COMMON Command Line Interface Reference Manual 9.0

12.21.2001

ENTERASYS NETWORKS™

9033603-01

ELECTRICAL HAZARD: Only qualified personnel should perform installation procedures.

NOTICE

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
35 Industrial Way
Rochester, NH 03866-5005

Order Number: 9033603-01 December 2001

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

INDUSTRY CANADA NOTICE

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CLASS A ITE NOTICE

WARNING: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

ENTERASYS NETWORKS, INC.
PROGRAM LICENSE AGREEMENT

**BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT,
CAREFULLY READ THIS LICENSE AGREEMENT.**

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc. ("Enterasys") that sets forth your rights and obligations with respect to the Enterasys software program ("Program") in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS (603) 332-9400. Attn: Legal Department.

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Enterasys.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

4. EXPORT REQUIREMENTS. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. EXCLUSION OF WARRANTY. Except as may be specifically provided by Enterasys in writing, Enterasys makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

ENTERASYS DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY ENTERASYS IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS ENTERASYS PRODUCT, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.

DECLARATION OF CONFORMITY

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer's Name:	**Enterasys Networks, Inc.**
Manufacturer's Address:	**35 Industrial Way** **PO Box 5005** **Rochester, NH 03867**
European Representative Name:	**Mr. Jim Sims**
European Representative Address:	**Enterasys Networks Ltd.** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG14 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EC Directive 73/23/EEC** **EN 55022** **EN 55024** **EN 60950** **EN 60825**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

Enterasys Networks, Inc. declares that the equipment packaged with this notice conforms to the above directives.

Contents

About This Manual

This manual provides reference information for the commands in the Enterasys Xpedition Command Line Interface (CLI). For product information not available in this manual, see the manuals listed in *Related Documentation* on page xvi.

What's New?

The latest revision of the *Enterasys Xpedition Common Command Line Interface Reference Manual* includes the following changes:

- Additional information has been added to the safety notice and licensing information printed at the beginning of this guide. It is recommended that the user become familiar with this information before installing or operating the product.

Who Should Read This Manual?

Read this manual if you are a network administrator responsible for configuring or managing the Xpedition.

What is Included in This Manual?

This manual includes definitions, descriptions and parameters on all **show** commands, as well as all **non-persistent command sets** available in the Common CLI syntax with the 3.1 firmware release. Please note that it does not include command sets implemented with the E8.0.0.0 release or above.

How to Use This Manual

The CLI commands and facilities are organized alphabetically in this manual. To locate information about a command, go to the chapter for the command or for the facility that contains the command. For example, to find information about the **enable** command, go to *enable Command* on page 65. To find information about the

show file command, go to *file Commands* on page 73, then locate the description of the **show file** command within that chapter.

Related Documentation

The Xpedition documentation set includes the following items. Refer to these other documents to learn more about your product.

For Information About...	See the...
Installing and setting up the Xpedition	*Enterasys [Product Number] Getting Started Guide*
How to use CLI (Command Line Interface) commands to configure and manage the Xpedition	*Enterasys Xpedition User Reference*
SYSLOG messages and SNMP traps	*Enterasys Xpedition Error Reference Manual*

CLI Parameter Types

The following table describes all the parameter types supported by the CLI.

Data Type	Descripton	Example
conditional	A numerical conditional expression. Special symbols are used to describe a numerical condition: > (greater than), < (less than) and != (not equal to).	<1024 or >2048 or !=4096
hexadecimal	A hexadecimal number	a7 or 0xa7
hostname	Hostname of an IP host	gauguin or john-pc
hostname/IP	Hostname or IP address of a host	nagasaki or 10.43.1.4
keyword	A keyword described in the list of acceptable keywords in the online help	on or off
interface name	Name of a single port, or vlan with created interface	ethernet1/4 or vlan100
IP address	An IP address of the form x.x.x.x. Some commands may explicitly require a unicast or multicast address.	10.1.2.3

Data Type	Descripton	Example
IP address list	A list of IP addresses separated by spaces but enclosed in quotes.	“10.1.4.4 10.1.5.5 10.1.6.6”
IPX network address	An IPX network address in hexadecimal	
IPX network**.**node address	An IPX network and node address of the form <netaddr>.<macaddr> where <netaddr> is the network address of a host and <macaddr> is the node or MAC address of the IPX host. For some commands, if the node address is not given, the node address is assumed to be a wildcard.	a1b2c3d4.08:20:a1:f3:38:11 or aa89f383
IPX SAP server name	An alphanumeric string representing a valid IPX SAP server name where the following characters are illegal: “*. / :;<=>?[] \ |	server1
MAC address	A MAC address specified in one of two forms: xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx	08:00:50:1a:2b:c3 or 080050:1a2bc3
number	An integer number	100
numerical range	A number or a range of numbers	3,5 or 7-10
port	A single port	ethernet1 / 4, gigabit2 / 1, hssi3 / 1 / 100, or serial4 / 2 / 200
port list	A list of one or more ports. To specify a range of ports within a module, describe the range in parenthesis. You can also specify non-consecutive ports by using commas to separate them.	gigabit1 / 3-8 or ethernet1 / (1,3,5), hssi(1-2) / 1 / 100, or serial4 / (1-3) / 200
slot number	A list of one or more occupied slots in the Xpedition	1 or 7

Data Type	Descripton	Example
IPX network address	An IPX network address in hexadecimal	
IPX network.node address	An IPX network and node address of the form <netaddr>.<macaddr> where <netaddr> is the network address of a host and <macaddr> is the node or MAC address of the IPX host. For some commands, if the node address is not given, the node address is assumed to be a wildcard.	a1b2c3d4.08:20:a1:f3:38:11 or aa89f383
IPX SAP server name	An alphanumeric string representing a valid IPX SAP server name where the following characters are illegal: “*. / :;<=>?[] \ |	server1
MAC address	A MAC address specified in one of two forms: xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx	08:00:50:1a:2b:c3 or 080050:1a2bc3
number	An integer number	100
numerical range	A number or a range of numbers	3,5 or 7-10
port	A single port	ethernet1 / 4, gigabit2 / 1, hssi3 / 1 / 100, or serial4 / 2 / 200
port list	A list of one or more ports. To specify a range of ports within a module, describe the range in parenthesis. You can also specify non-consecutive ports by using commas to separate them.	gigabit1 / 3-8 or ethernet1 / (1,3,5), hssi(1-2) / 1 / 100, or serial4 / (1-3) / 200
slot number	A list of one or more occupied slots in the Xpedition	1 or 7

Data Type	Descripton	Example
string	A character string. To include spaces in a string, specify the entire string in double quotes (“).	abc or “abc def”
URL	A Uniform Resource Locator. The type of URL depends on the command where the URL is used. Currently, two URLs are supported: TFTP: *tftp://host/pathname* RCP: *rcp://username@host/pathname*	tftp://10.1.4.5/test/abc.txt rcp://dave@rtr/test/abc.txt

Getting Help

For additional support related to the Common CLI syntax or this document, contact Enterasys Networks using one of the following methods:

World Wide Web	http://www.enterasys.com/
Phone	(603) 332-9400
Internet mail	support@enterasys.com
FTP	ftp://ftp.enterasys.com
Login	*anonymous*
Password	*your email address*

To send comments or suggestions concerning this document, contact the Technical Writing Department via the following email address: **TechWriting@enterasys.com**

Please include the document Part Number in the email message.

Before contacting Enterasys Networks, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)

- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

Changing the CLI Syntax

The Enterasys Xpedition firmware is designed to move easily between Native and Common CLI syntax.The following information instructs the user on maneuvering back and forth between these syntaxes.

Moving From Native to Common CLI Syntax

In order to switch from Native to Common CLI syntax, the Xpedition must first be in **Enable** mode. For more about Enable mode, see the *Enterasys Xpedition Native Command Line Interface Manual*. By default, the Xpedition boots up in User mode, under the Native CLI syntax engine.

When the Xpedition is in Enable mode, enter the following command:

```
ssr# cli set common
```

This command will switch the Xpedition over to Common CLI syntax.

Moving From Common to Native CLI Syntax

If the user wishes to switch back to the Native CLI syntax, the following command should be entered while in Common CLI **Privileged** mode:

```
ssr# terminal cli native
```

This command will return the Xpedition CLI to the Native syntax. For more information on Privileged mode, please see *enable Command* on page 65. For more information on the **terminal cli native** command, see *terminal cli native Command* on page 351

Note: The current CLI syntax is saved in the system NVRAM. This means that if the user reboots the Xpedition while in Native CLI syntax, it will start up in Native CLI syntax; likewise, if the Xpedition is rebooted while in Common CLI syntax, it will start up in Common CLI syntax.

Chapter 1

access-list Commands

The **access-list** commands allow the user to clear ACL (Access Control List) counters and display those Access Control Lists currently configured on the Xpedition

Command Summary

Table 1 lists the **access-list** commands. The sections following the table describe the command syntax.

Table 1. access-list commands

clear access-list counters <*num*> **|** <*name*>
show access-lists [<*num*> **|** <*string*> **| {interface** <*string*> **| all-ip}	service	{port** <*port-list*> **| all-ports}]**

clear access-list counters

Purpose

Clears one or all ACL counters.

Format

clear access-list counters <*num*> | <*name*>

Mode

Enable

Description

The **clear access-list counters** command allows the user to clear Access Control List counters.With ACL logging enabled, the router prints out a message verifying whether a packet is forwarded or dropped, and counters record these statistics. With this command, the user can clear the ACL counters.

Parameters

<*num*>	Clears counter based on the ACL number.
<*name*>	Clears counter based on the name of the ACL.

Restrictions

None.

Example

To clear counters for Access Control List 100:

```
clear access-list counters 100
```

show access-lists

Purpose

Displays one or more ACLs.

Format

show access-lists [<*num*>**|** <*string*>**|{interface** <*string*>**|all-ip}|service|{port** <*port-list*>**|all-ports}]**

Mode

Enable

Description

The **show access-lists** command allows the user to display currently configured Access Control Lists. The parameters associated with this command further allow the user to sort and display ACLs by name, interface, port, or service type.

Parameters

<*num*> Specifies ACL number.

<*string*> Specifies ACL name.

interface Displays ACLs attached to a specific interface.

- <*string*> Specifies name of interface
- **all-ip** Specifies all interfaces.

service Displays ACLs applied to services

port Displays ACLs applied to a specific port(s).

- <*port-list*> Specifies list of port(s).
- **all-ports** Specifies display of ACLs applied to all ports.

Restrictions

None.

Chapter 2

aging Commands

The **aging** commands control aging of learned MAC address entries in the Xpedition's L2 lookup tables or layer3/4 flows. Using the **aging** commands, you can show L2 or layer 3/4 aging information, set or disable L2 aging on specific ports, set or disable aging of layer 3/4 flows, or set or disable NAT or LSNAT flows.

Command Summary

Table 2 *lists the **l2** and **l3** aging commands. The sections following the table describe the command syntax.*

Table 2. aging commands

show mac-address-table aging-time
show mls aging

show mac-address-table aging-time

Purpose

Shows the L2 aging status for SwitchRouter ports.

Format

show mac-address-table aging-time

Mode

User

Description

The **show mac-address-table aging-time** command shows whether L2 aging is enabled or disabled on SwitchRouter ports. For ports on which L2 aging is enabled, this command also shows the aging time.

Parameters

None.

Restrictions

None.

show mls aging

Purpose

Shows the L3 aging status for Xpedition ports.

Format

show mls aging

Mode

User

Description

The **show mls aging** command shows whether L3/4 aging is enabled or disabled on Xpedition ports. For ports on which L3/4 aging is enabled, this command also shows the aging time.

Parameters

None.

Restrictions

None.

Example

To show whether layer 3/4 aging is enabled and the aging time for enabled ports:

```
ssr# show mls aging
L3 Aging: Timeout 30 seconds
```

Chapter 3

arp Commands

The **arp** commands enable you to add, display, and clear Address Resolution Protocol (ARP) entries on the Xpedition.

Command Summary

Table 3 lists the **arp** commands. The sections following the table describe the command syntax.

Table 3. arp commands

arp add <*host*> **mac-addr** <*MAC-addr*> **exit port** <*port*> **keep time** <*seconds*>
arp clear <*host*> **mac-addr** <*MAC-addr*> **exit port** <*port*> **keep time** <*seconds*>
arp show <*IPaddr*> **| all [undecoded] [unresolved] [interface** <*string*> **| all] [port** <*port*>**]**
show arp statistics <*IFname*>

arp add

Purpose

Adds an ARP entry.

Format

arp add <*host*> **mac-addr** <*MAC-addr*> **exit-port** <*port*> **keep-time** <*seconds*>

Mode

Privileged

Description

The **arp add** command allows the user to manually add ARP entries to the ARP table. Typically, the Xpedition creates ARP entries dynamically. Using the **arp add** command, you can create an ARP entry to last a specific amount of time. If the exit port is not specified, then packets to the IP address for which the ARP entry is created are transmitted on all ports of the interface. If an ARP request is received from the host for which the ARP entry was created, then the exit port is updated with the port on which the ARP request was received, so that subsequent packets are transmitted on one port only.

Parameters

<*host*>	Hostname or IP address of this ARP entry.
mac-addr <*MAC-addr*>	MAC address of the host.
exit-port <*port*>	The port for which you are adding the entry. Specify the port to which the host is connected.
keep-time <*seconds*>	The number of seconds this ARP entry should remain in the ARP table. A value of 0 means this is a permanent ARP entry.

Restrictions

None.

Examples

To create an ARP entry for the IP address 10.8.1.2 at port et.4.7 for 15 seconds:

```
ssr# arp add 10.8.1.2 mac-addr 08:00:20:a2:f3:49 exit-port et.4.7 keep-time 15
```

arp clear

Purpose

Removes an ARP entry from the ARP table.

Format

arp clear <*host*> **mac-addr** <*MAC-addr*> **exit-port** <*port*> **keep-time** <*seconds*>

Mode

Privileged

Description

The **arp clear** command lets you manually remove entries from the ARP table. The command can remove both dynamic and permanent entries.

Parameters

<*host*>	Hostname or IP address of the ARP entry to remove.
mac-addr <*MAC-addr*>	MAC address of the host.
exit-port <*port*>	The port for which you are clearing the entry. Specify the port to which the host is connected.
keep-time <*seconds*>	The number of seconds this ARP entry should remain in the ARP table. A value of 0 means this is a permanent ARP entry.

Examples

To remove the ARP for the host 10.8.1.2 from the ARP table:.

```
ssr# arp clear 10.8.1.2
```

To clear the entire ARP table.

```
ssr# arp clear all
```

arp show

Purpose

Displays the ARP table.

Format

arp show <*IPaddr*> **| all [undecoded] [unresolved] [interface** <*string*> **| all] [port <***port***>]**

Mode

Privileged

Description

The **arp show** command displays the entire ARP table.

Parameters

<*IPaddr*>	Shows the ARP entry for the specified IP address.
all	Shows all entries in the ARP table.
undecoded	Specify this optional parameter to show MAC addresses in hexadecimal format.
unresolved	Specify this optional parameter to show only MAC addresses in the ARP table that have yet to be mapped to an network layer address.
interface	Specify this optional parameter to show only addresses in the ARP table that is associated with the specific interface.
<*string*>	Specifies the interface name.
all	Specifies all interfaces.
port	Specify this optional parameter to show only addresses in the ARP table that corresponds to a specific exit port.
<*port*>	Specifies the exit port.

show arp statistics

Purpose

Displays ARP statistics.

Format

show arp statistics <*IFname*>

Mode

Privileged

Description

The **show arp statistics** command displays ARP statistics, such as the total number of ARP requests and replies.

Parameters

<*IFname*>	Displays ARP statistics for the specified interface. Failing to specify an interface will result in the display of ARP statistics for all interfaces.

Example

To display ARP statistics on interface ‘en0’:

```
ssr# show arp statistics en0

Interface en0:
      1 requests sent
      19 replies sent
      0 proxy replies sent
      Last 5 Requests Sent
      ----- no arp requests sent -----
      Last 5 Replies Sent
      134.141.179.129  | Yago     16:BF:21      |2000-04-17 13:12:49
      134.141.179.129  | Yago     16:BF:21      |2000-04-17 13:50:15
      134.141.179.129  | Yago     16:BF:21      |2000-04-17 15:32:32
      134.141.179.129  | Yago     16:BF:21      |2000-04-17 16:17:19
      134.141.179.129  | Yago     16:BF:21      |2000-04-17 11:12:44

      Last 5 ARP packets received on wrong interface
      ----- no arp packets received on wrong interface -----
```

- requests sent — Displays how many ARP requests have been sent out to an ARP server for address resolution.
- replies sent — Displays how many ARP replies have been sent out to an ARP client in response to request packets.
- proxy replies sent — Displays how many proxy ARP replies have been sent out in response to request packets. A proxy router serving as a gateway to a subnet would respond with a proxy reply.
- Last 5 Requests sent — Displays the last five ARP requests sent, including the following information: target MAC address, date and time sent.
- Last 5 Replies sent — Displays the last five ARP replies sent, including the following information: target IP address, date and time sent.
- Last 5 ARP packets received on wrong interface — Displays the last five ARP packets that has been received on the wrong interface.

Chapter 4

atm Command

The **show atm** command displays information specific to an Asynchronus Transfer Mode (ATM) port.

Format

show atm [vpl port <*port-list*>**] [vcl port** <*port-list*>**] [service** <*string*>**| all] [port-settings** <*port-list*> | **all-ports]**

Parameters

<*port list*> Is the port name, in the format: **`media.slot.port.vpi.vci`**

media Is the media type. This is **at** for an ATM port.

slot Is the slot number where the module is installed.

port Is the number of the port through which data is passing.

vpi Is the Virtual Path Identifier.

vci Is the Virtual Channel Identifier.

port-settings Shows the characteristics of an ATM port that were set by the **port set** command. Specify **all-ports** to show characteristics of all ATM ports.

service Shows all defined ATM service profiles. Specify **all** to show all ATM service profiles.

vcl port Shows VCL configurations on a port.

Specify **at.slot.port** to display all VCLs configured on the port.

Specify **at.slot.port.vpl** to display all VCLs for the specified VPL configured on the port.

Specify **at.slot.port.vpl.vcl** to display only the specified VCL configured on the port.

vpl port Shows VPL configurations on a port.

Specify **at.slot.port** to display all VPLs configured on the port.

Specify **at.slot.port.vpl** to display only the specified VPL configured on the port.

Restrictions

None.

Examples

To display information about the VPL configurations on ATM port 1:

```
ssr(atm-show)# vpl port at.9.1

VPL Table Contents for Slot 9, Port 1:
   Virtual Path Identifier: 1
   Adminstrative Status:    Up
   Operational Status:      Up
   Last State Change:       1581
   Service Definition:      ubr-default
      Service Class:      UBR
      Peak Bit Rate:      Best Effort
      Sustained Bit Rate: 0 Kbits/sec (0 cps)
      Maximum Burst Size: 0 cells
      Encapsulation Type: Routed LLC
      F5-OAM:             Requests & Responses
```

- Virtual Path Identifier — Identifies a particular VP.
- Administrative Status — Shows whether the VP is a viable network element.
  Up indicates a viable network element.
  Down indicates a non-viable network element.
- Operational Status — Shows whether the VP is passing traffic.
  Up indicates traffic.
  Down indicates no traffic.
- Last State Change — Shows the last time the VP went up or down. Time is in seconds relative to system bootup.

- Service Definition — Shows the name of the defined service and its traffic parameters

To display information about all the defined service profiles for UBR:

```
ssr# atm show service all

ubr-default
   Service Class:      UBR
   Peak Bit Rate:      Best Effort
   Sustained Bit Rate: 0 Kbits/sec (0 cps)
   Maximum Burst Size: 0 cells
   Encapsulation Type: Routed LLC
   F5-OAM:             Responses Only
```

- Service Class — Shows the type of service class.
  UBR indicates Unspecified Bit Rate
  CBR indicates Constant Bit Rate
  RT-VBR indicates Real-time Variable Bit Rate
  NRT-VBR indicates Non Real-time Variable Bit Rate
- Peak Bit Rate — Shows the maximum bit transmission rate.
- Sustained Bit Rate — Shows the average bit transmission rate (in Kilobits per second).
- Maximum Burst Size — Shows how many cells can be transmitted at the Peak Bit Rate.
- Encapsulation Type — Shows the encapsulation scheme to transport multi protocol data over the AAL5 layer.
  Routed-LLC indicates logical link control encapsulation (**default**).
  Routed-VCMUX indicates VC-based multiplexing encapsulation.
- F5-OAM — Shows how OAM (Operation, Administration, and Management) loopback cells provide loopback capabilities and confirm whether a VC connection is up. Only F5 OAM segments are supported, which provides loopback capabilities on a VC connection level.
  Responses Only indicates that the port will respond but doesn't generate OAM cells.
  Requests & Responses indicates that the port will respond and generate OAM cells.

To display port-setting information about ATM port 1:

```
ssr(atm-show)# port-settings at.9.1
Port information for Slot 9, Port 1:
   Port Type:         T3 ATM coaxial cable
   Xmt Clock Source:   Local
   Scramble Mode:      Payload
   Line Coding:        B3ZS
   Cell Mapping:       Direct
   Framing             Cbit-Parity
   VC Mode:            1 bit of VPI, 11 bits of VCI
   Service Definition: ubr-default
      Service Class:      UBR
      Peak Bit Rate:      Best Effort
      Sustained Bit Rate: 0 Kbits/sec (0 cps)
      Maximum Burst Size: 0 cells
      Encapsulation Type: Routed LLC
      F5-OAM:             Requests & Responses
```

- Port Type — Shows the type of PHY interface for the port.
- Xmt Clock Source — Shows the timing source for the port.
  Local indicates the onboard clock oscillator as the timing source.
  Loop indicates the receiver input as the timing source.
- Scramble Mode — Shows the scramble / descramble mode for the port.
  None indicates no scrambling.
  Payload indicates scrambling of the payload only.
  Frame indicates scrambling of the stream only.
  Both indicates scrambling of payload and stream.
- Line Coding — Shows the particular DS1 / T1 and DS3 / T3 coding convention.
- Cell Mapping — Shows the format used to map ATM cells.
  Direct indicates direct cell mapping.
  Plcp indicates physical layer convergence protocol mapping.
- Framing — Shows the type of framing scheme.
  cbit-parity is used for T3 framing.
  m23 is used for T3 framing.
  esf indicates extended super frame and is used for T1 framing.

	g832 is used for E3 framing. **g751** is used for E3 framing.
• VC Mode	Shows the bit allocation for VPI and VCI.
• Service Definition	Shows the name of the defined service on the port and its traffic parameters.

Chapter 5

bgp Commands

The **bgp** commands let you display and set parameters for the Border Gateway Protocol (BGP).

Command Summary

Table 4 lists the **bgp** commands. The sections following the table describe the command syntax.

Table 4. bgp commands

show ip bgp [<*IPaddr*><*IPmask*>**] [to-file]**
show ip bgp cidr-only <*IPaddr*> <*IPmask*> **[to-file]**
show ip bgp community {<*community-id*> <*as-num*>**| no export | no-advertise | no-export-subconfed | reserved-community** <*hex-num*>**} [to-file]**
show ip bgp neighbor <*IPaddr*> **received-routes | all-received-routes | advertised-routes [to-file]**
show ip bgp paths <*ASpath*> **[to-file]**
show ip bgp peer-as <*ASnum*> **[to-file]**
show ip bgp peer-group external | internal | igp | routing [to-file]
show ip bgp regexp <*exp*>
show ip bgp summary [to-file]
show ip bgp sync-tree

show ip bgp

Purpose

Displays entries in the BGP routing table.

Format

show ip bgp [<*IPaddr*><*IPmask*>**] [to-file]**

Mode

Privileged

Description

The **show ip bgp** command displays the IP address/netmask, next hop, and AS path for each BGP route.

Parameters

<*IPaddr*><*IPmask*>	Displays information about the specified route.
to-file	Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display the BGP routing table:

```
ssr# show ip bgp
Proto      Route/Mask NextHop        ASPath
BGP      172.16.70/24 172.16.20.2    (64900) 64901 IGP (Id 2)
BGP     172.16.220/24 172.16.20.2    (64900) 64901 IGP (Id 2)
BGP      192.68.20/24 172.16.20.2    (64900) 64901 IGP (Id 2)
BGP     192.68.222/24 172.16.20.2    (64900) 64901 64902 IGP (Id 3)
```

show ip bgp cidr-only

Purpose

Displays routes in the BGP routing table with CIDR network masks.

Format

show ip bgp cidr-only [*<IPaddr><IPmask>***] [to-file]**

Mode

Privileged

Description

The **bgp show cidr-only** command displays the same type of route information as the **show ip bgp** command. The difference is that the **show ip bgp cidr-only** command limits the display to CIDR routes only.

Parameters

<IPaddr><IPmask>	Displays information about the specified CIDR route.
to-file	Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display information all CIDR routes in the Xpedition's BGP route table:

```
ssr# bgp show cidr-only
Proto    Route/Mask NextHop        ASPath
BGP       12.2.19/25 207.135.89.65   (64800) 64753 64752 64751 6379 3561 11277 IGP (Id 13805)
BGP      12.5.172/22 207.135.89.65   (64800) 64753 64752 64751 6379 3561 1 IGP (Id 173)
BGP      12.5.252/23 207.135.89.65   (64800) 64753 64752 64751 6379 5646 1 7018 6301 IGP (Id 926)
BGP       12.6.42/23 207.135.89.65   (64800) 64753 64752 64751 6379 5646 1 7018 11090 IGP (Id 979)
BGP      12.6.134/23 207.135.89.65   (64800) 64753 64752 64751 6379 5646 1 701 7314 10562 IGP (Id 388)
BGP      12.7.214/23 207.135.89.65   (64800) 64753 64752 64751 6379 5646 7018 4129 IGP (Id 31004)
```

show ip bgp community

Purpose

Displays routes that belong to a specified community.

Format

show ip bgp community {<*community-id*> <*as-num*> | **no-export | no-advertise | no-export-subconfed | reserved-community** <*hex-number*>**} [to-file]**

Mode

Privileged

Description

The **show ip bgp community** command displays routes that belong to a specified community in a specified autonomous system.

Parameters

<*community-id*>
This is the community identifier portion of a community split. It combines with the autonomous-system value entered to create a value for the community attribute.

<*as-num*>
This is an autonomous system number.

no-export
This is a special community. It indicates the routes associated with this attribute must not be advertised outside a BGP confederation boundary. Since the Xpedition's implementation does not support confederations, this boundary is an AS boundary.

no-advertise
This is a special community. It indicates that the routes associated with this attribute must not be advertised to other BGP peers.

no-export-subconfed
This is a special community. It indicates the routes associated with this attribute must not be advertised to external BGP peers. (This includes peers in other members' autonomous systems inside a BGP confederation.)

reserved-community *<hex-number>*
This option specifies one of the reserved communities not mentioned above. A reserved community is one that is in one of the following ranges (0x0000000 - 0x0000FFFF) or (0xFFFF0000 - 0xFFFFFFFF).

to-file
Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display routes that belong to community 160 in AS 64900:

```
ssr# show ip bgp community 160 64900
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Path
*> 192.68.20/24     172.16.20.2                  64901 i
*> 192.68.222/24    172.16.20.2                  64901 64902 i
```

show ip bgp neighbor

Purpose

Displays status information about BGP peer hosts.

Format

show ip bgp neighbor <*IPaddr*> **received-routes | all-received-routes | advertised-routes [to-file]**

Mode

Privileged

Description

The **show ip bgp neighbor** command displays information related to a specified BGP peer host. Two types of information can be displayed: routes received and accepted from a BGP peer host, and all routes the Xpedition has advertised to a peer host.

