Model 3231

Industrial Ethernet Extender with LCD

CLI Reference Guide

Important
This is a Class A device and is intended for use in a light industrial environment. It is not intended nor approved for use in an industrial or residential environment.

Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Part Number: **07M3231-CLI, Rev. A**
Revised: **October 29, 2008**

Patton Electronics, Inc.

Trademark Statement

Copyright © 2008, Patton Electronics. All rights reserved.

The information in this document is subject to change without notice. Patton assumes no liability for errors that may appear in this document.

Warranty Information

Patton warrants all Model 3231 components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If this product fails or does not perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall Patton be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. Patton specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Note Conformity documents of all Patton products can be viewed online at www.patton.com under the appropriate product page.

Summary Table of Contents

Table of Contents

About this guide

This guide describes commands for configuring the Patton Model 3231 Industrial Ethernet Extender with LCD.

Note For general information regarding setting up, installing and operating the 3231, refer to the *Getting Started Guide*.

Audience

This guide is intended for administrators and operators.

Structure

- Chapter 1, "Alarm Commands" on page 13 describes commands for configuring alarms.
- Chapter 2, “Bridge Commands” on page 18 describes commands for configuring the bridge.
- Chapter 3, “CPE Config Commands” on page 27 describes commands for configuring the CPE. (These commands are only available from the CO unit).
- Chapter 4, “Ethernet Commands” on page 31 describes commands for configuring Ethernet transports.
- Chapter 5, “Firewall Commands” on page 38 describes commands for configuring the firewall.
- Chapter 6, “G.SHDSL Commands” on page 55 describes commands for configuring the G.SHDSL port.
- Chapter 7, “Help Commands” on page 76 describes commands for accessing the top-level CLI help.
- Chapter 8, “IP Commands” on page 78 describes commands for configuring IP interfaces.
- Chapter 9, “Logger Commands” on page 99 describes commands for logging into a remote host.
- Chapter 10, “Port Commands” on page 102 describes commands for configuring physical ports.
- Chapter 11, “PPP Commands” on page 105 describes commands for configuring PPP over HDLC.
- Chapter 12, “PPPoA Commands” on page 113 describes commands for configuring PPP over ATM.
- Chapter 13, “PPPoE Commands” on page 123 describes commands for configuring PPP over Ethernet.
- Chapter 14, “RFC1483 Commands” on page 133 describes commands for configuring RFC 1483 transports.
- Chapter 15, “Security Commands” on page 140 describes commands for configuring security features.
- Chapter 16, “SNMP Commands” on page 150 describes commands for configuring SNMP settings.
- Chapter 17, “Source Commands” on page 156 describes commands for viewing source files.
- Chapter 18, “System Commands” on page 158 describes commands for managing the system.
- Chapter 19, “Transport Commands” on page 174 describes commands for configuring transports.
- Chapter 20, “User Commands” on page 179 describes commands for managing user login information.
- Chapter 21, “Webserver Commands” on page 183 describes commands for configuring the Web Server.

Using the CLI

The Model 3231 may be configured through the CLI, although basic settings should be configured through the LCD menu on the unit.

Connect a PC and log in

Use an RS-232/Ethernet cable and DB9-RJ45 adapter to connect a PC's serial port to the 3231's *Console* port (see figure 1).

CAUTION

The interconnecting cables shall be acceptable for external use and shall be rated for the proper application with respect to voltage, current, anticipated temperature, flammability, and mechanical serviceability.

