 from 192.168.200.2
<DBUG:DVMR> dvrtrx.c 330: Replace RT (192.168.1.3/32 Metrix=1).  Flag=00/0
<DBUG:DVMR> dvrttx.c 492: Tx periodic report on VLAN(v49).  Len=49
<DBUG:DVMR> dvrx.c 159: Rx Report from 192.168.200.2 in VLAN(v49)
<DBUG:DVMR> dvrx.c 298: Rx route 172.17.1.0/24 Metric 1.34 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.2.0/30 Metric 0.34 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.100.0/30 Metric 1.34 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.1.1/32 Metric 1.34 from 192.168.200.2
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace dvmrp-timer

```
configure debug-trace dvmrp-timer <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for DVMRP timer errors to 3:

```
configure debug-trace dvmrp-timer 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-timer 3 v49
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace eaps-system

```
configure debug-trace eaps-system <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records software bugs and severe errors. 1 — Records warning messages. 2 — Records changes in state, such as a failure, and changes in port status, such as a port going down. 3 — Records events that do not cause a state change and basic debug information, such as failed PDU transmission, disabled or unconfigured ports, or inactive links. 4 — Records frequently occurring events, such as timers expiring, and detailed debug information, such as sending or receiving PDUs, VLAN ID and EAPS domain of each PDU, and configuration values. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for EAPS errors to 3:

```
configure debug-trace eaps-system 3
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace eaps-system 0
<DBUG:EAPS> eaps_runtime.c 1673: Complete state unchanged, EAPS="man1"
<DBUG:EAPS> eaps_runtime.c 931: Pdu="Health-Pdu", EAPS="man1" [MAC=00:01:30:33:14:00],
RcvdSeq#=14851, CurrSeq#
<DBUG:EAPS> eaps_runtime.c 852: pdu="Health-Pdu"
<DBUG:EAPS> eaps_runtime.c 843: [DEBUG] vlanId=10, eapsdInst=0
<DBUG:EAPS> eaps.c 520: [DEBUG] Found Control Vlan. EapsInst=0
<DBUG:EAPS> eaps.c 368: [DEBUG] Wowie!! Received EAPS_PDU_MSG
<DBUG:EAPS> eaps_runtime.c 804: EAPS-PDU Transmit OK, Vlan="c1"
<DBUG:EAPS> eaps_runtime.c 779: Sending EAPS pdu out port (1:2) vlan "c1" vlanId=10
<DBUG:EAPS> eaps_runtime.c 1295: EAPS "man1" Hello Timer expired.
```

```
<DBUG:EAPS> eaps_runtime.c 1673: Complete state unchanged, EAPS="man1"
<DBUG:EAPS> eaps_runtime.c 931: Pdu="Health-Pdu", EAPS="man1" [MAC=00:01:30:33:14:00],
RcvdSeq#=14850, CurrSeq#
```

History

This command was first available in ExtremeWare 6.1.9.

Platform Availability

This command is available on all platforms.

configure debug-trace flow-redirect

```
configure debug-trace flow-redirect <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — Records configuration changes and unexpected code states. 2 — Records next-hop resources becoming active or inactive. 3 — No additional information recorded. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for flow redirect errors to 2:

```
configure debug-trace flow-redirect 2
```

Following is the log output at this level:

```
<INFO:IPRT> redirect next hop http1 30.0.0.9 changed to up
<DBUG:SYST> i=1 Changing Nexthop fg=fffc Source=24.3.89.150 Nexthop=30.0.0.6 Nfg=fffb
<DBUG:SYST> i=0 Changing Nexthop fg=fffc Source=24.3.89.149 Nexthop=30.0.0.5 Nfg=fffa
<DBUG:SYST> i=4 Changing Nexthop fg=fffc Source=24.3.89.148 Nexthop=30.0.0.9 Nfg=ffff
<DBUG:SYST> i=3 Changing Nexthop fg=fffc Source=24.3.89.147 Nexthop=30.0.0.8 Nfg=fffe
<DBUG:SYST> i=2 Changing Nexthop fg=fffc Source=24.3.89.146 Nexthop=30.0.0.7 Nfg=fffd
<DBUG:SYST> i=1 Changing Nexthop fg=fffc Source=24.3.89.145 Nexthop=30.0.0.6 Nfg=fffb
<DBUG:SYST> i=0 Changing Nexthop fg=fffc Source=24.3.89.144 Nexthop=30.0.0.5 Nfg=fffa
<DBUG:SYST> Sag=fffc
<DBUG:SYST> Grps0 = fffa fffb fffd fffe ffff 0 0 0
<DBUG:SYST> rLBS inst=0 inUse=1 SA=24.3.89.144 sMask=fffffff 8 dPort=50
<DBUG:SYST> Looking for entries to balance in redirect 3
<DBUG:SYST> Looking for entries to balance in redirect 2
<DBUG:SYST> Looking for entries to balance in redirect 1
<DBUG:SYST> Looking for entries to balance in redirect 0
<INFO:IPRT> redirect next hop http1 30.0.0.8 changed to up <DBUG:SYST> Balancing group
ffff
```

```
<DBUG:SYST> Adding new flow for next hop ip 30.0.0.5 group fffe
<DBUG:SYST> Balancing group fffe
<DBUG:SYST> Adding new flow for next hop ip 30.0.0.5 group fffd
<DBUG:SYST> Balancing group fffd
<DBUG:SYST> Adding new flow for next hop ip 30.0.0.5 group fffb
<DBUG:SYST> Balancing group fffb
<DBUG:SYST> Looking for entries to balance in redirect 0
<DBUG:SYST> Entry Up: Adding new flow for next hop ip 30.0.0.5 group fffa
<DBUG:SYST> redirectServerListAdd 0 4
<DBUG:SYST> redirectServerListAdd 0 3
<DBUG:SYST> redirectServerListAdd 0 2
<DBUG:SYST> redirectServerListAdd 0 1
<DB UG:SYST> redirectServerListAdd 0 0
<INFO:SYST> msm-a-console admin: enable http1
<DBUG:SYST> redirectServerListDelEntry: Checking server entry 0x866c2efc 1 4
<DBUG:SYST> redirectServerListDelEntry 0x8 66c2f5c 0 4
<DBUG:SYST> redirectServerListDelEntry: Checking server entry 0x866c198c 2 4
<DBUG:SYST> redirectServerListDelEntry 0x866c19ec 0 4
<DBUG:SYST> redirectServerListDelEntry: Checking server entry 0x866c201c 3 4
<DBUG:SYST> redirectServerListDelEntry 0x866c207c 0 4
<DBUG:SYST> redirectServerListDelEntry: Freeing server entry 0x866c3efc 0 4
<DBUG:SYST> redirectServerListDelEntry 0x866c3f8c 0 4
<DBUG:SYST> Grps0 = 0 0 0 0 0 0 0 0
<DBUG:SYST> rLBS inst=0 inUse=1 SA=24.3.89.144 sMask=fffffff 8 dPort=50
<DBUG:SYST> Entry Down: Deleting sub flow for next hop ip 30.0.0.9 group fffe
<DBUG:SYST> Entry Down: Deleting sub flow for next hop ip 30.0.0.9 group fffd
<DBUG:SYST> Entry Down: Deleting sub flow for next hop ip 30.0.0.9 group fffb
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace flowstats

```
configure debug-trace flowstats <debug level>
```

Description

This command records debug information to the system log.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages, such as cannot open a socket, cannot bind a socket, or cannot add or remove a flow from health-check. 1 — No additional information recorded. 2 — No additional information recorded. 3 — No additional information recorded. 4 — No additional information recorded. 5 — Displays informational messages, such as adding or deleting a flow collector. 6 — No additional information recorded. 7 — Displays debug messages such as enabling and disabling ping-check, IP address of flow collector, and port, flow collector, and flow group information for each packet, as well as a packet dump.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for flowstats errors to 3:

```
configure debug-trace flowstats 3
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure debug-trace health-check

```
configure debug-trace health-check [<debug level> | {filter [real |
virtual] <ip address> [ftp | http | https | imap4 | ldap | nntp | pop3 |
smtp | socks | telnet | tftp | web | wildcard | www | <tcp port number>]}]
```

Description

This command records debug information to the syslog.

Syntax Description

filter	Specifies a filter.
real	Specifies a real IP address.
virtual	Specifies a virtual IP address.
ip address	Specifies the IP address.
ftp	Specifies FTP messages.
http	Specifies HTTP messages.
https	Specifies HTTPS messages.
imap4	Specifies IMAP4 messages.
ldap	Specifies LDAP messages.
nntp	Specifies NNTP messages.
pop3	Specifies POP3 messages.
smtp	Specifies SMTP messages.
socks	Specifies SOCKS messages.
telnet	Specifies Telnet messages.
tftp	Specifies TFTP messages.
web	Specifies HTTP messages.
wildcard	Specifies messages from all services.
www	Specifies HTTP messages.
debug level	Specifies a debug level: 0 — Records unable to initialize or add a health check due to unavailable internal resources (memory, tasks, sockets, timers, or queues). 1 — Records resources becoming active or inactive, unexpected code states, and internal resources unavailable. 2 — Records resources added to or removed from health-check, configuration parameters updated, and individual health-check activity. 3 — Records more verbose health-check activity and debug messages. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Health-check debug messages apply to all resources tracked by health-check. The messages recorded are in addition to messages you have configured for other features.

You can define a filter to limit the debug messages logged. Before you define a filter, you must configure the debug level. To define a filter, you must do the following:

1. Specify a real or virtual IP address. You can specify both a real and virtual IP address in the same command line. An IP address of 0.0.0.0 will match any IP address. Messages without associated IP addresses are logged regardless of the filters you define.
2. Specify a port or service. A service of wildcard or a port of 0 will match any service or port number.

The filter limits the recorded messages to those concerning the IP addresses and services you specify. If you do not configure a filter, debug-trace records messages at the debug level you specify for every service on every IP address.

When you save your configuration, you also save your configured filter values.