Parameters

<*IPaddr*>	Specifies the IP address of a BGP peer host
received-routes	Displays valid BGP routes received and accepted from the specified peer host
all-received-routes	Displays all valid BGP routes.
advertised-routes	Displays all routes the **Xpedition** has advertised to the specified peer host.
to-file	Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Examples

To display all valid BGP routes received and accepted from peer host 172.16.20.2:

```
ssr# show ip bgp neighbor 172.16.20.2 received-routes
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop       Metric LocPrf Path
*> 172.16.70/24     172.16.20.2                  64901 i
*> 172.16.220/24    172.16.20.2                  64901 i
*> 192.68.20/24     172.16.20.2                  64901 i
*> 192.68.222/24    172.16.20.2                  64901 64902 i
```

Displays all routes the Xpedition has advertised to peer host 172.16.20.2:

```
ssr# show ip bgp neighbor 172.16.20.2 advertised-routes
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop       Metric LocPrf Path
*> 172.16.20/24     172.16.20.1                  i
*> 192.68.11/24     192.68.11.1                  i
```

show ip bgp paths

Purpose

Displays BGP Autonomous System (AS) path information.

Format

show ip bgp paths <*ASpath*> **[to-file]**

Mode

Privileged

Description

The **show ip bgp paths** command displays information about a specified AS path or all AS paths. The AS path is listed along with the number of routes that use it.

Parameters

<*ASpath*>	Will display information about the specified AS path.
to-file	Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display information about all AS paths:

```
ssr# show ip bgp paths
Hash  Ref   Path
0     5     IGP (Id 1)
2     1     (64900) 64901 64902 IGP (Id 3)
7     4     (64900) 64901 IGP (Id 2)
```

show ip bgp peer-as

Purpose

Displays information about TCP and BGP connections to an Autonomous System.

Format

show ip bgp peer-as <*ASnum*> **[to-file]**

Mode

Privileged

Description

The **show ip bgp peer-as** command displays information about routers in a specified autonomous system that are peered with the Xpedition.

Parameters

<*ASnum*>	The AS number of a peer autonomous system.
to-file	Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display information about TCP and BGP connections to autonomous system 64901:

```
ssr# show ip bgp peer-as 64901
group type External AS 64901 local 64900 flags <>
 peer 172.16.20.2 version 4 lcladdr (null) gateway (null)
  flags 0x20
  state 0x6 <Established>
  options 0x0 <>
  metric_out -1  preference 170  preference2 0
  recv buffer size 0  send buffer size 0
  messages in 10039 (updates 5, not updates 10034) 190863 octets
  messages out 10037 (updates 1, not updates 10036) 190743 octets
```

show ip bgp peer-group

Purpose

Displays status information about BGP peers by group.

Format

show ip bgp peer-group external | internal | igp | routing [to-file]

Mode

Enable

Description

The **show ip bgp peer-group** command displays status information about BGP peers according to their group.

Parameters

external	Displays status information about external peers.
internal	Displays status information about internal peers.
igp	Displays status information about igp peers.
routing	Displays status information about routing peers.
to-file	Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display status information about external peers:

```
ssr# show ip bgp peer-group external
Group    Neighbor        V    AS MsgRcvd MsgSent State
external 172.16.20.2     4 64901   10045   10044 Established
BGP summary, 1 peers in group type "external"
```

show ip bgp regexp

Purpose

Displays the BGP routes matching the AS path regular expression.

Format

show ip bgp regexp *<exp>*

Mode

Privileged

Description

The **show ip bgp regexp** command searches through all BGP routes that contain specified keywords belonging to an AS path. These specified keywords are the AS path regular expression upon which the search is executed. The expression string can be a combination of AS numbers or names.

Some BGP character string shorthand conventions:

.	Matches any AS number
*****	Zero or more repetitions
+	One or more repetitions
?	Zero or one repetition
|	Alternation
( )	Parentheses group subexpressions

Parameters

<exp>	A string specifying the regular expression. Specify an AS.

Restrictions

None.

Example

To display the BGP routes starting with “64751”:

```
ssr# show ip bgp regexp “64751 .*”
Network          Next Hop        Metric LocPrf Path
*> 193.226.64/22 134.141.178.33              64751 6379 1 1239 11331 8338 i
```

show ip bgp summary

Purpose

Displays the status of all BGP connections.

Format

show ip bgp summary [to-file]

Mode

Privileged

Description

The **show ip bgp summary** command displays the status of all BGP peers of the Xpedition.

Parameters

to-file Causes output to be saved in the file **/gatedtrc/gated.dmp**.

Restrictions

None.

Example

To display the status of all BGP connections:

```
ssr# show ip bgp summary
Neighbor        V    AS MsgRcvd MsgSent     Up/Down State
172.16.20.2     4 64901   10033   10031    6d23h8m1s Established
BGP summary, 1 groups, 1 peers
```

show ip bgp sync-tree

Purpose

Displays the BGP synchronization tree.

Format

show ip bgp sync-tree

Mode

Privileged

Description

The **show ip bgp sync-tree** command displays the BGP synchronization tree. The synchronization tree is used by IBGP peers to resolve the next hop (forwarding address). It gives information about routes that are orphaned because the next hop could not be resolved.

Parameters

None.

Restrictions

None.

Examples

The following example shows the next hops for some of the routes that are not resolved (by showing orphaned routes):

```
ssr# show ip bgp sync tree
Task BGP_Sync_64805:
      IGP Protocol: Any       BGP Group: group type Routing AS 64805

      Sync Tree (* == active, + == active with alternate, - ==
inactive with alternate:
      Orphaned routes
            Forwarding address 172.23.1.18
                  3/255 peer 172.23.1.26 preference 170
                  128.36/255.255 peer 172.23.1.26 preference 170
                  128.152/255.255 peer 172.23.1.26 preference 170
                  129.200/255.255 peer 172.23.1.26 preference 170
                  129.253/255.255 peer 172.23.1.26 preference 170
                  130.44/255.255 peer 172.23.1.26 preference 170
                  130.50/255.255 peer 172.23.1.26 preference 170
                  130.132/255.255 peer 172.23.1.26 preference 170
                  134.54/255.255 peer 172.23.1.26 preference 170
                  134.120/255.255 peer 172.23.1.26 preference 170
                  134.173/255.255 peer 172.23.1.26 preference 170
                  134.217/255.255 peer 172.23.1.26 preference 170
                  134.244/255.255 peer 172.23.1.26 preference 170
                  136.1/255.255 peer 172.23.1.26 preference 170
                  137.49/255.255 peer 172.23.1.26 preference 170
                  137.159/255.255 peer 172.23.1.26 preference 170
                  138.239/255.255 peer 172.23.1.26 preference 170
```

The following example shows the next hop for all the routes that are resolved.:

```
ssr# bgp show sync-tree
Task BGP_Sync_64805:
      IGP Protocol: Any       BGP Group: group type Routing AS 64805

      Sync Tree (* == active, + == active with alternate, - ==
inactive with alternate:
      Node 3/8388608 route 3/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 4/8388608 route 4/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 6/8388608 route 6/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 9.2/32768 route 9.2/255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 9.20/16384 route 9.20/255.255.128 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 10.12.1/2 route 10.12.1/255.255.255.252 metric 0 interface
      Node 10.12.1.4/2 route 10.12.1.4/255.255.255.252 metric 2 next hop 172.23.1.22
      Node 10.200.12/128 route 10.200.12/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 10.203.12/128 route 10.203.12/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 10.204.12/128 route 10.204.12/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12/8388608 route 12/255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.2.19/64 route 12.2.19/255.255.255.128 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.2.97/128 route 12.2.97/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.3.123/128 route 12.3.123/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.4.5/128 route 12.4.5/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.4.164/128 route 12.4.164/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.5.164/128 route 12.5.164/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.5.172/512 route 12.5.172/255.255.252 metric -1 next hops 172.23.1.6 172.23.1.22
      Node 12.5.252/256 route 12.5.252/255.255.254 metric -1 next hops 172.23.1.6 172.23.1.22
```

Chapter 6

cli Commands

The **cli** commands allow you to change the behavior of the Command Line Interface (CLI) in terms of command completion and command history recall.

Command Summary

Table 5 lists the **cli** commands. The sections following the table describe the command syntax.

Table 5. cli commands

show history
show terminal
terminal command-completion on | off
terminal history <*buffer-size*>
terminal length <*screen-length*>
terminal width <*line-length*>
terminal monitor

show history

Purpose

Displays the command history from the current CLI session.

Format

show history

Mode

User

Description

The **show history** command shows the commands you have issued during the current CLI session. A number is associated with each command. A command's number is useful for re-entering, modifying, or negating the command.

Note: You also can perform a command history recall by entering **!*** at any command prompt.

Parameters

None.

Restrictions

None.

show terminal

Purpose

Displays information about the current terminal settings.

Format

show terminal

Mode

User

Description

The **show terminal** command shows information about the terminal settings. The terminal settings affect the display characteristics of your CLI session.

Parameters

None.

Restrictions

None.

terminal command completion

Purpose

Turns on or off command completion support.

Format

terminal command completion on | off

Mode

User

Description

The **terminal command completion** command lets you enable or disable command completion support. This command affects only the user's current login session.

Parameters

on Turns on command completion.

off Turns off command completion.

Restrictions

None.

terminal history size

Purpose

Modifies command history recall characteristics.

Format

terminal history size buffer-size

Mode

User

Description

The **terminal history size** command lets you to set the size of the command history buffer. Each command stored in this buffer can be recalled without having the user type in the same, complete command again. By setting the size of this history buffer, one tells the router how many of the most recently executed commands should be stored. When the buffer is full, the oldest command is pushed out to make space for the newest command. This command affects only the user's current login session.

Parameters

<*buffer-size*>	A number specifying how many of the most recently executed commands should be kept. To disable history support, specify a size of 0.

Restrictions

None.

Examples

To set the history buffer size to 100 commands:

```
ssr# terminal history size 100
```

terminal length

Purpose

Modifies terminal screen's column settings for the current session.

Format

terminal length <*screen-length*>

Mode

User

Description

The **terminal length** command lets you modify the terminal screen's column size for the current session.

Parameters

<*screen-length*>	Number of columns for your terminal. Enter a number between 0-512.

Restrictions

None.

Example

To set the number of columns to 100 lines:

```
ssr# terminal length 100
```

terminal width

Purpose

Modify terminal screen's row settings for current session.

Format

terminal width <*line-length*>

Mode

User

Description

The **terminal width** command allows you to modify the terminal screen's row settings for the current session. Specifying the number of rows available on your terminal causes the system to automatically pause when screen output fills the entire screen.

Parameters

<*line-length*>	Number of rows for your terminal. Enter a number between 0-512. To prevent output from pausing after screen fills, set the value to 0.

Restrictions

None.

Examples

To set the number of rows to 100 lines:

```
ssr# terminal width 100
```

terminal monitor

Purpose

Allows the current CLI session to receive or not receive console output.

Format

terminal monitor

Mode

Privileged

Description

Some system messages are normally only sent to the management console. The **terminal monitor** command allows the current CLI session to also receive those messages. This command is useful only if you have a current Telnet CLI session and you want the debugging output that is normally sent to the management console to also be displayed on the Telnet session.

Parameters

None.

Restrictions

None.

Chapter 7

copy Commands

The **copy** commands allow the user to copy a file.

Command Summary

Table 6 lists the **copy** commands. The sections following the table describe the command syntax.

Table 6. copy commands

copy tftp | rcp | active | scratchpad | startup | <*filename*> **tftp | rcp | active | scratchpad | startup |** <*filename*>
copy tftp flash

copy tftp

Purpose

Copy configuration information or files.

Format

copy tftp | rcp | active | scratchpad | startup | <*filename*>
tftp | rcp | active | scratchpad | startup | <*filename*>

Mode

Privileged

Description

The **copy** command is primarily for transferring configuration information. You can copy configuration information between the Xpedition and external hosts using protocols such as TFTP or RCP. Within the Xpedition, you can copy configuration information between the Xpedition file system, the scratchpad (configuration database), the active (running) configuration or the Startup configuration. You also can use the **copy** command to make backup copies of a configuration file.

If the Xpedition has two Control Modules, you can copy the startup configuration of the primary Control Module to the secondary Control Module.

Parameters

tftp	Downloads or uploads a file on a TFTP server.
rcp	Downloads or uploads a file on an RCP server.
active	Specifies information from the active configuration database (the running system configuration).
scratchpad	Specifies configuration changes from the scratchpad.
startup	Copies the Startup configuration information stored in the Control Module's NVRAM.
<*filename*>	Specifies the name of a file on the Xpedition's local file system (NVRAM or PCMCIA card).

Restrictions

The Xpedition does not allow some combinations of source and destination pair. Typically, you cannot have the same location for both source and destination; for example, you cannot copy from one TFTP server directly to another TFTP server or copy from scratchpad to scratchpad.

In addition, you cannot copy directly into the active configuration from anywhere except the scratchpad. All changes to the running system must come through the scratchpad.

Examples

To copy configuration information from the scratchpad to the active database, enter the following command. This command activates all the uncommitted changes, thus immediately placing the changes into effect.

```
ssr# copy scratchpad active
```

To copy the file config.john to config.debi:.

```
ssr# copy config.john config.debi
```

To copy the Startup configuration to a TFTP server for backup purposes, enter the following command. The CLI prompts for the TFTP server's IP address or hostname and the filename:

```
ssr# copy startup tftp-server
```

To copy a previously saved configuration from a TFTP server to the Startup configuration, enter the following command. Note the use of an URL to specify the TFTP server and the filename.

```
ssr# copy tftp://10.1.2.3/backup/config.org startup
```

To copy the active configuration to a remote server using RCP, enter the following command. Notice that in this example a URL specifies the RCP user name, server, and filename.

```
ssr# copy active rcp://john@server1/config/config.dec25
```

copy tftp flash

Purpose

Copies a system software image to the Xpedition.

Format

copy tftp flash

Mode

Privileged

Description

The **copy tftp flash** command copies a system software image from a TFTP server into the PCMCIA flash card on the Control Module. By default, if the Xpedition has two Control Modules, the system software image is copied to both Control Modules.

Parameters

None. The Xpedition will prompt for information as needed.

Restrictions

None.

Chapter 8

dhcp Commands

The **dhcp** commands allow the user to display and clear *scopes* (sets of IP address pools and network parameters) that are to be used by Dynamic Host Configuration Protocol (DHCP) clients and apply them to interfaces on the Xpedition.

Command Summary

Table 7 lists the **dhcp** commands. The sections following the table describe the command syntax.

Table 7. dhcp commands

clear ip dhcp
show ip dhcp binding [active | expired | static]
show ip dhcp num-clients

clear ip dhcp

Purpose

Forces the DHCP server to update its lease database.

Format

clear ip dhcp

Mode

Privileged

Description

While the DHCP server is running, you can force the server to immediately update its lease database by using the clear ip **dhcp** command.

Parameters

None.

Restrictions

None.

show ip dhcp binding

Purpose

Display information from the lease database.

Format

show ip dhcp binding [**active | expired | static**]

Mode

Privileged

Description

The **show ip dhcp binding** command displays information from the lease database. If you do not specify any parameters, the DHCP server displays the entire lease database.

Parameters

active	Displays currently active leases only.
expired	Displays expired leases only.
static	Displays leases with static IP address assignments only.

Restrictions

None.

Examples

To display information from the lease database:

```
ssr# show ip dhcp binding
IP address Hardware Address Lease Expiration     Type
---------- ---------------- ----------------     ----
10.20.1.22 00:40:05:41:f1:2d 1999-05-24 17:45:06 dynamic
10.20.1.23 00:00:b4:b1:29:9c 1999-05-24 17:45:04 dynamic
10.20.1.21 00:00:b4:b0:f4:83 1999-05-24 17:45:01 dynamic
10.20.1.20 00:80:c8:e1:20:8a 1999-05-24 09:24:30 dynamic
10.30.7.9  08:00:20:11:22:33 ---                 static
10.30.7.44 08:00:20:44:55:66 ---                 static
```

show ip dhcp num-clients

Purpose

Displays the number of allocated bindings for the DHCP server and the maximum number allowed.

Format

show ip dhcp num-clients

Mode

Privileged

Description

This **show ip dhcp num-clients** command displays the number of allocated bindings for the DHCP server and the maximum number allowed.

Parameters

None.

Restrictions

None.

Examples

To display information:

```
ssr# show ip dhcp num-clients
15 current clients (253 maximum)
```

Chapter 9

dvmrp Commands

The **dvmrp** commands allow the user to display information about Distance Vector Multicast Routing Protocol (DVMRP) interfaces.

Command Summary

Table 8 lists the **dvmrp** commands. The sections following the table describe the command syntax.

Table 8. dvmrp commands

show ip dvmrp interface *<IPaddr>*
show ip dvmrp route [*<type><slot/port><IPaddr>***]**
show ip dvmrp rules

show ip dvmrp interface

Purpose

Displays DVMRP interfaces.

Format

show ip dvmrp interface [<*IPaddr*>**]**

Mode

Privileged

Description

The **show ip dvmrp interface** command displays the state of an interface running DVMRP, along with other neighbor-related information. Neighbors are displayed with their DVMRP version and capability flags and Generation IDs; this information can help in debugging. If rules are in effect for an interface, they are indicated by ExportPol or the ImportPol flags.

Parameters

<*IPaddr*> Displays DVMRP information for the specified interface.

Restrictions

None.

Examples

Here is an example of the **show ip dvmrp interface** command.

```
ssr# show ip dvmrp interface
Address: 10.50.1.1          Subnet: 10.50.1/24       Met: 1   Thr: 1
Name   : pc                 State: Dn   Igmp  Dvmrp

Address: 207.135.89.10      Subnet: 207.135.89.0/27   Met: 1   Thr: 1
Name   : corp               State: Up   Igmp  Dvmrp Querier  ExportPol
Peer   : 207.135.89.1       Version:   3.255        Flags:0xe  GID: 0x31a

Address: 10.55.89.101       Subnet: 10.55.89/24      Met: 1   Thr: 1
Name   : lab                State: Up   Dvmrp
Peer   : 10.55.89.100       Version:   3.255        Flags:0xe  GID: 0x179

Address: 207.135.89.10      Remote: 207.137.137.1    Met: 1   Thr: 1  Rate: 1000
Name   : mbone              State: Tunnel  Up   Dvmrp ExportPol
Peer   : 207.137.137.1      Version:   3.8          Flags:0xe  GID: 0x6c19d135
```

show ip dvmrp route

Purpose

Displays DVMRP unicast routing table.

Format

show ip dvmrp route [*<type><slot/port><IPaddr>***]**

Mode

Privileged

Description

The **show ip dvmrp route** command displays the contents of DVMRP unicast routing table.

The DVMRP route shows the topology information for the internet multicasting sites. It is independent of IP unicast routing table or protocol. In this table, the information is presented about a address prefix (in form of network-address / network-mask length), the interface and the uplink (parent) router through which this subnet can be reached. This table also shows information about any routers / interfaces which consider this router as their uplink (that is, those routers which depend on this router if traffic were to originate from this subnet). These routers / interfaces are shown as children of the parent router.

Note: The **show ip dvmrp route** command can search on the basis of subnet and on the basis of those routes whose parent is a particular interface and / or a particular router.

Note: This command only shows DVMRP routes and not information about current multicast sessions.

Parameters

<type>

<slot/port>

<IPaddr> Displays the route to the specified router.

Restrictions

None.

Examples

To display DVMRP routes offered by the next-hop router 207.137.137.1:

```
ssr# show ip dvmrp route router 207.137.137.1
DVMRP Routing Table (4232 routes,   8 hold-down-routes)
Net: 128.119.3.16/29        Gateway: 207.137.137.1     Met:  9   Age:  35
Parent: mbone             Children: corp
                                    lab

Net: 128.119.3.8/29         Gateway: 207.137.137.1     Met:  9   Age:  35
Parent: mbone             Children: corp
                                    lab

Net: 209.12.162.16/28       Gateway: 207.137.137.1     Met: 26   Age:  35
Parent: mbone             Children: corp
                                    lab

Net: 208.197.171.112/28     Gateway: 207.137.137.1     Met:  7   Age:  35
Parent: mbone             Children: corp
                                    lab

Net: 208.151.215.240/28     Gateway: 207.137.137.1     Met:  7   Age:  35
Parent: mbone             Children: corp
                                    lab

Net: 208.151.215.192/28     Gateway: 207.137.137.1     Met:  7   Age:  35
Parent: mbone             Children: corp
                                    lab

Net: 208.151.215.96/28      Gateway: 207.137.137.1     Met:  7   Age:  35
Parent: mbone             Children: corp
```

To show non-advertised routes on interface lab:

```
ssr# show ip dvmrp route interface lab permission
DVMRP Routing Table (4232 routes,   5 hold-down-routes)
Net: 100.100.100/24         Gateway: 10.55.89.100      Met:  2   Age:  25
Parent: lab              Children: corp
                            mbone           leaf NoAdv

Net: 20.20.20/24            Gateway: 10.55.89.100      Met:  2   Age:  25
Parent: lab              Children: corp
                            mbone           leaf NoAdv

Net: 10.55.89/24            Gateway: ----              Met:  1   Age:  --
Parent: lab              Children: corp             leaf NoAdv
                            mbone           leaf NoAdv

Total Routes Printed: 3
```

show ip dvmrp rules

Purpose

Displays the rules in effect for filtering routes from DVMRP neighbor routers.

Format

show ip dvmrp rules

Mode

Privileged

Description

The **show ip dvmrp rules** command displays the filtering rules in effect for DVMRP routes.

Parameters

None.

Restrictions

None.

Example

In this example, the following rules are in effect:

```
dvmrp advertise route 207.135.89.0/24 interface mbone
dvmrp noadvertise route 0/0 interface mbone
dvmrp advertise route 207.135.88.0/24 interface mbone
dvmrp noadvertise route 10/8 interface corp
```

To display information about these rules:

```
# show ip dvmrp rules
NoAdvertise: 10.0.0.0/8              IF: corp
Advertise  : 207.135.89.0/24         IF: mbone
Advertise  : 207.135.88.0/24         IF: mbone
NoAdvertise: default                 IF: mbone
```

These rules would affect the routing table as follows:

```
# show ip dvmrp route net 10/8 permissions

Net: 10.55.89/24          Gateway: ----          Met:  1   Age:  --
Parent: lab               Children: corp         leaf NoAdv
                                    mbone        leaf NoAdv
```

These rules prevent a directly connected route on this router from being visible to interface corp and mbone. The leaf flag indicates there is no downstream neighbor on the interface.

Chapter 10

enable Command

The **enable** command switches the CLI session from User mode to Privileged mode.

Format

enable

Mode

User

Description

The **enable** command switches your CLI session from User mode to Privileged mode. After you issue the command, the CLI will prompt you for a password if a password is configured. If no password is configured, a warning message advising you to configure a password will display.

If a password is configured and you do not know your password -- or pressing Return does not work -- see your Xpedition administrator.

To exit from the Privileged mode and return to the User mode, use the **exit** command.

Parameters

None.

Restrictions

None.

Chapter 11

exit Command

The **exit** command exits the current CLI mode to the previous mode. For example, if you are in the Privileged mode, **exit** returns you to the User mode. If you are in User mode, **exit** closes your CLI session and logs you off the Xpedition.

Format

exit

Mode

All modes

Parameters

None.

Restrictions

None.

Chapter 12

fddi Commands

The **fddi** commands enable the user to clear and display information related to the Fiber Distributed Data Interface (FDDI).

Command Summary

Table 9 lists the **fddi** commands. The sections following the table describe the command syntax.

Table 9. fddi commands

clear fddi <*port-list*>
show fddi fddi-fdx-mode | fddi-mode | fddi-status | mac-group | mac-restricted-token | media-type | path-group | port-group | ring-purger | smt-config | smt-group | translation | version <*port-list*> **| all-ports**

clear fddi

Purpose

Clears specified FDDI port.

Format

clear fddi <*port-list*>

Mode

Privileged

Description

The **clear fddi** command clears a specified FDDI port.

Parameters

<*port-list*> Specifies which FDDI port(s) to clear.

Restrictions

None.

show fddi

Purpose

Displays specified information for one or more FDDI ports.

Format

show fddi fddi-fdx-mode | fddi-mode | fddi-status | mac-group | mac-restricted-token | media-type | path-group | port-group | ring-purger | smt-config | smt-group | translation | version <*port-list*> **| all-ports**

Mode

Privileged

Description

The **show fddi** command displays specified information for one or more FDDI ports.

Parameters

fddi-fdx-mode	Shows FDDI full duplex value for specified port(s).
fddi-mode	Shows operating FDDI mode for specified port(s).
fddi-status	Shows FDDI status for specified port(s).
mac-group	Shows MAC configuration parameters for specified port(s).
mac-restricted-token	Shows MAC restricted token time-out for specified port(s).
media-type	Shows the media type for specified port(s).
path-group	Shows PATH configuration parameters for specified port(s).
port-group	Shows PORT configuration parameters for specified port(s).
ring-purger	Shows ring purger value for specified port(s).
smt-config	Shows SMT configuration parameters for specified port(s).

smt-group	Shows SMT configuration parameters for specified port(s).
translation	Shows IPX/ARP Appletalk translation settings.
version	Shows firmware version of port(s) specified.
<*port-list*> **| all-ports**	Specifies FDDI port(s) for which to display chosen information. Entering **all-ports** will display that information for all FDDI ports.

Restrictions

None.

Chapter 13

file Commands

The **file** commands enable the user to display a directory of the files on a storage device, display the contents of a file on the console, and delete a file.

Command Summary

Table 10 lists the **file** commands. The sections following the table describe the command syntax.

Table 10. file commands

delete <*file-name*>
dir <*device-name*>
show file <*file-name*>

delete

Purpose

Deletes a file.

Format

delete <*file-name*>

Mode

Privileged

Description

The **delete** command deletes the specified file. The filename can include a device name. By default, if a device name is not specified, it is assumed to be the **bootflash:** device which is where all configuration files are stored.

Parameters

<*file-name*> Name of the file to delete. The filename can include a device name using this format: <*device*>:<*file-name*>. By default, if a device name is not specified, it is assumed to be the **bootflash** device. The **bootflash** device is the default device for storing configuration files.

Restrictions

None.

Examples

To delete the file config.old:

```
ssr# delete config.old
```

dir

Purpose

Displays contents of a file system.

Format

dir <*device-name*>

Mode

User

Description

Displays a directory of the files on the specified storage device.

Parameters

<*device-name*> Device name. You can specify one of the following:

bootflash: The Control Module's NVRAM.

slot0: The PCMCIA flash card in slot 0 (the upper slot).

slot1: The PCMCIA flash card in slot 1(the lower slot).

Restrictions

None.

Examples

To display the contents of the **bootflash** device:

```
ssr# dir bootflash:
```

show file

Purpose

Displays the contents of a file.

Format

show file <*file-name*>

Mode

Privileged

Description

Displays the contents of a file.

Parameters

<*file-name*> Name of the file to display. The filename can include a device name using this format: <*device*>**:**<*file-name*>. By default, if a device name is not specified, it is assumed to be the **bootflash** device. The **bootflash** device is the default device for storing configuration files.

Restrictions

None.

Examples

To display the contents of the file startup (the startup configuration file):

```
ssr# show file startup
```

Chapter 14

filters Commands

The **filters** commands allow the user to display information on the following types of security filters:

- **Address filters.** Address filters block traffic based on a frame's source MAC address, destination MAC address, or both. Address filters are always configured and applied on the input port.
- **Static entry filters.** Static entry filters allow or force traffic to go to a set of destination ports based on a frame's source MAC address, destination MAC address, or both. Static entry filters are always configured and applied on the input port. You can configure source static entry filters, destination static entry filters, and flow static entry filters. Source static entry filters allow or disallow frames based on their source MAC address; destination static entry filters allow or disallow frames based on their destination MAC address. Flow static entries allow or disallow traffic based on their source *and* destination MAC addresses.
- **Port-to-address locks.** Port-to-address lock filters "lock" a user to a port or set of ports, disallowing them access to other ports.
- **Secure ports.** Secure port filters shut down Layer 2 access to the Xpedition from a specific port or drop all Layer 2 packets received by a port. Used by themselves, secure ports secure unused Xpedition ports. When used in conjunction with static entry filters, secure ports drop all received or sent traffic (depending on the static entry filter) except traffic forced to or from the port by the static entry filter.