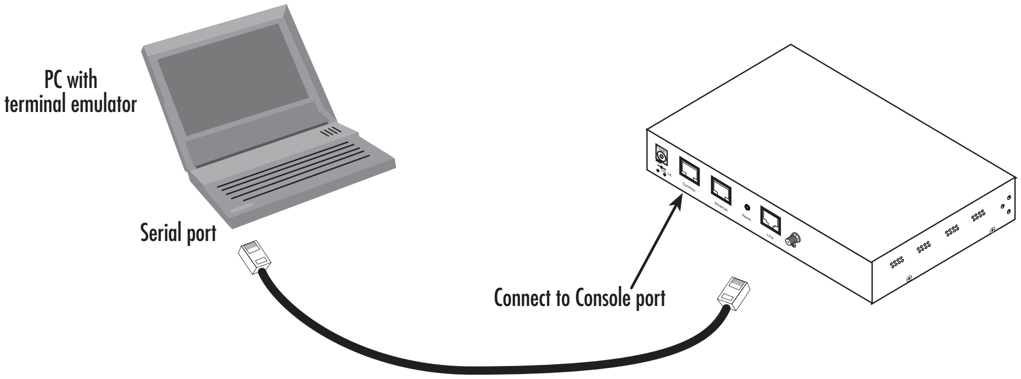

Figure 1. Connecting the 3231 to the PC's serial port

1. Start a HyperTerminal session on the PC using the settings:
   9600 bps, 8 data bits, no parity, 1 stop bit, no flow control
2. Log in to the 3231 using the factory-default login (*superuser*) and password (*superuser*):

Precautions

Notes, cautions, and warnings, which have the following meanings, are used throughout this guide to help you become aware of potential problems.

Note A note presents additional information or interesting sidelights.

IMPORTANT

The alert symbol and IMPORTANT heading calls attention to important information.

CAUTION

The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.

Typographical conventions used in this document

This section describes the typographical conventions and terms used in this guide.

General conventions

The procedures described in this manual use the following text conventions:

Table 1. General conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you have finished reviewing the reference, click on the **Go to Previous View** button ◀ in the Adobe® Acrobat® Reader toolbar to return to your starting point.
Futura bold type	Commands and keywords are in **boldface** font.
Futura bold-italic type	Parts of commands, which are related to elements already named by the user, are in ***boldface italic*** font.
Italicized Futura type	Variables for which you supply values are in *italic* font
Futura type	Indicates the names of fields or windows.
Garamond bold type	Indicates the names of command buttons that execute an action.

Chapter 1 Alarm Commands

Chapter contents

alarm all alarmStatus

Set the alarm state for all alarms.

Table 2. alarm all alarmStatus

Command	Explanation
alarm all alarmStatus clear	Set the alarm state to "clear" for all alarms. Does not clear the number of occurences and the time of the most recent occurrence.
alarm all alarmStatus reset	Set the alarm state to "clear" for all alarms. Clears the number of occurrences and the time of the most recent occurrence.

alarm set <index> alarmSeverity

Set the index for the severity level of an alarm.

Table 3. alarm set <index> alarmSeverity

Command	Explanation
alarm set <index> alarm Severity critical	Determine the level of importance for specific alarms. Critical/Major = The most severe alarms Ignore/Informational/Minor = Non-severe alarms
alarm set <index> alarm Severity ignore	
alarm set <index> alarm Severity informational	
alarm set <index> alarm Severity major	
alarm set <index> alarm Severity minor	

alarm set <index> alarmStatus

Set the index for the status level of an alarm.

Table 4. alarm set <index> alarmStatus

Command	Explanation
alarm set <index> alarm Status active	Mark the alarm condition as a currently present alarm.
alarm set <index> alarm Status clear	Clear a specific alarm. Does not clear the number of occurrences or the most recent occurrence.
alarm set <index> alarm Status inactive	Mark the alarm condition as not currently present.
alarm set <index> alarm Status reset	Clear a specific alarm. Clears the number of occurrences or the most recent occurrence.

alarm show

Show alarm status.

Table 5. alarm show

Command	Explanation
alarm show	Show alarm status.

Example Output: alarm show

```
--> alarm show

Current Box State: Major

Alarm Table

                                             Alarm
 Active |  ID  | Alarm String            |    Severity      |    Time    | Count
--------|-----|------------------------|-----------------|-----------|------
        | 1   | PP Over Threshold      | Informational   | 00:00:00s |  0
        | 2   | NP Over Threshold      | Informational   | 00:00:00s |  0
        | 3   | G.SHDSL Loss Of Signal | Major           | 00:00:00s |  0
  ****  | 4   | Ethernet Link Down     | Major           | 00:00:05s |  1
----------------------------------------------------------------------------
```

Chapter 2 Bridge Commands

Chapter contents

bridge add interface

Add a named interface to the bridge.

Table 6. bridge add interface

Command	Explanation
bridge add interface <name>	Add a named interface to the bridge.

bridge attach

Attach existing transport to existing bridge interface.