Example

The following command enables level 2 debug-tracing:

```
configure debug-trace health-check 2
```

The following command then configures a filter for a specific server and service:

```
configure debug-trace health-check filter real 1.2.3.4 : http
```

This configuration logs health-check debug messages at levels 0, 1, and 2 for the following:

- Generic health-check messages
- ping-check for IP address 1.2.3.4
- tcp-port-check for IP 1.2.3.4 port 80 (HTTP)
- service-check for IP 1.2.3.4 port 80 (including any virtual servers that use SLB pool member 1.2.3.4 port 80)

Alternate Example

The following command enables level 2 debug-tracing:

```
configure debug-trace health-check 2
```

The following command configures a filter that provides all of the information in the preceding example, and also logs service-checks specifically for the SLB virtual server (5.6.7.8 port 80) that references SLB pool member 1.2.3.4 port 80:

```
configure debug-trace health-check filter real 1.2.3.4 : http virtual 5.6.7.8 : http
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace iparp

```
configure debug-trace iparp <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug	Specifies a debug level: 0 — Records IP and ARP conflicts, and duplicate IP addresses. 1 — Records the following errors: • ARP interface down • No bridge for router interface • No free new entry • Filter out multicast and broadcast source address • Header too short • ARP Ethernet/IP • Invalid hw/prot length • Wrong length 2 — Records the following errors: • Router interface down • Bad IP destination • No mbuf available • Failed to ARP • SubVLAN proxy ARP disabled, replied, or ARPing • No bridge available • No ARP available • No router interface in ARPT • Loopback entry created • Suppressed re-ARP • New ARP entry for IP/MAC address • Filtering own ARP • Target matched primary, secondary, or backup 3 — No additional information recorded. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for IP ARP errors to 3:

```
configure debug-trace iparp 3
```

Following is the log output at this level:

```
<DBUG:SYS > arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBUG:SYS > arpresolve: START ac=0x82f3d6e0 m=0x849a6800 IP=192.168.192.12
<DBUG:SYS > arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBUG:SYS > arpresolve: START ac=0x82f3d6e0 m=0x849a6c00 IP=192.168.192.12
<DBUG:SYS > arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBUG:SYS > arpresolve: START ac=0x82f3d6e0 m=0x849a6c00 IP=192.168.192.12
<DBUG:SYS > arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBUG:SYS > arpresolve: START ac=0x82f3d6e0 m=0x849a6800 IP=192.168.192.12
<DBUG:SYS > arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<INFO:SYST> serial admin: configure debug-trace iparp 3 t2
<INFO:SYST> Port 2:1 link active 100Mbs FULL duplex
<INFO:SYST> serial admin: configure t2 add ports 2 : 1
<INFO:SYST> serial admin: configure t2 delete ports 1 : 1
<INFO:SYST> serial admin: enable ipforwarding t2
<INFO:SYST> serial admin: configure t2 ipaddress 192.168.192.1 / 24
<INFO:SYST> serial admin: configure t2 add ports 1 : 1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace ipxgns-message

```
configure debug-trace ipxgns-message <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — None. 2 — Verifies that IPX GNS messages are being sent and received. 3 — Verifies the contents of the messages. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for IPX GNS message errors to 3:

```
configure debug-trace ipxgns-message 3
```

Following is the log output at this level:

```
<DBUG:XSAP> SAP Traverse: Stuffing entry into packet
<DBUG:XSAP> SAP Traverse: Ignoring type 0278
<DBUG:XSAP> SAP Traverse: Ignoring type 026b
<DBUG:XSAP> SAP Traverse: Ignoring type 0640
<DBUG:XSAP> SAP Traverse: Ignoring type 0278
<DBUG:XSAP> SAP Traverse: Ignoring type 026b
<DBUG:XSAP> SAP Traverse: Ignoring type 0640
<DBUG:XSAP> type 0004 net: 3646f895 mac: 00:90:27:a1:44:3c socket: 1105
<DBUG:XSAP> SAP Traverse: Stuffing entry into packet
<DBUG:XSAP> last message repeated 9 times
<DBUG:XSAP> Rcv bcast GNS type(3) from (f0003606, 00:a0:c9:59:a4:5e) for service=0x4
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace ipxrip-message

```
configure debug-trace ipxrip-message <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — None. 2 — Verifies that ipxrip messages are being sent and received. 3 — Verifies the contents of the messages. 4 — Displays a dump of each packet. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for IPX RIP message errors to 4:

```
configure debug-trace ipxrip-message 4
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace ipxrip-message 4 ipxvlan
<INFO:SYST> Log cleared
<INFO:SYST> serial admin: clear log
<DBUG:KERN> 0x0881347d82: 00 03                                                 **
<DBUG:KERN> 0x0881347d72: 00 02 00 00 36 12 00 01 00 01 00 00 10 69 00 02
****6********i**
<DBUG:XRIP> Sending Rsp msg to f0001964:ff:ff:ff:ff:ff:ff len 18
<DBUG:XRIP> Added entry net 1069 hops 2 ticks 3 to rsp
<DBUG:XRIP> Added entry net 3612 hops 1 ticks 1 to rsp
<INFO:EAPS> eaps_runtime.c 1426: State Change, Failed -> Complete, EAPS="man1"
<INFO:EAPS> eaps_runtime.c 277: Primary Port Change, Down -> Up
<INFO:SYST> Port 1:2 link active 1000Mbs FULL duplex
<DBUG:KERN> 0x0881347d82: 00 03                                                 **
<DBUG:KERN> 0x0881347d72: 00 02 00 00 36 12 00 01 00 01 00 00 10 69 00 02
****6********i**
<DBUG:XRIP> Sending Rsp msg to f0001964:ff:ff:ff:ff:ff:ff len 18
```

```
<DBUG:XRIP> Added entry net 1069 hops 2 ticks 3 to rsp
<DBUG:XRIP> Added entry net 3612 hops 1 ticks 1 to rsp
<INFO:EAPS> eaps_runtime.c 1449: State Change, Complete -> Failed, EAPS="man1"
<INFO:EAPS> eaps_runtime.c 1018: Pdu="Link-Down-Pdu", EAPS="man1"
[MAC=00:01:30:32:ef:00]
<INFO:EAPS> eaps_runtime.c 303: Primary Port Change, Up -> Down
<INFO:SYST> Port 1:2 link down
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace ipxrip-route

```
configure debug-trace ipxrip-route <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — None. 2 — Displays route additions and deletions. 3 — No additional information recorded. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for IPX RIP route errors to 2:

```
configure debug-trace ipxrip-route 2
```

Following is the log output at this level:

```
<DBUG:XRIP> Added route to net f0220666 g/w f0001964:00:01:30:32:8d:00, hops 2, tics 2
<INFO:SYST> Log cleared
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace ipxsap-entry

```
configure debug-trace ipxsap-entry <debug level>
```

Description

This command is not currently supported.

Syntax Description

debug level	Specifies a debug level: 0 — Not currently supported. 1 — Not currently supported. 2 — Not currently supported. 3 — Not currently supported. 4 — Not currently supported. 5 — Not currently supported.

Default

The default level is 0.

Usage Guidelines

This command is not currently supported.

Example

This command is not currently supported.

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace ipxsap-message

```
configure debug-trace ipxsap-message <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — None. 2 — Verifies that IPX SAP messages are being sent and received. 3 — Verifies the contents of the messages. 4 — Displays a dump of each packet. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for IPX SAP message errors to 3:

```
configure debug-trace ipxsap-message 3
```

Following is the log output at this level:

```
<INFO:USER> admin logged in through console
<DBUG:XSAP> Generating SAP query (opcode=0001, svc type=ffff)
<INFO:SYST> Port 2:1 link active 100Mbs FULL duplex
<INFO:SYST> Port 2:1 link down
<INFO:SYST> User admin logged out from console
<INFO:SYST> Log cleared
<INFO:SYST> serial admin: clear log
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace isis-cli

```
configure debug-trace isis-cli <level>
```

Description

Controls logging of debug messages related to CLI actions.

Syntax Description

debug level	Specifies a debug level. Following are the debug levels: 0 — Critical/Error Messages 1 — Warning Messages 2 — Concise Messages 3 — Verbose Messages 4 — Packet Dumps

Default

The default is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure debug-trace isis-event

```
configure debug-trace isis-event <level>
```

Description

Controls logging of debug messages related to miscellaneous actions.

Syntax Description

debug level	Specifies a debug level. Following are the debug levels: 0 — Critical/Error Messages 1 — Warning Messages 2 — Concise Messages 3 — Verbose Messages 4 — Packet Dumps

Default

The default is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure debug-trace isis-hello

```
configure debug-trace isis-hello <level> vlan [<vlan name> | all]
```

Description

Controls logging of debug messages related to sending and receiving, and decoding and encoding of Hello messages.

Syntax Description

debug level	Specifies a debug level. Following are the debug levels: 0 — Critical/Error Messages 1 — Warning Messages 2 — Concise Messages 3 — Verbose Messages 4 — Packet Dumps
vlan name	Specifies a VLAN name.

Default

The default is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure debug-trace isis-lsp

```
configure debug-trace isis-lsp <level>
```

Description

Controls logging of debug messages related to sending and receiving and decoding and encoding of LSP Messages.

Syntax Description

debug level	Specifies a debug level. Following are the debug levels: 0 — Critical/Error Messages 1 — Warning Messages 2 — Concise Messages 3 — Verbose Messages 4 — Packet Dumps

Default

The default is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure debug-trace isis-snp

```
configure debug-trace isis-snp <level>
```

Description

Controls logging of debug messages related to sending and receiving, and decoding and encoding of PSNP and CSNP Messages.

Syntax Description

debug level	Specifies a debug level. Following are the debug levels: 0 — Critical/Error Messages 1 — Warning Messages 2 — Concise Messages 3 — Verbose Messages 4 — Packet Dumps

Default

The default is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure debug-trace isis-spf

```
configure debug-trace isis-spf <level>
```

Description

Controls logging of debug messages related to SPF Calculation.

Syntax Description

debug level	Specifies a debug level. Following are the debug levels: 0 — Critical/Error Messages 1 — Warning Messages 2 — Concise Messages 3 — Verbose Messages 4 — Packet Dumps

Default

The default is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on all platforms.

configure debug-trace mpls

```
configure debug-trace mpls <level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — Records error and warning messages, such as session up, state machine errors, Initialization errors, label allocation errors, patricia tree failures, invalid message type or format, memory allocation errors, NVRAM parse errors, TLS tunnel creation errors, socket errors, label manager problems, and null pointer or handle. 2 — Records informational messages, such as LDP entity up, LDP parameter setting, LSP bind event, NHLFE creation, and MPLS GPP and session down errors. 3 — Records debug information, such as patricia Tree Adds/Deletes, Label Propagation and Release Msgs, Message encoding, Parameter setting, MPLS enable messages, Memory initialization, TLS setup messages, Invalid value messages, LSP Init/Teardown msgs, Event processing, RDB (route) callback information. 4 — Records more detailed debug information. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for MPLS errors to 3:

```
configure debug-trace mpls 3
```