Command Summary

Table 11 lists the **filters** commands. The sections following the table describe the command syntax.

Table 11. filters commands

show filters [address-filter] [all-source | all-destination | all-flow] [source-mac <*MACaddr*> **des-mac** <*MACaddr*>**] [ports** <*ports-list*>**] [vlan** <*VLAN-num*>**]**
show filters [port-address-lock] [ports <*port-list*>**] [vlan** <*VLAN-num*>**] [source-mac** <*MACaddr*>**]**
show filters [secure-port]
show filters [static-entry] [all-source | all-destination | all-flow] ports <*port-list*> **vlan** <*VLAN-num*> **[source-mac** <*MAC-addr*>**] [des-mac** <*MAC-addr*>**]**

show filters [address-filter]

Purpose

Displays the address filters.

Format

show filters [address-filter] [all-source | all-destination | all-flow] [source-mac <*MACaddr*> **des-mac** <*MACaddr*>**] [ports** <*ports-list*>**] [vlan** <*VLAN-num*>**]**

Mode

Privileged

Description

The **show filters [address-filter]** command displays the address filters currently configured on the Xpedition.

Parameters

all-source | all-destination | all-flow
Specifies the types of filters you want to display.

source-mac <*MACaddr*>
Restricts the display to only those address filters that have been applied to this source MAC address.

des-mac <*MACaddr*>
Restricts the display to only those address filters that have been applied to this destination MAC address.

ports <*port-list*>
Restricts the display to only those address filters that have been applied to the specified ports.

vlan <*VLAN-num*>
Restricts the display to only those address filters that have been applied to the specified VLANs.

Restrictions

None.

show filters [port-address-lock]

Purpose

Displays the port address locks.

Format

show filters [port-address-lock] [ports <*port-list*>**] [vlan** <*VLAN-num*>**] [source-mac** <*MACaddr*>**]**

Mode

Privileged

Description

The **show filters [port-address-lock**] command displays the port-address-lock filters currently configured on the Xpedition.

Parameters

ports <*port-list*>
Restricts the display to only those port address locks that have been applied to the specified ports.

vlan <*VLAN-num*>
Restricts the display to only those port address locks that have been applied to the specified VLANs.

source-mac <*MACaddr*>
Restricts the display to only those port address locks that have been applied to this source MAC address.

Restrictions

None.

show filters [secure-port]

Purpose

Displays the port security filters.

Format

show filters [secure-port]

Mode

Privileged

Description

The **show filters [secure-port]** command displays the secure-port filters currently configured on the Xpedition.

Parameters

None.

Restrictions

None.

show filters [static-entry]

Purpose

Displays the static entry filters.

Format

show filters [static-entry] [all-source | all-destination | all-flow] ports <*port-list*> **vlan** <*VLAN-num*> **[source-mac** <*MAC-addr*>**] [des-mac** <*MAC-addr*>**]**

Mode

Privileged

Description

The **show filters [static-entry]** command displays the static-entry filters currently configured on the Xpedition.

Parameters

all-source | all-destination | all-flow
Specifies the types of static entries you want to display.

ports <*port-list*>
Restricts the display to only those static entries that have been applied to the specified ports.

vlan <*VLAN-num*>
Restricts the display to only those static entries that have been applied to the specified VLANs.

source-mac <*MACaddr*>
Restricts the display to only those static entries that have been applied to this source MAC address.

des-mac <*MACaddr*>
Restricts the display to only those static entries that have been applied to this destination MAC address.

Restrictions

None.

Chapter 15

frame-relay Commands

The **frame-relay** commands allow you to clear frame relay service profiles, and monitor frame relay High-Speed Serial Interface (HSSI) and standard serial ports.

Command Summary

Table 12 lists the **frame-relay** commands. The sections following the table describe the command syntax.

Table 12. frame relay commands

clear frame-relay [frame-drop-qdepth-counter] [max-frame-enqued-counter] [frame-drop-red-counter] [rmon] [<*port-list*>**]**
show frame-relay service <*service-name*> **| all**
show frame-relay stats [ports <*port-list*> **| all-ports] [lmi] [last-error] [mibII] [summary]**

clear frame-relay

Purpose

Clears the specified statistics counter.

Format

clear frame-relay [frame-drop-qdepth-counter] [max-frame-enqued-counter] [frame-drop-red-counter] [rmon] [<*port list*>**]**

Mode

Enable

Description

The **clear frame-relay** command allows you to specify a particular statistic counter and have those statistics reset to zero. There are statistic counters on each WAN port, and you can use the **clear frame-relay** to clear the counter for an individual WAN port or for a group of ports.

Parameters

frame-drop-qdepth-counter	Specify this optional parameter to reset the frame drop counter to zero.
max-frame-enqued-counter	Specify this optional parameter to reset the max enquedframes counter to zero.
frame-drop-red-counter	Specify this optional parameter to reset the packet drop counter to zero.
rmon	Specify this optional parameter to reset the rmon counter to zero.
<*port list*>	The WAN port(s) that you wish to clear the counter.

Restrictions

Usage is restricted to WAN ports only.

Example

To clear the frame drop counter to zero on WAN port hssi3/1:

```
ssr# clear frame-relay frame-drop-qdepth-counter hssi3/1
```

show frame-relay service

Purpose

Displays frame relay service profiles.

Format

show frame-relay service <*service-name*> | **all**

Mode

Privileged

Description

The **show frame-relay service** command allows the user to display the available frame relay service profiles.

Parameters

<*service name*> The name of a particular pre-defined service profile.

all Displays all of the available frame relay service profiles.

Restrictions

None.

Example

To display the available frame relay service profiles named “prof1”:

```
ssr# show frame-relay service prof1
```

show frame-relay stats

Purpose

Displays frame relay statistics.

Format

show frame-relay stats [ports <*port-list*> **| all-ports] [lmi] [last-error] [mibII] [summary]**

Mode

Privileged

Description

The **show frame-relay stats** command allows the user to display the following frame relay port statistics for a given port:

- The last reported frame relay error.
- The active frame relay LMI parameters.
- The MIBII statistics for frame relay WAN ports.

Parameters

port <*port name*>
The port or ports for which you want to display statistics. Using the keyword **all-ports** will display statistics for all available ports.

lmi
Specifying the **lmi** keyword allows you to display the active frame relay LMI parameters.

last-error
Specifying the **last-error** keyword allows you to display the last reported frame relay error for the given port.

mibII
Specifying the **mibII** keyword allows you to display the MIBII statistics for frame relay WAN ports.

summary
Specifying the **summary** keyword allows you to display all of the summary information for VC statistics.

Restrictions

The **last error**, **mibii**, and **lmi** commands are for ports only (no VC designators allowed). Otherwise, the port name may have the “VC” designator.

Examples

To display statistics for serial port 1 of slot 3:

```
ssr# show frame-relay stats port serial3/1
```

Chapter 16

igmp Commands

The **igmp** commands let you display Internet Group Management Protocol (IGMP) parameters.

Command Summary

Table 13 lists the **igmp** commands. The sections following the table describe the command syntax.

Table 13. igmp commands

show ip igmp interface <*port-list*>
show ip igmp groups <*IPaddr*>
show ip igmp timers
show ip igmp vlans

show ip igmp interface

Purpose

Shows the interfaces running IGMP.

Format

show ip igmp interface <*port-list*>

Mode

Privilege

Description

The **show ip igmp interface** command shows memberships on a specified interface or for a multicast group address. When you use the command to show interfaces by group, all interfaces containing the group membership are shown.

Note: This command is similar to **show ip igmp groups**, except where the **show ip igmp interface** command shows interface details, the **show ip igmp groups** command shows ports.

Parameters

<*port-list*>

The port name, in the format: **`media.slot.port.vpi.vci`**

media Is the media type. This is **at** for an ATM port.

slot Is the slot number where the module is installed.

port Is the number of the port through which data is passing.

vpi Is the Virtual Path Identifier.

vci Is the Virtual Channel Identifier.

Restrictions

None.

Example

To show information about the interfaces running IGMP:

```
ssr# show ip igmp interface

Address: 172.1.1.10 Subnet: 172.1.1/24 Met: 1 Thr: 1
Name : mls15 State: Up Querier Leaf Igmp Dvmrp

Address: 207.135.89.64 Subnet: 207.135.89.0/25 Met: 1 Thr: 1
Name : company State: Up Querier Leaf Igmp Dvmrp
Groups : 224.0.1.12
224.1.127.255
224.0.1.24
224.2.127.253
224.2.127.254

Address: 10.135.89.10 Subnet: 10.135.89.0/25 Met: 1 Thr: 1
Name : test State: Up Querier Igmp Dvmrp

Address: 207.135.122.11 Subnet: 207.135.122.8/29 Met: 1 Thr: 1
Name : mbone State: Up Igmp Dvmrp
Groups : 224.0.1.11
224.0.1.12
224.2.127.254
239.255.255.255
224.2.127.253
```

show ip igmp groups

Purpose

Displays IGMP host memberships.

Format

show ip igmp groups <*IPaddr*>

Mode

Privileged

Description

The **show ip igmp groups** command displays IGMP host members on a specific interface and / or for a particular multicast group.

Parameters

<*Ipaddr*>	Address of the multicast group for which to display host memberships.

Restrictions

None.

Examples

To display host members for multicast group 225.0.1.20:

```
ssr# show ip igmp groups 225.0.1.20
```

To display host members for multicast group 225.0.1.20 on port ethernet1 / 1:

```
ssr# show ip igmp groups 225.0.1.20 ethernet1/1
```

The following is a fuller example.

```
ssr# show ip igmp groups

Group : 224.0.1.11 Ports: et.1.1
Group : 224.0.1.12 Ports: et.1.1
et.5.1
Group : 224.0.1.24 Ports: et.5.1
Group : 224.1.127.255 Ports: et.5.1
Group : 224.2.127.253 Ports: et.1.1
et.5.1
Group : 224.2.127.254 Ports: et.1.1
et.5.1
Group : 239.255.255.255 Ports: et.1.1
```

show ip igmp timers

Purpose

Displays IGMP timers.

Format

show ip igmp timers

Mode

Privileged

Description

The **show ip igmp timers** command displays IGMP timers.

Parameters

None.

Restrictions

None.

igmp show vlans

Purpose

Displays IGMP VLANs.

Format

show ip igmp vlans

Mode

Privileged

Description

The **igmp show vlans** command displays IGMP VLANs.

Parameters

None.

Restrictions

None.

Chapter 17

ip Commands

The **ip** commands allow the user to display route table entries and various IP related tables.

Command Summary

Table 14 lists the **ip** commands. The sections following the table describe the command syntax.

Table 14. ip commands

ip clear reverse-flows
show ip hash-variant
show ip helper-address
show ip interface <*port-list*> **[brief]**
show ip reverse-flows
show ip route
show ip route [bgp | connected | ospf | ospf-ase | rip | static]
show ip route summary
show ip route static/show ip route rip
show tcp [dns-lookup]
show udp [dns-lookup]

ip clear reverse-flows

Purpose

Clears reverse flow statistics.

Format

ip clear reverse-flows

Mode

Privileged

Description

The **ip clear reverse-flows** command deletes all reverse flow statistics. Reverse flows are IP traffic flows in the opposite direction, where source information becomes destination information and vice versa.

Parameters

None.

Restrictions

None.

Example

To clear the reverse flow statistics:

```
ssr# ip clear reverse-flows
```

show ip hash-variant

Purpose

Displays IP hash variant per module.

Format

show ip hash-variant

Mode

Privileged

Description

The **show ip hash-variant** command displays hash variant information. There are a total of 16 modules using the hash variant feature (1-16).

Enabling hash variant causes a variation to the basic hashing algorithm. This variation will prevent clustering of hash values and will provide a more even distribution across the L3 lookup table. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). The default hashing algorithm is 0.

Swizzling shifts the hash value by a certain amount of bits, causing a more random distribution across the L3 lookup table. Auto-hashing allows the Xpedition to auto-select a hashing algorithm optimized for ‘best case’ L3 table distribution.

Parameters

None.

Restrictions

None.

Example

To display IP hash variant information on all 16 modules:

```
ssr# show ip hash-variant
IP Module                 Hash Variant
--------------------------------------------------
Module 2                  variant-0
Module 3                  variant-0
Module 4                  variant-0
Module 5                  variant-1
Module 6                  variant-0
Module 7                  variant-0
Module 8                  variant-2
Module 9                  variant-0
Module 10                 variant-7
Module 11                 variant-0
Module 12                 variant-6
Module 13                 variant-0
Module 14                 variant-0
Module 15                 variant-0
```

show ip helper-address

Purpose

Displays the configuration of IP helper addresses.

Format

show ip helper-address

Mode

Privileged

Description

The **show ip helper-address** command displays the configuration of IP helper addresses configured on the system.

Parameters

None.

Restrictions

None.

Example

The following example shows that interface int4 has one helper address configured while interface int3 has one helper address configured for the port mapper service (port 111).

```
ssr# show ip helper-address
Interface      IP address      Helper Address
---------      ----------      --------------
int6           10.1.17.1       none
int5           10.1.16.1       none
int4           10.1.15.1       10.4.1.45
int1           10.1.12.1       none
int0           10.1.11.1       none
int3           10.1.14.1       10.5.78.122(111)
```

show ip interface

Purpose

Displays the configuration of IP interfaces.

Format

show ip interface <*port-list*> **[brief]**

Mode

Privileged

Description

The **show ip interface** command displays the configuration of an IP interface. If you issue the command without specifying an interface name then the configuration of all IP interfaces is displayed.

Parameters

<*port-list*>	Port for which to display IP statistics.
brief	This optional keyword displays a brief summary of IP interface status and configuration.

Restrictions

None.

Example

To display the configuration of the IP interface “ethernet1/1”:

```
ssr# ip show interface ethernet1/1
ethernet1/1 is administratively up, link state is down
IP processing is disabled
Internet address is 192.168.1.1/24, Broadcast address is 192.168.1.255
Encapsulation is ARPA
MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP in enabled
ICMP redirect message are always sent
VLAN 100 is defined for IP traffic types
IP processing is enabled
Internet address is 100.1.2.1/24 Broadcast address is 100.1.1.255
Encapsulation is ARPA
MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP in enabled
ICMP redirect message are always sent
```

show ip reverse-flows

Purpose

Displays reverse flow statistics.

Format

show ip reverse-flows

Mode

Privileged

Description

The **show ip reverse-flows** command displays the reverse flow statistics. Reverse flows are IP traffic flows in the opposite direction, where source information becomes destination information and vice versa. This command shows the number of reverse flow packets.

Parameters

None.

Restrictions

None.

Example

To display the reverse flow statistics:

```
ssr# show ip reverse-flows
IP Reverse Flow Statistics :
Total reverse-flow packets                  : 0
Successful reverse-flow packets             : 0
Unsuccessful reverse-flow packets           : 0
Arphold packets                         : 0
Find Flow entry success packets             : 0
Sum of arp hold and flow entry success packets : 0
```

show ip route

Purpose

Displays ARP entries on the IP routing table.

Format

show ip route

Mode

Privileged

Description

The **show ip route** command displays ARP entries on the IP routing table.

Parameters

None.

Restrictions

None.

Restrictions

None.

show ip route [bgp|connected|ospf|ospf-ase|rip|static]

Purpose

Displays various portions of the IP routing table.

Format

show ip route [bgp | connected | ospf | ospf-ase | rip | static]

Mode

Privileged

Description

This **show ip route** command displays the IP routing table. Different command options can be used to show different aspects of the routing table.

Parameters

bgp	Shows all BGP (Border Gateway Protocol) routes.
connected	Shows all connected routes.
ospf	Shows all OSPF (Open Shortest Path First) routes.
ospf-ase	Shows all OSPF (Open Shortest Path First) Autonomous System-External routes.
rip	Shows all RIP (Routing Information Protocol) routes.
static	Shows all manually defined routes.

Restrictions

None.

show ip route summary

Purpose

Displays a summary of IP routing table entries.

Format

show ip route summary

Mode

Privileged

Description

The **show ip route summary** command displays a summary of all route entries.

Parameters

None.

Restrictions

None.

show tcp

Purpose

Displays all TCP connections and services.

Format

show tcp [dns-lookup]

Mode

Privileged

Description

The **show tcp** command displays all existing TCP connections to the Xpedition as well as TCP services available on the Xpedition.

Parameters

dns-lookup This command attempts to do a reverse DNS lookup to look for the hostname associated with the IP address and display the hostname instead.

Restrictions

None.

Example

The following example displays all established TCP onnections and services of the Xpedition.

```
ssr# show tcp
Active TCP connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  *:gated-gii            *:*                    LISTEN
tcp        0      0  *:http                 *:*                    LISTEN
tcp        0      0  *:telnet               *:*                    LISTEN
```

show udp

Purpose

Displays all UDP connections and services.

Format

show udp [dns-lookup]

Mode

Privileged

Description

The **show udp** command displays all existing UDP connections to the Xpedition as well as UDP services available on the Xpedition.

Parameters

dns-lookup This command attempts to do a reverse DNS lookup to look for the hostname associated with the IP address and display the hostname instead.

Restrictions

None.

Example

The following example displays all established UDP connections and services of the Xpedition

```
ssr# show udp
Active UDP connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
udp        0      0  127.0.0.1:1025         127.0.0.1:162
udp        0      0  *:snmp                 *:*
udp        0      0  *:snmp-trap            *:*
udp        0      0  *:bootp-relay          *:*
udp        0      0  *:route                *:*
udp        0      0  *:*                    *:*
```

Chapter 18

ip-policy Commands

The **ip-policy** commands allow the user to clear and display the policies that cause the Xpedition to forward packets to a specified IP address based on information in a packet's L3/L4 IP header fields.

Command Summary

Table 15 lists the **ip-policy** commands. The sections following the table describe the command syntax.

Table 15. ip-policy commands

clear route-map [policy-name <*name*> **| all]**
show route-map [[policy-name <*name*> **| all] [interface** <*name*> **| all]]**

clear route-map

Purpose

Clears IP policy statistics.

Format

clear route-map [policy-name <*name*> **| all]**

Mode

Privileged

Description

The **clear route-map** command is used in conjunction with the **show route-map** command, which gathers statistics about IP policies. The **clear route-map** command lets you reset IP policy statistics to zero.

Parameters

<*name*> Specifies which active IP policy to clear.

all Causes statistics to be cleared for all IP policies.

Restrictions

None.

Examples

To clear statistics for IP policy p1:

```
ssr# clear route-map policy-name p1
```

To clear statistics for all IP policies:

```
ssr# clear route-map all
```

show route-map

Purpose

Displays information about active IP policies.

Format

show route-map [[policy-name <*name*> **| all] [interface** <*name*> **| all]]**

Mode

Privileged

Description

The **show route-map** command displays information about active IP policies, including profile definitions, policy configuration settings, and next-hop gateways. The command also displays statistics about packets that have matched an IP policy statement as well as the number of packets that have been forwarded to each next-hop gateway.

Parameters

policy-name <*name*> **| all**
Names a specific IP policy. Use the **all** keyword to display all active policies.

Note: The **show route-map all** command works identically to the **show route-map policy-name all** command

interface <*name*> **| all**
Displays information about IP policies that have been applied to a specified interface. If you use the **all** keyword, the command displays information about IP policies which have been applied to all interfaces.

Restrictions

None.

Example

To display information about IP policy p1:

```
ssr# show route-map policy-name p1

--------------------------------------------------------------------------------
IP Policy name     : p1 (1)
Applied Interfaces : int1 (2)
Load Policy        : first available (3)

(4)            (5)              (6)            (7)      (8)      (9) (10)
ACL         Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort   TOS Prot
---         --------------     --------------     --------- --------- --- ----
prof1       9.1.1.5/32         15.1.1.2           any       any       0 IP
prof2       2.2.2.2/32         anywhere           any       any       0 IP
everything  anywhere           anywhere           any       any       0 IP

                                      Next Hop Information
                                      --------------------
 (11)  (12)  (13)        (14)  (15)                (16)          (17)  (18)
Seq   Rule  ACL       Cnt Action                Next Hop       Cnt Last
---   ----  --------  --- ------------          --------       --- ----
10    permit prof1    0   Policy Only           11.1.1.2       0   Dwn
20    permit prof2    0   Policy Last           1.1.1.1        0   Dwn
                                                2.2.2.2        0   Dwn
                                                3.3.3.3        0   Dwn
999   permit everything 0   Policy Only           drop           N/A N/A
65536 deny   deny      0   N/A                   normal fwd     N/A N/A
(21)
```

Legend:

1. The name of the IP policy.
2. The interface where the IP policy was applied.
3. The load distribution setting for IP-policy statements that have more than one next-hop gateway; either first available (the default) or round-robin.
4. The names of the profiles (created with an **acl** statement) associated with this IP policy.
5. The source address and filtering mask of this flow.
6. The destination address and filtering mask of this flow.
7. For TCP or UDP, the number of the source TCP or UDP port.
8. For TCP or UDP, the number of the destination TCP or UDP port.
9. The TOS value in the packet.
10. IP protocol (ICMP, TCP UDP).

11. The sequence in which the statement is evaluated. IP policy statements are listed in the order they are evaluated (lowest sequence number to highest).
12. The rule to apply to the packets matching the profile: either permit or deny
13. The name of the profile (ACL) of the packets to be forwarded using an IP policy.
14. The number of packets that have matched the profile since the IP policy was applied (or since the **clear route-map** command was last used)
15. The method by which IP policies are applied with respect to dynamic or statically configured routes; possible values are Policy First, Policy Only, or Policy Last.
16. The list of next-hop gateways in effect for the policy statement.
17. The number of packets that have been forwarded to this next-hop gateway.
18. The state of the link the last time an attempt was made to forward a packet; possible values are up, dwn, or N/A.
19. Implicit deny rule that is always evaluated last, causing all packets that do not match one of the profiles to be forwarded normally (with dynamic routes).

Chapter 19

ip-redundancy Commands

The **ip-redundancy** commands allow the user to both display and clear the Virtual Router Redundancy Protocol (VRRP) on the Xpedition. VRRP is defined in RFC 2338.

Command Summary

Table 16 lists the **ip-redundancy** commands. The sections following the table describe the command syntax.

Table 16. ip-redundancy commands

clear vrrp statistics interface *<IFnum>*
show vrrp [interface *<IFnum>***] | summary | verbose**

clear vrrp statistics

Purpose

Clears statistics gathered for VRRP.

Format

clear vrrp statistics interface <*IFnum*>

Mode

Privileged

Description

The **clear vrrp statistics** command resets a number of statistics to zero. These statistics include the number of times a Backup router became the Master, the number of VRRP advertisements received, and counts of VRRP packets that contain errors.

Parameters

<*IFnum*>	Causes VRRP statistics to be cleared for all virtual routers on the specified interface.

Restrictions

None.

Example

To clear statistics for virtual routers on interface int1:

```
ssr# clear vrrp statistics interface int1
```

show vrrp

Purpose

Displays parameters for a virtual router.

Format

show vrrp [interface <*IFnum*>**] | summary | verbose**

Mode

Privileged

Description

The **show vrrp** command displays parameters for a virtual router.

Parameters

interface <*IFnum*>
Specifies the interface where the virtual router resides. If you choose this parameter, you may enter the following keywords:

id <*vrid*>	Identifies and displays information about a virtual router. Specify a number between 1-255.
summary	Displays summary information about each virtual router on the interface.
verbose	Displays detailed information about each virtual router on the interface

summary
Displays summary information about each virtual router.

verbose
Displays detailed information about each virtual router.

Restrictions

None.

Examples

To show statistics for virtual router 1 on interface int1:

```
ssr# show vrrp interface int1 1 summary
```

To show statistics for all virtual routers:

```
ssr# show vrrp summary
```

Chapter 20

ip-router Commands

The **ip-router** commands allow the user to monitor features and functions that work across the various routing protocols.

Command Summary

Table 17 lists the **ip-router** commands. The sections following the table describe the command syntax.

Table 17. ip-router commands

ip find rib-route <*IPaddr*> **[ignore-state]**
show gated-config active | permanent
show ip route [summary]
show ip route <*network*> <*mask*> **[detail]**
show ip route state

ip find rib-route

Purpose

Finds the active route in the RIB which the packet will use.

Format

ip find rib-route <*IPaddr*> [**ignore-state]**

Mode

Privileged

Parameters

<*IPaddr*>
Specifies the destination of the packet.

ignore-state
This optional parameter allows inactive routes to be considered in route determination.

Restrictions

None.

show gated-config

Purpose

Displays the active or startup configuration file in GateD format.

Format

show gated-config active | permanent

Mode

Privileged

Parameters

active	Shows the active GateD configuration file in RAM; this is the default.
permanent	Shows the permanent GateD configuration file in NVRAM, if available.

Restrictions

None.

show ip route

Purpose

Displays routing information base.

Format

show ip route [summary]

Mode

Privileged

Description

The **show ip route** command shows the route-manager's routing information base (RIB). For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) next to it. If a route has been the last active route and is also the current active route, then it is shown with a asterisk (*) sign next to it. The legend is as follows:

- "+"Active Route
- "-" Last Active
- "*" Both

If the **summary** option is used, then additional information is displayed about these routes. The announcements bits for the active route are shown, which displays the protocol into which this route is advertised.

Parameters

summary Allows user to view additional information about the routes in the RIB.

Restrictions

None.

Examples:

A sample output of the **show ip route** command:

```
ssr# show ip route
Routing Tables:
Generate Default: no
Destinations: 63776    Routes: 63776
Holddown: 0    Delete: 53811    Hidden: 1
Codes: Network - Destination Network Address
      S - Status + = Best Route, - = Last Active, * = Both
      Src - Source of the route :
      Ag - Aggregate, B - BGP derived, C - Connected
      R - RIP derived, St - Static, O - OSPF derived
      OE - OSPF ASE derived, D - Default
      Next hop - Gateway for the route ; Next hops in use: 4
      Netif - Next hop interface
      Prf1 - Preference of the route, Prf2 - Second Preference of the route
      Metrc1 - Metric1 of the route, Metrc2 - Metric2 of the route
      Age - Age of the route
Network/Mask       S Src Next hop            Netif Prf1 Metrc1 Metrc2       Age
------------       - --- --------           ----- ---- ------ ------       ---
3/8              *   B 134.141.178.33       mls0  170              70:34:28
4/8              *   B 134.141.178.33       mls0  170              70:34:28
4.17.106/24        *   B 134.141.178.33       mls0  170              70:34:28
4.17.115/24        *   B 134.141.178.33       mls0  170              70:34:28
4.24.148.128/25    *   B 134.141.178.33       mls0  170              70:34:28
6/8              *   B 134.141.178.33       mls0  170              70:34:28
6.80.137/24        *   B 134.141.178.33       mls0  170              70:34:28
9.2/16           *   B 134.141.178.33       mls0  170              70:34:28
9.20/17          *   B 134.141.178.33       mls0  170              70:34:28
10.50/16         *   C 10.50.90.1           en    0      0      0 113:31:09
10.60.90/24        *   C 10.60.90.1           mls2    0      0      0 113:31:09
12/8             *   B 134.141.178.33       mls0  170              70:34:28
12.1.248/24        *   B 134.141.178.33       mls0  170              70:34:28
12.2.19/25         *   B 134.141.178.33       mls0  170              12:47:48
12.2.76/24         *   B 134.141.178.33       mls0  170              31:03:36
12.2.97/24         *   B 134.141.178.33       mls0  170              1:41:30
12.2.109/24        *   B 134.141.178.33       mls0  170              87:55:47
12.2.169/24        *   B 134.141.178.33       mls0  170              113:31:01
12.3.63/24         *   B 134.141.178.33       mls0  170              70:34:28
12.4.5/24        *   B 134.141.178.33       mls0  170              70:34:28
12.4.126/24        *   B 134.141.178.33       mls0  170              70:34:28
12.4.164/24        *   B 134.141.178.33       mls0  170              70:34:28
12.4.175/24        *   B 134.141.178.33       mls0  170              95:47:57
12.4.196/22        *   B 134.141.178.33       mls0  170              70:34:28
12.5.48/21         *   B 134.141.178.33       mls0  170              70:34:28
12.5.164/24        *   B 134.141.178.33       mls0  170              113:31:01
12.5.252/23        *   B 134.141.178.33       mls0  170              70:34:28
12.6.42/23         *   B 134.141.178.33       mls0  170              70:34:28
12.6.97/24         *   B 134.141.178.33       mls0  170              70:34:28
```

ITo see a specific route, use the **show ip route** <*network*> command.

show ip route <*network*>

Purpose

Displays the state of GateD.