Table 7. bridge attach

Command	Explanation
bridge attach <name> <transport>	Attach existing transport to existing bridge interface.

bridge clear interfaces

Remove all bridge interfaces.

Table 8. bridge clear interfaces

Command	Explanation
bridge clear interfaces	Remove all bridge interfaces.

bridge delete interface

Remove specific bridge interface.

Table 9. bridge delete interface

Command	Explanation
bridge delete interface <name>	Remove specific bridge interface.

bridge detach

Detach a transport from a bridge interface.

Table 10. bridge detach

Command	Explanation
bridge detach <name>	Detach a transport from a bridge interface.

bridge list interfaces

List bridge interfaces.

Table 11. bridge list interfaces

Command	Explanation
bridge list interfaces	List bridge interfaces.

Example Output: bridge list interfaces

```
--> bridge list interfaces

Bridge Interfaces:

 ID  |     Name      | Filter Type  |     Transport
-----|--------------|--------------|------------------
   1 | br1          | All          | eth1
   2 | br2          | All          | ppp1
   3 | br3          | All          | rfc1
------------------------------------------------------
```

bridge set

Configure bridge attributes.

Table 12. bridge set

Command		Explanation
bridge set dhcpFilteredPort	**<port>**	Set the DHCP filtered port.
bridge set dhcpMACFiltering	**disable**	Disable DHCP MAC filtering.
	enable	Enable DHCP MAC filtering.
bridge set filterage	**<filterage>**	Set the time of no activity after which MAC addresses are removed from the filter table.
bridge set interface <name>	**filtertype all**	Allow all types of ethernet packets through the port.
	filtertype ip	Allow only IP/ARP types of ethernet packets through the port.
	filtertype pppoe	Allow only PPPoE types of ethernet packets through the port.
	portfilter <port>	Set the other ports to which this interface can bridge.
	spanning cost <pathcost>	Allow STP to make better decisions on which port to forward on. The lower the cost, the more likely that port is to enter the forwarding state. For example, you might assign a low cost to the Ethernet port and a higher one to a PPP interface because the Ethernet interface has more bandwidth.
	spanning priority<priority>	Allow STP to advertise different priorities out different interfaces.
bridge set spanning	**disabled**	Ensure that the bridge acts as a transparent bridge.
	enabled	Allow the bridge to use the spanning tree protocol.
	forwarddelay <delay>	Set the time that the bridge spends in listening or learning states when the bridge is or is attempting to become the root bridge.
	hellotime <hellotime>	Set the time after which the spanning tree process sends notification of changes to the root bridge.
	maxage <maxage>	Set the maximum age of received spanning tree protocol information before it is discarded.
	priority <priority>	Assign priority to the bridge; The lower the priority number, the more significant the bridge becomes in protocol terms.

bridge show

Display bridge/interface settings.

Table 13. bridge show

Command	Explanation
bridge show	Display bridge/interface settings.
bridge show interface <name>	Display named interface settings.

Example Output: bridge show

```
--> bridge show

Global bridge configuration:

         Filter age: 300
 DHCP MAC Filtering: false
 DHCP Filtered Port: bun/port=ethernet

Spanning bridge configuration:

       Spanning: false
       Priority: 32768
  Forward delay: 15
     Hello time: 2
       Max. age: 20
```

Example Output: bridge show interface br1

```
--> bridge show interface br1

Bridge Interface: br1

  Filter Type: All
  Port Filter: All
```

Chapter 3 CPE Config Commands

Chapter contents

cpeconfig action

Note This command is only available on the CO unit. Refer to the *Getting Started Guide* for more information.

Transmit/receive the CPE configuration.

Table 14. cpeconfig action

Command	Explanation
cpeconfig action get	Request CPE to send it's configuration.
cpeconfig action set	Command CPE to configure itself.

cpeconfig set

Note This command is only available on the CO unit. Refer to the *Getting Started Guide* for more information.

Set CPE configurable parameters.