Following is the log output at this level:

```
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 2 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
```

```
<DBUG:IPHS> last message repeated 2 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<INFO:SYST> msm-a-console admin: configure debug-trace mpls 0
<DBUG:MPLS> Slot6 MPLS: KRT CHG - Can’t Add MpIdx 17 from Nh Entry 1324
<DBUG:MPLS> Slot6 MPLS: processNhlfeTableAddMpIdx: Attempting to add Mp Entry 17 to
’unused’ Nhlfe Idx 1324
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:MPLS> ip_output.c 664: CONTINUING IP OUTPUT
<INFO:MPLS> mpls_lpe.c 3277: mpls_lpe_common_input() returned
MPLS_LPE_PACKET_UNLABELLED
<DBUG:MPLS> mpls_lsp_endpt.c 346: Attempt to delete endpt entry 10.3.1.1/32
:advertise=0
<DBUG:MPLS> mpls_gpp.c 1037: MPLS Del NHLFE
<INFO:MPLS> mpls_gpp.c 1617: Create ILM for FecIp=10.3.1.1, NhlfeIx=1324,
EndptIx=1332, InLabel=0x11, OutLabel=
<DBUG:MPLS> mpls_gpp.c 796: MPLS Del ILM
<DBUG:MPLS> mpls_lsp_bind.c 1434: Unbinding label 0x00000011 from outgoing Ifc 3 Label
0x00000003
<DBUG:MPLS> mpls_rdb.c 2689: RDB REQ not able to find 10.3.1.1/32 nhop 0.0.0.0
<DBUG:MPLS> mpls_rdb.c 2524: RDB REQ - Get Recompute Next Hop
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002356
<DBUG:MPLS> mpls_lsp_bind.c 1034: Ingress torn down for unknown LSP to endpt
10.3.1.1:32 LSP ID 0x00002356
<INFO:MPLS> mplsevnt.c 394: LMS Notify (0x8d3d1f2c): LSP TORN DOWN (5) FEC:10.3.1.1:32
nhop 0.0.0.0 LSPID:9046
<DBUG:MPLS> mpls_lsp_bind.c 466: Unbinded LSP to 10.3.1.1:32 Label 0x00000003
<DBUG:MPLS> mpls_lsp_endpt.c 765: MPLS Initiating SPF caculation for unbinded LSP to
10.3.1.1
<DBUG:MPLS> mpls_lsp_endpt.c 759: Cannot unbind LSP to 10.3.1.1:32 Type 1 nhop
10.0.1.2 without route entry
<DBUG:MPLS> mpls_rdb.c 2689: RDB REQ not able to find 10.3.1.1/32 nhop 10.0.1.2
<DBUG:MPLS> mpls_lsp_endpt.c 735: unbind_from_ipv4_endpoint: 10.3.1.1:32 Type 1 nhop
10.0.1.2
<DBUG:MPLS> mpls_rdb.c 2689: RDB REQ not able to find 10.3.1.1/32 nhop 0.0.0.0
<DBUG:MPLS> mpls_rdb.c 2524: RDB REQ - Get Recompute Next Hop
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 17.17.17.1/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 956: Recompute Issued for 10.3.1.1/32 nhop 10.0.1.2
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 10.3.1.1/32 nhop
10.0.1.2 orig=33 watch 2
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 192.168.100.12/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 192.168.100.11/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 192.168.100.2/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 20.0.0.1/32 nhop
10.0.1.2 orig=33 watch 0
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002371
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002362
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 12.0.0.1/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 1060: du_recognize_new_fec: ifIndex=3,
destIp=192.168.100.11/32, nHop=10.0.2.2
<DBUG:MPLS> mpls_rdb.c 578: mpls_rdb_callback: add route to 192.168.100.11/32 nhop
10.0.2.2 watch 0 orig=33
```

```
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002355
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002352
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x0000236D
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002350
<DBUG:MPLS> mpls_rdb.c 1060: du_recognize_new_fec: ifIndex=3, destIp=17.17.17.1/32,
nHop=10.0.2.2
<DBUG:MPLS> mpls_rdb.c 578: mpls_rdb_callback: add route to 17.17.17.1/32 nhop
10.0.2.2 watch 0 orig=33
<DBUG:MPLS> mpls_rdb.c 1060: du_recognize_new_fec: ifIndex=3,
destIp=192.168.100.12/32, nHop=10.0.2.2
<DBUG:MPLS> mpls_rdb.c 578: mpls_rdb_callback: add route to 192.168.100.12/32 nhop
10.0.2.2 watch 0 orig=33
<INFO:MPLS> mpls_gpp.c 1617: Create ILM for FecIp=10.3.1.1, NhlfeIx=1324,
EndptIx=1332, InLabel=0x11, OutLabel=
<DBUG:MPLS> mpls_gpp.c 763: MPLS Add ILM
<DBUG:MPLS> mpls_lpe.c 1302: Bind LSP Req Label 0x00000011 to endpt 10.3.1.1:32 Type 1
<INFO:MPLS> mplsevnt.c 369: LMS Notify (0x8d3d1f2c): LSP SUCCESSFUL  FEC:10.3.1.1:32
LSPID:9046  DNS LABEL:3
<DBUG:MPLS> mpls_lsp_bind.c 1783: Binded LSP to endpt 10.3.1.1:32 nhop 10.0.1.2 Label
0x00000003
<DBUG:MPLS> mpls_gpp.c 1002: MPLS Add NHLFE
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the MPLS module.

configure debug-trace mpls-signalling

```
configure debug-trace mpls-signalling <level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — Records peer interface state msgs. 2 — No additional information recorded. 3 — Records finite state machine events 4 — No additional information recorded. 5 — Records MPLS signalling packets, such as hello packets and label mappings.

Default

The default level is 1.

Usage Guidelines

The debug level range is 1 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for MPLS signalling subsystem errors to 1:

```
configure debug-trace mpls-signalling 1
```

Following is the log output at this level:

```
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<INFO:SYST> User admin logged out from telnet (100.100.105.1)
<INFO:USER> admin logged in through telnet (100.100.105.1)
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 3 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
```

```
<DBUG:MSIG>  => NewSt:DU_DORMANT    OldSt:ESTABLISHED   EV:INT_DEL_UPS
<DBUG:MSIG>  => SESS: 10.0.1.1 0 Peer: 10.3.1.1 0
<DBUG:MSIG> DOWN_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG>  => NewSt:ESTABLISHED   OldSt:ESTABLISHED   EV:INT_DEL_UPS
<DBUG:MSIG>  => SESS: 10.0.1.1 0 Peer: 10.3.1.1 0
<DBUG:MSIG> DOWN_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG> SESS: 10.0.2.1 0 Peer: 100.100.61.1 0 NewSt:OPERATIONAL  OldSt:OPERATIONAL
EV:OTHER_MSG_RX
<DBUG:MSIG>  => NewSt:IDLE             OldSt:UPS_RLS_AWT      EV:RELEASE_REQ
<DBUG:MSIG>  => NH: 10.0.1.2 (4) SESS: 10.0.2.1 0 Peer: 100.100.61.1 0
<DBUG:MSIG> UP_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG>  => NewSt:UPS_RLS_AWT      OldSt:ESTABLISHED      EV:RTE_RECOMP_REQ
<DBUG:MSIG>  => NH: 10.0.1.2 (4) SESS: 10.0.2.1 0 Peer: 100.100.61.1 0
<DBUG:MSIG> UP_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG>  => NH: 10.0.1.2 (4) NewNH_NoRouteToDestination (0x2) SESS: 10.0.2.1 0
Peer: 100.100.61.1 0
<DBUG:MSIG> UP_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG>  => NH: 10.0.1.2 (4) NewSt:IDLE      OldSt:EST       EV:RTE_RECOMP_REQ
<DBUG:MSIG> ING_UP_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG>  => NH: 10.0.1.2 (4) NewNH_NoRouteToDestination (0x2)
<DBUG:MSIG> ING_UP_FSM: FEC: 10.3.1.1/32
<DBUG:MSIG>  => NewSt:ESTABLISHED      OldSt:RESP_AWAITED     EV:INT_DNS_MAP
<DBUG:MSIG>  => NH: 10.0.1.2 (4) SESS: 10.0.2.1 0 Peer: 100.100.61.1 0
<DBUG:MSIG> UP_FSM: FEC: 10.3.1.1/32
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the MPLS module.

configure debug-trace npcard

```
configure debug-trace npcard <debug level>
```

Description

This command enables system-level debug tracing for the MPLS, PoS, ARM, and ATM modules.

Syntax Description

debug level	Specifies a debug level:	
	0—	Indicates that a severe event has occurred that most likely will result in the termination or improper operation of the ARM.
	1—	Indicates that a major event has occurred. It may represent a negative operation. It should be reviewed to ensure proper continuation of ARM operation.
	2—	Indicates a minor event has occurred.
	3—	Provides additional information to support engineers for the purpose of diagnosing network problems.
	4 —	No additional information recorded.
	5 —	No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 1 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for module errors to 3:

```
configure debug-trace npcard 3
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the MPLS, PoS, ARM, and ATM modules.

configure debug-trace pim-cache

```
configure debug-trace pim-cache <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the detailed process of adding, deleting, and modifying a multicast cache. The IP multicast cache is a hardware forwarding entry identified by a ptag index number. The following command displays the cache entries:

```
show ipmc cache [detail] <IP multicast group>
```

The trace is based on the ingress VLAN of a cache. Use this tool if the egress list of a cache is incorrect, if there are missing cache entries, or if any multicast stream jitters.

Example

The following command sets the reporting level for PIM cache errors to 3:

```
configure debug-trace pim-cache 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-cache 3
<DBUG:PIM> PIM: 142.168.100.100/236.58.16.16: pimSendRegStop: dst 15.1.6.3
<DBUG:PIM> PIM: ProcRegister: sptree flow exists
<DBUG:PIM> PIM: 142.168.100.100/236.58.16.16: entry timer starting for 210
<DBUG:PIM> PIM: 142.168.100.100/236.58.16.16: fwd: extending entry's life
<DBUG:PIM> PIM: ProcRegister: NoBorder: rp:15.1.4.1 src:15.1.6.3
<DBUG:PIM> PIM: ProcRegister: 142.168.100.100/236.58.16.16
<DBUG:PIM> PIM: ProcRegister: null bit set
<DBUG:PIM> PIM: 142.168.100.100/235.49.1.6: pimSendRegStop: dst 15.1.6.3
```

```
<DBUG:PIM> PIM: ProcRegister: sptree flow exists
<DBUG:PIM> PIM: 142.168.100.100/235.49.1.6: entry timer starting for 210
<DBUG:PIM> PIM: 142.168.100.100/235.49.1.6: fwd: extending entry’s life
<DBUG:PIM> PIM: ProcRegister: NoBorder: rp:15.1.6.1 src:15.1.6.3
<DBUG:PIM> PIM: ProcRegister: 142.168.100.100/235.49.1.6
<DBUG:PIM> PIM: ProcRegister: null bit set
<DBUG:PIM> PIM: 142.168.100.101/235.48.13.0: pimSendRegStop: dst 15.1.6.3
<DBUG:PIM> PIM: ProcRegister: sptree flow exists
<DBUG:PIM> PIM: 142.168.100.101/235.48.13.0: entry timer starting for 210
<DBUG:PIM> PIM: 142.168.100.101/235.48.13.0: fwd: extending entry’s life
<DBUG:PIM> PIM: ProcRegister: NoBorder: rp:15.2.1.1 src:15.1.6.3
<DBUG:PIM> PIM: ProcRegister: 142.168.100.101/235.48.13.0
<DBUG:PIM> PIM: ProcRegister: null bit set
<DBUG:PIM> PIM: ProcRegister: NoBorder: rp:15.1.4.1 src:15.1.6.3
<DBUG:PIM> PIM: ProcRegister: 192.168.100.201/229.55.150.208
<DBUG:PIM> PIM: ProcRegister: NoBorder: rp:15.1.4.1 src:15.2.1.2
<DBUG:PIM> PIM: ProcRegister: 15.2.2.2/229.55.150.208
<DBUG:PIM> PIM: ProcRegister: NoBorder: rp:15.1.4.1 src:15.1.6.3
<DBUG:PIM> PIM: ProcRegister: 192.168.100.201/229.55.150.208
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace pim-hello

```
configure debug-trace pim-hello <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all PIM hello messages coming into a VLAN. Use this command if switches connected to a common network have problems establishing or maintaining normal neighbor relationships.

Example

The following command sets the reporting level for PIM hello errors to 3:

```
configure debug-trace pim-hello 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-hello 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.2.1.2 thro 15.2.1.1
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.4.2 thro 15.1.4.1
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.2.1.1 to 224.0.0.13
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.4.1 to 224.0.0.13
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.6.3 thro 15.1.6.1
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.6.1 to 224.0.0.13
<INFO:SYST> msm-a-console admin: configure debug-trace pim-hello 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
```

```
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.4.1 to 224.0.0.13
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.6.3 thro 15.1.6.1
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.6.1 to 224.0.0.13
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.2.1.2 thro 15.2.1.1
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.4.2 thro 15.1.4.1
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.2.1.1 to 224.0.0.13
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.4.1 to 224.0.0.13
<DBUG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.6.3 thro 15.1.6.1
<DBUG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.6.1 to 224.0.0.13
<INFO:SYST> msm-a-console admin: configure debug-trace pim-hello 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<INFO:SYST> Log cleared
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace pim-message

```
configure debug-trace pim-message <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all PIM system messages (join, prune, graft, graft acknowledgement, assert, and BSRM) coming into a VLAN. Use this command if a multicast stream cannot be stopped or does not come down to the receiver after the IGMP snooping entry is verified, or if the CPU load is unexpectedly high.

Example

The following command sets the reporting level for PIM message errors to 3:

```
configure debug-trace pim-message 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-message 3 vlan all
<DBUG:PIM> PIM: Xmitting RP Adv(8) pkt of len 22 from src 15.2.1.1 to 15.1.6.3
<DBUG:PIM> PIM: Xmitting RP Adv(8) pkt of len 22 from src 15.1.6.1 to 15.1.6.3
<DBUG:PIM> PIM: Xmitting RP Adv(8) pkt of len 22 from src 15.1.4.1 to 15.1.6.3
<DBUG:PIM> PIM: ProcPrune: src 0.0.0.0 rp 15.1.4.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 0 prunes 1
<DBUG:PIM> PIM: ProcJPG: handling 235.1.1.201/255.255.255.255
<DBUG:PIM> PIM: ProcJPG: una=15.1.4.1 peerRtr=0 hold_time=210 #grp=1
<DBUG:PIM> PIM: Receiving Join/Prune(3) pkt of len 34 from src 15.1.4.2 to dst
224.0.0.13 thro 15.1.4.1
```

```
<DBUG:PIM> PIM: Receiving Bootstrap(4) pkt of len 116 from src 15.1.4.2 to dst
224.0.0.13 thro 15.1.4.1
<DBUG:PIM> PIM: Receiving Bootstrap(4) pkt of len 116 from src 15.1.6.3 to dst
224.0.0.13 thro 15.1.6.1
<DBUG:PIM> PIM: ProcJoin: src 142.168.100.101 rp 15.2.1.1 type (s,g)
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.2.1.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 2 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 235.48.13.0/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.2.1.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 224.0.1.113/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.1.6.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 227.37.32.6/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.1.6.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 227.37.32.5/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.1.6.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 227.37.32.4/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.2.1.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 227.37.32.3/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.2.1.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 227.37.32.2/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 0.0.0.0 rp 15.2.1.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 1 prunes 0
<DBUG:PIM> PIM: ProcJPG: handling 227.37.32.1/255.255.255.255
<DBUG:PIM> PIM: ProcJoin: src 142.168.100.100 rp 15.1.4.1 type (s,g)
<DBUG:PIM> PIM: ProcJoin: src 142.168.100.101 rp 15.1.4.1 type (s,g)
<DBUG:PIM> PIM: ProcJPG: una=15.2.1.1 peerRtr=0 hold_time=210 #grp=12
<DBUG:PIM> PIM: Receiving Join/Prune(3) pkt of len 294 from src 15.2.1.2 to dst
224.0.0.13 thro 15.2.1.1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace pim-neighbor

```
configure debug-trace pim-neighbor <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the state of all PIM neighbors on a common VLAN to monitor if, when, or how frequently a neighbor is added or deleted.

Example

The following command sets the reporting level for PIM neighbor errors to 3:

```
configure debug-trace pim-neighbor 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-neighbor 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<INFO:SYST> Port 8:1 link down
<INFO:SYST> Port 8:2 link down
<INFO:SYST> Port 8:3 link down
<INFO:SYST> Port 8:4 link down
<DBUG:PIM> PIM: pimDelNbr: nbr 15.1.4.2 thro iface 15.1.4.1
<INFO:SYST> Port 8:4 link down
<INFO:SYST> Port 8:3 link down
<INFO:SYST> Port 8:2 link down
<INFO:SYST> Port 8:1 link down
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace pim-rp-mgmt

```
configure debug-trace pim-rp-mgmt <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records error messages. 1 — Records warnings. 2 — Records verbose warnings. 3 — Displays a dump of each packet. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all RP advertisement and bootstrap messages carrying rp-set information coming into a VLAN. Use this command if RP or BSR is absent or unstable. This command is for sparse mode only.

Example

The following command sets the reporting level for PIM RP management errors to 3:

```
configure debug-trace pim-rp-mgmt 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-rp-mgmt 3
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<DBUG:PIM> PIM: ProcBootstrap: Wrong iif for BSR 15.1.6.3
<DBUG:PIM> PIM: ProcBootstrap: from 15.1.4.2 in 15.1.4.1 len 56
<DBUG:PIM> PIM: rpDelEntry: 15.3.1.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.3.1.1 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.4.2 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.4.2 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.8.2 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.8.2 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.4.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.4.1 no longer listed
```

```
<DBUG:PIM> PIM: rpDelEntry: 15.2.1.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.2.1.1 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.6.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.6.1 no longer listed
<DBUG:PIM> PIM: rpGetEntry: 192.168.100.3
<DBUG:PIM> PIM: ProcBootstrap: rp 192.168.100.3
<DBUG:PIM> PIM: rpGetEntry: 15.1.6.3
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.6.3
<DBUG:PIM> PIM: rpGetEntry: 15.1.8.3
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.8.3
<DBUG:PIM> PIM: ProcBootstrap: grp 224.0.0.0
<DBUG:PIM> PIM: ProcBootstrap: fragment Tag 40585
<DBUG:PIM> PIM: ProcBootstrap: from 15.1.6.3 in 15.1.6.1 len 56
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.4.2 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.8.2 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.8.2 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.2.1.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.2.1.1 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.6.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.6.1 no longer listed
<DBUG:PIM> PIM: rpDelEntry: 15.1.4.1 (Bootstrap)
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.4.1 no longer listed
<DBUG:PIM> PIM: rpGetEntry: 192.168.100.3
<DBUG:PIM> PIM: ProcBootstrap: rp 192.168.100.3
<DBUG:PIM> PIM: rpGetEntry: 15.1.6.3
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.6.3
<DBUG:PIM> PIM: rpGetEntry: 15.1.8.3
<DBUG:PIM> PIM: ProcBootstrap: rp 15.1.8.3
<DBUG:PIM> PIM: ProcBootstrap: grp 224.0.0.0
<DBUG:PIM> PIM: ProcBootstrap: fragment Tag 41065
<DBUG:PIM> PIM: ProcBootstrap: from 15.1.6.3 in 15.1.6.1 len 56
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace rip-message

```
configure debug-trace rip-message <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — None. 2 — None. 3 — Records that the switch received a response from w.x.y.z (pier) len 24 at time.time. Records that the switch sent a response to 224.0.0.9 at time.time. 4 — Displays a dump of the RIP response. Displays a dump of the RIP response received. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for RIP message errors to 3:

```
configure debug-trace rip-message 3
```

Following is the log output at this level:

```
<DBUG:RIP > Sending Rsp to 224.0.0.9 at 1012569160.950000
<INFO:SYST> msm-a-console admin: configure debug-trace rip-message 3 vlan all
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace rip-route-change

```
configure debug-trace rip-route-change <debug level> vlan <vlan name | all>
```

Description

This command is not currently supported.

Syntax Description

debug level	Specifies a debug level: 0 — Not currently supported. 1 — Not currently supported. 2 — Not currently supported. 3 — Not currently supported. 4 — Not currently supported. 5 — Not currently supported.
vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

The default level is 0.

Usage Guidelines

This command is not currently supported.

Example

This command is not currently supported.

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace rip-triggered-update

```
configure debug-trace rip-triggered-update <debug level> vlan <vlan name |
all>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — None. 1 — None. 2 — None. 3 — Records that the switch is suppressing triggered updates for x seconds. 4 — No additional information recorded. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.
all	Specifies all VLANs.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for RIP triggered update errors to 3:

```
configure debug-trace rip-triggered-update 3
```

Following is the log output at this level:

```
<DBUG:RIP > Suppressing triggered updates for 1 secs.
<INFO:SYST> msm-a-console admin: enable rip
<INFO:SYST> msm-a-console admin: disable rip
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace slb-3dns

```
configure debug-trace slb-3dns <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records serious errors that can cause 3DNS support to fail. This includes problems associated with system resources, invalid iQuery messages, and internal SLB and 3DNS table maintenance. 1 — Records task and or socket layer errors. These errors might indicate other more serious problems. 2 — Records informational 3DNS member change notifications, state changes, or age-outs. 3 — Decodes and displays incoming and outgoing 3DNS iQuery messages. Also displays some internal table data when the 3DNS member entries are created or updated. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for SLB 3DNS errors to 3:

```
configure debug-trace slb-3dns 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace slb-connection

```
configure debug-trace slb-connection <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records critical failures such as insufficient memory unexpected internal state. 1 — Records unaccepted or dropped connections, as well as physical ports removed from a GoGo mode group since a failed health check and physical ports added to a GoGo mode group since a passed health check. 2 — Records GoGo mode resources that fail health check, or that change health check status from fail to pass. An associated debug level 1 message will accompany this message only if this was either the first health-check to fail on a port, or the last remaining health-check to pass on a port. 3 — Records all events associated with connecting and disconnecting resources, and some SLB configuration debugging information. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for SLB connection errors to 3:

```
configure debug-trace slb-connection 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace slb-failover

```
configure debug-trace slb-failover <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records possible software errors such as unexpected function call failures and bad function arguments. 1 — Records configuration errors, insufficient memory, and bad data from a peer SLB switch. 2 — Records when a peer SLB switch has come up or gone down. 3 — Displays debug messages. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for SLB failover errors to 3:

```
configure debug-trace slb-failover 3
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace transceiver-test

```
configure debug-trace transceiver-test <debug level>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Disables debug tracing for the transceiver test and stops recording information to the syslog. 1 — Enables debug tracing for the transceiver test and records information to the syslog. 2 — No additional information recorded. 3 — No additional information recorded. 4 — No additional information recorded. 5 — No additional information recorded.

Default

The default level is 0.

Usage Guidelines

The debug level range is 0 to 5. Level 0 disables the debug-trace for the transceiver testing, and level 1 enables debug-trace for the transceiver testing.

For levels 2 through 5, debug-trace for transceiver testing is enabled, but no additional information is recorded.

Example

The following command enables debug-trace for transceiver testing:

```
configure debug-trace transceiver-test 1
```

Following is sample log output at this level:

```
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 2 returns pass
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 4 returns pass
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: CPU SRAM test on BPLNE returns pass
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: CPU FLASH test on BPLNE returns pass
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: CPU NVRAM test on BPLNE returns pass
07/09/2003 15:09:14.03 <Info:TRXDIAG> trxdiag: TWISTER test on BPLNE returns pass
07/09/2003 15:09:14.03 <Info:TRXDIAG> trxdiag: QUAKE test on BPLNE returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 1 returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 2 returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 4 returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: CPU SRAM test on BPLNE returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: CPU FLASH test on BPLNE returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: CPU NVRAM test on BPLNE returns pass
```

```
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: TWISTER test on BPLNE returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: QUAKE test on BPLNE returns pass
```

The following command disables debug-trace for transceiver testing:

```
configure debug-trace transceiver-test 0
```

History

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability

This command is available on modular switches only.

configure debug-trace udp-forwarding

```
configure debug-trace udp-forwarding <debug level> vlan <vlan name>
```

Description

This command is not currently supported.

Syntax Description

debug level	Specifies a debug level: 0 — Not currently supported. 1 — Not currently supported. 2 — Not currently supported. 3 — Not currently supported. 4 — Not currently supported. 5 — Not currently supported.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

This command is not currently supported.

Example

This command is not currently supported.

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all platforms.

configure debug-trace vrrp

```
configure debug-trace vrrp <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records critical errors, such as a task crash or an interface down. 1 — Records warning messages. 2 — Records concise packet information. 3 — Records the same information recorded in level 2, with more detail. 4 — Displays a dump of each packet. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The debug `level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for VRRP to 5:

```
configure debug-trace vrrp 5
```

Following is the log output at this level:

```
<DBUG:SYS > Vlan/Vrid=vlan1/1 Putting virtualMac (00:00:5e:00:01:01) into arpcom
<DBUG:SYS > Vlan/Vrid=vlan1/1 Putting systemMac (00:01:30:04:c8:00) into arpcom
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure debug-trace vrrp-hello

```
configure debug-trace vrrp-hello <debug level> vlan <vlan name>
```

Description

This command records debug information to the syslog.

Syntax Description

debug level	Specifies a debug level: 0 — Records critical errors, such as a task crash or an interface down. 1 — Records warning messages, such as incorrect address, incorrect protocol, and failed checksum. 2 — Records information such as VLAN, VRID, priority, auth-type, advert-interval, and IP address. 3 — Records the same information recorded in level 2, with more detail. 4 — Displays a dump of each packet. 5 — No additional information recorded.
vlan name	Specifies a VLAN name.

Default

The default level is 0.

Usage Guidelines

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for VRRP hello messages to 4:

```
configure debug-trace vrrp-hello 4
```

Following is the log output at this level:

```
<DBUG:SYS > Vlan=Default: vrrpTransmit: vrid=1,pri=255,cnt_ip_addr=1,auth_type=0
advert=1,ipaddr=10.45.208.10
<DBUG:SYS > Vlan=Default: vrrpTransmit: vrid=1,pri=255,cnt_ip_addr=1,auth_type=0
advert=1,ipaddr=10.45.208.10
<DBUG:SYS > Sending vrrp-pkt(0x8313d630) len 40 to 224.0.0.18 if rif0,
mac=00:00:5e:00:01:01
<DBUG:KERN> <--- Start of chain (84859200) --->
<DBUG:KERN> m0 @ 0x84859200:  Length=40   m_off=20   m_data=0x84859214
<DBUG:KERN> 0x0884859214: 00 00 00 28 00 00 00 00 ff 70 00 00 00 00 00 00
***(*****p******
<DBUG:KERN> 0x0884859224: e0 00 00 12 21 01 ff 01 00 01 05 c4 0a 2d d0 0a
****!********-**
<DBUG:KERN> 0x0884859234: 00 00 00 00 00 00 00 00 ********
<DBUG:KERN> <--- End of chain (84859200) --->
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all platforms.

configure diagnostics

```
configure diagnostics [extended | fastpost | normal | off]
```

Description

Runs switch diagnostics at boot-up.

Syntax Description

extended	Selects an extended diagnostic routine to run at boot-up. Takes the switch fabric and ports offline, and performs extensive ASIC, ASIC-memory, packet switch, and packet loopback tests. This parameter is not supported in ExtremeWare 6.1.9 or 6.2.
fastpost	Selects fastpost diagnostic routine to run at boot-up. Takes the switch fabric offline and performs a simple ASIC test.
normal	Selects normal diagnostic routine to run at boot-up. Takes the switch fabric and ports offline, and performs a simple ASIC and packet loopback test on all the ports. This parameter is not supported in ExtremeWare 6.1.9 or 6.2.
off	Stops boot-up diagnostics.

Default

Fastpost.

Usage Guidelines

To run diagnostics on an I/O module, use the following command:

```
run diagnostics [normal | extended] [<slot> | msm-a | msm-b]
```

To view results of the diagnostics test, use the following command:

```
show diagnostics
```

If the diagnostics fail, replace the module with another module of the same type.

Example

The following command configures the MSM64i to run the fastest diagnostics at boot-up:

```
configure diagnostics fastpost
```

History

This command was first available in ExtremeWare 6.1.9.

Platform Availability

This command is available on "*i*" series BlackDiamond switches.

configure reboot-loop-protection

```
configure reboot-loop-protection threshold <time-interval> <count>
```

Description

Configures reboot loop protection.

Syntax Description

time-interval	The length of time during which the switch can reboot the specified `count` before entering minimal mode. The range is 0 - 255 minutes.
count	The number of reboots within the specified `time-interval`. The range is 1 - 7.

Default

If you enter a `time-interval` but not a `count`, the default `count` is 3.

Usage Guidelines

Specifying a time interval of 0 disables reboot loop protection. Specifying any other value enables it. To view the current settings, use the `show switch` or `show configuration` commands.

If you reboot the switch manually or use the `run msm-failover` or `run diagnostics` commands, the time interval and count are both reset to 0.

Example

The following command configures the time interval to 5 minutes and the count to 4:

```
configure reboot-loop-protection threshold 5 4
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on all platforms.

configure system-dump server

```
configure system-dump server <ip address>
```

Description

Configures the IP address to which to transfer a dump if the system-dump option is specified in the configuration.

Syntax Description

ip address	Specifies the IP address to which to transfer a system dump.

Default

The default is 0 or “no IP”.

Usage Guidelines

The IP address specified is also used if no address is provided in the upload system-dump command. The IP address must be reachable through the VLAN *mgmt*.

Example

The following command configures the IP address to transfer a system dump to 10.10.10.1:

```
configure system-dump server 10.10.10.1 3
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on platforms with an Ethernet management port.

configure system-dump timeout

```
configure system-dump timeout <seconds>
```

Description

Configures an optional timeout for the dump transfer.

Syntax Description

seconds	Specifies a time in seconds for the system dump timeout.

Default

The default is 0.

Usage Guidelines

The minimum non-zero value is 120 seconds. The minimum recommended value is 480 seconds.

Example

The following command configures the system dump timeout to 600 seconds:

```
configure system-dump timeout 600
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on platforms with an Ethernet management port.

disable log debug-mode

```
disable log debug-mode
```

Description

Disables debug mode. The switch stops generating debug events.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command disables debug mode. Debug mode must be enabled prior to configuring advanced debugging capabilities. These include allowing debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

The following configuration options require that debug mode be enabled:

- including a severity of `debug-summary`, `debug-verbose`, or `debug-data` when configuring filters
- target format options `process-name`, `process-id`, `source-function`, and `source-line`)

Example

The following command disables debug mode:

```
disable log debug-mode
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

enable log debug-mode

```
enable log debug-mode
```

Description

Enables debug mode. The switch generates debug events.

Syntax Description

This command has no arguments or variables.

Default

Disabled.

Usage Guidelines

This command enables debug mode. Debug mode must be enabled prior to configuring advanced debugging capabilities. These include allowing debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

The following configuration options require that debug mode be enabled:

- including a severity of `debug-summary`, `debug-verbose`, or `debug-data` when configuring filters
- target format options `process-name`, `process-id`, `source-function`, and `source-line`.

Example

The following command enables debug mode:

```
enable log debug-mode
```

History

This command was first available in ExtremeWare 7.1.0.

Platform Availability

This command is available on all platforms.

nslookup

```
nslookup <hostname>
```

Description

Displays the IP address of the requested host.

Syntax Description

hostname	Specifies a hostname.

Default

N/A.

Usage Guidelines

None.

Example

The following command looks up the IP address of a computer with the name of *bigserver.xyz_inc.com*:

```
nslookup bigserver.xyz_inc.com
```

History

This command was first available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

ping

```
ping {udp} {continuous} {size <start_size> {-<end_size>}} [<ip_address> |
<hostname>] {from <src_ipaddress> | with record-route | from
<src_ipaddress> with record-route}
```

Description

Enables you to send User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo messages or to a remote IP device.

Syntax Description

udp	Specifies that the ping request should use UDP instead of ICMP.
continuous	Specifies that UDP or ICMP echo messages to be sent continuously. This option can be interrupted by pressing any key.
start_size	Specifies the size, in bytes, of the packet to be sent, or the starting size if incremental packets are to be sent.
end_size	Specifies the maximum size, in bytes, of the packet to be sent in the UDP or ICMP request. When both the start_size and end_size are specified, ICMP requests are transmitted using 1 byte increments, per packet.
ipaddress	Specifies the IP address of the host.
hostname	Specifies the name of the host.
src_ipaddress	Uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used.
record-route	Decodes the list of recorded routes and displays them when the ICMP echo reply is received.

Default

N / A.

Usage Guidelines

The `ping` command is used to test for connectivity to a specific host.

The `ping` command is available for both the user and administrator privilege level.

If a `ping` request fails, the switch continues to send `ping` messages until interrupted. Press any key to interrupt a `ping` request.

For ExtremeWare 6.1:

- You must configure DNS in order to use the `hostname` option.

For ExtremeWare 6.2:

- If you specify UDP as the protocol, the `from <source>` and `with <record-route>` options are not supported.