Format

show ip route <*network*> <*mask*> **[detail]**

Mode

Privileged

Description

The **show ip route** <*network*> command displays a specific route in the route-manager's routing information base (RIB). For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) next to it. If a route has been the last active route and is also the current active route, then it is shown with a asterisk (*) sign next to it. The legend is as follows:

- "+" Active Route
- "-" Last Active
- "*" Both

If the **detail** option is used, then additional information is displayed about this routes. The announcements bits for the active route are shown, which displays the protocol into which this route is advertised.

Parameters

<*network*> <*mask*>
Allows user to specify a particular IP address mask for the RIB route in question.

detail
Allows user to view additional information about the routes in the RIB.

Restrictions

None.

Examples

A sample output of the **ip-router show route detail** command:

```
ssr# show ip route 10.12.1.0/255.255.255.252 detail
10.12.1         mask 255.255.255.252
entries 2    announce 1
TSI:
RIP 150.1.255.255mc  <> metric 1
RIP 222.1.1.255mc  <> metric 1
BGP_Sync_64805 dest 10.12.1/2 metric 0
BGP group type Routing AS 64805 no metrics
Instability Histories:

*Direct    Preference:   0
*NextHop: 10.12.1.2         Interface: 10.12.1.2(to-c4500)
State: <Int Active Retain>
Age: 5:12:10    Metric: 0    Metric2: 0    Tag: 0
Task: IF
Announcement bits(5):
2-KRT 4-RIP.0.0.0.0+520 5-RIP.0.0.0.0+520
6-BGP_Sync_64805
7-BGP_Group_64805
AS Path: IGP (Id 1)

OSPF    Preference: -10
*NextHop: 10.12.1.1         Interface: 10.12.1.2(to-c4500)
State: <NotInstall NoAdvise Int Hidden Gateway>
Local AS: 64805
Age: 1:20:05   Metric: 1    Metric2: -1    Tag: 0
Task: OSPF
AS Path: (64805) IGP (Id 9551)
Cost: 1    Area: 0.0.0.0    Type: Net    AdvRouter:
172.23.1.14
```

In this case there are two routes to network: 10.12.1.0 and 255.255.255.252. One of them is a direct route and other route is learned through OSPF. The direct route has a better preference (lower preference is considered better preference), and is thus the active route. The direct route has been installed since 5 hours, 12 minutes and 10 seconds. This direct route is being announced to the Forwarding Information Base (FIB) which is indicated by KRT, over two RIP interfaces (which is indicated by 4-RIP.0.0.0.0+520, 5-RIP.0.0.0.0+520) and also to the BGP internal peer-group for autonomous system 64805.

To see all the routes in the RIB, use the **show ip route** command.

show ip route state

Purpose

Displays the state of GateD.

Format

show ip route state

Mode

Privileged

Description

The **show ip route state** command displays information on the route-manager's routing information base (RIB).

Parameters

None.

Restrictions

None.

Chapter 21

ipx Commands

The **ipx** commands let you add entries to the Internet Package Exchange (IPX) SAP table for SAP servers and display the IPX forwarding database, RIP table, and SAP table.

Command Summary

Table 18 lists the **ipx** commands. The sections following the table describe the command syntax.

Table 18. ipx commands

ipx find rip *<address>*
ipx find sap [*<type>* **| all] [***<SrvcName>* **| all] [***<network>* **| all]** *<entrytype>*
show ipx buffers
show ipx interface *<IFname>*
show ipx rib destination
show ipx route
show ipx servers {sorted [hops | net | name | type]} | unsorted

ipx find rip

Purpose

Finds an IPX address in the routing table.

Format

ipx find rip <*address*>

Mode

Privileged

Description

The **ipx find rip** command searches for an IPX address in the routing table.

Parameter

<*address*> The IPX network address of this interface. Specify the IPX address using its hexadecimal value.

Restrictions

None.

Example

To find an IPX network in the route table:

```
ssr# ipx find rip A1B2C3F5
```

ipx find sap

Purpose

Finds a SAP entry in the routing table.

Format

ipx find sap [<*type*> | **all] [**<*SrvcName*> | **all] [**<*network*> | **all]** <*entrytype*>

Mode

Privileged

Description

The **ipx find sap** command searches for a SAP entry in the routing table.

Parameters

<*type*> | **all** Defines the types of service. Specify the service type using its hexadecimal value. Specify **all** for all types of service.

<*SrvcName*> | **all**
Defines the IPX service. You can use any characters in the name except the following: “* . / : ; < = > ? [ ] \ |

Note: Lowercase characters are changed to uppercase characters.

Specify **all** for all IPX services.

<*network*> | **all**
Defines the network on which the service resides. Specify an IPX network address in the following format: <*netaddr.*> Example: a1b2c3d4. Specify **all** for all networks.

<*entrytype*> Defines the types of entry you want to find. Specify one of the following:

all Finds static and dynamic SAP entries.

dynamic Finds only the dynamic SAP entries.

static Finds only the static SAP entries.

Restrictions

None.

Example

To find a SAP entry in the route table:

```
ssr# ipx find sap 4 FILESERVER a2b2c3d4 dynamic
```

show ipx buffers

Purpose

Displays the RIP and SAP socket buffer sizes.

Format

show ipx buffers

Mode

Enable

Description

The **show ipx buffers** command displays the RIP and SAP socket buffer sizes.

Parameters

None.

Restrictions

None.

show ipx interface

Purpose

Displays the configuration of IPX interfaces.

Format

show ipx interface <*IFname*> **[brief]**

Mode

Privileged

Description

The **show ipx interface** command displays the configuration of an IPX interface. If you issue the command without specifying an interface name then the configuration of all IPX interfaces is displayed.

Parameters

<*IFname*>	Name of the IPX interface; for example, ssr14.
brief	Displays a brief summary of IPX interface status and configuration.

Restrictions

If you specify an interface name, the name must belong to an existing IPX interface.

Example

To display the configuration of all IPX interfaces:

```
ssr# show ipx interface
ethernet5/1 is administratively up, link state is down
IPX address is 00000FFF.00:00:1D:17:ED:23 encapsulation ARPA
ethernet6/1 is administratively up, link state is down
IPX address is 00000FF4.00:00:1D:17:ED:23 encapsulation ARPA
```

show ipx rib destination

Purpose

Show IPX RIP table output sorted by destination.

Format

show ipx rib destination

Mode

User

Description

The **show ipx rib destination** command displays IPX RIP table output sorted by destination.

Parameters

None.

Restrictions

None.

show ipx servers

Purpose

Displays IPX server information.

Format

show ipx servers {sorted [hops | net | name | type]} | unsorted

Mode

User

Description

The **show ipx servers** command displays IPX server information sorted by any, all, or none of the optional arguments. Sorting is done based on the order of optional arguments given.

Parameters

sorted Confirms that user wants information sorted. Accompanies one or all of the following arguments:

- **hops** Sorts by number of hops away the service is.
- **net** Sorts by the interface type over which the service arrived.
- **name** Sorts by the Sap service name.
- **type** Sorts by the Sap service type.

unsorted Confirms that user does not want information sorted.

Restrictions

None.

show ipx route

Purpose

Shows summary of the IPX RIP / SAP tables.

Format

show ipx route

Mode

User

Description

The **show ipx route** command displays a summary of the IPX RIP / SAP tables.

Parameters

None

Chapter 22

irdp Command

The **show ip irdp** command displays the state of router discovery on the Xpedition.

Format

show ip irdp

Mode

Privileged

Description

The **show ip irdp** command displays the state of router discovery on the Xpedition.

Parameters

None.

Restrictions

None.

Examples

To display router discovery information:

```
ssr# show ip irdp


Task State: <Foreground NoResolv NoDetach> (1)

   Send buffer size 2048 at 812C68F8
   Recv buffer size 2048 at 812C60D0

Timers:

   RouterDiscoveryServer Priority 30

      RouterDiscoveryServer_SSR2_SSR3_IP <OneShot>
        last: 10:17:21 next: 10:25:05 (2)

Task RouterDiscoveryServer:
   Interfaces:
      Interface SSR2_SSR3_IP: (3)
         Group 224.0.0.1: (4)
            minadvint 7:30 maxadvint 10:00 lifetime 30:00 (5)

            Address 10.10.5.254: Preference: 0 (6)

   Interface policy:
      Interface SSR2_SSR3_IP* MaxAdvInt 10:00 (7)
```

Legend:

1. Information about the RDISC task.
2. Shows when the last router advertisement was sent and when the next advertisement will be sent.
3. The interface on which router advertisement is enabled.
4. Multicast address.
5. Current values for the intervals between the sending of router advertisements and the lifetime of addresses sent in a router advertisement.
6. IP address that is included in router advertisement. The preference of this address as a default route is 0, the default value.
7. Shows configured values for the specified interface.

Chapter 23

load-balance Commands

The **load-balance** commands allow you to distribute session load across a pool of servers. These commands provide a way to load balance network traffic to multiple servers.

Command Summary

Table 19 lists the **load-balance** commands. The sections following the table describe the command syntax.

Table 19. load-balance commands

load-balance set server-status
show load-balance acv-options
show load-balance hash-stats
show load-balance source-mappings
show load-balance statistics
show load-balance virtual hosts

load-balance set server-status

Purpose

Sets the status of a load balancing server.

Format

load-balance set server-status

Mode

Privileged

Description

The **load-balance set server-status** command allows you to set the status of a load balancing server.

Parameters

None.

Restrictions

None.

show load-balance acv-options

Purpose

Displays load balance application content verification (acv) options.

Format

show load-balance acv-options

Mode

Privileged

Description

The **show load-balance acv-options** command allows you to display load balancing acv options.

Parameters

None.

Restrictions

None.

show load-balance hash-stats

Purpose

Displays load balancing hashing statistics.

Format

show load-balance hash-stats

Mode

Privileged

Description

The **show load-balance hash-stats** command allows you to display load balancing hash statistics.

Parameters

None.

Restrictions

None.

Example

To display hash statistitics:

```
ssr# show load-balance hash-stats
Total Mappings: 4502

Top 10 Hash Depths:

+---------+---------------+-----------------------+
| Index |  Hash Depth  | Hash Depth Occurence |
+---------+---------------+-----------------------+
|1      |0             |11882                  |
|2      |1             |4226                   |
|3      |2             |138                    |
+---------+---------------+-----------------------+

Top 10 Hash Depth Occurences:

+---------+-----------------------+---------------+
| Index | Hash Depth Occurence |  Hash Depth  |
+---------+-----------------------+---------------+
|1      |11882                  |0             |
|2      |4226                   |1             |
|3      |138                    |2             |
+---------+-----------------------+---------------+
```

show load-balance source-mappings

Purpose

Displays load balancing source-destination bindings.

Format

show load-balance source-mappings

Mode

Privileged

Description

The **show load-balance source-mappings** command allows you to display load balancing source-destination bindings.

Parameters

None.

Restrictions

None.

Example

To display source-destination bindings:

```
ssr# show load-balance source-mappings

Current Mappings:

FC: Flow Count
AC: Age Count
SPort: Source Port
VPort: Virtual Port
DPort: Destination Port

+---------------+-----+---------------+-----+---------------+-----+----+----+
| Source Address |Sport| Virtual IP |VPort| Dst. Address |DPort| FC | AC |
+---------------+-----+---------------+-----+---------------+-----+----+----+
|70.1.0.71 |1024 |50.1.1.18 |80 |52.1.1.73 |80 |2 |0 |
|70.1.0.71 |1025 |50.1.1.17 |80 |52.1.1.71 |80 |2 |0 |
|70.1.0.72 |1026 |50.1.1.17 |80 |52.1.1.72 |80 |2 |0 |
|70.1.0.72 |1027 |50.1.1.18 |80 |52.1.1.74 |80 |2 |0 |

4 source mapping(s) displayed.
```

show load-balance statistics

Purpose

Displays load balancing statistics.

Format

show load-balance statistics

Mode

Privileged

Description

The **show load-balance statistics** command allows you to display load balancing statistics.

Parameters

None.

Restrictions

None.

Example

To display load balance statistics:

```
ssr# show load-balance statistics

Load Balancing Packets Dropped:
      No Such Virtual-IP Packet drop count: 73
      TTL expired Packet drop count: 0

Load Balance Group Statistics:

      Group Name: telnet Virtual-IP: 50.1.1.17 Virtual-Port: 23
            No destination selected Packet drop count            : 0
            Memory Allocation error Packet drop count            : 0
            No forward route found Packet drop count             : 0
            Number of Packets forwarded                          : 23437
            Channel not Load Balancing compliant Packet drop count : 0
            No hosts in group Packet drop count                  : 0
            Client in Access List Packet drop count              : 2

      Group Name: http Virtual-IP: 50.1.1.17 Virtual-Port: 80
            No destination selected Packet drop count            : 2
            Memory Allocation error Packet drop count            : 0
            No forward route found Packet drop count             : 0
            Number of Packets forwarded                          : 34429
            Channel not Load Balancing compliant Packet drop count : 0
            No hosts in group Packet drop count                  : 0
            Client in Access List Packet drop count              : 1

Statistics of 2 groups shown.
```

show load-balance virtual-hosts

Purpose

Displays hosts in a load balancing group.

Format

show load-balance virtual-hosts

Mode

Privileged

Description

The **show load-balance virtual-hosts** command allows you to display the hosts in a load balancing group.

Parameters

None.

Restrictions

None.

Example

To display load balance groups:

```
ssr# show load-balance virtual-hosts

Load Balanced Groups:

Flow Mode Count: 0

OS: Operational state of server
AS: Admin state of server

+---------------+---------------+------+-------------+----------+------------+
|   Group Name  |   Virtual IP  | Port | Hosts Added | Hosts Up | Next Index |
+---------------+---------------+------+-------------+----------+------------+
|telnet         |50.1.1.17      |23    |2            |2         |0           |
+---------------+---------------+------+-------------+----------+------------+
+-------+---------------+------+----------------+----+----+------------+
| Index |    Host IP    | Port |  Client Count  | OS | AS | Load Count |
+-------+---------------+------+----------------+----+----+------------+
|0      |52.1.1.73      |23    |0               |Up  |Up  |0           |
|1      |52.1.1.74      |23    |0               |Up  |Up  |0           |
+-------+---------------+------+----------------+----+----+------------+


+---------------+---------------+------+-------------+----------+------------+
|   Group Name  |   Virtual IP  | Port | Hosts Added | Hosts Up | Next Index |
+---------------+---------------+------+-------------+----------+------------+
|http           |50.1.1.17      |80    |2            |2         |0           |
+---------------+---------------+------+-------------+----------+------------+
+-------+---------------+------+----------------+----+----+------------+
| Index |    Host IP    | Port |  Client Count  | OS | AS | Load Count |
+-------+---------------+------+----------------+----+----+------------+
|0      |52.1.1.71      |80    |0               |Up  |Up  |0           |
|1      |52.1.1.72      |80    |0               |Up  |Up  |0           |
+-------+---------------+------+----------------+----+----+------------+
```

Chapter 24

logout Command

The **logout** command ends the CLI session.

Format

logout

Mode

All modes

Description

The **logout** command ends your CLI session. If you have uncommitted changes in the scratchpad, a message warns you that the changes are not saved and gives you an opportunity to cancel the logout and save the changes.

Parameters

None.

Restrictions

None.

Chapter 25

mac-address-table Commands

The **mac-address-table** commands allow the user to display various L2 tables related to Media Access Control (MAC) addresses.

Command Summary

Table 20 lists the **mac-address-table** commands. The sections following the table describe the command syntax.

Table 20. mac-address-table commands

show mac-address-table all-flows [vlan <*VLAN-num*>**] [source-mac** <*mac*>**] [undecoded]**
show mac-address-table all-macs [vlan <*VLAN-num*>**] [source-mac** <*mac*>**] [source] [destination] [multicast]**
show mac-address-table bridge-management
show mac-address-table igmp-mcast-registration [vlan <*VLAN-num*>**]**
show mac-address-table address <*MACaddr*> **vlan** <*vlan-num*>
show mac-address-table mac-table-stats
show mac-address-table port-macs <*port-list*> **| all-ports [verbose [vlan** <*VLAN-num*>**] [source] [destination] [multicast] [undecoded] [no-stats]]**
show mac-address-table vlan-igmp-status vlan <*vlan-num*>

show mac-address-table all-flows

Purpose

Shows all L2 flows (for ports in flow-bridging mode).

Format

show mac-address-table all-flows [vlan <*VLAN-num*>**] [source-mac** <*mac*>**] [undecoded]**

Mode

User or Privileged

Description

The **show mac-address-table all-flows** command shows all the L2 flows learned by the Xpedition. The Xpedition learns flows on ports that are operating in flow-bridging mode.

Parameters

vlan <*VLAN-num*>
Specifies the VLAN number associated with the flows. The VLAN number can be from 1 – 4095.

source-mac <*mac*>
Specifies the source MAC address of the flows. Enter the MAC address in either of the following formats:

xx:xx:xx:xx:xx:xx
xxxxxx:xxxxxx

source
Specifies the source address associated with the flows.

destination
Specifies the destination address associated with the flows.

multicast
Specifies the multicast address associated with the flows.

Restrictions

None.

show mac-address-table all-macs

Purpose

Displays all MAC addresses currently in the L2 tables.

Format

show mac-address-table all-macs [vlan <*VLAN-num*>**] [source-mac** <*mac*>**] [source] [destination] [multicast]**

Mode

User or Privileged

Description

The **show mac-address-table all-macs** command shows how many MAC addresses the Xpedition has in its L2 tables. You can format the displayed information based on VLAN, source MAC address, destination MAC address or multicast.

Parameters

vlan <*VLAN-num*>Displays only MAC addresses in the specified VLAN.

source-mac <*MACaddr*>
Displays only the source MACaddress. Specify this address in either of the following formats:

xx:xx:xx:xx:xx:xx
xxxxxx:xxxxxx

source Displays only source addresses.

destination Displays only destination addresses.

multicast Displays only multicast and broadcast addresses.

Restrictions

None.

show mac-address-table bridge-management

Purpose

Shows information about all MAC addresses registered by the system.

Format

show mac-address-table bridge-management

Mode

User or Privileged

Description

The **show mac-address-table bridge-management** command shows MAC addresses that have been inserted into the L2 tables for management purposes. Generally, these entries are configured so that a port forwards a frame to the Control Module if the management MAC matches the frame's destination MAC.

An example of a bridge-management MAC is Spanning Tree's bridge group address (0180C2:000000), which is be registered in the L2 tables of Xpedition ports on which the Spanning Tree Protocol (STP) is enabled.

Parameters

None.

Restrictions

None.

show mac-address-table igmp-mcast-registration

Purpose

Displays information about multicast MAC addresses registered by IGMP.

Format

show mac-address-table igmp-mcast-registration [vlan <*VLAN-num*>**]**

Mode

User or Privileged

Description

The **show mac-address-table igmp-mcast-registration** command displays the multicast MAC addresses that IGMP has registered with the L2 tables. The Xpedition forwards the multicast MAC addresses only to the ports that IGMP specifies.

Parameters

vlan <*VLAN-num*>	Displays only the multicast MAC addresses registered for the specified VLAN.

Restrictions

None.

show mac-address-table address

Purpose

Displays information about a particular MAC address.

Format

show mac-address-table address <*MACaddr*> **vlan** <*VLAN-num*>

Mode

User or Enable

Description

The **show mac-address-table address** command displays the port number on which the specified MAC address resides.

Parameters

<*MACaddr*> Specifies a MAC address. Enter the MAC address in either of the following formats:

xx:xx:xx:xx:xx:xx
xxxxxx:xxxxxx

vlan <*VLAN-num*>Displays the MAC address for this VLAN.

Restrictions

None.

show mac-address-table mac-table-stats

Purpose

Displays statistics for the MAC addresses in the MAC address tables.

Format

show mac-address-table mac-table-stats

Mode

User or Privileged

Description

The **show mac-address-table mac-table-stats** command displays statistics for the master MAC address table in the Control Module and the MAC address tables on the individual ports.

Parameters

None.

Restrictions

None.

show mac-address-table port-macs

Purpose

Displays information about MACs residing in a port's L2 table.

Format

show mac-address-table port-macs <*port-list*> **| all-ports [verbose [vlan** <*VLAN-num*>**] [source] [destination] [multicast] [undecoded] [no-stats]]**

Mode

User or Privileged

Description

The **show mac-address-table port-macs** command shows the information about the learned MAC addresses in individual L2 MAC address tables. Each port has its own MAC address table. The information includes the number of source MAC addresses and the number of destination MAC addresses in the table. If you enter the **verbose** option, the MAC addresses also are displayed.

Parameters

<*port-list*> **| all-ports**
Specifies the port(s) for which you want to display MAC address information. You can specify a single port or a comma-separated list of ports. If you use the **all-ports** keyword, MAC address information is displayed for all ports.

verbose
Shows detailed statistics for each MAC address entry.

vlan <*VLAN-num*>
Specifies the type of MAC address for which you want to show statistics.

source
Displays statistics for only source addresses.

destination
Displays statistics for only destination addresses.

multicast
Displays statistics for only multicast and broadcast addresses.

undecoded
Displays the MAC addresses in hexadecimal format rather than undecoded format. Undecoded format dos not show the vendor name in place of the first three hexadecimal digits (example: Enterasys:33:44:55). The default is undecoded (example: 00:11:22:33:44:55).

no-stats
Lists the MAC addresses without displaying any statistics.

Restrictions

None.

show mac-address-table vlan-igmp-status

Purpose

Shows whether IGMP is on or off on a VLAN.

Format

show mac-address-table vlan-igmp-status vlan <*VLAN-num*>

Mode

Privileged

Description

The **show mac-adress-table vlan-igmp-status** command shows the multicast MAC addresses that IGMP has registered with the L2 tables. This command also shows the ports to which the multicast MAC addresses are forwarded.

Note: For IGMP forwarding to occur for a multicast MAC address, IGMP must be enabled on the VLAN with which the MAC address is associated.

Parameters

vlan <*VLAN-num*>Specifies the VLAN number. The VLAN number can range from 1 – 4095.

Restrictions

None.

Chapter 26

mtrace Command

The **mtrace** command tracks the multicast path from a source to the Xpedition.

Format

mtrace <*source*>

Mode

Privileged

Description

The **mtrace** command tracks the multicast path from a source to a receiver. A trace probe is sent in a reverse path from the receiver back to the source. As the probe passes from hop to hop, it collects information such as interface address and packet counts from each router. Because the **mtrace** command is executed with only the source parameter, a multicast path is calculated from the source to the Xpedition.

Parameters

<*source*>	IP address of the source.

Restrictions

None.

Examples

To display the multicast path from IP address 2.2.2.2 to the Xpedition:

```
ssr# mtrace 2.2.2.2
```

Chapter 27

multicast Commands

The **multicast** commands allow the user to display information about IP multicast interfaces.

Command Summary

Table 21 lists the **multicast** commands. The sections following the table describe the command syntax.

Table 21. multicast commands

show ip multicast interface
show mroute [child <*IPaddr*>**] [group** <*IPaddr*>**] [parent** <*IPaddr*>**]**

show ip multicast interface

Purpose

Displays information about IP multicast interfaces.

Format

show ip multicast interface

Mode

Privileged

Description

The **show ip multicast interface** command displays interfaces that are running IGMP or DVMRP.

Note: This command is a superset of the **show dvmrp interface** and **show igmp interface** commands.

Parameters

None.

Restrictions

None.

Example

To display IP multicast information:

```
ssr# show ip multicast interface

Address: 172.1.1.10 Subnet: 172.1.1/24 Met: 1 Thr: 1
Name : mls15 State: Up Querier Leaf Igmp Dvmrp

Address: 207.135.89.64 Subnet: 207.135.89.0/25 Met: 1 Thr: 1
Name : company State: Up Querier Leaf Igmp Dvmrp
Groups : 224.0.1.12
224.1.127.255
224.0.1.24
224.2.127.253
224.2.127.254

Address: 10.135.89.10 Subnet: 10.135.89.0/25 Met: 1 Thr: 1
Name : test State: Up Querier Igmp Dvmrp
Peer : 10.135.89.67 Flags: 0xe Version: 3.255

Address: 190.1.0.1 Subnet: 190.1/16 Met: 1 Thr: 1
Name : rip State: Dis

Address: 207.135.122.11 Subnet: 207.135.122.8/29 Met: 1 Thr: 1
Name : mbone State: Up Igmp Dvmrp
Peer : 207.135.122.10 Flags: 0xe Version: 3.255
Groups : 224.0.1.11
224.0.1.12
224.2.127.254
239.255.255.255
224.2.127.253

Address: 10.40.1.10 Subnet: 10.40.1/24 Met: 1 Thr: 1
Name : downstream State: Up Dvmrp
Peer : 10.40.1.1 Flags: 0xf Version: 3.255

Address: 10.100.1.1 Subnet: 10.100.1/24 Met: 1 Thr: 1
Name : dan State: Dn Dvmrp
```

show mroute

Purpose

Displays the IP multicast routing table.

Format

show mroute [child <*IPaddr*>**] [group** <*IPaddr*>**] [parent** <*IPaddr*>**]**

Mode

Privileged

Description

The **show mroute** command displays the IP multicast routing table entry for the specified multicast group address.

This command lists all the multicast distribution trees, showing the parent interface (from where the traffic is coming), and the children distribution interfaces (to which the traffic is being forwarded). It would also show any cache information available either in hardware forwarding mechanism or in the main processor (for software based forwarding).

Note: The cache information can be timed out when not enough traffic is present, but multicast routes can still be present. Cache information is presented in number of flows (Layer 4 sessions). Multicast routes stay at least for 5 minutes, while the hardware forwarding mechanism can time out a flow faster.
Any pruning information, if present, is also shown.

The search can always be narrowed by looking at a particular group, and/or looking at a particular parent interface, and/or looking at a particular child interface.
Multicast routes are not the same as DVMRP routes.

Parameters

child <*IPaddr*> Address of a child interface.

group <*IPaddr*> Address of a multicast group.

parent <*IPaddr*> Address of a parent interface.

Restrictions

None.

Examples

To display the IP multicast route entry for the group 225.0.0.10:

```
ssr# show mroute group 225.0.0.10
```

Below is a fuller example of the output from this command:

```
ssr# show mroute
Network: 130.207.8/24 Group: 224.2.1.1 Age: 99s
Parent : mbone Child: test
downstream
Source : 130.207.8.82 Pkts: 383 Flows: 1

Network: 131.120.63/24 Group: 224.2.1.1 Age: 63s
Parent : mbone Pruned Child: test Pruned
downstream Pruned
Source : 131.120.63.33 Pkts: 0 Flows: 0

Network: 147.6.65.0/25 Group: 224.2.2.1 Age: 48s
Parent : mbone Pruned Child: test Pruned
downstream Pruned
Source : 147.6.65.38 Pkts: 0 Flows: 0
```

Chapter 28

nat Commands

The **nat** commands allow the user to clear and display Network Address Translation (NAT) bindings for local (inside) and global (outside) network addresses.

Command Summary

Table 22 lists the **nat** commands. The sections following the table describe the command syntax.

Table 22. nat commands

clear ip nat out-of-globals | port-mode
clear ip nat translation [pool-specified [local-acl-pool <*local-ACL*>**] [global-pool** <*IPaddr/IPaddr-range*>**]]**
show ip nat [statistics | timeouts | translations]

clear ip nat

Purpose

Clears NAT error statistics.