Table 15. cpeconfig set

Command	Explanation
cpeconfig set defaultgw <newvalue>	Set default GW as format: xxx.xxx.xxx.xxx
cpeconfig set dslrateTS <newvalue>	Set DSL data rate as n_64kbps.
cpeconfig set ipaddress <newvalue>	Set IP Address as format: xxx.xxx.xxx.xxx
cpeconfig set netmask <newvalue>	Set Net Mask as format: xxx.xxx.xxx.xxx

cpeconfig show

Note This command is only available on the CO unit. Refer to the *Getting Started Guide* for more information.

Show the CPE's configuration.

Table 16. cpeconfig show

Command	Explanation
cpeconfig show	Show the CPE's configuration.

Example Output: cpeconfig show

```
    --> cpeconfig show

      Configuration State: Initializing

                Timeslots: 36
               IP Address: 192.168.200.10
                  Netmask: 255.255.255.0
          Default Gateway: 0.0.0.0
```

Chapter 4 Ethernet Commands

Chapter contents

ethernet add transport

Create ethernet transport.

Table 17. ethernet add transport

Command	Explanation
ethernet add transport <name> <port>	Create ethernet transport.

ethernet clear transports

Remove all ethernet transports

Table 18. ethernet clear transports

Command	Explanation
ethernet clear transports	Remove all ethernet transports.

ethernet delete transport

Remove single ethernet transport.

Table 19. ethernet delete transport

Command	Explanation
ethernet delete transport <name>	Remove single ethernet transport.

ethernet list

List ethernet ports and transports.

Table 20. ethernet list

Command	Explanation
ethernet list ports	List ports available to transport ethernet data.
ethernet list transports	Show ethernet transports.

Example Output: ethernet list ports

```
--> ethernet list ports

Valid ethernet port names:
    ethernet
```

Example Output: ethernet list transports

```
--> ethernet list transports

Ethernet transports:

 ID  |    Name    |    Port
-----|------------|------------
   1 | eth1       | ethernet
-------------------------------
```

ethernet set transport

Set port of an existing ethernet transport.

Table 21. ethernet set transport

Command	Explanation
ethernet set transport <name> ethernetport <port>	Set the port to be used as a physical Ethernet port.
ethernet set transport <name> port <port>	Set the port that an existing Ethernet port uses to transport ethernet data.

ethernet show transport

Display existing ethernet transport.

Table 22. ethernet set transport

Command	Explanation
ethernet show transport <name>	Display existing ethernet transport.

Example Output: ethernet show transport eth1

```
--> ethernet show transport eth1

Ethernet transport: eth1

Description: eth1
       Port: ethernet
```

Chapter 5 Firewall Commands

Chapter contents

firewall add policy

Add a firewall policy.

Table 23. firewall add policy

Command		Explanation
firewall add policy <name> dmz-internal		Add a firewall policy between the DMZ interface and the internal interface.
	allowonly-val	Allow only traffic to and/or from the IP address set in the firewall add validator command.
	blockonly-val	Block only traffic to and/or from the IP address set in the firewall add validator command.
firewall add policy <name> external-dmz		Add a firewall policy between the external interface and the DMZ interface.
	allowonly-val	Allow only traffic to and/or from the IP address set in the firewall add validator command.
	blockonly-val	Block only traffic to and/or from the IP address set in the firewall add validator command.
firewall add policy <name>external-internal		Add a firewall policy between the external interface and the internal interface.
	allowonly-val	Allow only traffic to and/or from the IP address set in the firewall add validator command.
	blockonly-val	Block only traffic to and/or from the IP address set in the firewall add validator command.

firewall add portfilter

Add a port filter to a firewall policy.

Note Begin each top-level command in the table below with **`firewall add portfilter <name> <policyname>`**.