Example

The following command enables continuous ICMP echo messages to be sent to a remote host:

```
ping continuous 123.45.67.8
```

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support the `hostname`, `from`, and `with record-route` parameters, and incremental packets.

This command was modified in ExtremeWare 6.2 to support UDP.

Platform Availability

This command is available on all platforms.

run diagnostics

```
run diagnostics [extended | normal | packet memory] slot [<slot number> |
msm-a | msm-b]
```

Description

Runs normal or extended diagnostics on the switch, slot, or management module.

Syntax Description

extended	Runs an extended diagnostic routine. Takes the switch fabric and ports offline, and performs extensive ASIC, ASIC-memory, packet memory, and packet loopback tests.
normal	Runs a normal diagnostic routine. Takes the switch fabric and ports offline, and performs a simple ASIC and packet loopback test on all the ports.
packet memory	Runs packet memory diagnostics on an “i” series blade or stackable.
slot number	Specifies the slot number of an I/O module. This option is available only on BlackDiamond switches.
msm-a | msm- b	Specifies the slot letter of an MSM64i. This option is available only on BlackDiamond switches.

Default

N/A.

Usage Guidelines

If you run the diagnostic routine on an I/O module, that module is taken off-line while the diagnostic test is performed. The ports on the module do not forward traffic. Once the diagnostic test is completed, the I/O module is automatically reset and becomes operational again.

NOTE

Run diagnostics when the switch can be brought off-line. The tests conducted are extensive and affect traffic that must be processed by the system CPU. The diagnostics are processed by the CPU whether you run them on an I/O or a management module.

On an I/O module, the extended diagnostic routine can require significantly more time to complete, depending on the number of ports on the module.

The normal diagnostics are short series of tests that do not test all the internal ASIC functions. On a management module, the extended diagnostic routine tests all components including the internal ASIC functions. The management module is taken off-line while the diagnostic test is performed. It is reset and operational once the test is completed.

To view results of normal or extended diagnostics tests, use the following commands:

```
show diagnostics {slot [msm-a | msm-b | <slot number>]}
```

If the results indicate that the diagnostic failed, replace the module with another module of the same type.

To configure a BlackDiamond switch to run diagnostics on an MSM64i at boot-up, use the following command:

```
configure diagnostics [extended | fastpost | normal | off]
```

Example

The following command runs extended diagnostics on the module in slot 3 of a BlackDiamond chassis:

```
run diagnostics extended slot 3
```

A warning is displayed about the impact of this test, and you have the opportunity to continue or cancel the test.

```
Running extended diagnostics will disrupt network traffic on the system.
Extended diagnostic will also execute Packet Memory Scan........
WARNING:  Device may be taken offline. To prevent this
          first configure "sys-health-check auto-recovery online"

Are you sure you want to continue?  yes/no
y
```

Extended diagnostics can cause the following messages to appear in the log:

```
<CRIT:SYST> task tdiagTask cpu utilization is 98% PC: 806266e8

<INFO:SYST> task tdiagTask cpu utilization is 98% PC: 806266e8
```

You can ignore these messages, as they indicate that the system is busy running the diagnostics.

History

This command was first available in ExtremeWare 6.1.5.

The command was modified to support the MPLS module in an ExtremeWare IP Technology Services Release based on ExtremeWare 6.1.8b12.

The command was modified to support MSM64i modules in ExtremeWare 6.1.9.

The command was modified to support Alpine and Summit switches in ExtremeWare 6.2.

Platform Availability

This command is available on “*i*” series switches.

run diagnostics packet-memory slot

```
run diagnostics packet-memory slot <slot number>
```

Description

Executes packet memory scanning for all packet memory associated with the specified I/O slot on a BlackDiamond 6808 or 6816.

Syntax Description

slot number	Specifies the slot number of an I/O module. This option is available only on BlackDiamond switches. In v 6.2.1, cannot specify an MSM. In v 6.2.2 this option is available on "i" series, stackables, and Alpine.

Default

N/A.

Usage Guidelines

If you run the diagnostic routine on an I/O module, that module is taken off-line while the diagnostic test is performed. The ports on the module do not forward traffic. Once the diagnostic test is completed, the I/O module is automatically reset and becomes operational again.

NOTE

Run diagnostics when the switch can be brought off-line. The tests conducted are extensive and affect traffic that must be processed by the system CPU. The diagnostics are processed by the CPU whether you run them on an I/O or a management module.

Packet memory scanning scans the specified blade, module, or stackable to detect single bit-related memory defects and their associated buffer locations. If packet memory defects are detected, their locations are recorded in the blade's EEPROM. Up to eight occurrences can be recorded. If a defect was found during the scan process, the module is reset, the defective buffer is mapped out from further use, and the I/O module is returned to the operational state. If more than eight defects are detected, or if the defects cannot be mapped out, the module is treated as a failed module and left offline, unless `sys-health-check` is configured for `online`. The module should then be returned through the RMA process with Extreme Networks Technical Support.

When you enter the run diagnostic command, you are warned about any potential impacts on your switch and network (since the module will be taken offline during the diagnostic process) and you will have an opportunity to confirm or cancel the test.

To show the results of a packet-memory diagnostic, use the following command:

```
show diagnostics packet-memory slot <slot number>
```

Example

The following command runs a packet-memory scan on the board in slot 4 on a BlackDiamond:

```
run diagnostics packet-memory slot 4
```

The command initially generates the following messages:

```
Running packet memory diagnostics will disrupt network traffic on the system.
WARNING:  Device may be taken offline. To prevent this
          first configure "sys-health-check auto-recovery online"

Are you sure you want to continue?  yes/no
```

If you respond with “y” the scan proceeds.

If you run the packet-memory test on a slot that has no packet memory errors, the output from the command will be similar to the following:

```
* BD3>:17 # Starts scanning packet memory on card 4.
<diagPM-1> INFO: entering packet memory scanning for card 4
................|................|................
Finished scanning packet memory for card 4 --
>>> No new defect <<<
```

If packet memory errors are detected, output similar to the following is displayed:

```
* BD3>:23 # Starts scanning packet memory on card 2.
<diagPM-1> INFO: entering packet memory scanning for card 2
................|................|............
Checking Struct...has 0 entries
Received Packet
00  | 34 26 49 80 64 50 14 1f 60 54 1d a3 27 ee 5c 44
10  | 01 fd 1b 2a 15 0c 4e 79 71 c5 3c 19 1e 6b 36 83
20  | 40 39 35 79 67 2e 25 6c 7e ae 01 06 49 10 61 0e
30  | 3d da 55 9d 02 67 40 62 2a 2f 3a 64 47 dc 00 86
Transmit Packet
00  | 34 26 49 80 64 50 14 1f 60 54 1d a3 27 ee 5c 44
10  | 01 fd 1b 2a 15 0c 4e 79 71 c5 3c 19 1e 6b 36 83
20  | 44 39 35 79 67 2e 25 6c 7e ae 01 06 49 10 61 0e
30  | 3d da 55 9d 02 67 40 62 2a 2f 3a 64 47 dc 00 86

MEMID=9, recov=0, bit_position=0  , addr=101290,  entry=0...
Finished scanning packet memory for card 2 --
>>> New defect(s) detected <<<
```

History

This command was first available in ExtremeWare 6.1.5.

The command was modified to support the MPLS module in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

The command was modified to support MSM64i modules in ExtremeWare 6.1.9.

The command was modified to support Alpine and Summit switches in ExtremeWare 6.2.

The command was modified to support Packet Memory scanning for Black Diamond I/O blades in ExtremeWare 6.2.1. See the Release Note for information on which blades are supported.

Platform Availability

This command is available on “*i*” series switches.

show debug-trace

```
show debug-trace [accounting | bootprelay | card-state-change | debug-link|
dvmrp-cache | dvmrp-hello | dvmrp-message | dvmrp-neighbor | dvmrp-route |
dvmrp-timer | e1 | eaps-system | eaps-slave-msm | flow-redirect | flowstats
| health-check | iparp | iproute | ipxgns-messages | ipxrip-message |
ipxrip-route | ipxsap-entry | ipxsap-message | isis-cli | isis-event |
isis-hello | isis-lsp | isis-snp | isis-spf | lcp | mpls | mpls-signaling |
nat | ncp | netlogin | npcard | npdiag | pim-cache | pim-hello |
pim-message | pim-neighbor | pim-rp-mgmt | pppauth | ppphexdump |
rip-message | rip-route-change | rip-triggered-update | slave-msm |
slb-3dns | slb-connection | slb-failover | snmp-trace | stp-in-pdu |
stp-out-pdu | stp-system | t1 | t3 | transceiver-test | udp-forwarding |
vrrp | vrrp-hello | xp] vlan <vlan name>
```

Description

Displays the configured debug-trace levels.

Syntax Description

accounting	Specifies accounting level.
bootprelay	Specifies BOOTP relay level.
card-state-change	Specifies card state change level.
debug-link	Specifies link detection level.
dvmrp-cache	Specifies DVMRP cache level.
dvmrp-hello	Specifies DVMRP hello level.
dvmrp-message	Specifies DVMRP message level.
dvmrp-neighbor	Specifies DVMRP neighbor level.
dvmrp-route	Specifies DVMRP route level.
dvmrp-timer	Specifies DVMRP timer level.
e1	Specifies E1level.
eaps-system	Specifies EAPS system level.
eaps-slave-msm	Specifies EAPS slave MSM level.
flow-redirect	Specifies flow redirect level.
flowstats	Specifies flow statistics level
health-check	Specifies health check level.
iparp	Specifies IP ARP level.
iproute	Specifies IP routing level.
ipxgns-messages	Specifies IPX GNS message level.
ipxrip-message	Specifies IPX RIP message level.
ipxrip-route	Specifies IPX RIP route level.
ipxsap-entry	Specifies IPX SAP entry level.
ipxsap-message	Specifies IPX SAP message level.
isis-cli	Specifies ISIS CLI level.
isis-event	Specifies ISIS event level.

isis-hello	Specifies ISIS hello level.
isis-lsp	Specifies ISIS LSP level.
isis-snp	Specifies ISIS SNP level.
isis-spf	Specifies ISIS SPF level.
lcp	Specifies LCP level.
mpls	Specifies MPLS level.
mpls-signaling	Specifies MPLS signaling level.
nat	Specifies NAT level.
ncp	Specifies NCP level.
netlogin	Specifies Network Login level.
npcard	Specifies NP card level
npdiag	Specifies NP diagnostic level.
pim-cache	Specifies PIM cache level.
pim-hello	Specifies PIM hello level.
pim-message	Specifies PIM message level.
pim-neighbor	Specifies PIM neighbor level.
pim-rp-mgmt	Specifies PIM RP level.
pppauth	Specifies PPP authorization level
ppphexdump	Specifies the level of the PPP hex dump.
rip-message	Specifies RIP message level.
rip-route-change	Specifies RIP route level.
rip-triggered-update	Specifies RIP triggered update level.
slave-msm	Specifies slave MSM level.
slb-3dns	Specifies SLB 3DNS level.
slb-connection	Specifies SLB connection level.
slb-failover	Specifies SLB failover level.
snmp-trace	Specifies SNMP trace level.
stp-in-pdu	Specifies incoming STP PDU level.
stp-out-pdu	Specifies outgoing STP PDU level.
stp-system	Specifies STP system level.
t1	Specifies T1 level.
t3	Specifies T3 level.
transceiver-test	Specifies transceiver-test level.
udp-forwarding	Specifies UDP forwarding level.
vrrp	Specifies VRRP level.
vrrp-hello	Specifies VRRP hello level.
xp	Specifies XP level.
vlan name	Specifies a VLAN name.