Format

clear ip nat out-of-globals | port-mode

Mode

Privileged

Description

The **clear ip nat** command allows you to clear specific NAT error statistics such as out-of-globals messages in the case of dynamic bindings and port misconfiguration.

Parameters

out-of-globals Clears error statistics during dynamic binding in the case where there are no more global IP addresses in the global address pool.

port-mode Clears error statistics that occur because of port misconfigurations. Such cases are where the port is set to either destination-based forwarding or host-flow based forwarding.

Restrictions

None

Example

To clear all out-of-global error statistics:

```
ssr# clear ip nat out-of-globals
```

clear ip nat translation

Purpose

Clears dynamic NAT bindings.

Format

clear ip nat translation [pool-specified [local-acl-pool <*local-ACL*>**] [global-pool** <*IPaddr/IPaddr-range*>**]]**

Mode

Privileged

Description

The **clear ip nat translation** command deletes dynamic address bindings. You can delete the dynamic address bindings for specific address pools.

Parameters

pool-specified
Deletes NAT dynamic bindings based on local and global acl pools.

local-acl-pool <*local-ACL*>
The ACL that corresponds to the local IP address pool.

global-pool <*IPaddr/IPaddr-range*>
The global address pool, defined in one of the following ways:

A single IP address in the form a.b.c.d

An IP address range in the form 10.10.1.1-10.10.1.50

IP address and mask in the form 1.2.0.0 / 255.255.0.0 or 1.2.3.0 / 16

Restrictions

None.

Examples

To delete dynamic address bindings for the local address pool that corresponds to the ACL ‘lcl’ and the global address pool that corresponds to 136.1.1.1-136.1.1.254:

```
ssr# clear ip nat translation pool-specified local-acl-pool lcl global-pool 136.1.1.0/24
```

show ip nat

Purpose

Displays NAT information.

Format

show ip nat [statistics | timeouts | translations]

Mode

Privileged

Description

The **show ip nat** command allows you to display NAT address statistics, timeouts, and translations.

Parameters

statistics	Displays NAT statistics.
timeouts	Displays the current set of timeouts.
translations	Displays NAT translations.

Restrictions

None.

Examples

To display active NAT translations:

```
ssr# show ip nat translations

Proto Local/Inside          Global/Outside IP     Type           No. of flows
----- --------------------- --------------------- -------------- ------------
TCP   15.15.15.15:1896      100.1.1.1:1026        Dyn. ovr.      2
TCP   15.15.15.15:1897      100.1.1.1:1028        Dyn. ovr.      0
TCP   15.15.15.15:1894      100.1.1.1:1024        Dyn. ovr.      2
TCP   15.15.15.15:1895      100.1.1.1:1025        Dyn. ovr.      2
TCP   15.15.15.15:1892      100.1.1.1:1027        Dyn. ovr.      0
IP    10.10.10.10:*         200.1.1.1:*           Dynamic        20
IP    4.4.4.4:*             202.1.1.1:*           Static         789
```

To display NAT timeouts:

```
ssr# show ip nat timeouts

All values in minutes
Flow    FTP Sess.  DNS Sess.  Dyn. Sess.
------  ---------  ---------  ----------
2       30         30         1440
```

Chapter 29

ntp Commands

The **ntp** commands configure and display the characteristics of the NTP (Network Time Protocol) client.

Command Summary

Table 23 lists the **ntp** commands. The sections following the table describe the command syntax.

Table 23. ntp commands

ntp synchronize server *<host>*
show ntp

ntp synchronize server

Purpose

Manually forces the Xpedition to immediately synchronize with an NTP server.

Format

ntp synchronize server <*host*>

Mode

Privileged

Description

The **ntp synchronize server** command forces the Xpedition to immediately synchronize its clock with the NTP server.

Parameters

<*host*> Specifies the hostname or the IP address of the NTP server.

Restrictions

None.

Examples

To synchronize the Xpedition against the NTP server 10.13.1.1:

```
ssr# ntp synchronize server 10.13.1.1
%NTP-I-TIMESYNC, Time synchronized to Thu Aug 3 23:11:28 2000
```

show ntp

Purpose

Displays NTP information about the Xpedition.

Format

show ntp

Mode

Privileged

Description

The **show ntp** command displays various NTP information about the Xpedition, for example, the last time a successful synchronization was made, synchronization interval, NTP version number, etc.

Parameters

None.

Restrictions

None.

Example

```
ssr# show ntp
NTP status:
        Synchronization interval: 60 mins
        Version: NTPv3
        Last successful contact: Thu Jan 23 23:08:15 1999
```

Chapter 30

ospf Commands

The **ospf** commands allow the user to display parameters for the Open Shortest Path First (OSPF) routing protocol.

Command Summary

Table 24 lists the **ospf** commands. The sections following the table describe the command syntax.

Table 24. ospf commands

show ip ospf
show ip ospf interface

show ip ospf

Purpose

Displays OSPF information.

Format

show ip ospf

Mode

Privileged

Description

The **show ip ospf** command displays information about the OSPF.

Parameters

None.

Restrictions

None.

show ip ospf interface

Purpose

Displays OSPF interfaces.

Format

show ip ospf interface

Mode

Privileged

Description

The **show ip ospf interface** command displays all OSPF interfaces.

Parameters

None.

Restrictions

None.

Chapter 31

ping Command

The **ping** command tests connection between the Xpedition and an IP host.

Format

ping <*hostname-or-IPaddr*> **packets** <*num*> **size** <*num*> **wait** <*num*> **[flood] [dontroute]**

Mode

Privileged

Description

The **ping** command test connection between the Xpedition and an IP host. The ping command sends ICMP echo packets to the host you specify.

- If the packets reach the host, the host sends a ping response to the Xpedition and the CLI displays messages stating that the host can be reached.
- If the host does not respond, the Xpedition assumes the host cannot be reached from the Xpedition and the CLI display messages stating that the host did not reply.

Parameters

<*hostname-or-IPaddr*>
The host name or IP address you want to ping.

packets <*num*>
The number of ping packets you want to send. The default is 1.

size <*num*>
The packet size. For Ethernet, specify a number from 0 – 1364.

wait <*num*>
The number of seconds the Xpedition will wait for a positive response from the host before assuming that the host has not responded. The default is 1.

flood
Causes the Xpedition to send a new ping request as soon as a ping reply is received. If you do not specify the **flood** option, the Xpedition waits to send a new request. The amount of time the Xpedition waits is specified by the **wait** option.

dontroute
Restricts the ping to locally attached hosts.

Restrictions

None.

Chapter 32

port Commands

The **port** commands display the following parameters:

- Port state (enabled or disabled)
- Bridging status (flow-based or address-based)
- Port operating mode (half duplex or full duplex)
- Port speed for the 10/100 ports (10-Mbps or 100-Mbps)
- Port mirroring (used for analyzing network traffic)
- Port shut down if broadcast threshold is reached

Command Summary

Table 25 lists the **port** commands. The sections following the table describe the command syntax.

Table 25. port commands

show bmon
show bridging
show interfaces accounting | <*port-list*>
show port 8021
show port auto-negotiation <*port-list*>
show port auto-negotiation capabilities <*port-list*>
show port MAU [<*port-list*>**]**
show port MAU-statistics [<*port-list*>**]**

Table 25. port commands (Continued)

show port mirroring [<*port-list*>**| acls]**
show port status <*port-list*>
show pvst <*name*> **interface** <*port-list*>
show stp interface <*port-list*>
show vlan interface <*port-list*>

show bmon

Purpose

Displays broadcast monitoring information for Xpedition ports.

Format

show bmon

Mode

Privileged

Description

The **show bmon** command allows the user to display broadcast monitoring information for all Xpedition ports.

Parameters

None.

Restrictions

None.

Example

To display the state of ports with broadcast monitoring:

```
ssr# show bmon
Port: ethernet1/1 State: On

Port: ethernet6/8 State: ShutDn Expire: 39 (sec)

Port: ethernet7/8 State: On
```

The above example shows three ports, with the port ethernet6/8 shut down for 39 seconds.

show bridging

Purpose

Displays the bridging status of all Xpedition ports.

Format

show bridging

Mode

Privileged

Description

The **show bridging** command lets you display bridging-status information for all Xpedition ports.

Parameters

None.

Restrictions

None.

Example

To display the bridging status for available ports:

```
ssr# show bridging
Port        Mgmt Status  phy-state     link-state Bridging Mode
----        -----------  ---------     ---------- -------------
ethernet4/1      No Action    Disabled      Link Down  Address
ethernet4/2      No Action    Disabled      Link Down  Address
ethernet4/3      No Action    Forwarding    Link Up    Address
ethernet4/4      No Action    Disabled      Link Down  Address
ethernet4/5      No Action    Disabled      Link Down  Address
ethernet4/6      No Action    Forwarding    Link Up    Address
ethernet4/7      No Action    Disabled      Link Down  Address
ethernet4/8      No Action    Disabled      Link Down  Address
```

show interfaces

Purpose

Displays the user defined descriptions of Xpedition ports.

Format

show interfaces accounting | <*port-list*>

Mode

Privileged

Description

The **show interfaces** command allows you display the user defined description for Xpedition ports.

Parameters

accounting	Displays interface accounting.
<*port-list*>	Specifies the port(s) for which you want to display the description(s).

Restrictions

This command is valid for Ethernet and WAN only.

Examples

To display status for ethernet3/1-2:

```
ssr# show interfaces ethernet3/1-2
ethernet3/1 is administratively up, link state is up
Hardware is 10/100-Mbit Ethernet, address is 0000.1d17.ed21
  Internet address is 100.1.2.1/24
  MTU 1522 bytes, Speed 1 Mbits
  Encapsulation ETHERNET_II, loopback not set, Half duplex
  ARP type: ARPA, ARP keep-time not set (permanent)
  Statistics was never cleared.
  Five minute input rate 1008 bits/sec, 1 packets/sec
  Five minute output rate 1008 bits/sec, 1 packets/sec
    3198 packets input, 402886 bytes, 0 no buffer
    Received 0 multicast, 0 broadcast, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 bad frames, 0 overrun
    3252 packets output, 409205 bytes, 0 underruns
    Received 56 multicast, 56 broadcast
    0 output errors, 0 collisions, 0 late collisions
    0 deferred, 0 false carriers, 0 buffer failures
ethernet3/2 is administratively up, link state is down
  Hardware is 10/100-Mbit Ethernet, address is 0000.1d17.ed21
  Internet address is 100.1.3.1/24
  MTU 1522 bytes, Speed N/A
  Encapsulation ETHERNET_II, loopback not set
  ARP type: ARPA, ARP keep-time not set (permanent)
  Statistics was never cleared.
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 multicast, 0 broadcast, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 bad frames, 0 overrun
    0 packets output, 0 bytes, 0 underruns
    Received 0 multicast, 0 broadcast
    0 output errors, 0 collisions, 0 late collisions
    0 deferred, 0 false carriers, 0 buffer failures
```

To display accounting statistics for all ports:

```
ssr# show interfaces accounting
Interface ethernet6/1:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total        3486      439174        3541      445747
            IP            0           0           0           0
           IPX            0           0           0           0
Interface ethernet6/2:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total           0           0           0           0
            IP            0           0           0           0
Interface ethernet6/3:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total           0           0           0           0
            IP            0           0           0           0
Interface ethernet6/4:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total           0           0           0           0
            IP            0           0           0           0
Interface ethernet6/5:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total           0           0           0           0
            IP            0           0           0           0
Interface ethernet6/6:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total           0           0           0           0
            IP            0           0           0           0
Interface ethernet6/7:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total           0           0           0           0
            IP            0           0           0           0
Interface ethernet6/8:
        Protocol     Pkts In    Bytes In    Pkts Out   Bytes Out
          Total         103       12346           1         126
            IP            0           0           0           0
```

show port 8021p

Purpose

Displays 802.1p encapsulation status.

Format

show port 8021p

Mode

Privileged

Description

The **show port 8021p** command displays whether 802.1p encapsulation is enabled or disabled on a port or list of ports. The 802.1p standard provides the ability to classify traffic into eight priority categories or class of services. This classification scheme is based upon MAC frame information and is used for QoS (Quality of Service) for VLANs.

Parameters

None.

Restrictions

None.

Example

To display 802.1p encapsulation status for port ethernet2/1:

```
ssr# port show 8021p ethernet2/1

Port        802.1p Status
 ----        -------------
 ethernet2/1        Disabled
```

show port auto-negotiation

Purpose

Displays auto-negotiation information.

Format

show port auto-negotiation <*port-list*>

Mode

Privileged

Description

The **show port auto-negotiation** command displays auto-negotiation information. This command displays port number, administration status, current status, remote signaling, fault advertised, and fault received. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

Parameters

<*port-list*>	Specifies the ports for which you want to display the description. Failing to specify a port will result in the display of all the Xpedition ports.

Restrictions

None.

Example

To display auto-negotiation information for port ethernet2/1:

```
ssr# show port autonegotiation ethernet2/1

              Admin    Current      Remote      Fault        Fault
Port   Status  Status       Signalling  Advertised   Received
------ -------- ------------ ----------- ------------ ----------
ethernet2/1  disabled  other        not detected  n/a          n/a
```

show port autonegotiation-capabilities

Purpose

Displays auto-negotiation capabilities.

Format

port show auto-negotiation capabilities <*port-list*>

Mode

Privileged

Description

The **show port auto-negotiation capabilities** command displays a list of port capabilities, advertised capabilities, and any received capabilities from another port. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

Parameters

<*port-list*>	Specifies the ports for which you want to display capabilities. Failing to specify a port will result in the display of all the Xpedition ports.

Restrictions

None.

Example

To display auto-negotiation capabilities for port ethernet2/1:

```
ssr# show port autonegotiation-capabilities ethernet2/1

Port    Capability       Advertised       Received
------  ---------------  ---------------  ---------------
et2/1   other            other
        10 baseT         10 baseT
        10 baseT FD      10 baseT FD
        100 baseT4       100 baseT4
        100 baseTX       100 baseTX
        100 baseTX FD    100 baseTX FD
        100 baseT2       100 baseT2
        100 baseT2 FD    100 baseT2 FD
        Pause            Pause
        Asymetric Pause  Asymetric Pause
        Symmetric Pause  Symmetric Pause
        Asym-Sym Pause   Asym-Sym Pause
        1000 baseX       1000 baseX
        1000 baseX FD    1000 baseX FD
        1000 baseT       1000 baseT
        1000 baseT FD    1000 baseT FD
```

show port MAU

Purpose

Displays Media Access Control information.

Format

show port MAU <*port-list*>

Mode

Privileged

Description

The **show port MAU** command displays Media Access Control (MAC) information. This command displays port number, media type, default media type, jack type, operational status, and support level.

Parameters

<*port-list*>	Specifies the ports for which you want to display the description.

Restrictions

None.

Example

To display MAC information for port ethernet2/1:

```
ssr# show port MAU ethernet2/1

Port     MUA Type        Default Type     Jack Type   Status Supported
------   --------------  --------------   ---------   -----------   ---
et.2.1   100 BaseFX HD    100 BaseFX HD    fiber SC    operational   no
```

show port MAU-statistics

Purpose

Displays Media Access Control statistics.

Format

show port MAU-statistics <*port-list*>

Mode

Privileged

Description

The **show port MAU-statistics** command displays Media Access Control (MAC) statistics. This command displays port number, media availability, media availability state exits totals, jabber (excessively long frames) state, jabbering state enters totals, and false carriers totals.

Parameters

<*port-list*>	Specifies the ports for which you want to display the description.

Restrictions

None.

Example

To display MAC statistics for port ethernet2/1:

```
ssr# show port MAU-statistics ethernet2/1

                                        Media Avail.   Jabber      Jabbering      False
Port     Media Avail.       State Exits   State       State Enters Carriers
------   ----------------   -----------   ---------   ------------ ----
ethernet2/1   not available      0             other       0            0
```

show port mirroring

Purpose

Shows the port mirroring status for ports and ACLs in the Xpedition chassis.

Format

show port mirroring <*port-list*> **| acls**

Mode

Privileged

Description

The **show port mirroring** command shows the following port mirroring status information for the specified ports or ACLs:

- Whether port mirroring is enabled
- The ports or slots that are being mirrored
- The mirroring mode (input port, output slot, or both)

Parameters

<*port-list*>	Specifies the ports for which you want to display port mirroring status.
acls	Displays information for all flow mirroring rules.

Restrictions

None.

Examples

To display the port mirroring status for port ethernet2/1:

```
ssr# show port mirroring ethernet2/1
```

show port status

Purpose

Displays various information about specified ports.

Format

show port status <*port-list*>

Mode

Privileged

Description

The **show port status** command lets you display port-status information for Xpedition ports.

Parameters

<*port-list*>	Specifies the LAN / WAN ports for which you want to display status information.

Restrictions

This command does not show Virtual Circuit (VC) information. To see the state of sub-interfaces, you need to use the appropriate facility command, such as the **show frame-relay** command.

Example

To display the port status for all ports on ethernet1/2:

```
ssr# show port status ethernet1/2

Flags: M - Mirroring enabled  S - SmartTRUNK port

                                                    Link  Admin
Port    Port Type            Duplex Speed     Negotiation State State Flags
----    ---------            ------ -----     ----------- ----- ----- -----
et.1.1  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.2  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.3  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.4  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.5  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.6  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.7  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
et.1.8  10/100-Mbit Ethernet Half   10 Mbits   Manual      Up    Up
```

show pvst

Purpose

Displays Spanning Tree (STP) information for a particular spanning tree.

Format

show pvst <*name*> **interface** <*port-list*>

Mode

Privileged

Description

The **show pvst** command allows the user to display Spanning-Tree information for a particular spanning tree.

Parameters

<*name*>	Specifies the name of the spanning tree for which you want to display information.
interface <*port-list*>	Specifies the ports for which you want to display information.

Restrictions

None.

Example

To display the spanning tree information for spanning tree ‘stp1’ on port ethernet2/1:

```
ssr# show pvst stp1 interface ethernet2/1
```

show stp interface

Purpose

Displays Spanning Tree (STP) information for Xpedition ports.

Format

show stp interface <*port-list*>

Mode

Privileged

Description

The **show stp interface** command allows the user to display Spanning-Tree information for Xpedition ports.

Parameters

<*port-list*>	Specifies the ports for which you want to display information. If no port list is specified, the command will display information for all Xpedition ports.

Restrictions

None.

Example

To display the spanning tree information for all available ports:

```
ssr# show stp interface
Designated
Port     Priority  Cost   STP      State      Designated-Bridge     Port
----     --------  ----   ---      -----      -----------------  ----------
et.1.1      128    00100  Enabled  Listening  8000:00e063111111     80 01
et.1.2      128    00100  Enabled  Listening  8000:00e063111111     80 02
et.1.3      128    00100  Enabled  Listening  8000:00e063111111     80 03
et.1.4      128    00100  Enabled  Listening  8000:00e063111111     80 04
et.1.5      128    00100  Enabled  Listening  8000:00e063111111     80 05
et.1.6      128    00100  Enabled  Listening  8000:00e063111111     80 06
et.1.7      128    00100  Enabled  Listening  8000:00e063111111     80 07
et.1.8      128    00100  Enabled  Listening  8000:00e063111111     80 08
```

show vlan interface

Purpose

Displays VLAN information for Xpedition ports.

Format

show vlan interface <*port-list*>

Mode

Privileged

Description

The **show vlan interface** command allows the user to display VLAN information about Xpedition ports.

Parameters

<*port-list*>	Specifies the ports for which you want to display information.If no port list is specified, the command will display information for all Xpedition ports.

Restrictions

None.

Example

To display the VLAN information for all available ports:

```
ssr# show vlan interface
Port       Access Type    IP VLANs    IPX VLANs    Bridging VLANs
------     ---------      ---------   --------     --------------
et.4.1     access         DEFAULT     DEFAULT      DEFAULT
et.4.2     access         DEFAULT     DEFAULT      DEFAULT
et.4.3     access         DEFAULT     DEFAULT      DEFAULT
et.4.4     access         DEFAULT     DEFAULT      DEFAULT
et.4.5     access         DEFAULT     DEFAULT      DEFAULT
et.4.6     access         DEFAULT     DEFAULT      DEFAULT
et.4.7     access         DEFAULT     DEFAULT      DEFAULT
et.4.8     access         DEFAULT     DEFAULT      DEFAULT
```

Chapter 33

ppp Commands

The **ppp** commands allow the user to specify and monitor Point-to-Point Protocol (PPP) service profiles and PPP High-Speed Serial Interface (HSSI) and standard serial ports.

Command Summary

Table 26 lists the **ppp** commands. The sections following the table describe the command syntax.

Table 26. ppp commands

clear ppp stats-counter ports <*port-list*> **[[frame-drop-qdepth-counter] [max-frame-enqued-counter] frame-drop-red-counter] [rmon]]**
ppp restart lcp-ncp ports <*port-list*>
show ppp mlp <*mlp-list*> **| all-ports**
show ppp service <*service name*> **| all**
show ppp stats port <*port*> **[bridge-ncp] [ip-ncp] [link-status] [summary]**

clear ppp stats-counter

Purpose

Clears the specified statistics counter.

Format

ppp clear stats-counter ports <*port list*> **[[frame-drop-qdepth-counter] [max-frame-enqued-counter] [frame-drop-red-counter] [rmon]]**

Mode

Privileged

Description

The **clear ppp stats-counter** command allows the user to specify a particular statistic counter and reset those statistics to zero. There are statistic counters on each PPP WAN port, and you can use the **clear ppp stats-counter** to clear the counter for an individual WAN port or for a group of ports.

Parameters

ports <*port list*>	The WAN port(s) for which you wish to clear counter.
frame-drop-qdepth-counter	Specifying this optional parameter will reset the frame drop counter to zero.
max-frame-enqued-counter	Specifying this optional parameter will reset the max enquedframes counter to zero.
frame-drop-red-counter	Specifying this optional parameter will reset the packet drop counter to zero.
rmon	Specifying this optional parameter will reset the rmon counter to zero.

Restrictions

Usage is restricted to PPP WAN ports only.

Example

To clear the frame drop counter to zero on WAN port hs.3.1:

```
ssr# clear ppp port hs.3.1 frame-drop-qdepth-counter
```

ppp restart lcp-ncp

Purpose

Restarts PPP LCP / NCP negotiation.

Format

ppp restart lcp-ncp ports <*port list*>

Mode

Privileged

Description

The **ppp restart lcp-ncp** command allows the user to reset and restart the LCP / NCP negotiation process for PPP WAN ports.

Parameters

ports <*port list*> The ports for which you would like to re-establish LCP / NCP negotiation.

Restrictions

This command line is available only for PPP WAN ports.

Example

To restart LCP / NCP negotiation on serial ports 1 and 2 of slot 4:

```
ssr# ppp restart lcp-ncp ports serial4/1-2
```

show ppp mlp

Purpose

Displays the PPP ports that have been added into an MLP bundle.

Format

show ppp mlp <*mlp list*> | **all-ports**

Mode

Privileged

Description

The **show ppp mlp** command allows the user to display information about one or more MLP bundles.

Parameters

<*mlp list*>	The name(s) of the MLP bundles on which you want information. You can specify a single bundle or a comma-separated list of MLP bundles.
all-ports	Displays information on all MLP ports.

Restrictions

None.

Example

To display the PPP ports for mp.1:

```
ssr# show ppp mlp mp.1
mp.1:
  Slot: 4
  PPP ports: serial4/1,serial4/3
```

show ppp service

Purpose

Displays PPP service profiles.

Format

show ppp service <*service name*> | **all**

Mode

Privileged

Description

The **show ppp service** command allows you to display one or all of the available PPP service profiles.

Parameters

<*service name*> The service profile you wish to display.

all Displays all of the available PPP service profiles.

Restrictions

None.

Example

To display the available PPP service profiles named profile_4:

```
ssr# show ppp service profile_4
```

show ppp stats

Purpose

Displays bridge NCP, IP NCP, and link-status parameters.

Format

show ppp stats port <*port*> **[bridge-ncp] [ip-ncp] [link-status] [summary]**

Mode

Privileged

Description

The **show ppp stats** command allows the user to display parameters for bridge NCP, IP NCP, and link-status on PPP WAN ports. You may specify one, two, or three of the available parameter types.

Parameters

port <*port*>	The PPP WAN port for which you wish to view bridge NCP, IP NCP, and / or link-status parameters.
bridge-ncp	Specifies that you wish to view bridging NCP parameters for the given port.
ip-ncp	Specifies that you wish to view IP NCP parameters for the given port.
link-status	Specifies that you wish to view link-status parameters for the given port.
summary	Specifies that you wish to view summarized display.

Restrictions

None.

Example

To display the available link-status and IP NCP parameters for the PPP WAN interface located at slot 4, port 1:

```
ssr# show ppp stats port serial4/1 ip-ncp link-status
```

Chapter 34

pvst Command

The **show pvst** command displays Shielded Twisted Pair (STP) bridging information for a particular VLAN.

Format

show pvst <*VLANid*>

Mode

Privileged

Description

The **show pvst** command displays STP bridging information for a particular VLAN.

Parameters

<*VLANid*> The name of the VLAN for which to display STP information.

Note: For default VLAN, use **stp** commands.

Restrictions

For PVST, the spanning tree instance must have previously been created.

Chapter 35

qos Commands

The **qos** commands display Quality of Service (QoS) parameters.

Command Summary

Table 27 lists the **qos** commands. The sections following the table describe the command syntax.

Table 27. qos commands

show qos ip
show qos ipx
show qos l2 all-destination all-flow ports <*port-list*> **vlan** <*VLANid*> **source-mac** <*MACaddr*> **dest-mac** <*MACaddr*>
show qos precedence ip | **ipx**
show qos priority-map <*string*> | **all**
show qos wred [input port <*port-list*> | **all-ports] [port** <*port-list*> | **all-ports]**
show qos wfq <*port-list*> | **all-ports**

show qos ip

Purpose

Displays QoS information for IP flows.

Format

show qos ip

Mode

Privileged

Description

The **show qos ip** command allows the user to display QoS information for IP flows.

Parameters

None.

Restrictions

None.

show qos ipx

Purpose

Displays QoS information for IPX flows.

Format

show qos ipx

Mode

Privileged

Description

The **show qos ipx** command allows the user to display QoS information for IPX flows.

Parameters

None.

Restrictions

None.

show qos l2

Purpose

Displays QoS information for L2 flows.

Format

show qos l2 all-destination all-flow ports <*port-list*> **vlan** <*vlanID*> **source-mac** <*MACaddr*> **dest-mac** <*MACaddr*>

Mode

Privileged

Description

The **show qos l2** command allows the user to display QoS information for L2 flows. You may filter the display according to the following:

- Destinations
- Flows
- Ports
- VLANs
- Source MAC addresses
- Destination MAC addresses
- Priority

Parameters

all-destination
Filters the display to show all the L2 destination priorities.

all-flow
Filters the display to show all the L2 flow priorities.

ports <*port-list*>
Filters the display to show L2 priority information for specific ports.

vlan <*vlanID*>
Filters the display to show L2 priority information for specific VLANs.

source-mac <*MACaddr*>Filters the display to show L2 priority information for specific source MAC addresses.

dest-mac <*MACaddr*>
Filters the display to show L2 priority information for specific destination MAC addresses.

Restrictions

None.

show qos precedence

Purpose

Displays IP or IPX precedence values.

Format

show qos precedence ip | ipx

Mode

Privileged

Description

The **show qos precedence** command allows the user to display the precedence values for all fields in a flow.

IP flows consist of the following fields: destination port, destination address, source port, source IP address, TOS, interface, protocol.

IPX flows consist of the following fields: destination network, source network, destination node, source node, destination port, source port, interface.

Parameters

ip Displays the precedence values for IP flows.

ipx Displays the precedence values for IPX flows.

Restrictions

None.

show qos priority-map

Purpose

Displays the priority mapping and the ports that it is applied.

Format

show qos priority-map <*string*> **| all**

Mode

Privileged

Description

The **show qos priority-map** command allows the user to display the priority mapping that is configured on a port. The command details how each set of 802.1p tag values is mapped to a specific internal priority queue.