Table 24. firewall add portfilter <name> <policyname>

Command			Explanation
ftp	**both**		Allow inbound/outbound transport of FTP packets between inside and outside interfaces.
	inbound		Allow transport of FTP packets from an outside interface to an inside interface. Outbound transport is not allowed..
	outbound		Allow transport of FTP packets from an inside interface to an outside interface. Inbound transport is not allowed.
http	**both**		Allow inbound/outbound transport of HTTP packets between inside and outside interfaces.
	inbound		Allow transport of HTTP packets from an outside interface to an inside interface. Outbound transport is not allowed.
	outbound		Allow transport of HTTP packets from an inside interface to an outside interface. Inbound transport is not allowed.
icmp	**both**		Allow inbound/outbound transport of ICMP packets between inside and outside interfaces
	inbound		Allow transport of ICMP packets from an outside interface to an inside interface. Outbound transport is not allowed.
	outbound		Allow transport of ICMP packets from an inside interface to an outside interface. Inbound transport is not allowed.
protocol	**<number>**	**both**	Allow inbound/outbound transport of packets of the specified protocol number between inside and outside interfaces.
		inbound	Allow transport of packets of the specified protocol number from an outside interface to an inside interface. Outbound transport is not allowed.
		outbound	Allow transport of packets of the specified protocol number from an inside interface to an outside interface. Inbound transport is not allowed.

Table 24. firewall add portfilter <name> <policyname>

Command				Explanation
smtp	**both**			Allow inbound/outbound transport of SMTP packets between inside and outside interfaces
	inbound			Allow transport of SMTP packets from an outside interface to an inside interface. Outbound transport is not allowed.
	outbound			Allow transport of SMTP packets from an inside interface to an outside interface. Inbound transport is not allowed.
tcp	**<startport>**	**<endport>**	**both**	Allow inbound/outbound transport of TCP packets between inside and outside interfaces.
			inbound	Allow transport of TCP packets from an outside interface to an inside interface. Outbound transport is not allowed.
			outbound	Allow transport of TCP packets from an inside interface to an outside interface. Inbound transport is not allowed.
telnet	**both**			Allow inbound/outbound transport of Telnet packets between inside and outside interfaces.
	inbound			Allow transport of Telnet packets from an outside interface to an inside interface. Outbound transport is not allowed.
	outbound			Allow transport of Telnet packets from an inside interface to an outside interface. Inbound transport is not allowed.
udp	**<startport>**	**<endport>**	**both**	Allow inbound/outbound transport of UDP packets between inside and outside interfaces.
			inbound	Allow transport of UDP packets from an outside interface to an inside interface. Outbound transport is not allowed.
			outbound	Allow transport of UDP packets from an inside interface to an outside interface. Inbound transport is not allowed.

firewall add validator

Add a validator to a firewall policy.

Note Begin each top-level command in the table below with `firewall add validator <name> <policyname>`.

Table 25. firewall add validator

Command			Explanation
both	**<ipaddress>**	**<hostipmask>**	Filter inbound and outbound traffic based on IP addresses.
inbound	**<ipaddress>**	**<hostipmask>**	Block incoming traffic based on IP addresses.
outbound	**<ipaddress>**	**<hostipmask>**	Block outgoing traffic based on IP addresses.

firewall clear

Delete all firewall policies or portfilters from an existing configuration.

Table 26. firewall clear

Command	Explanation
firewall clear policies	Delete all exisiting policies from the firewall configuration.
firewall clear portfilters <policyname>	Delete all portfilters that were added to an existing firewall policy using the firewall add portfilter command.

firewall delete

Delete a firewall policy or portfilter from an existing configuration

Table 27. firewall delete

Command	Explanation
firewall delete policy <name>	Delete a specific existing policy from the firewall configuration.
firewall delete portfilter <name> <policyname>	Delete a specific existing portfilter from the firewall configuration.
firewall delete validator <name> <policyname>	Delete a specific existing validator from a named policy.

firewall disable

Disable firewall features.

Table 28. firewall disable

Command	Explanation
firewall disable	Disable all firewall features.
firewall disable IDS	Disable IDS features of the firewall.
firewall disable blockinglog	Disable logging of firewall blocking.
firewall disable intrusionlog	Disable logging of firewall intruders.
firewall disable sessionlog	Disable logging of firewall sessions.

firewall enable

Enable firewall features.

Table 29. firewall enable

Command	Explanation
firewall enable	Enable all firewall features.
firewall enable IDS	Enable IDS features of the firewall.
firewall enable blockinglog	Enable logging of firewall blocking.
firewall enable intrusionlog	Enable logging of firewall intruders.
firewall enable sessionlog	Enable logging of firewall sessions.

firewall list

Show information about specific firewall features.