Default

N / A.

Usage Guidelines

Use this command to display the debug trace level configured for a particular system, and VLAN. Some of the debug trace systems commands can be applied to a particular VLAN, some apply to the switch as a whole, so the `vlan` option is not available with all systems.

Example

The following command displays the debug trace levels configured:

```
show debug-trace
```

Following is the output from this command:

```
OSPF SPF                            3
Flowstats                           3

Vlan                    Debug                   Level
-------------------------------------------------------------------------
v49                     DVMRP route             3

Port Number             Debug                   Level
-------------------------------------------------------------------------
No port-based debug-tracing configured
```

History

This command was first available in ExtremeWare 6.1.

Beginning in ExtremeWare 7.1.0, many debug trace facilities were moved to EMS.

Platform Availability

This command is available on all platforms.

show diagnostics

```
show diagnostics {slot [<slot number> | msm-a | msm-b]}
```

Description

Displays the status of the system health checker as well as information from the last diagnostic test run on the switch.

Syntax Description

slot number	Specifies the slot number of an I/O module.
msm-a | msm- b	Specifies the MSM64i.

Default

N/A.

Usage Guidelines

Use this command to display the status of the system health checker as well as information from the last diagnostic test run on the switch. The switch diagnostics are displayed in a tabular format with the day, month, date, year, and time of the diagnostic test at the top of the table.

Table 30: Show Diagnostics Command Field Definitions

Field	Definitions
System Platform	Specifies system type.
System Part No.	Specifies system part number, revision level, and serial number.
Main Board No.	Specifies main board part number, revision level, and serial number.
MAC Address	Specifies system MAC address.
Slot	Specifies the slot for which the results are displayed.
CPU System	Indicates diagnostic results.
Registers Test	Indicates diagnostic results.
Memory Test	Indicates diagnostic results.
System Test	Indicates diagnostic results.

To run diagnostics on a I/O module or MSM64i, use the following command:

```
run diagnostics [extended | normal] slot [msm-a | msm-b | <slot number>]
```

Depending on the software version running on your switch or the model of your switch, additional or different diagnostics information might be displayed.

Example

The following command displays the results of module diagnostics for the MSM64i in slot B:

```
show diagnostics slot msm-b
```

The results are similar to the following:

```
--------------------------------------------------------------------------
        Diagnostic Test Result run on Thu Jan 31 14:59:26 2002


--------------------------------------------------------------------------
Slot           :   B
--------------------------------------------------------------------------
CPU System     |   Passed
--------------------------------------------------------------------------
Registers Test |   Passed
--------------------------------------------------------------------------
Memory Test    |   Passed
--------------------------------------------------------------------------
System Test    |   Passed
--------------------------------------------------------------------------
```

The following command shows the results of diagnostics run on a stand-alone switch:

```
show diagnostics
```

The results are similar to the following:

```
--------------------------------------------------------------------------
        Diagnostic Test Result run on Thu Sep 14 16:01:15 2000


--------------------------------------------------------------------------
CPU System     |   Passed
--------------------------------------------------------------------------
Registers Test |   Passed
--------------------------------------------------------------------------
Memory Test    |   Passed
--------------------------------------------------------------------------
System Test    |   Passed
--------------------------------------------------------------------------
```

History

This command was available in ExtremeWare 4.1.19, and in ExtremeWare 6.1.5.

The command was modified to include MSM64i modules in ExtremeWare 6.1.9.

The command was modified to support Alpine and Summit switches in ExtremeWare 6.2.

Platform Availability

This command is available on all platforms.

show diagnostics backplane arm mapping

```
show diagnostics backplane arm mapping {active}
```

Description

Displays diagnostic information related to the ARM module internal backplane switch ports. This command also displays the external I/O port to internal ARM module backplane switch port mappings.

Syntax Description

active	Specifies to limit the port mapping display to active external I/O ports only.

Default

N/A.

Usage Guidelines

This command is only supported when the backplane load-sharing policy mode is port-based. If the active parameter is specified, the port mapping display is limited to active external I/O ports only. Used in conjunction with the `show diagnostics backplane utilization` command, these commands are helpful for diagnosing over-subscription problems related to backplane I/O port switch mappings.

Example

The following command displays diagnostic information related to the ARM module internal backplane switch ports:

```
show diagnostics backplane arm mapping
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the ARM module in the BlackDiamond switch.

show diagnostics backplane mpls mapping

```
show diagnostics backplane mpls mapping {active}
```

Description

Displays diagnostic information related to the MPLS module internal backplane switch ports. This command also displays the external I/O port to internal MPLS module backplane switch port mappings.

Syntax Description

active	Specifies to limit the port mapping display to active external I/O ports only.

Default

N/A.

Usage Guidelines

This command is only supported when the backplane load-sharing policy mode is port-based. If the active parameter is specified, the port mapping display is limited to active external I/O ports only. Used in conjunction with the `show diagnostics backplane utilization` command, these commands are helpful for diagnosing over-subscription problems related to backplane I/O port switch mappings.

Example

The following command displays diagnostic information related to the MPLS module internal backplane switch ports:

```
show diagnostics backplane mpls mapping
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the MPLS module in the BlackDiamond switch.

show diagnostics backplane utilization

```
show diagnostics backplane utilization
```

Description

Displays backplane link utilization information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Displays information including:

- Real-time traffic utilization on configured backplane links between active modules and MSM64i modules.
- The number of packets transmitted and received.
- The percentage of bandwidth used on the link.

Backplane utilization statistics can be reset by pressing 0 while the information is being displayed.

Example

The following command displays backplane link utilization information:

```
show diagnostics backplane utilization
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on the ARM and MPLS modules in the BlackDiamond switch.

show diagnostics packet-memory slot

```
show diagnostics packet-memory [slot <slot number>]
```

Description

Displays the results of the packet memory scan on BlackDiamond 6808 and BlackDiamond 6816 I/O modules.

Syntax Description

slot number	Specifies the slot number of an I/O module.

Default

N/A.

Usage Guidelines

Use this command to display the results of a packet memory scan. The command output displays the number of defects identified, and the number that were recoverable. If packet memory defects were found, it displays information about each defect.

In ExtremeWare 6.2.1, this applies only to the G8Xi, G8Ti, G12SXi, and F48Ti. MSM blades are not supported in this release. In ExtremeWare 6.2.2, this apples to all “i”series modules and switches.

Example

The following command displays the results of a PM scan for slot 2, where a single defect was found:

```
show diagnostics packet-memory slot 2
```

If no defects are found, the output will look similar to the following:

```
-----------------------------------------------------
         Packet memory defect info for card 1
-----------------------------------------------------

Num of defects = 0, num of recoverable defects = 0


-----------------------------------------------------
```

If defects are found, the output displays the number of defects, and provides information about each identified defect.

```
-----------------------------------------------------
         Packet memory defect info for card 2
-----------------------------------------------------

Num of defects = 1, num of recoverable defects = 1

Defect information:

Defect entry 1
```

```
        recoverable = 0
        mem ID = 9
        bit position = 0
        address = 0x18baa

-------------------------------------------------------
```

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all “i” series switches.

show diagnostics slot fdb

```
show diagnostics slot <slot-number> fdb {<mac_address> | vlan <vlan name> |
tls-tunnel <tunnel_name>}
```

Description

Displays the MAC cache for a specific MPLS module.

Syntax Description

slot number	Specifies a slot.
mac_address	Specifies the MAC cache entry.
vlan name	Specifies a name of a VLAN.
tunnel_name	Specifies a tunnel name.

Default

By default, the entire MAC cache is displayed.

Usage Guidelines

This command displays the MAC cache for a specific MPLS module. By default, the entire MAC cache is displayed. If you specify the <mac_address> parameter, only the matching MAC cache entry is displayed. Specifying the VLAN displays all MAC cache entries learned on the VLAN. Specifying the TLS tunnel displays all MAC cache entries learned on the TLS tunnel. The MAC address, VLAN name, and TLS tunnel name are displayed for each MAC cache entry.

Example

The following command displays the MAC cache entries learned on the VLAN test_1 for the MPLS module in slot 2:

```
show diagnostics slot 2 fdb vlan test_1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare 6.1.8b12.

This command was subsequently updated in ExtremeWare 7.0.0.

Platform Availability

This command is available on the BlackDiamond switch only.

show system-dump

```
show system-dump
```

Description

Displays the system-dump server IP and dump-timeout.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to display configured parameters for a system dump transfer. Dump transfers should not be initiated without the assistance of Technical Support.

Following are the fields displayed:

Server ip	Displays the IP address to which a triggered system dump is sent. Indicates whether the server is reachable through the VLAN *mgmt*.
Dump timeout	Displays the time in seconds until a system dump transfer is halted.