Parameters

<*string*>	Specifies the name of the priority map.
all	Displays all priority maps.

Restrictions

None.

show qos wred

Purpose

Displays WRED parameters for each port.

Format

show qos wred [input port <*port list*> **| all-ports] [port** <*port list*> **| all-ports]**

Mode

Privileged

Description

The **show qos wred** command allows the user to display WRED information for a certain port or all ports. You may display WRED parameter information according to the following:

- Input ports
- All Ports

Parameters

input port <*port list*> **| all-ports**
Displays input port WRED parameters. Specify **all-ports** to display parameters for all ports.

port <*port list*> **| all-ports**
Displays WRED parameters for each port. Specify **all-ports** to display parameters for all ports.

Restrictions

None.

show qos wfq

Purpose

Displays bandwidth allocated for each port.

Format

show qos wfq port <*port list*> **|all-ports**

Mode

Privileged

Description

The **show qos wfq** command allows the user to display the bandwidth for each port allocated with weighted-fair queuing.

Parameters

port <*port list*> **|all-ports**
Displays bandwidth allocated for each port. Specify a list of ethernet or wan ports. Specify **all-ports** to display bandwidth for all ports.

Restrictions

None.

Chapter 36

radius Command

The **show radius** command displays information about Remote Authentication Dial-In Service (RADIUS) configuration on the Xpedition.

Format

show radius

Mode

Privileged

Description

The **show radius** command displays statistics and configuration parameters related to RADIUS configuration on the Xpedition. The statistics displayed include:

accepts Number of times each server responded and validated the user successfully.

rejects Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied.

timeouts Number of times each server did not respond.

Parameters

None.

Restrictions

None.

Chapter 37

rarpd Command

The **show rarpd** command displays information about the Xpedition's Reverse Address Resolution Protocol (RARP) configuration.

Format

show rarpd interface | mappings

Mode

Privileged

Description

The **show rarpd** command displays information about the configuration of the Xpedition's RARP server. You may list the MAC-to-IP address mappings or the interfaces to which the Xpedition responds to RARP requests.

Parameters

interface Lists the interfaces to which the Xpedition responds to RARP requests.

mappings Displays the list of MAC-to-IP address mappings.

Restrictions

None.

Example

To display the RARP server's list of MAC-to-IP address mappings:

```
ssr# show rarpd mappings
```

Chapter 38

rate-limit Command

The **show rate-limit** command displays rate limiting policies.

There are three different types of rate limiting supported:

- flow rate limiting: rate limiting for individual flows
- aggregate rate limiting: rate limiting for an aggregation of flows
- port level rate limiting: rate limiting for individual ports

Format

show rate-limit [all] | [policy-type flow-policies|aggregate-policies|portlevel-policies|all] | [policy-name <*name*>**] | [interface** <*interface*>**] | [port-level port** <*port list*>**|all-port] | [port-level policy-name** <*name*>**] | [rate-limiting-mode]**

Mode

Privileged

Description

The **show rate-limit** command displays information about rate limiting policies.

Parameters

all Displays information on all rate limit policies configured on the Xpedition.

policy-type

The type of the rate limit policy. The keyword **all** shows all rate limit types. You can specify the following types of policies:

flow-policies All flow policies

aggregate-policies All aggregate policies

portlevel-policies All port level policies

all All policies

policy-name <*name*> | **all**
The name of the rate limiting policy. The keyword **all** shows all rate limit policies.

interface <*interface*> | **all**
The name of the IP interface. The keyword **all** shows rate limiting policies for all IP interfaces.

port-level port <*port list*> | **all-ports**
The name of the port. The keyword **all-ports** shows rate limiting policies for all ports.

port-level policy-name <*name*>
The name of the rate limiting policy name.

rate-limiting-mode
Displays the current rate limiting mode, whether per-flow rate limiting or aggregate rate limiting.

Restrictions

None.

Example

To display all configured rate limit policies:

```
ssr# show rate-limit all

--------------------------------------------------------------------------------
Rate Limit Policy name : rlpol (1)
Applied Interfaces : if0 (2)

 (3)        (4)             (5)          (6)       (7)     (8)  (9)
ACL     Source IP/Mask    Dest. IP/Mask    SrcPort   DstPort   TOS  Prot
---     --------------    -------------    --------- --------- ---- ---
100     10.212.10.11/32   anywhere         any       any       any  IP
200     10.212.10.12/32   anywhere         any       any       any  IP
300     10.212.10.13/32   anywhere         any       any       any  IP
400     10.212.10.14/32   anywhere         any       any       any  IP
500     10.212.10.10/32   anywhere         any       any       any  IP

 (10) (11)       (12)          (13)
Seq ACL      Rate Limit Exceed Action
--- ----     --------  -------------
10  100      26000     Low
10  200      26000     Low
10  300      26000     Low
10  400      26000     Low
10  500      26000     Low
```

Legend:

1. The name of the rate limit.
2. The IP interface to which the rate limit is applied.
3. The name of the ACL(s) that define the rate limit.
4. The source address and filtering mask specified by the ACL.
5. The destination address and filtering mask specified by the ACL.
6. The number of the TCP or UDP source port.
7. The number of the TCP or UDP destination port.
8. The Type of Service value.
9. The protocol for the ACL.
10. The sequence number for this policy.
11. The name of the ACL.
12. The rate limit for the flow.

13. The action to be taken if the rate limit is reached: packets can be dropped or the priority set to low, medium, or high.

Chapter 39

reload Command

The **reload** command reboots the Xpedition.

Format

reload

Mode

Privileged

Parameters

None.

Restrictions

None.

Chapter 40

rip Commands

The Routing Information Protocol, Version 1 and Version 2 (RIPv1 and RIPv2), is the most commonly used interior gateway protocol. RIP selects the route with the lowest metric as the best route. The metric is a hop count representing the number of gateways through which data must pass in order to reach its destination. The longest path that RIP accepts is 15 hops. If the metric is greater than 15, a destination is considered unreachable and the Xpedition discards the route. RIP assumes that the best route is the one that uses the fewest gateways, that is, the shortest path. RIPv1 is described in RFC 1058 and RIPv2 is described in RFC 1723.

The **rip** commands allow the user to display various information about the RIP.

Command Summary

Table 28 lists the **rip** commands. The sections following the table describe the command syntax.

Table 28. rip commands

rip trace [packets | request | response | local options] [detail] [send | receive]
show rip *<option list>*

rip trace

Purpose

Traces RIP packets.

Format

rip trace [packets | request | response | local-options] [detail | send | receive]

Mode

Privileged

Description

The **rip trace** command traces the following sets of RIP packets:

- RIP request packets sent or received by the Xpedition
- RIP response packets sent or received by the Xpedition

Depending on the options you specify, you may trace all packets, request packets only, or receive packets only. In addition, you may choose to trace the request packets, receive packets, or both that are sent by the Xpedition, received by the Xpedition, or all packets (both sent packets and received packets).

Parameters

packets Traces all RIP packets, both request packets and response packets. This is the default.

request Traces only request packets, such as REQUEST, POLL and POLLENTRY packets.

response Traces only response packets.

For the **packets**, **request**, and **response** parameters, you may optionally specify one of the following:

detail Shows detailed information about the traced packets.

send Shows information about traced RIP packets sent by the **Xpedition**.

receive Shows information about traced RIP packets received by the Xpedition.

Note: The default shows both send and receive packets.

local-options Sets trace options for this protocol only. Specify one or more of the following:

all Turns on all tracing.

general Turns on normal and route tracing.

state Traces state machine transitions in the protocols.

normal Traces normal protocol occurrences.

Note: Abnormal protocol occurrences are always traced.

policy Traces application of protocol and user-specified policies to routes being imported and exported.

task Traces system processing associated with this protocol or peer.

timer Traces timer usage by this protocol or peer.

route Traces routing table changes for routes installed by this protocol or peer.

Restrictions

None.

show rip

Purpose

Displays RIP information.

Format

show rip <*option-list*>

Mode

Privileged

Description

The **show rip** command displays RIP information.

Parameters

<*option-list*>
Specifies the RIP dump information you want to display. Specify one or more of the following:

all
Displays all RIP tables.

globals
Displays RIP globals.

timers
Displays RIP timers.

interface
Displays RIP interfaces.

active-gateways
Displays active gateways running RIP.

interface-policies
Displays RIP interface policies.

import-policies
Displays RIP import policies.

export-policies
Displays RIP export policies.

Restrictions

None.

Chapter 41

rmon Commands

The **rmon** commands allow the user to display and set parameters for Remote Network Monitor (RMON) device statistics on a per-port basis. RMON information corresponds to RFCs 1757 and 2021.

Command Summary

Table 29 lists the **rmon** commands. The sections following the table describe the command syntax.

Table 29. rmon commands

clear rmon cli-filter
clear rmon statistics
rmon apply cli-filter *<filter-id>*
show rmon [alarms | events | filter | history | matrix | packet-capture | status]

clear rmon cli-filter

Purpose

Clears currently-selected CLI RMON filters.

Format

clear rmon cli-filter

Mode

Privileged

Description

The **clear rmon cli-filter** command clears the CLI RMON filters that were applied with the **rmon apply cli-filter** command.

Parameters

None.

Restrictions

None.

clear rmon statistics

Purpose

Clears RMON statistics.

Format

clear rmon statistics

Mode

Privileged

Description

The **clear rmon statistics** command clears RMON statistics for all Xpedition ports. When you clear statistics, the Xpedition sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

Parameters

None.

Restrictions

None.

rmon apply cli-filter

Purpose

Applies a specific CLI RMON filter.

Format

rmon apply cli-filter <*filter-id*>

Mode

Privileged

Description

The **rmon apply cli-filter** command applies a specific CLI RMON filter to the current Telnet or Console session. This enables different users to select the different CLI filters.

Use the **rmon clear cli-filter** command to clear an applied filter.

Parameter

<*filter id*>	This is a number between 1 and 65535 which identifies the filter ID to apply.

Restrictions

None.

Example

To apply filter ID 2:

```
ssr# rmon apply cli-filter 2
```

show rmon

Purpose

Displays statistics related to various RMON perameters.

Format

show rmon [alarms | events | filters | history | matrix | packet-capture | status]

Mode

Privileged

Description

The **show rmon** command displays statistics related to various RMON parameters.

Parameters

alarms	Displays the RMON Alarm table.
events	Displays configured events and the logs, if any, of triggered events.
filters	Displays the contents of the Filter table.
history	Displays statistical samples that are stored in the RMON History group. Entries in this table are created automatically when default tables are turned on for the Lite group.
matrix	Displays entries in the Matrix table. Entries in this table are automatically created when default tables are turned on for the Standard group. **Note:**If CLI filters have been applied, they will take effect when the Matrix table is displayed. This command will display control r ows and their corresponding logs only if there are logs. A control row that has no data is not displayed.
packet-capture	Displays the buffer table for captured packets.
status	Displays RMON 1 and II status and memory information.

Chapter 42

sfs Commands

The **sfs** commands display Cabletron Discovery Protocol (CDP) parameters

Command Summary

Table 30 lists the **sfs** commands. The sections following the table describe the command syntax.

Table 30. sfs commands

show sfs cdp-hello- port-status <*port-list*> **| all-ports**
show sfs cdp-hello transmit-frequency

show sfs cdp-hello port-status

Purpose

Displays CDP Hello status of a port.

Format

show sfs cdp-hello port-status <*port-list*> | **all-ports**

Mode

Privileged

Description

The **show sfs cdp-hello port-status** command displays CDP Hello information of Xpedition ports.

Parameters

<*port-list*> | **all-ports** Specifies the ports for which you want to display information. The **all-ports** keyword displays the selected information for all the Xpedition ports.

Restrictions

None.

Examples

To display CDP Hello status on all Xpedition ports:

```
ssr# show sfs cdp-hello port-status all-ports
```

show sfs cdp-hello transmit-frequency

Purpose

Displays the transmit frequency of CDP Hello packets.

Format

show sfs cdp-hello transmit-frequency

Mode

Privileged

Description

The **show sfs cdp-hello transmit-frequency** command display the transmit frequency of CDP Hello packets on the Xpedition.

Parameters

None.

Restrictions

None.

Examples

To display the transmit frequency of CDP Hello packets:

```
ssr# show sfs cdp-hello transmit-frequency
```

Chapter 43

smarttrunk Commands

The **smarttrunk** commands allow the user to display parameters for SmartTRUNK ports. SmartTRUNK ports are groups of ports that have been logically combined to increase throughput and provide link redundancy.

Command Summary

Table 31 lists the **smarttrunk** commands. The sections following the table describe the command syntax.

Table 31. smarttrunk commands

clear smarttrunk load-distribution <*num*>
show smarttrunk [distribution | protocol-state | connections] <*numlist*>

clear smarttrunk load-distribution

Purpose

Clears load distribution statistics for ports in a SmartTRUNK.

Format

clear smarttrunk load-distribution <*num*>

Mode

Privileged

Description

The **clear smarttrunk load-distribution** command is used in conjunction with the **show smarttrunk distribution** command, which gathers statistics for the transmitted bytes per second flowing through the SmartTRUNK and each port in it. The **clear smarttrunk load-distribution** command lets you reset load distribution statistics to zero.

Parameters

<*num*> Specifies name of one or more existing SmartTRUNKs.

Restrictions

None.

Example

To clear load distribution information from SmartTRUNK st.1:

```
ssr# clear smarttrunk load-distribution st.1
```

show smarttrunk

Purpose

Displays information about SmartTRUNKs on the Xpedition

Format

show smarttrunk [distribution | protocol-state | connections] <*numlist*>

Mode

Privileged

Description

The **show smarttrunk** command displays statistics about SmartTRUNKs on the Xpedition.

Parameters

distribution	Provides statistics on how traffic is distributed across the ports in a SmartTRUNK.
protocol-state	Shows information about the control protocol on a SmartTRUNK.
connections	Shows information about the SmartTRUNK connection, including the MAC address of the remote switch, and the module number and port number of each remote port. Connection information is reported only if the Hunt Group protocol is enabled for the SmartTRUNK.
<*numlist* >	Specifies name of one or more SmartTRUNKs.

Restrictions

None.

Examples

To show how traffic is distributed across the ports on all SmartTRUNKs:

```
ssr# show smarttrunk distribution

SmartTRUNK  Member  % Link Utilization    Link Status     Grp Status
----------  ------  ------------------    -----------     ----------
st.1        et.2.4      0.00              Forwarding          Up
st.1        et.2.5      0.00              Forwarding          Up
st.1        et.2.6      0.00              Forwarding          Up
```

To show information about the control protocol for SmartTRUNK st.1:

```
ssr# show smarttrunk protocol-state st.1

SmartTRUNK  Protocol       State     Port    Port State
----------  --------       -----     ----    ----------
st.1        HuntGroup      Down      et.3.1  Negotiate
                           et.3.2  Negotiate
```

To show connection information for all SmartTRUNKs:

```
ssr# show smarttrunk connections
SmartTRUNK Local Port  Remote Switch       Remote Module   Remote Port  State
---------- ----------  -------------       -------------   -----------  -----
st.1       ether2/1    Enterasys A9:6E:57  3               1            Up
st.1       ether2/2    Enterasys A9:6E:57  3               2            Up
st.1       ether2/3    Enterasys A9:6E:57  3               3            Up
st.1       giga3/1     Enterasys A9:6E:57  4               5            Up
st.2       ether2/4    --                  --              --           Up
st.2       ether2/5    --                  --              --           Up
st.2       ether2/6    --                  --              --           Up
```

Note: In the example above, SmartTRUNK st.2 has no control protocol enabled, so no connection information is reported.

Chapter 44

snmp Commands

The **snmp** commands allow the user to display and test parameters for Simple Network Management Protocol (SNMP).

Command Summary

Table 32 lists the **snmp** commands. The sections following the table describe the command syntax.

Table 32. snmp commands

show snmp access | chassis-id | community | mibs | statistics | tfpt | trap
snmp test trap type coldstart | linkdown | linkup | ps-failure | ps-recover | vrrpnewmaster

show snmp

Purpose

Allows the user to display SNMP parameters, including SNMP community names.

Format

show snmp access | chassis-id | community | mibs | statistics | tfpt | trap

Mode

Privileged

Description

The **show snmp** command displays the following SNMP information:

- Community strings set on the Xpedition
- SNMP Statistics
- IP address of SNMP trap target server

Parameters

access	Displays the last five SNMP clients to access the Xpedition.
chassis-id	Displays the Xpedition's SNMP name.
tftp	Displays tftp SNMP status.
trap	Displays the IP address of the trap target server.
community	Displays the Xpedition's community string.
statistics	Displays SNMP statistics.
mibs	Displays the SNMP MIB registry.

Restrictions

None.

Examples

The following command displays a log of SNMP access to the Xpedition. The host that accessed the Xpedition and the Xpedition system time when the access occurred are listed.

```
ssr# snmp show access
SNMP Last 5 Clients:
        10.15.1.2           Wed Feb 10 18:42:59 1999
        10.15.1.2           Wed Feb 10 18:42:55 1999
        10.15.1.2           Wed Feb 10 18:42:56 1999
        10.15.1.2           Wed Feb 10 18:42:57 1999
        10.15.1.2           Wed Feb 10 18:42:58 1999
```

To display the SNMP identity of the Xpedition:

```
ssr# snmp show chassis-id

SNMP Chassis Identity:
s/n 123456
```

To display the IP address of the trap target server:

```
ssr# snmp show trap

Trap Table:
Index    Trap    Target    Addr    Community String    Status
1.               10.15.1.2         public              enabled
2.               1.2.3.4           public123           disabled
3.               5.6.7.8           public20            disabled
```

snmp test trap

Purpose

Tests SNMPv1 notifications to currently configured managers.

Format

snmp test trap type coldstart | linkdown | linkup | ps-failure | ps-recover | vrrpnewmaster

Mode

Privileged

Description

The **snmp test trap** command allows the user to test SNMPv1 notifications to currently configured managers. The user may test the following notification types:

- Coldstart
- Linkdown
- Linkup
- PS-failure
- PS-recover
- VRRPNewMaster

Parameters

coldstart Tests the cold start trap notification.

linkdown Tests link down notification for ifIndex 1.

linkup Tests link up notification for ifIndex 1.

ps-failure Tests the power supply failure trap notification.

ps-recover Tests the power supply recover trap notification.

vrrpNewMaster Tests the Virtual Router Redundancy New Master Trap.

Restrictions

None.

Chapter 45

sonet Commands

The **sonet** commands allows the user to display various parameters for Synchronous Optical Network (SONET) encapsulation. These commands also allow the user to accommodate Packet-over-SONET (POS) and ATM (Asynchronous Transfer Mode) transmission using the Xpedition.

Packet-over-SONET technology provides the ability to transmit IP packets and ATM cells over a SONET backbone by encapsulating them into a SONET frame. In reference to the OSI Layer model, the SONET layer rests right beneath the IP layer or the ATM layer. Based on the transmission mechanism of SONET frames, the result is larger traffic bandwidth and faster line speed (OC-3), accommodating QoS guarantees as well as the ability to deliver voice / video data over an internetwork.

SONET frames carry a large amount of data stored as overhead. This overhead information provide the information for OAM&P (operation, administration, management, and provisioning) capabilities, such as performance monitoring, automatic protection switching, and path tracing.

Enterasys SONET technology features Automatic Protection Switching, performance monitoring capabilities, as well as commercial circuit identification.

Command Summary

Table 33 lists the **sonet** commands. The sections following the table describe the command syntax.

Table 33. sonet commands

show sonet aps <*SONETports*>
show sonet loopback <*SONETports*>
show sonet medium <*SONETports*>
show sonet pathtrace <*SONETports*>

show sonet aps

Purpose

Displays APS status.

Format

show sonet aps <*SONETports*>

Mode

Privileged

Description

The **show sonet aps** command allows the user to display APS (Automatic Protection Switching) status. This command allows you to display such APS parameters as protection level, working or protecting port, directionality, and switch status.

Parameters

<*SONETports*> Specifies the SONET port name(s).

Restrictions

None.

Example

To display the APS status for port so.2.1:

```
ssr# show sonet aps so.2.1
```

show sonet loopback

Purpose

Displays loopback status.

Format

show sonet loopback <*SONETports*>

Mode

Privileged

Description

The **show sonet loopback** command allows the user to display loopback status for a specified SONET port. Loopback is used to verify connectivity between two devices.

Parameters

<*SONETports*> Specifies the SONET port name(s).

Restrictions

None.

Example

To display the loopback status for port so.2.1:

```
ssr# show sonet loopback so.2.1
```

show sonet medium

Purpose

Displays SONET optical line values.

Format

show sonet medium <*SONET ports*>

Mode

Privileged

Description

The **show sonet medium** command allows the user to display the various SONET optical line values associated with a SONET port. This command will allow you to display values such as framing status, line type, and administrator-specified circuit identifier.

Parameters

<*SONETports*>	Specifies the SONET port name(s).

Restrictions

None.

Example

To display optical line values for port so.2.1:

```
ssr# show sonet medium so.2.1
```

show sonet pathtrace

Purpose

Displays received path trace messages.

Format

show sonet pathtrace <*SONETports*>

Mode

Privileged

Description

The **show sonet pathtrace** command allows the user to display path trace messages received on a specified SONET port.

Parameters

<*SONETports*> Specifies the SONET port name(s).

Restrictions

None.

Example

To display the path trace messages for port so.2.1:

```
ssr# show sonet pathtrace so.2.1
```

Chapter 46

statistics Commands

The **statistics** commands allow the user to display statistics for various Xpedition features. The user may also clear some statistics.

Command Summary

Table 34 lists the **statistics** commands. The sections following the table describe the command syntax.

Table 34. statistics commands

clear interface [<*port-list*>**] [errors | packets | statistics]**
clear ip statistics
clear ipx statistics
show ip icmp statistics
show ip multicast
show ip traffic
show ipx traffic
show port errors [<*port-list*>**]**
show port packets [<*port-list*>**]**
show port stats [<*port-list*>**]**
show processes cpu
show rarp [<*IFname*>**]**

Table 34. statistics commands (Continued)

show tcp statistics
show traffic
show udp statistics

clear interface

Purpose

Clears various statistics.

Format

clear interface [<*port-list*>**] [errors | packets | statistics]**

Mode

Privileged

Description

The **clear interface** command clears port statistics, error statistics, or RMON statistics. When you clear statistics, the Xpedition sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

Parameters

<*port-list*>
The ports for which you are clearing statistics. You can specify a single port or a comma-separated list of ports. Example: ethernet1/3,ethernet.(1-3).(4,6-8). If no port is specified, the **clear interface** command will clear statistics for all *Xpedition* ports.

errors Clears all error statistics for the specified port.

packets Clears all packet statistics for the specified port.

statistics Clears all normal (non-error) statistics for the specified port.

Restrictions

None.

clear ip statistics

Purpose

Clears Internet Protocol (IP) statistics.

Format

clear ip statistics

Mode

Privileged

Description

The **clear ip statistics** command clears IP statistics for all Xpedition ports. When you clear statistics, the Xpedition sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

Parameters

None.

Restrictions

None.

clear ipx statistics

Purpose

Clears IPX statistics.

Format

clear ipx statistics

Mode

Privileged

Description

The **clear ipx statistics** command clears IPX statistics for all Xpedition ports. When you clear statistics, the Xpedition sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

Parameters

None.

Restrictions

None.

show ip icmp statistics

Purpose

Displays internet control message protocol (ICMP) statistics.

Format

show ip icmp statistics

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display ICMP statistics:

```
ssr# show ip icmp statistics
icmp:
      0 messages with bad code fields
      0 messages smaller than minimum length
      0 bad checksums
      0 messages with bad length
      0 message responses generated
```

- messages with bad code fields — Displays the number of ICMP messages processed by the router with a bad code field. The code field within the ICMP header uses a number to specify the message content of the ICMP message. An invalid number within the code field would show in this statistic parameter.

- messages smaller than min length — Displays the number of ICMP messages processed by the router that didn't meet a minimum length requirement.
- bad checksums — Displays the number of ICMP messages processed by the router with bad checksums. The checksum field within the ICMP header is used to verify that the message was transmitted error-free. A bad checksum indicates an ICMP message with errors.
- messages with bad length — Displays the number of ICMP messages processed by the router with bad or invalid length.
- message responses generated — Displays the number of ICMP responses that have been generated by the router in response to ICMP messages.

show ip multicast

Purpose

Displays multicast statistics.

Format

show ip multicast

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display multicast statistics:

```
ssr# show ip multicast
multicast forwarding:
        0 multicast forwarding cache lookups
        0 multicast forwarding cache misses
        0 upcalls to mrouted
        0 upcall queue overflows
        0 upcalls dropped due to full socket buffer
        0 cache cleanups
        0 datagrams with no route for origin
        0 datagrams arrived with bad tunneling
        0 datagrams could not be tunneled
        0 datagrams arrived on wrong interface
        0 datagrams selectively dropped
        0 datagrams dropped due to queue overflow
        0 datagrams dropped for being too large
```

show ip traffic

Purpose

Displays Internet Protocol (IP) and unicast IP routing statistics.

Format

show ip traffic

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display IP and IP routing statistics:

```
ssr# show ip traffic
ip:
      78564 total packets received
      0 bad header checksums
      0 packets with size smaller than minimum
      0 packets with data size < data length
      0 packets with header length < data size
      0 packets with data length < header length
      0 packets with bad options
      0 packets with incorrect version number
      0 fragments received
      0 fragments dropped (dup or out of space)
      0 fragments dropped after timeout
      0 packets reassembled ok
      2984 packets for this host
      0 packets for unknown/unsupported protocol
      0 packets forwarded
      75580 packets not forwardable
      0 redirects sent
      2120 packets sent from this host
      0 packets sent with fabricated ip header
      0 output packets dropped due to no bufs, etc.
      0 output packets discarded due to no route
      0 output datagrams fragmented
      0 fragments created
      0 datagrams that can't be fragmented
routing:
      0 bad routing redirects
      0 dynamically created routes
      0 new gateways due to redirects
      1141 destinations found unreachable
      0 uses of a wildcard route
```

IP Statistics:

- total packets received — Displays the total number of IP packets received by the router, including all forwarded and dropped packets.
- bad header checksums — Displays the number of IP packets received by the router with bad checksums. The checksum field within the IP header is used to verify that the packet was transmitted error-free. A bad checksum indicates an IP packet with errors.

- packets w / size smaller than min Displays the number of IP packets received by the router that didn't meet a minimum length requirement.

- packets w / data size<data length Displays the number of IP packets received by the router containing a data size smaller than the specified data length. The data length field in the IP header specifies the data length contained within the packet.

- packets w / header length<data size Displays the number of IP packets received by the router containing a IP header length smaller than the data size within the packet.

- packets w / data length<header length Displays the number of IP packets received by the router containing a data length smaller than the IP header length.

- packets w / incorrect version number Displays the number of IP packets received by the router with an incorrect IP version number. The IP version number field in the IP header is used to specify whether the packet is formatted for IPv4 or IPv6.

- fragments received Displays the number of datagram fragments received by the router. A datagram that does not fit into an IP packet must be fragmented into two or more packets.

- fragments dropped Displays the number of datagram fragments dropped by the router. A datagram that does not fit into an IP packet must be fragmented into two or more packets.

- fragments dropped after timeout Displays the number of datagram fragments dropped by the router after a certain time period. A datagram that does not fit into an IP packet must be fragmented into two or more packets.

- packets reassembled ok Displays the number of IP packets containing fragmented datagrams that were reassembled successfully at the destination.