Table 30. firewall list

Command	Explanation
firewall list policies	Show information about policies that were added to the firewall.
firewall list portfilters <policyname>	Show information about portfilters that were added to a firewall policy.
firewall list protocol	List the port numbers assigned to various protocols as given in RFC 1700. These numbers can be used in commands that require a protocol number.
firewall list validators <policyname>	Show information about validators that were added to a policy.

Example Output: firewall list policies

```
--> firewall list policies

Firewall Policies:

  ID |    Name    |   Type 1   |   Type 2   | Validator Allow Only
-------------------------------------------------------------------
   1 | pex_in     | external   | internal   | false
   2 | pex_dmz    | external   | dmz        | false
   3 | pdmz_in    | dmz        | internal   | false
-------------------------------------------------------------------
```

Example Output: firewall list portfilters pex_in

```
--> firewall list portfilters pex_in

Firewall Port Filters:

  ID |    Name    | Type |  Port Range   |  In  | Out  | Raw  | TCP  | UDP
----------------------------------------------------------------------------
   1 | hei_http   | 6    | 80    - 80    |false |true  |false |true  |false
   2 | hei_dns    | 17   | 53    - 53    |false |true  |false |false |true
   3 | hei_tdns   | 6    | 53    - 53    |false |true  |false |true  |false
   4 | hei_ftp    | 6    | 21    - 21    |false |false |false |true  |false
   5 | hei_tnet   | 6    | 23    - 23    |false |false |false |true  |false
   6 | hei_smtp   | 6    | 25    - 25    |false |true  |false |true  |false
   7 | hei_pop3   | 6    | 110   - 110   |false |true  |false |true  |false
   8 | hei_nntp   | 6    | 119   - 119   |false |false |false |true  |false
   9 | hei_rav    | 17   | 7070  - 7070  |false |false |false |false |true
  10 | hei_icmp   | 1    | 0     - 0     |false |true  |true  |false |false
  11 | hei_h323   | 6    | 1720  - 1720  |false |false |false |true  |false
  12 | hei_t120   | 6    | 1503  - 1503  |false |false |false |true  |false
  13 | hei_ssh    | 6    | 22    - 22    |false |false |false |true  |false
----------------------------------------------------------------------------
```

Example Output: firewall list protocol

```
--> firewall list protocol

Assigned Internet Protocol Numbers
see RFC 1700 "Assigned Numbers"
section "Protocol Numbers" pages 7 - 9

 1  ICMP     Internet Control Message
 2  IGMP     Internet Group Management
 3  GGP      Gateway-to-Gateway
 4  IP       IP in IP (encapsulation)
 6  TCP      Transmission Control
 8  EGP      Exterior Gateway Protocol
 9  IGP      any private interior gateway
17  UDP      User Datagram
46  RSVP     Reservation Protocol
47  GRE      General Routing Encapsulation
89  OSPFIGP  OSPFIGP
92  MTP      Multicast Transport Protocol
94  IPIP     IP-within-IP Encapsulation Protocol
```

Example Output: firewall list validators pdmz_in

```
--> firewall list validators pdmz_in

Firewall Host Validators:

  ID |    Name     | Direction |      Host IP     |      Mask
--------------------------------------------------------------------
   1 |  item0      | both      | 192.168.200.1    | 255.255.255.0
--------------------------------------------------------------------
```

firewall set IDS

Configure the firewall Intrusion Detection Service (IDS) feature.

Table 31. firewall set IDS

Command			Explanation
firewall set IDS	**DOSattackblock**	**<duration>**	Set the length of time (in seconds) that the firewall blocks suspicious hosts for once a DOS attack attempt has been detected by the firewall.
	MaxICMP	**<max>**	Set the maximum number (per second) of ICMP packets that are allowed before an ICMP Flood attempt is detected.
	MaxPING	**<max>**	Set the maximum number (per second) of pings that are allowed before an Echo Storm attempt is detected.
	MaxTCPopenhandshake	**<max>**	Set the maximum number of unfinished TCP handshaking sessions per second that are allowed by the firewall before a SYN Flood is detected.
	SCANattackblock	**<duration>**	Set the length of time (in seconds) that the firewall blocks all suspicious hosts for after it has detected scan activity on the firewall.
	blacklist	**clear**	Clear blacklisting of an external host.
		disable	Disable blacklisting of an external host if IDS has detected an intrusion from that host.
		enable	Enable blacklisting of an external host if IDS has detected an intrusion from that host.
	victimprotection	**disable**	Disable the victim protection feature.
		enable	Protect the victim from an attempted spoofing attack.

firewall set securitylevel

Set the desired level of security for the firewall.