To specify the IP address to which a system dump is sent, use the following command:

```
configure system-dump server
```

To specify the timeout, use the following command:

```
configure system-dump timeout
```

Example

The following command displays the system-dump server IP and dump-timeout:

```
show system-dump
```

Following is the output from this command with nothing configured:

```
Server ip : none
Dump timeout : none
```

Following is the output from this command with both an IP address and timeout configured:

```
Server ip : 10.5.2.82 (ok)
Dump timeout : 300 seconds
```

Following is the output from this command with an unreachable IP address:

```
Server ip : 1.2.3.4 - currently unreachable via "Mgmt" vlan
```

```
Dump timeout : 300 seconds
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on platforms with an Ethernet management port.

show tech-support

```
show tech-support
```

Description

Displays the output of various show commands to assist in monitoring and troubleshooting the switch.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

The `show tech-support` command displays the output for the following show commands:

- show version
- show switch
- show configuration
- show diag
- show slot
- show fdb
- show iparp
- show ipfdb
- show ipstats
- show iproute
- show ipmc cache detail
- show ipmc fdb
- show igmp snooping detail
- show memory detail
- show log

It also displays the output from internal debug commands. This command disables the CLI paging feature.

This information can be useful for your technical support representative if you experience a problem.

Depending on the software version running on your switch, additional or different show command output is displayed.

Example

The following command displays the show command output on the switch:

```
show tech-support
```

History

This command was first available in ExtremeWare 6.1.9.

This command was modified to capture the `show ipmc fbd` command output in ExtremeWare 6.22.

Platform Availability

This command is available on all platforms.

top

```
top
```

Description

Displays real-time CPU utilization information by process.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Use this command to show the percentage of CPU processing devoted to each task, sampled every 30 seconds. In a healthy ExtremeWare system, only the BGTask takes up significant CPU processing power. Investigate tasks showing consistent or periodic high CPU utilization.

You can change the display by typing a character while the display is active. These single character commands are as follows:

Table 31: TOP command display options

u	Go up one screen
d	Go down one screen
c	Clear max utilization
%	Sort tasks by CPU utilization
t	Sort tasks by task id
p	Sort tasks by program counter
n	Sort tasks by name
s	Sort tasks by task state
m	Sort tasks by max CPU utilization
h	Show the help screen
<space>	go to next sort type
q <esc> <return>	Exit top

The following table defines the tasks. Depending on your switch model and the functions it is executing, you will see only a subset of these tasks.

Table 32: ExtremeWare Task Descriptions

Task	Description
httpd	The HTTP daemon task manages the HTTP web management interface on the system.
Logpoll	In an active dual CPU system, the master CPU will initiate the log polling task (Logpoll) to periodically poll the secondary or slave CPU(s). This process clears the individual syslogs and consolidates them onto the master CPU switch log.
mportTask	The management port task.
pifstate	The port interface state task (pifstate) processes port link state changes. It is watchdog timer poll driven as opposed to interrupt driven by hardware events.
tAsyncSave	The tAsyncSave tasks the NVRAM asynchronous save/write processing task. This process manages the save or writes to the NVRAM.
tbgpTask	The border gateway protocol task (tbgpTask) implements and processes BGP on the switch.
tbgpTimerTask	The BGP internal process timer task (tbgpTimerTask) manages the internal BGP timer delays for checking BGP networks and next hops.
tBgQosMon	The background Quality of Service monitor task (tBgQosMon) is a background version of the QoS monitoring task that monitors transmit count and kill count of ports and cycles as long as the monitor is enabled.
tBGTask	The background task (tBGTask) is the core task switching process. It receives packets from the hardware ASICs and switches them to the appropriate functional task to process that packet type or group. The tBGTask typically runs with a high CPU utilization (90% or greater). It is constantly checking for packets to be sent up by the hardware ASICs. It only releases control of the CPU if packets are sent to the switch or if timer functions signal another task to become active.
tCardTask	The I/O card event task (tCardTask) manages the event signaling hardware and state machine for the I/O cards in a chassis-based system.
tChecksumPoll	The checksum polling task (tChecksumPoll) periodically polls the boards for fabric checksum errors.
tConsole	The console task.
tdiagTask	The diagnostic task (tdiagTask) executes the diagnostic routines for the particular hardware platform.
tDvmrpTask	The distance vector multicast routing protocol task (tDvmrpTask) implements and processes DVMRP on the switch.
tEapsTask	The Ethernet automatic protection switching task implements and processes EAPS on the switch.
tEdpTask	The Extreme Discovery Protocol task (tEdpTask) implements and processes the EDP neighbor discovery process.
tEsrpTask	The Extreme Standby Router Protocol (tEsrpTask) implements and processes ESRP on the switch.
tExcTask	If the operating system recognizes an exception condition, it will invoke the exception handling task (tExcTask).
tFastTimer	The fast timer task (tFastTimer) is used to maintain a queue of timer events triggering periodic or single event functions. These events have a small delay in time between re-occurrences. The tFastTimer has a higher priority than the slow timer task (tSlowTimer). Therefore, tFastTimer events are processed prior to iSlowTimer events occurring at the same time.
tfdbAgeTask	The forwarding database aging task (tfdbAgeTask) performs the aging of MAC FDB entries in the hardware and software tables.
tIpxTask	The IPX input task (tIpxTask) handles inbound IPX control packets such as RIP, SAP, and Xping.

Table 32: ExtremeWare Task Descriptions (continued)

Task	Description
tIpxTx	The IPX transmit task (tIpxTx) handles the IPX transmission of control packets such as RIP and SAP.
tIquery	The iQuery support task for 3DNS (tIquery) processes iQuery requests.
TIRDP	The ICMP router discovery protocol task (tIRDP) implements and processes IRDP on the switch.
tISRtask	The interrupt service routine task (tISRtask) manages the interrupt driven port link state changes.
tLinkEvent	The link event task (tLinkEvent) is the interrupt driven link event processing task. It handles hardware interrupts for link events.
tMACPoll	The media access controller poll task (tMACPoll) polls the various MAC PHY chips on the switch to pull up MAC Layer control messages for the CPU to process.
tmt32LinkPoll	F32F module link poll task.
tmuTelnetd	The telnet daemon task.
tNetTask	The network stack task (tNetTask) handles all the software-based processing of packets including: • Packets that cannot be handled by the switch's ASIC because the forwarding tables do not have entries built in. • Packets destined to the CPU for one of the router interfaces. • Packets that must be examined or snooped by the CPUPackets detected for copying to the CPU.
tNMCEvent	The network management controller event task (tNMCEvent) manages event signaling hardware and state machine on a BlackDiamond switch's redundant MSM CPU modules.
tOpenPort	A server load balancing (SLB) Layer 4/Layer 7 health check sub-task.
tospfMsgTask	The OSPF message processing task (tospfMsgTask) implements and manages the processing of OSPF messages.
tospfSpfTask	The OSPF shortest path forward task (tospfSpfTask) executes the SPF algorithm run processing for OSPF.
tospfTimer	The OSPF timer task (tospfTimer) manages the internal timer trigger functions and delays for OSPF.
tPCSPoll	The tPCSPoll task services the Gigabit Ethernet PCS poll messages.
tPhyPoll	The PHY layer poll task (tPhyPoll) polls the Road Runner PHY layer every 2 seconds to verify the proper operation.
tPimTask	The protocol independent multicast task (tPimTask) implements and processes PIM on the switch.
tPingServer	The server load balancing (SLB) Layer 3 ping health check sub-task.
tPortProbe	A server load balancing (SLB) Layer 4/Layer 7 health check sub-task.
tPortUtilization	The port utilization data collection task (tPortUtilization) is a 30 second task that pulls physical port data statistics from the hardware and updates the software database tables.
tRip	The Routing Information Protocol task (tRip) implements and processes RIP on the switch.
tRipTimer	The RIP timer task (tRipTimer) manages the internal timer trigger functions and delays for RIP.
TRmonTask	The remote monitoring task
tRRPoll	The Road Runner poll task (tRRPoll) pulls the MAC and PHY layer statistics from the store in the software based tables.

Table 32: ExtremeWare Task Descriptions (continued)

Task	Description
tRxMsgTask	The receive message task (tRxMsgTask) is located on the secondary system. ExtremeWare 6.2 commences use of the secondary CPU in BlackDiamond switches. This is the secondary slave CPU inter-CPU receive task.
tServAlive	The server load balancing (SLB) health check server task.
tShell	The core operating system internal shell process (tShell) is spawned whenever the internal shell is accessed.
tSlbFailover	The server load balancing failover task.
tSlowTimer	The slow timer task (tSlowTimer) maintains a queue of timer events triggering periodic or single event functions. Typically these events have a large period gap in terms of time between recurrences.
tsmartTrap	Extreme smart trap task.
tSnmpd	The SNMP daemon task manages all SNMP processing on the system.
tSntpc	The simple network time protocol client task (tSntpc) implements the SNTP client function and processing.
tsshshell	The secure shell (SSH) task.
tStatsPoll	The port interface statistics poll task (tStatsPoll) polls the port interfaces for statistic counters.
tstpTask	The Spanning Tree protocol task (tstpTask) implements the STP algorithm and processing.
tSwFault	The software fault handler task (tSwFault) will perform a stack dump for any task that has crashed.
tsyslogTask	The system log task (tsyslogTask) receives messages/text from other tasks and asynchronously logs these to the switch NVRAM log area.
tTimeout	The Timeout task (tTimeout) is used to manage and execute various functions on timeouts.
tTRRecv	The trace route receiver task (tTrRecv) is spawned dynamically when the trace route utility is used.
tvrrpTask	The virtual router redundancy protocol task (tvrrpTask) implements and processes VRRP on the switch.

Investigate tasks that, for no apparent reason, show CPU utilization consistently above 25% (except for the BGTask). Configure the appropriate debug-trace command and look for messages indicating a problem. Common problems are source or destination addresses.

Example

The following command displays the show command output on the switch:

```
top
```

The output of this command looks similar to the following:

```
Total number of tasks: 46
Task Name       Task Id         Task PC         Status   % CPU Max % util
================================================================================
   tBGTask      836f18e0        80748f98        READY        99   99
  tExcTask      8137ce90        8075ab2c        PEND          0    0
  tLogTask      8135e2a0        8075ab2c        PEND          0    0
tSlowTimer      813ccf50        8075ab2c        PEND          0    0
tFastTimer      813ff1f0        8075ab2c        PEND          0    0
```

```
  tTimeout      81384f50        8075ab2c        PEND          0    0
tsyslogTas      81389660        8075ab2c        PEND+T        0    0
tledPollTa      81390ef0        8075ab2c        PEND          0    0
tAsyncSave      814feb10        8075ab2c        PEND          0    0
 tpifstate      81a85590        8075ab2c        PEND          0    0
  tbgpTask      81eaacd0        807169f4        PEND+T        0    0
tbgpTimerT      81eaecd0        80749164        DELAY         0    0
 tBgQosMon      81eb6be0        8075ab2c        PEND          0    0
 tEapsTask      82bd2a00        8075ab2c        PEND          0    0
  tSwFault      82c75530        8075ab2c        PEND          0    0
tFdbAgeTas      82c85530        8075ab2c        PEND          0    0
tFdbSyncTa      82c89530        807489a0        SUSPEND       0    0
 tdiagTask      82c8d620        8075ab2c        PEND          0    0
  tIpxTask      82c91620        8075ab2c        PEND          0    0
    tIpxTx      836e97f0        8075ab2c        PEND          0    1
Press ‘h’ for help
```

History

This command was available in ExtremeWare 4.0.

Platform Availability

This command is available on all platforms.

unconfigure system-dump

```
unconfigure system-dump
```

Description

Unconfigures the system dump.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Returns the system-dump configuration to the defaults.

Example

The following command unconfigures the system dump:

```
unconfigure system-dump
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on platforms with an Ethernet management port.

upload system-dump

```
upload system-dump [<ip address>]
```

Description

This command transfers a system dump to an IP address.

Syntax Description

ip address	Specifies the IP address to which to transfer a system dump.

Default

N/A.

Usage Guidelines

If you do not specify an IP address, the configured system-dump server IP address is used.

Example

The following command transfers a system dump to 10.10.10.1:

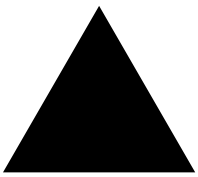
```
upload system-dump 10.10.10.1 3
```

History

This command was first available in ExtremeWare 6.2.2.

Platform Availability

This command is available on platforms with an Ethernet management port.



Index of Commands

D

E

T

U

X