- packets for this host — Displays the total number of IP packets received that were intended for the router as the destination.
- packets for unknown protocol — Displays the number of IP packets received by the router that is of an unknown or unsupported routed protocol.
- packets forwarded — Displays the number of IP packets received by the router that were forwarded onto another host.
- packets not forwardable — Displays the total number of IP packets received by the router that could not be forwarded onto another host.
- redirects sent — Displays the number of redirects sent by the router.
- packets sent from this host — Displays the total number of IP packets sent out by the router.
- packets sent w/fabricated ip header — Displays the total number of IP packets sent out by the router after attaching an IP header onto the packet.
- output packets dropped due to no bufs — Displays the total number of IP packets dropped before being sent out by the router because of lack of output buffer space.
- output packets discarded due to no route — Displays the total number of IP packets dropped before being sent out by the router because of no IP routing information.
- output datagrams fragmented — Displays the total number of datagrams that were fragmented into two or more IP packets before being sent out by the router.
- fragments created — Displays the total number of datagram fragments created.
- datagrams that can't be fragmented — Displays the total number of datagrams that was not successfully fragmented into two or more IP packets.

Routing Statistics:

• bad routing redirects	Displays the number of bad redirects have occurred. A redirect occurs in the case where the destination interface is the same as the source interface.
• dynamically created routes	Displays the number of IP routes have been created using a routing protocol, as opposed to static routes which are user-defined.
• new gateways due to redirects	Displays the number of new gateways have been added into the routing table due to redirects.
• destinations found unreachable	Displays the number of destination addresses that have been found to be unreachable in the routing table. A destination may be unreachable due to the route being expired or being unavailable due to network changes.
• uses of a wildcard route	Displays the number of times that a wildcard route has been used to forward a packet onto the next-hop destination.

show ipx traffic

Purpose

Displays internetwork packet exchange (IPX) and IPX routing statistics.

Format

show ipx traffic

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display IPX statistics:

```
ssr# statistics show ipx
ipx:
        0 total packets received
        0 packets with bad checksums
        0 packets smaller than advertised
        0 packets smaller than a header
        0 packets forwarded
        0 packets not forwardable
        0 packets for this host
        0 packets sent from this host
        0 packets dropped due to no bufs, etc.
        0 packets discarded due to no route
        0 packets too big
        0 packets with too many hops
        0 packets of type 20
        0 packets discarded due to infiltering
        0 packets discarded due to outfiltering
        0 packets with misc protocol errors
        0 rip packets discarded due to socket buffer full
        0 sap packets discarded due to socket buffer full
        0 rip req packets discarded due to socket buffer full
        0 sap gns packets discarded due to socket buffer full
        0 packets discarded due to port of entry zero
        0 packets discarded due to sourced by us
routing:
        0 bad routing redirects
        0 dynamically created routes
        0 new gateways due to redirects
        1141 destinations found unreachable
        0 uses of a wildcard route
```

show port errors

Purpose

Displays port error statistics.

Format

show port errors [<*port-list*>**]**

Mode

Privileged

Parameters

<*port-list*>	Specifies the port. If no port is specified, command will display port error statistics for all physical and logical ports.

Restrictions

None.

Example

To display port error statistics on port ethernet2/1:

```
ssr# show port errors ethernet2/1

Port: et.2.1
----
Error Stats                    Error Stats

-----------                    -----------

CRC errors              0      Carrier sense errors      0

Single collision (tx OK)  0    Many collisions (tx OK)   0

Many collisions (drop)    0    Late collisions           0

Long frames  >1518 bytes  0    Invalid long frames       0

Short frames <64 bytes    0    Alignment errors          0

Deferred transmissions    0    Transmit underruns        0

IP - bad version          0    IP - bad checksum         0

IP - bad header           0    IP - small datagram       0

IP - expand TTL ring      0    IPX - bad header          0

Non-IP/IPX protocol       0    Invalid MAC encap.        0

Internal frame tx error   0    Internal frame rx error   0

Input buffer overflow     0    Packet request overflow   0

Out buffer (low) ovflow   0    Out buffer (med) ovflow   0

Out buffer (high) ovflow  0    Out buffer (ctrl) ovflow  0

Input VLAN drop frame     0
Error stats cleared   * Never Cleared *
```

show port packets

Purpose

Displays port packet statistics.

Format

show port packets [<*port-list*>**]**

Mode

Privileged

Parameters

<*port-list*>	Specifies the port. If no port is specified, command will display port packet statistics for all physical and logical ports.

Restrictions

None.

Example

To display port packet statistics on port et.2.1:

```
ssr# show port packets et.2.1

Port: et.2.1
----
RMON Stats                Received              Transmitted

----------                --------              -----------

Unicast frames            0                     0

Multicast frames          0                     0

Broadcast frames          0                     0

64 byte frames            0                     0

65-127 byte frames        0                     0

128-255 byte frames       0                     0

256-511 byte frames       0                     0

512-1023 byte frames      0                     0

1024-1518 byte frames     0                     0

RMON stats cleared   * Never Cleared *
```

show port stats

Purpose

Displays normal (non-error) port statistics.

Format

show port stats [<*port-list*>**]**

Mode

Privileged

Parameters

<*port-list*>	Specifies the port. If no port specified, command will display port statistics for all physical and logical ports.

Restrictions

None.

Example

To display port statistics on port et.2.1:

```
ssr# show port stats et.2.1

Port: et.2.1
-------------
Port Stats                Received              Transmitted

----------                --------              -----------

Frames/Packets              0                     0

. Switched frames (bridging)  0                     0

. Local frames (bridging)     0                   N/A
. Routed packets              0                     0

  . Switched (data)           0                   N/A
  . Consumed by CPU           0                   N/A
Bytes                       0                     0

. Bridged bytes             0                     0

. Routed bytes              0                     0

L2 table misses             0                   N/A
IP table misses             0                   N/A
IPX table misses            0                   N/A
IP TTL expirations          0                   N/A
IPX TC expirations          0                   N/A
1 minute traffic rates
. Average bits/sec          0                     0

. Packet discards           0                     0

. Packet errors             0                     0

. Unicast packets           0                     0

. Multicast packets         0                     0

. Broadcast packets         0                     0

Port stats cleared  * Never Cleared *
```

- **Frames/Packets**
- **Switched frames**Shows the number of frames that have been bridged or forwarded.

- **Local frames**Shows the number of local frames (frames destined for a port that is the same as the port of entry) that was dropped.
- **Routed packets**
- **Switched (data)**Shows the number of packets that was forwarded by the hardware.
- **Consumed by CPU**Shows the number of packets that was sent to the control module to be forwarded.
- **Bytes**
- **Bridged bytes**Shows the number of total bytes that has been bridged.
- **Routed bytes**Shows the number of total bytes that has been routed.
- **L2 table misses** Shows the number of times that a Layer-2 frame could not be resolved by the L2 Table.
- **IP table misses** Shows the number of times that an IP packet could not be resolved by the IP Routing Table.
- **IPX table misses** Shows the number of times that an IPX packet could not be resolved by the IPX Routing Table.
- **IP TTL expirations** Shows the number of IP packets that have been received by the port with a Time-to-Live (TTL) header with a value of 1. The IP packet will then be expired at this point.
- **IPX TC expirations** Shows the number of IPX packets that have been received by the port with a TC header with a value of 1. The IPX packet will then be expired at this point.
- **1 minute traffic rates**
- **Average bits/sec**Shows an average traffic rate in bits / second for a one-minute time period for a port.
- **Packet discards**Shows the number of packets discarded by a port within a one-minute time period.
- **Packet errors**Shows the number of packets containing errors that was seen by the port within a one-minute time period.

- **Unicast packets**Shows the number of unicast packets that was seen by the port within a one-minute time period.
- **Multicast packets**Shows the number of multicast packets that was seen by the port within a one-minute time period.
- **Broadcast packets**Shows the number of broadcast packets that was seen by the port within a one-minute time period.
- **Port stats Cleared** Shows the date and time when the port stats were last cleared.

show processes cpu

Purpose

Displays active tasks.

Format

show processes cpu

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display active tasks:

```
ssr# show processes cpu

Timestamp: 2000-04-25 17:56:32
CPU Idle : 98%   (since system startup 441751425.0 sec ago)
NAME       USAGE %     RELATIVE %
--------   -------     ----------
STP_T        0.2         47.65
PHY_POLL     0.0         17.57
L2_AGE_T     0.0          7.90
L3_AGE_T     0.0          7.10
IPC          0.0          4.60
CONS_T       0.0          4.25
STATS_T      0.0          3.96
TNTASK       0.0          2.41
SYSTEM H     0.0          0.88
HBT_T        0.0          0.82
SNMP         0.0          0.67
GATED        0.0          0.58
IPXROUTE     0.0          0.48
CONS2T       0.0          0.33
LOWEST       0.0          0.25
PPP_TASK     0.0          0.24
PINGER_T     0.0          0.11
L2_LRN_T     0.0          0.07
CDP_T        0.0          0.02
LFAP_CN      0.0          0.00
LGRP_T       0.0          0.00
MPS          0.0          0.00
TNETD        0.0          0.00
ETHH         0.0          0.00
NI H         0.0          0.00
ARP_T        0.0          0.00
HSWAP        0.0          0.00
IPRED_T      0.0          0.00
SYS_TK       0.0          0.00
SNMP_CF      0.0          0.00
WAN_TOD_     0.0          0.00
DHCP         0.0          0.00
BOUNCE       0.0          0.00
IP_T         0.0          0.00
IPX_T        0.0          0.00
PHX_T        0.0          0.00
NTP          0.0          0.00
ERROR_LO     0.0          0.00
L3_ACL_T     0.0          0.00
MCAST        0.0          0.00
PROFILE      0.0          0.00
PRI_L3MD     0.0          0.00
L3_RL_T      0.0          0.00
```

show rarp

Purpose

Displays reverse ARP statistics.

Format

show rarp [<*IFname*>**]**

Mode

Privileged

Parameters

<*IFname*>	Specifies the interface name. If no interface name specified, command will display reverse ARP statistics for all interfaces.

Restrictions

None.

Example

To display reverse ARP statistics on interface ‘en0’:

```
ssr# show rarp en0

Interface en0:
    0 requests received
    0 replies sent
    0 requests received on interface with rarpd disabled
    0 requests received that failed sanity check
    0 requests received that did not result in a match
    Last 5 Requests Received
    ----- no rarp requests received -----
    Last 5 Replies Sent
    ----- no rarp replies sent -----
```

show tcp statistics

Purpose

Displays Transmission Control Protocol (TCP) statistics.

Format

show tcp statistics

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display TCP statistics:

```
ssr# show tcp statistics
tcp:
        235 packets sent
                232 data packets (22777 bytes)
                1 data packet (494 bytes) retransmitted
                0 resends initiated by MTU discovery
                2 ack-only packets (5 packets delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                0 control packets
        320 packets received
                227 acks (for 22776 bytes)
                3 duplicate acks
                0 acks for unsent data
                158 packets (185 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                0 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packets too short
        0 connection requests
        1 connection accept
        1 bad connection attempt
        0 listen queue overflows
        1 connection established (including accepts)
        0 connections closed (including 0 drops)
                0 connections updated cached RTT on close
                0 connections updated cached RTT variance on close
                0 connections updated cached ssthresh on close
        0 embryonic connections dropped
        226 segments updated rtt (of 228 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
                0 connections dropped by persist timeout
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        0 correct ACK header predictions
        88 correct data packet header predictions
```

show traffic

Purpose

Displays recent traffic summary statistics.

Format

statistics show summary-stats

Mode

Privileged

Parameters

None.

Restrictions

None.

show udp statistics

Purpose

Displays User Datagram Protocol (UDP) statistics.

Format

show udp statistics

Mode

Privileged

Parameters

None.

Restrictions

None.

Example

To display UDP statistics:

```
ssr# show udp statistics
udp:
      0 datagrams received
      0 datagrams with incomplete header
      0 datagrams with bad data length field
      0 datagrams with bad checksum
      0 datagrams dropped due to no socket
      0 broadcast/multicast datagrams dropped due to no socket
      0 datagrams dropped due to full socket buffers
      0 datagrams not for hashed pcb
      0 delivered
      0 datagrams output
```

Chapter 47

stp Command

The **show stp** command displays Shielded Twisted Pair (STP) bridging information.

Format

show stp [bridge]

Mode

Privileged

Description

The **show stp** command, when followed by the **bridge** keyword, displays STP bridging information for the Xpedition.

Parameters

bridge Displays information for STP bridging.

Restrictions

None.

Chapter 48

system Commands

The **system** commands allow the user to display and change system parameters.

Command Summary

Table 35 lists the **system** commands. The sections following the table describe the command syntax.

Table 35. system commands

clock set hh:mm:ss d m y
disconnect session-id
erase <*filename*> **primary-cm | backup-cm**
show bootlog
show bootprom
show buffers
show clock
show contact
show diagbus
show environment
show flash
show location
show login-banner
show logging

Table 35. system commands (Continued)

show logging buffer
show memory
show name
show poweron-selftest-mode
show processes
show running-config
show scratchpad
show sessions
show startup-config
show terminal
show timezone
show uptime
show users
show version
system hostswap out|in <*channel number*>
system image choose <*filename*> **primary-cm|backup-cm**
system promimage-upgrade <*hostname-or-IPaddr*> <*filename*>

clock set

Purpose

Sets the system time and date.

Format

clock set <*hh:mm:ss d m y*>

Mode

Privileged

Description

The **clock set** command sets the system time and date for the Xpedition. The Xpedition keeps the time in a battery-backed realtime clock. To display the time and date, enter the **show clock** command.

Parameters

hh:	A number from 0 - 23 for the hour, in military time. (Example: **06: [6 a.m.]**; **18: [6 p.m.]**; the number **00** means midnight)
mm:	A number from 0 - 59 for the minutes.
ss	A number from 0 - 59 for the second.
day	A number from 1 – 31 for the day.
month	Name of the month. You must spell out the month name. (Example: **March**).
year	Four-digit number for the year. (Example: **2000**)

Restrictions

None.

disconnect

Purpose

Disconnects a specified Telnet session.

Format

disconnect <*session-id*>

Mode

Privileged

Description

The **disconnect** command kills the Telnet session specified by the session ID. Use the **show users** command to display the list of current Telnet users and session IDs.

Parameters

<*session-id*>
The Telnet connection slot number, which can be 0, 1, 2, or 3. The **show users** command displays the session ID number in the first column. You can only specify one session ID per **disconnect** command.

Restrictions

None.

Example

To show the active Telnet sessions.

```
ssr# show users
Current Terminal User List:
# Login ID      Mode          From            Login Timestamp
- --------      ----          ----            ---------------
               enabled       console         Thu Feb 25 13:07:411999
0              enabled       10.9.0.1        Thu Feb 25 13:07:591999
2              login-prompt  10.9.0.1
3              login-prompt  10.9.0.1
```

Then, to disconnect Telnet session 2:

```
ssr# disconnect 2
Telnet session 2 (from 10.9.0.1) killed
```

Shows the contents of the boot log file, which contains all the system messages generated during bootup.

Shows the contents of the boot log file, which contains all the system messages generated during bootup.

erase

Purpose

Deletes a system software image file from the PCMCIA flash card.

Format

erase <*filename*> **primary-cm | backup-cm**

Mode

Privileged

Description

The **erase** command deletes a system software image file from the PCMCIA flash card on the Control Module.

Parameters

<*filename*> The name of the system software image file you want to delete.

primary-cm This parameter deletes the image file from the primary control module.

backup-cm This parameter deletes the image file from the backup control module.

Restrictions

None.

show bootlog

Purpose

Displays bootlog information.

Format

show bootlog

Mode

Privileged

Description

The **show bootlog** command displays the contents of the boot log file, which contains all the system messages generated during bootup.

Parameters

None.

Restrictions

None.

show bootprom

Purpose

Displays bootprom information.

Format

show bootprom

Mode

Privileged

Description

The **show bootprom** command displays boot PROM parameters for TFTP downloading of the system image. This information is useful only if you have configured the system to download the system image via TFTP.

Parameters

None.

Restrictions

None.

show buffers

Purpose

Displays usage information.

Format

show buffers

Mode

Privileged

Description

The **show buffers** command displays usage information about various resources on the Xpedition.

Parameters

None.

Restrictions

None.

show clock

Purpose

Displays system time and date.

Format

show clock

Mode

Privileged

Description

The **show clock** command displays the system time and date determined with the **clock set** command.

Parameters

None.

Restrictions

None.

show contact

Purpose

Displays contact information.

Format

show contact

Mode

Privileged

Description

The **show contact** command displays administrator contact information.

Parameters

None.

Restrictions

None.

show diagbus

Purpose

Displays system hardware information.

Format

show diagbus

Mode

Privileged

Description

The **show diagbus** command displays system hardware information.

Parameters

None.

Restrictions

None.

show environment

Purpose

Displays system environment information.

Format

show environment

Mode

Privileged

Description

The **show environment** command displays system environment information, such as temperature and power supply status.

Parameters

None.

Restrictions

None.

show flash

Purpose

Lists the system software image files on the PCMCIA flash card.

Format

show flash backup-cm | primary-cm

Mode

Privileged

Description

The **show flash** command lists the system software image files contained on the PCMCIA flash card on the Control Module.

Parameters

backup-cm This parameter lists the image files on the backup control module.

primary-cm This parameter lists the image files on the primary control module.

Restrictions

None.

show location

Purpose

Displays location of the Xpedition.

Format

show location

Mode

Privileged

Description

The **show location** command displays the location of the Xpedition.

Parameters

None.

Restrictions

None.

show login-banner

Purpose

Displays login banner for the Xpedition.

Format

show login-banner

Mode

Privileged

Description

The **show login-banner** command displays the Xpedition's login banner.

Parameters

None.

Restrictions

None.

show logging

Purpose

Displays SYSLOG information.

Format

show logging

Mode

Privileged

Description

The **show logging** command displays the IP address of the SYSLOG server and the level of messages the Xpedition sends to the server.

Parameters

None.

Restrictions

None.

show logging buffer

Purpose

Displays SYSLOG buffer information.

Format

show logging buffer

Mode

Privileged

Description

The **show logging buffer** command shows how many SYSLOG messages the Xpedition's SYSLOG message buffer can hold.

Parameters

None.

Restrictions

None.

show memory

Purpose

Displays memory resource information.

Format

show memory

Mode

Privileged

Description

The **show logging buffer** command displays information about memory resources on the Xpedition.

Parameters

None.

Restrictions

None.

show name

Purpose

Displays the Xpedition's name.

Format

show name

Mode

Privileged

Description

The **show name** command displays the name of the Xpedition.

Parameters

None.

Restrictions

None.

show poweron-selftest-mode

Purpose

Displays Power-On Self Test (POST) information.

Format

show poweron-selftest-mode

Mode

Privileged

Description

The **show poweron-selftest-mode** command displays the type of Power-On Self Test (POST) that should be performed, if any.

Parameters

None.

Restrictions

None.

show processes

Purpose

Displays information on the CPU.

Format

show processes

Mode

Privileged

Description

The **show processes** command displays the percentage of the CPU that is currently being used.

Parameters

None.

Restrictions

None.

show running-config

Purpose

Displays system's active configuration.

Format

show running-config

Mode

Privileged

Description

The **show running-config** command displays the active configuration of the system.

Parameters

None.

Restrictions

None.

show scratchpad

Purpose

Displays configuration information.

Format

show scratchpad

Mode

Privileged

Description

The **show scratchpad** command displays the configuration changes in the scratchpad. These changes have not yet been activated.

Parameters

None.

Restrictions

None.

show sessions

Purpose

Displays Telnet session information.

Format

show sessions

Mode

Privileged

Description

The **show sessions** command lists the last five Telnet connections to the Xpedition.

Parameters

None.

Restrictions

None.

show startup-config

Purpose

Displays contents of startup configuration file.

Format

show startup-config

Mode

Privileged

Description

The **show startup-config** command displays the contents of the startup configuration file.

Parameters

None.

Restrictions

None.

show terminal

Purpose

Displays terminal information.

Format

show terminal

Mode

Privileged

Description

The **show terminal** command displays default terminal settings (number of rows, number of columns, and baud rate).

Parameters

None.

Restrictions

None.

show timezone

Purpose

Displays the time zone.

Format

show timezone

Mode

Privileged

Description

The **show timezone** command shows the time zone offset from UCT in minutes.

Parameters

None.

Restrictions

None.

show uptime

Purpose

Displays up-time information.

Format

show uptime

Mode

Privileged

Description

The **show uptime** command shows how much time has elapsed since the most recent reboot.

Parameters

None.

Restrictions

None.

show users

Purpose

Shows current Telnet connections to the Xpedition.

Format

show users

Mode

Privileged

Description

The **show users** command shows all current Telnet connections to the Xpedition.

Parameters

None.

Restrictions

None.

show version

Purpose

Shows software version running on Xpedition.

Format

show version

Mode

Privileged

Description

The **show version** command displays the software version currently running on the Xpedition.

Parameters

None.

Restrictions

None.

system hotswap

Purpose

Activates or deactivates a line card.

Format

system hotswap out|in <*channel number*>

Mode

Privileged

Description

The **system hotswap out** command deactivates a line card in a specified slot on the Xpedition, causing it to go offline. The command performs the same function as if you had pressed the Hot Swap button on the line card.

The **system hotswap in** command causes a line card that was deactivated with the **system hotswap out** command to go online again. The command performs the same function as if you had removed the card from its slot and inserted it again.

See the *Enterasys Xpedition User Reference* for more information on hot swapping line cards.

Parameters

out Causes the line card in the specified slot to be deactivated.

in Causes an inactive line card in the specified slot to be reactivated.

Note: The **system hotswap in** command works only on a line card that was deactivated with the **system hotswap out** command.

<*channel number*>
Specifies the slot where the line card resides. Enter any number between 0-15.

Restrictions

None.

Example

To deactivate the line card in slot 7 on the Xpedition:

```
ssr# system hotswap out slot 7
```

system image-choose

Purpose

Selects a system software image file.

Format

system image-choose <*filename*> **primary-cm | backup-cm**

Mode

Privileged

Description

The **system image-choose** command specifies the system software image file on the PCMCIA flash card that you would like the Xpedition to use the next time you reboot the system.

Parameters

<*filename*> The name of the system software image file. If you would like to specify no image chosen for the next reboot, enter **none**.

primary-cm This parameter specifies that the image file is chosen for the primary control module.

backup-cm This parameter specifies that the image file is chosen for the backup control module.

Restrictions

None.

system promimage-upgrade

Purpose

Upgrades the boot PROM software on the Control Module.

Format

system promimage-upgrade <*hostname-or-IPaddr*> <*filename*>

Mode

Privileged

Description

The **system promimage-upgrade** command copies and installs a boot PROM software image from a TFTP server onto the internal memory on the Control Module. The boot PROM software image is loaded when you power on the Xpedition and in turn loads the system software image file.

Parameters

<*hostname-or-IPaddr*>
The host name or IP address of the TFTP server or a TFTP URL.

<*filename*>
The name of the boot PROM software image file.

Restrictions

None.

Example

The command in the following example downloads a boot PROM image file from the TFTP server 10.50.89.88.

```
ssr# system promimage-upgrade tftp://10.50.89.88 qa/prom-upgrade
Downloading image ‘qa/prom-upgrade’ from host ‘10.50.89.88’
tftp complete
checksum valid. Ready to program.
flash found at 0xbfc00000
erasing...
programming...
verifying...
programming successful.
Programming complete.
```

Chapter 49

tacacs/tacacs-plus Command

The **show tacacs** command displays information about TACACS and TACACS Plus configuration on the Xpedition.

Format

show tacacs

Mode

Enable

Description

The **show tacacs** command displays statistics and configuration parameters related to TACACS and TACACS Plus configuration on the Xpedition. The statistics displayed include:

accepts Number of times each server responded and validated the user successfully.

rejects Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied.

timeouts Number of times each server did not respond.

Parameters

None.

Restrictions

None.

Chapter 50

tech-support Command

The **show tech-support** command displays general information about the Xpedition for use when reporting a problem.This command is available in Common CLI syntax only.

Format

show tech-support

Mode

Privileged

Description

The **show tech-support** command simultaneously lists the information found in each of the following **system** commands:

- **show buffers**
- **show hardware**
- **show interfaces**
- **show processes**
- **show running-config**
- **show version**

This information is helpful when reporting a problem to Enterasys Technical Support.

Parameters

None.

Restrictions

None.

Chapter 51

telnet Command

The **telnet** command opens a Telnet session to the specified host.

Format

telnet <*hostname-or-IPaddr*> <*socket-number*>

Mode

User or Privileged

Description

The **telnet** command allows you to open a Telnet session to the specified host.

Parameters

<*hostname-or-IPaddr*>
The host name or IP address of the remote computer that you would like to access.

<*socket-number*>
The TCP port through which the Telnet session will be opened. If this parameter is not specified, the Telnet port (socket number 23) is assumed. This parameter can be used to test other ports; for example, socket number 21 is the port for FTP.

Restrictions

None.

Example

To open a Telnet session on the host “ssr4”:

```
ssr# telnet ssr4
```

Chapter 52

terminal cli native Command

The **terminal cli native** command switches the CLI environment over to the Native CLI engine.

Format

terminal cli native

Mode

Privileged

Description

The **terminal cli native** command switches the CLI environment over to the Native CLI engine. When excuted in Privileged mode, the CLI of the system will become configured to use the Native CLI commands and attributes.

Note: All current and future login sessions will use the Native CLI, until the user switches back to the Common CLI engine.

Parameters

None.

Restrictions

None.

Chapter 53

traceroute Command

The **traceroute** command traces the path a packet takes to reach a remote host.

Format

traceroute <*host*> **[max-ttl** <*num*>**] [probes** <*num*>**] [size** <*num*>**] [source** <*host*>**] [tos** <*num*>**] [wait-time** <*secs*>**] [verbose] [noroute]**

Mode

User

Description

The **traceroute** command traces the route taken by a packet to reach a remote IP host. The **traceroute** command examines the route taken by a packet traveling from a source to a destination. By default, the source of the packet is the Xpedition. However, one can specify a different source and track the route between it and a destination. The route is calculated by initially sending a probe (packet) from the source to the destination with a TTL of 1. Each intermediate router that is not able to reach the final destination directly will send back an ICMP Time Exceeded message. Subsequent probes from the source will increase the TTL value by 1. As each Time Exceeded message is received, the program keeps track of the address of each intermediate gateway. The probing stops when the packet reaches the destination or the TTL exceeds the **max-ttl** value.

Parameters

<*host*>
Hostname or IP address of the destination

max-ttl <*num*>
Maximum number of gateways (“hops”) to trace

probes <*num*>
Number of probes to send

size <*num*>
Packet size of each probe

source <*host*>
Hostname or IP address of the source

tos <*num*>
Type of Service value in the probe packet

wait-time <*secs*>
Maximum time to wait for a response

verbose
Displays results in verbose mode

noroute
Ignores the routing table and sends a probe to a host on a directly attached network. If the destination is not on the local network, an error is returned.

Restrictions

None.

Example

To display the route from the Xpedition to the host *othello* in verbose mode:

```
ssr# traceroute othello verbose
```

Chapter 54

vlan Command

The **show vlan** command displays a list of all VLANs active on the Xpedition.

Format

show vlan

Mode

Privileged

Description

The **show vlan** command lists all the VLANs that have been configured on the Xpedition.

Parameters

None.

Restrictions

None.

Chapter 55

web-cache Commands

The **web-cache** commands allow you to transparently redirect HTTP requests to a group of local cache servers. This feature can provide faster user responses and reduce demands for WAN bandwidth.

Command Summary

Table 36 lists the **web-cache** commands. The sections following the table describe the command syntax.

Table 36. web-cache commands

clear ip web-cache all | cache-name <*cache-name*>
show ip web-cache [all] [cache-name <*cache-name*> **| all] [servers cache** <*cache-name*> **| all]**

clear ip web-cache

Purpose

Clears statistics for the specified caching policy.

Format

clear ip web-cache all | cache-name <*cache-name*>

Mode

Privileged

Description

The **clear web-cache** command allows the user to clear statistics for all caching policies or for specified policies.

Parameters

all
Clears statistics for all caching policies.

cache-name <*cache-name*>

Clears statistics for the specified caching policy.

Restrictions

None.

Examples

To clear statistics for the caching policy ‘websrv1’:

```
ssr# clear ip web-cache cache-name websrv1
```

show ip web-cache

Purpose

Displays information about caching policies.