Table 32. firewall set securitylevel

Command		Explanation
firewall set securitylevel	**high**	Use a **high** level of firewall security between interfaces.
	low	Use a **low** level of firewall security between interfaces.
	medium	Use a **medium** level of firewall security between interfaces.
	none	Block all IP traffic for every security interface.
	userdefined <slevel>	Select a security configuration that was previously created.

firewall set validator

Configure the settings for a validator.

Note Begin each top-level command in the table below with `firewall set validator <name> <policyname>`.

Table 33. firewall set validator

Command	Explanation
disabled	Disable a validator that has been added to a policy. This allows it to be temporarily disabled without forcing the user to delete and then recreate it. This could be useful in a testing scenario.
enabled	Enable a validator that has been added to a policy.
interface <interface-name>	This validator will use the IP address of an existing IP interface.
ipaddress <ipaddress>	Set the validator IP address.
netmask <hostipmask>	Set the validator netmask.

firewall show

Display information about a firewall setting.

Table 34. firewall show

Command	Explanation
firewall show IDS blacklist	Show the hosts that are currently blacklisted by the intrusion detection system.
firewall show policy <name>	Display information about a specific policy that was added to the firewall.
firewall show portfilter <name> <policyname>	Display information about a specific portfilter that was added to a firewall policy.
firewall show validator <name> <policyname>	Display information about a specific validator that was added to a firewall policy.

Example Output: firewall show IDS

```
--> firewall show IDS

Firewall IDS:

                       IDS Enabled: true
                     Use Blacklist: false
             Use Victim Protection: false
         Dos Attack Block Duration: 1800
        Scan Attack Block Duration: 86400
  Victim Protection Block Duration: 600
    Max TCP Open Handshaking Count: 100
                    Max PING Count: 15
                    Max ICMP Count: 100
```

Example Output: firewall show IDS blacklist

```
--> firewall show IDS blacklist

ALCWGetIDSBlackList succeeded, returned number = 0
```

Example Output: firewall show policy pex_in

```
--> firewall show policy pex_in

Firewall Policy: pex_in

Interface Type 1: external
Interface Type 2: internal

Allow Only Validator: false
```

Example Output: firewall show portfilter hei_http pex_in

```
--> firewall show portfilter hei_http pex_in

Firewall Port Filter: hei_http

         Transport type: 6
      Port number start: 80
        Port number end: 80
     Inbound permission: false
    Outbound permission: true
                 Raw IP: false
         TCP permission: true
         UDP permission: false
```

Example Output: firewall show validator item0 pdmz_in

```
--> firewall show validator item0 pdmz_in

Firewall Host Validator: item0

Direction: both
  Host IP: 192.168.200.1
Host Mask: 255.255.255.0
```

firewall status

Display information about the firewall security level and logging status.

Table 35. firewall status

Command	Explanation
firewall status	Display information about the firewall security level and logging status.

Example Output: firewall status

```
--> firewall status
Firewall enabled.
Firewall security level: high.
Firewall session logging enabled.
Firewall blocking logging enabled.
Firewall intrusion logging disabled.
```

Chapter 6 **G.SHDSL Commands**

Chapter contents

gshdsl set BERMeterMode

Configure patetrn generation

Table 36. gshdsl set BERMeterMode

Command	Explanation
gshdsl set BERMeterMode 511	Configure pattern generation mode.
gshdsl set BERMeterMode 511E	Configure pattern generation mode that inserts errors into the pattern every two seconds.
gshdsl set BERMeterMode off	Disable pattern generation/detection.

gshdsl set Clocking

Configure clock mode.

Table 37. gshdsl set Clocking

Command	Explanation
gshdsl set Clocking central_internal	DSL clock is provided by the unit; Set the unit as CO.
gshdsl set Clocking remote_receive_recover	Recover clock from DSL; Set the unit as CPE.

gshdsl set EthLinkKill

Configure the EthLinkKill feature.