Format

show ip web-cache [all] [cache-name <*cache-name*> **| all] [servers cache** <*cache-name*> **| all]**

Mode

Privileged

Description

The **show web-cache** command allows the user to display web caching information for specific caching policies or server lists.

Parameters

all
Displays all web cache information for all caching policies and all server lists.

cache-name <*cache-name*> | **all**
Displays web cache information for the specified caching policy. **all** displays all caching policies.

servers cache <*cache-name*> | **all**
Displays information for the servers configured for the specified caching policy. **all** displays all configured cache servers.

Restrictions

None.

Examples

To display web cache information for a specific caching policy:

```
ssr# show ip web-cache cache-name cache1
Cache Name : cache1 ❶
Applied Interfaces : ip1 ❷
Bypass list : none ❸
HTTP Port : 80 ❹

 ❺          ❻             ❼          ❽        ❾    ❿ ⓫
ACL     Source IP/Mask   Dest. IP/Mask   SrcPort   DstPort   TOS Port
---     --------------   --------------   --------- --------- --- ----
deny207  172.89.1.1/32    207.135.0.0/16  any       http      0   IP

  ⓬       ⓭         ⓮
Server   Max con IP address
---- --  ------- ----------
s1       2000    176.89.10.50 - 176.89.10.60

Access Users ⓯
------ -----
Permit All Users
Deny   profile deny207
```

Legend:

1. The name of the cache policy.
2. The outbound interface where the cache policy was applied, typically an interface that connects to the Internet.
3. Destination sites for which HTTP requests are *not* redirected to cache servers and are sent direct.
4. The HTTP port used by a proxy server.
5. The names of the profiles (created with an **acl** statement) associated with this cache policy.
6. The source address and filtering mask.
7. The destination address and filtering mask.
8. The source port.
9. The destination port.
10. The TOS value in the packet.
11. The protocol.
12. The server list name.

13. The maximum number of connections that can be handled by each server in the server list.
14. The list or range of IP addresses of the servers in the server list.
15. The hosts (users) whose HTTP requests *are* redirected to the cache servers and the hosts whose HTTP requests are *not* redirected to the cache servers. If no **permit** command is specified, all HTTP requests are redirected to the cache servers.

To display information for all configured web cache servers:

```
ssr# show ip web-cache servers cache cache1
Cache name : cache1 ❶

 ❷     ❸          ❹       ❺       ❻
Block IP address    Max Conn  Used Cnt  Status
----- ----------    --------  --------  ------
s1    176.89.10.50  2000      0         Down
s1    176.89.10.51  2000      0         Down
s1    176.89.10.52  2000      0         Down
s1    176.89.10.53  2000      0         Down
s1    176.89.10.54  2000      0         Down
s1    176.89.10.55  2000      0         Down
s1    176.89.10.56  2000      0         Down
s1    176.89.10.57  2000      0         Down
s1    176.89.10.58  2000      0         Down
s1    176.89.10.59  2000      0         Down
s1    176.89.10.60  2000      0         Down
```

Legend:

1. The name of the cache policy.
2. The server list name.
3. The IP address of a server in the server list.
4. The maximum number of connections that can be handled by the server.
5. The number of connections currently being handled by the server.
6. The current status of the server.

Appendix A

CLI Conversion Matrix

The following matrix allows the user to convert Xpedition Native CLI commands to Common CLI commands.

Expedition v8.0 CLI	Common CLI	Mode
ACL (ACCESS LIST) COMMANDS		
acl clearcounters aclname all | interface | service | port	clear access-list counters <*num*> | <*name*>	PRIV
acl show [aclname <*string*> | all] | [interface <*string*> | all-ip] | [service] | [port <*port-list*> | all-ports] | [all]	show access-lists [<*num*> | <*string*> | {interface <*string*> | all-ip} | service | {port <*port-list*> \ all-ports}]	PRIV
AGING COMMANDS		
aging l2 show status	show mac-address-table aging-time	USER
aging l3 show status	show mls aging	USER
ARP COMMANDS		
arp add <*host*> mac-addr <*MAC-addr*> exit-port <*port*> keep-time <*seconds*>	arp add <*host*> mac-addr <*MAC-addr*> exit-port <*port*> keep-time <*seconds*>	PRIV
arp clear <*host*> | all [interface <*string*> | all] [port <*port*>]	arp clear <*host*> mac-addr <*MAC-addr*> exit-port <*port*> keep-time <*seconds*>	PRIV
arp show <*IPaddr*> | all [undecoded] [unresolved] [interface <*string*> | all] [port <*port*>]	arp show <*IPaddr*> | all [undecoded] [unresolved] [interface <*string*> | all] [port <*port*>]	PRIV
statistics show arp	show arp statistics	PRIV
ATM COMMAND		

Expedition v8.0 CLI	Common CLI	Mode
atm show [vpl port <*port-list*>] [vcl port <*port-list*>] [service] [port-settings <*port-list*> | all-ports]	show atm [vpl port <*port-list*>] [vcl port <*port-list*>] [service] [port-settings <*port-list*> | all-ports]	PRIV
BGP COMMANDS		
bgp show routes <*IPaddr-mask*> | default | all [to-terminal | to-file]	show ip bgp [<*IPaddr*> <*IPmask*>] [to-file]	PRIV
bgp show cidr-only <*IPaddr-mask*> | default | all [to-terminal | to-file]	show ip bgp cidr-only [<*IPaddr*> <*IPmask*>] [to-file]	PRIV
bgp show community community-id <*number*> autonomous-system <*number*> | well-known-community [no-export | no-advertise | no-export subconfed] | reserved-community <*number*>] [to-terminal | to-file]	show ip bgp community {<*community-id*> | <*ASnum*> | no-export | no-advertise | no-export subconfed | reserved-community <*hexnum*>} [to-file]	PRIV
bgp show peer-host <*IPaddr*> received-routes | all-received-routes | advertised-routes [to-terminal | to-file]	show ip bgp neighbor <*IPaddr*> routes | received-routes | advertised-routes [to-file]	PRIV
bgp show peer-as <*number*> [to-terminal | to-file]	show ip bgp peer-as <*number*> [to-file]	PRIV
bgp show peer-group-type external | internal | igp | routing [to-terminal | to-file]	show ip bgp peer-group external | internal | igp | routing [to-file]	PRIV
bgp show regexp <*regexp*>	show ip bgp regexp <*regexp*>	PRIV
bgp show summary [to-terminal | to-file]	show ip bgp summary [to-file]	PRIV
bgp show sync-tree	show ip bgp sync-tree	PRIV
CLI COMMANDS		
cli show history	show history	USER
cli show terminal	show terminal	USER
cli set command completion on | off	terminal command-completion on | off	USER
cli set history size <*num*> | default | maxsize	terminal history size <*buffer-size*>	USER
cli set terminal rows <*num*> columns <*num*>	terminal length <*screen-length*> terminal width <*line-length*>	USER
cli terminal monitor on | off	terminal monitor	PRIV
COPY COMMANDS		

Expedition v8.0 CLI	Common CLI	Mode
copy [active | scratchpad | tftp-server | rcp-server | startup | <*filename*> | <*url*>] to [backup-CM | active | scratchpad | tftp-server | rcp-server | startup | <*filename*> | <*url*>]	copy [tftp | rcp | active | scratchpad | startup | <*filename*>] [tftp | rcp | active | scratchpad | startup | <*filename*>]	PRIV
system image add <*IPaddr-or-hostname*> <*filename*>	copy tftp flash	PRIV
DHCP COMMANDS		
dhcp flush	clear ip dhcp	PRIV
dhcp show binding [active | expired | static]	show ip dhcp binding [active | expired | static]	PRIV
dhcp show num-clients	show ip dhcp num-clients	PRIV
DVMRP COMMANDS		
dvmrp show interface [<*IPaddr*>]	show ip dvmrp interface <*IPaddr*>	PRIV
dvmrp show routes host <*IPaddr*> | interface <*IPaddr*> | net <*netaddr*> | router <*IPaddr*>	show ip dvmrp route [<*port-list*> | <*IPaddr*>]	PRIV
dvmrp show rules	show ip dvmrp rules	PRIV
ENABLE COMMAND		
enable	enable	PRIV
EXIT COMMAND		
exit	exit	PRIV
FDDI COMMANDS		
fddi reset <*port-list*>	clear fddi <*port-list*>	PRIV
fddi show fddi-fdx-mode | fddi-mode | fddi-status | mac-group | mac-restricted-token | media-type | path-group | port-group | ring-purger | smt-config | smt-group | translation | version <*port-list*> | all-ports	show fddi fddi-fdx-mode | fddi-mode | fddi-status | mac-group | mac-restricted-token | media-type | path-group | port-group | ring-purger | smt-config | smt-group | translation | version <*port-list*> | all-ports	PRIV
FILE COMMANDS		
file delete <*file-name*>	delete <*file-name*>	PRIV
file dir <*device-name*>	dir <*device-name*>	USER
file type <*file-name*>	show file <*file-name*>	PRIV
FILTERS COMMANDS		

Expedition v8.0 CLI	Common CLI	Mode
filters show address-filter [all-source | all-destination | all-flow] [source-mac <*MACaddr*> dest-mac <*MACaddr*>] [ports <*port-list*>] [vlan <*VLANnum*>]	show filters address-filter [all-source | all-destination | all-flow] [source-mac <*MACaddr*> dest-mac <*MACaddr*>] [ports <*port-list*>] [vlan <*VLANnum*>]	PRIV
filters show port-address-lock [ports <*port-list*>] [vlan <*VLANnum*>] [source-mac <*MACaddr*>]	show filters [port-address-lock] [ports <*port-list*>] [vlan <*VLANnum*>] [source-mac <*MACaddr*>]	PRIV
filters show secure port	show filters [secure-port]	PRIV
filters show static-entry [all-source | all-destination | allow-flow] ports <*port-list*> vlan <*VLANnum*> [source-mac <*MACaddr*> dest-mac <*MACaddr*>]	show filters [static-entry] [all-source | all-destination | allow-flow] ports <*port-list*> vlan <*VLANnum*> [source-mac <*MACaddr*> dest-mac <*MACaddr*>]	PRIV
FRAME RELAY COMMANDS		
frame-relay clear stats-counter [frame-drop-qdepth-counter][max-frame-enqued-counter][frame-drop-red-counter][rmon] ports <*port-list*>	clear frame-relay [frame-drop-qdepth-counter][max-frame-enqued-counter] [frame-drop-red-counter][rmon][<*port-list*>]	PRIV
frame-relay show service <*service-name*> | all	show frame-relay service	PRIV
frame-relay show stats port <*port-name*> [last-error] [lmi] [mibII] [summary]	show frame-relay stats	PRIV
IGMP COMMANDS		
igmp show interfaces [group <*IPaddr*> | interface <*name/IPaddr*>]	show ip igmp interface <*port-list*>	PRIV1
igmp show memberships [group <*IPaddr*> | port <*port-list*>]	show ip igmp groups <*IPaddr*>	PRIV
igmp show timers	show ip igmp timers	PRIV
igmp show vlans	show ip igmp vlans	PRIV
IP COMMANDS		
ip clear reverse-flows	ip clear reverse-flows	PRIV
ip show hash-variant <*num*> | all	show ip hash-variant	PRIV
ip show helper-address	show ip helper-address	PRIV
ip show interfaces [<*interface-name*>] [brief]	show ip interface	PRIV
ip show reverse-flows	show ip reverse-flows	PRIV
ip show routes [no-lookup][show-arps][show-multicast][verbose]	show ip route	PRIV

Expedition v8.0 CLI	Common CLI	Mode
ip show routes show-protocol [bgp | direct | ospf | ospf-ase | rip | static]	show ip route [bgp | connected | ospf | ospf-ase | rip | static]	PRIV
ip show routes show-summary	show ip route summary	PRIV
ip show connections [no-lookup]	show tcp [dns-lookup] show udp [dns-lookup]	PRIV
IP-POLICY COMMANDS		
ip-policy clear policy-name <*name*> | all	clear route-map [policy-name <*name*> | all]	PRIV
IP-REDUNDANCY COMMANDS		
ip-redundancy clear vrrp-stats interface <*name*> id <*VRid*>	clear vrrp <*VRid*> interface <*name*>	PRIV
ip-redundancy set vrrp <*VRid*> interface <*name*> [priority <*num*>][adv-interval <*num*>][preempt-mode enabled | disabled | owner-disabled][auth-type none | text][auth-key <*key*>][warmup-period <*num*>]	show vrrp <*VRid*> interface <*name*>	PRIV
IP-ROUTER COMMANDS		
ip-router find route <*IPaddr*> [ignore-state]	ip find rib-route <*IPaddr*> [ignore-state]	PRIV
ip-router show configuration-file active | permanent	show gated-config active | permanent	PRIV
ip-router show rib [detail]	show ip route [summary]	PRIV
ip-router show route [ip-addr-mask | default][detail]	show ip route <*IPaddr*> [detail]	PRIV
ip-router show state [all][memory] [timers][to-file][to-terminal][task <*string*> | all | gii | icmp | inet | interface | krt | route]	show ip route state	PRIV
IPX COMMANDS		
ipx find rip <*address*>	ipx find rip <*address*>	PRIV
ipx find sap <*type*> | all <*SRVCname*> | all <*network*> | all <*entrytype*>	ipx find sap <*type*> | all <*SRVCname*> | all <*network*> | all <*entrytype*>	PRIV
ipx show buffers	show ipx buffers	PRIV
ipx show interfaces <*interface*> [brief]	show ipx interface [<*interface*>]	PRIV
ipx show rib <*destination*>	show ipx rib destination	USER
ipx show servers hops | net | name | type	show ipx servers {sorted [hops | net | name | type]} | unsorted	USER
ipx show tables routing | rip | sap | summary	show ipx route	USER

Expedition v8.0 CLI	Common CLI	Mode
L2 (MAC ADDRESS TABLE) COMMANDS		
l2-tables show all-flows {vlan <*VLANnum*> [source-mac <*MACaddr*>]} [undecoded]	show mac-address-table all-flows [vlan <*VLANnum*>][source-mac <*MACaddr*>][undecoded]	USER PRIV
l2-tables show all-macs {verbose [undecoded]}[vlan <*VLANnum*>] [source][destination][multicast]	show mac-address-table all-macs [vlan <*VLANnum*>][source-mac <*MACaddr*>] [source][destination][multicast]	USER PRIV
l2-tables show bridge-management	show mac-address-table bridge-management	USER PRIV
l2-tables show igmp-mcast-registrations [vlan <*VLANnum*>]	show mac-address-table igmp-mcast-registration [vlan <*VLANnum*>]	USER PRIV
l2-tables show mac <*MACaddr*> vlan <*VLANnum*>	show mac-address-table address <*MACaddr*> vlan <*VLANnum*>	USER PRIV
l2-tables show mac-table-stats	show mac-address-table mac-table-stats	USER PRIV
l2-tables show port-mac <*port-list*> | all-ports {[vlan <*VLANnum*>][source] [destination][multicast][undecoded][no-stats] verbose}	show mac-address-table port-macs <*port-list*> | all-ports {verbose [vlan <*VLANnum*>][source] [destination][multicast][undecoded][no-stats]}	USER PRIV
l2-tables show vlan-igmp-status vlan <*VLANnum*>	show mac-address-table vlan-igmp-status vlan <*VLANnum*>	PRIV
LFAP COMMANDS		
lfap show all	show lfap	PRIV
lfap show configuration	show lfap configuration	PRIV
lfap show servers	show lfap servers	PRIV
lfap show statistics	show lfap statistics	PRIV
lfap show status	show lfap status	PRIV
LOAD-BALANCE COMMANDS		
load-balance set server-status server-ip <*IPaddr*> server-port <*port*> group-name <*string*> status up | down	load-balance set server-status	PRIV
load-balance show acv-options [group-name <*string*>][destination-host-ip <*IPaddr*>][destination-host-port <*port*>]	show load-balance acv-options	PRIV
load-balance show hash-stats	show load-balance hash-stats	PRIV

Expedition v8.0 CLI	Common CLI	Mode
load-balance show source-mappings client-ip <*IPaddr*> virtual-ip <*IPaddr*> virtual-port <*port*> destination-host-ip <*IPaddr*>	show load-balance source-mappings	PRIV
load-balance show statistics group-name <*string*> virtual-ip <*IPaddr*> virtual-port <*port*>	show load-balance statistics	PRIV
load-balance show virtual-hosts group-name <*string*> virtual-ip <*IPaddr*> virtual-port <*port*>	show load-balance virtual-hosts	PRIV
LOGOUT COMMAND		
logout	logout	ALL
MTRACE COMMAND		
mtrace <*source*>	mtrace <*source*>	PRIV
MULTICAST COMMANDS		
multicast show interface [<*IPaddr*> | <*hostname*>]	show ip multicast interface	PRIV
multicast show mroutes [child <*IPaddr*>][group <*IPaddr*>][parent <*IPaddr*>]	show mroute [child <*IPaddr*>][group <*IPaddr*>][parent <*IPaddr*>]	PRIV
NAT COMMANDS		
nat clear-err-stats out-of-globals | port-mode	clear ip nat out-of-globals | port-mode	PRIV
nat flush-dynamic-binding all | pool-specified [local-acl-pool <*localACL*>] [global-pool <*IPaddr/range*>]	clear ip nat translation {pool-specified [local-acl-pool <*localACL*>] [global-pool <*IPaddr/range*>]}	PRIV
nat show [translations][timeouts][statistics]	show ip nat [statistics | timeouts | translations]	PRIV
NTP COMMANDS		
ntp synchronize server <*host*>	ntp synchronize server <*host*>	PRIV
ntp show all	show ntp [associated | status]	PRIV
OSPF COMMANDS		
ospf show <*option-list*>	show ip ospf show ip ospf interface	PRIV
PING COMMAND		
ping <*hostname-or-IPaddr*> packets <*num*> size <*num*> wait <*num*> [flood][dontroute]	ping <*hostname-or-IPaddr*> packets <*num*> size <*num*> wait <*num*> [flood][dontroute]	PRIV

Expedition v8.0 CLI	Common CLI	Mode
PORT COMMANDS		
port show bmon	show bmon	PRIV
port show bridging-status <*port-list*> | all-ports	show bridging	PRIV
port show description <*port-list*> | all-ports	show interface <*port-list*>	PRIV
port show 8021p <*port-list*> | all-ports	show port 8021	PRIV
port show autonegotiation <*port-list*> | all-ports	show port autonegotiation <*port-list*> | all-ports	PRIV
port show autonegotiation-capabilities <*port-list*> | all-ports	show port autonegotiation-capabilities <*port-list*> | all-ports	PRIV
port show MAU <*port-list*> | all-ports	show port MAU <*port-list*>	PRIV
port show MAU-statistics <*port-list*> | all-ports	show port MAU-statistics <*port-list*>	PRIV
port show mirroring-status <*port-list*> | all-ports | all-acls	show port-mirroring [<*port-list*> | acls]	PRIV
port show port-status <*port-list*> | all-ports	show port status <*port-list*>	PRIV
port show stp-info <*port-list*> | all-ports	show stp interface <*port-list*>	PRIV
port show pvst-info <*port-list*> | all-ports	show pvst <*name*> interface <*port-list*>	PRIV
port show vlan-info <*port-list*> | all-ports	show vlan interface <*port-list*>	PRIV
PPP COMMANDS		
ppp clear stats-counter [frame-drop-qdepth-counter][max-frame-enqued-counter] [frame-drop-red-counter][rmon] port <*port-list*>	clear ppp stats-counter ports <*port-list*> {[frame-drop-qdepth-counter][max-frame-enqued-counter] [frame-drop-red-counter][rmon]}	PRIV
ppp restart lcp-ncp ports <*port-list*>	ppp restart lcp-ncp ports <*port-list*>	PRIV
ppp show mlp <*port-list*> | all-ports	show ppp mlp <*port-list*> | all-ports	PRIV
ppp show service <*service-name*> | all	show ppp service <*service-name*> | all	PRIV
ppp show stats port <*port*> [bridge-ncp] [ip-ncp][link-status][summary]	show ppp stats port <*port*> [bridge-ncp] [ip-ncp][link-status][summary]	PRIV
PVST COMMAND (STP)		
pvst show bridging-info spanning-tree <*VLANnum*>	show pvst <*VLANnum*>	PRIV
QOS COMMANDS		
qos show ip	show qos ip	PRIV

Expedition v8.0 CLI	Common CLI	Mode
qos show ipx	show qos ipx	PRIV
qos show l2 all-destination all-flow ports <*port-list*> vlan <*VLANnum*> source-mac <*MACaddr*> dest-mac <*MACaddr*>	show qos l2 all-destination all-flow ports <*port-list*> vlan <*VLANnum*> source-mac <*MACaddr*> dest-mac <*MACaddr*>	PRIV
qos show precedence ip | ipx	show qos precedence ip | ipx	PRIV
qos show priority-map <*string*> | all	show qos priority-map <*string*> | all	PRIV
qos show wred [input port <*port-list*> | all-ports][port <*port-list*> | all-ports]	show qos wred [input port <*port-list*> | all-ports][port <*port-list*> | all-ports]	PRIV
qos show wfq port <*port-list*> | all-ports	show qos wfq <*port-list*> | all-ports	PRIV
RADIUS COMMAND		
radius show stats | all	show radius	PRIV
RARPD COMMAND		
rarpd show interface | mappings	show rarpd interface | mappings	PRIV
RATE-LIMIT COMMAND		
rate-limit show [all] | [policy-type flow-policies | aggregate-policies | portlevel-policies | all] | [policy-name <*name*>] | [interface <*interface*>] | [port-level port <*port-list*> | all-port] | [port-level policy-name <*name*>] | [rate-limiting-mode]	show rate-limit [all] | [policy-type flow-policies | aggregate-policies | portlevel-policies | all] | [policy-name <*name*>] | [interface <*interface*>] | [port-level port <*port-list*> | all-port] | [port-level policy-name <*name*>] | [rate-limiting-mode]	PRIV
RDISC (IRDP) COMMAND		
rdisc show	show ip irdp	PRIV
REBOOT COMMAND		
reboot	reload	PRIV
RIP COMMANDS		
rip trace [packets | request | response | local-options][detail][send | receive]	rip trace [packets | request | response | local-options][detail][send | receive]	PRIV
rip show <*option-list*>	show rip <*option-list*>	PRIV
RMON COMMANDS		
rmon clear cli-filter	clear rmon cli filter clear rmon statistics	PRIV
rmon apply cli-filters <*filter-id*>	rmon apply cli-filters <*filter-id*>	PRIV
rmon show <*option-list*>	show rmon [alarms | capture | events | filter | history | matrix | statistics | task | topn]	PRIV
SFS COMMANDS		

Expedition v8.0 CLI	Common CLI	Mode
sfs show cdp-hello port-status <*port-list*> | all-ports	show sfs cdp-hello port-status <*port-list*> | all-ports	PRIV
sfs show cdp-hello transmit-frequency	show sfs cdp-hello transmit-frequency	PRIV
SMARTTRUNK COMMANDS		
smarttrunk clear load-distribution <*smartTRUNK*>	clear smarttrunk load-distribution <*smartTRUNK*>	PRIV
smarttrunk show <*option*>	show smarttrunk [distribution | protocol-state | connections] <*numlist*>	PRIV
SNMP COMMANDS		
snmp show access | all | chassis-id | community | statistics | trap	show snmp	PRIV
SONET COMMANDS		
sonet show aps <*SONETports*>	sonet show aps <*SONETports*>	PRIV
sonet show loopback <*SONETports*>	sonet show loopback <*SONETports*>	PRIV
sonet show medium <*SONETports*>	sonet show medium <*SONETports*>	PRIV
sonet show pathtrace <*SONETports*>	sonet show pathtrace <*SONETports*>	PRIV
STATISTICS COMMANDS		
statistics clear [port-errors | port-packets | port-stats] <*port-list*>	clear interface [<*port-list*>][errors | packets | statistics]	PRIV
statistics clear ip	clear ip statistics	PRIV
statistics clear ipx	clear ipx statistics	PRIV
statistics show icmp	show ip icmp statistics	PRIV
statistics show multicast	show ip multicast	PRIV
statistics show ip-routing	show ip traffic	PRIV
statistics show ipx-routing	show ipx traffic	PRIV
statistics show port-errors <*port-list*> | all-ports	show port errors [<*port-list*>]	PRIV
statistics show port-packets <*port-list*> | all-ports	show port packets [<*port-list*>]	PRIV
statistics show port-stats <*port-list*> | all-ports	show port stats [<*port-list*>]	PRIV
statistics show top	show processes cpu	PRIV
statistics show rarp <*ifname*> | all	show rarp [<*ifname*>]	PRIV
statistics show tcp	show tcp statistics	PRIV

Expedition v8.0 CLI	Common CLI	Mode
statistics show summary-stats	show traffic	PRIV
statistics show udp	show udp statistics	PRIV
STP COMMAND		
stp show bridging-info	show stp [bridge]	PRIV
SYSTEM COMMANDS		
system set date year <*num*> month <*num*> day <*num*> hour <*num*> min <*num*> second <*num*>	clock set <*hh:mm:ss*> <*day*> <*month*> <*year*>	PRIV
system kill telnet-session <*session-id*>	disconnect <*session-id*>	PRIV
system image delete <*filename*> [primary-cm | backup-cm]	erase <*filename*> [primary-cm | backup-cm]	PRIV
system show bootlog	show bootlog	PRIV
system show bootprom	show bootprom	PRIV
system show capacity	show buffers show memory	PRIV
system show date	show clock	PRIV
system show contact	show contact	PRIV
system show hardware	show diagbus	PRIV
system show environmental-info	show environment	PRIV
system image list [primary-cm | backup-cm | all]	show flash	PRIV
system show location	show location	PRIV
system show login-banner	show login-banner	PRIV
system show syslog	show logging	PRIV
system show buffer	show logging buffer	PRIV
system show name	show name	PRIV
system show poweron-selftest-mode	show poweron-selftest-mode	PRIV
system show cpu-utilization	show processes	PRIV
system show active-config	show running-config	PRIV
system show scratchpad	show scratchpad	PRIV
system show telnet-access	show sessions	PRIV
system show startup-config	show startup-config	PRIV

Expedition v8.0 CLI	Common CLI	Mode
system show terminal	show terminal	PRIV
system show timezone	show timezone	PRIV
system show uptime	show uptime	PRIV
system show users	show users	PRIV
system show version	show version	PRIV
system hotswap [out | in] channel <*number*>	system hotswap [out | in] channel <*number*>	PRIV
system image choose <*filename*> [primary-cm | backup-cm | none]	system image choose <*filename*> [primary-cm | backup-cm]	PRIV
system promimage upgrade <*hostname/IPaddr*> <*filename*>	system promimage upgrade <*hostname/IPaddr*> <*filename*>	PRIV
TACACS COMMAND		
tacacs show stats | all	show tacacs	PRIV
TACACS-PLUS COMMAND		
tacacs-plus show stats | all	show tacacs	PRIV
TELNET COMMAND		
telnet <*hostname/IPaddr*> [socket <*socket-number*>]	telnet	USER PRIV
TRACE ROUTE COMMAND		
traceroute <*host*> [max-ttl <*num*>][probes <*num*>][size <*num*>][source <*host*>][tos <*num*>][wait-time <*secs*>][verbose] [noroute]	traceroute <*host*> [max-ttl <*num*>][probes <*num*>][size <*num*>][source <*host*>][tos <*num*>][wait-time <*secs*>][verbose] [noroute]	USER
VLAN COMMAND		
vlan show	show vlan	PRIV
WEB-CACHE COMMANDS		
web-cache clear [all | cache-name <*cache-name*>]	clear ip web-cache [all | cache-name <*cache-name*>]	PRIV
web-cache show [all][cache-name <*cache-name*> | all][servers cache <*cache-name*> | all]	show ip web-cache [all][cache-name <*cache-name*> | all][servers cache <*cache-name*> | all]	PRIV
COMMON-MODE ONLY: TECH SUPPORT COMMAND		
No Equivalent	show tech-support	PRIV