Table 38. gshdsl set EthLinkKill

Command	Explanation
gshdsl set EthLinkKill disable	Disable EthLinkKill feature.
gshdsl set EthLinkKill enable	Disconnect the Ethernet link if the DSL link is down.

gshdsl set LineProbe

Configure the line probe feature.

Table 39. gshdsl set LineProbe

Command	Explanation
gshdsl set LineProbe disable	Disable Line Probe feature.
gshdsl set LineProbe enable	Find highest rate automatically that the line will support and set the DSL rate (up to 2.3 Mbps).

gshdsl set action

Save or shut down DSL configurations.

Table 40. gshdsl set action

Command	Explanation
gshdsl set action deactivate	Shut down the DSL port.
gshdsl set action start	Save DSL configuration changes; Always run after making changes to the DSL configuration.

gshdsl set clockingcombination

Configure clock mode.

Table 41. gshdsl set clockingcombination

Command	Explanation
gshdsl set clockingcombination central_internal	DSL clock is provided by the unit; Set the unit as CO.
gshdsl set clockingcombination remote_receive_recover	Recover clock from DSL; Set the unit as CPE.

gshdsl set dataratel

Set I-bit of data rate.

Table 42. gshdsl set dataratel

Command	Explanation
gshdsl set dataratel <newvalue>	Set I-bit of data rate (0-7).

gshdsl set dslrateTS

Set data rate.

Table 43. gshdsl set dslrateTS

Command	Explanation
gshdsl set dslrateTS <newvalue>	Set data rate (n times 64kbps).

gshdsl set errMonIntervalCnt

Set the number of intervals in error before the DSL link restarts.

Table 44. gshdsl set errMonIntervalCnt

Command	Explanation
gshdsl set errMonIntervalCnt <newvalue>	Set the number of intervals in error before the DSL link restarts.

gshdsl set errMonIntervalThreshold

Set the number of allowable errors per interval.

Table 45. gshdsl set errMonIntervalThreshold

Command	Explanation
gshdsl set errMonIntervalThreshold <newvalue>	Set the number of allowable errors per interval.

gshdsl set errMonIntervalTime

Set the length in seconds of the current interval.

Table 46. gshdsl set errMonIntervalTime

Command	Explanation
gshdsl set errMonIntervalTime <newvalue>	Set the length in seconds of the current interval.

gshdsl set errMonStartupDelay

Set the amount of time to wait, after the link is up, before monitoring the DSL link.

Table 47. gshdsl set errMonStartupDelay

Command	Explanation
gshdsl set errMonStartupDelay <newvalue>	Set the amount of time to wait, after the link is up, before monitoring the DSL link.

gshdsl set errMonTotalIntervals

Set the number of intervals to test before monitoring is disabled.

Table 48. gshdsl set errMonTotalIntervals

Command	Explanation
gshdsl set errMonTotalIntervals <newvalue>	Set the number of intervals to test before monitoring is disabled.

gshdsl set gshannex

Set the annex for the dsl port.

Table 49. gshdsl set gshannex

Command	Explanation
gshdsl set gshannex AnnexA	Set Annex A for countries using T1.
gshdsl set gshannex AnnexB	Set Annex B for countries using E1 or RFC1483.

gshdsl set interface

Set the interface for the dsl port.

Table 50. gshdsl set interface

Command	Explanation
gshdsl set interface atm	Set when using pppoa.
gshdsl set interface hdlc	Set when using pppoh.

gshdsl set terminal

Set the unit as a CO or a CPE.

Table 51. gshdsl set terminal

Command	Explanation
gshdsl set terminal central	Set the unit as a CO.
gshdsl set terminal remote	Set the unit as a CPE.

gshdsl seta

Modify an attribute for G.SHDSL.

Table 52. gshdsl seta

Command	Explanation
gshdsl seta <attrname> <newvalue>	Modify an attribute.

gshdsl show

Display an atttribute for G.SHDSL.

Table 53. gshdsl show

Command	Explanation
gshdsl show	Display all attributes.
gshdsl show <attrname>	Display a specific attribute.

Example Output: gshdsl show

```
    --> gshdsl show

    General Information:
                     Version : 1.00
                    Platform : Unknown
            Zip Wire Version : Software:4.2.0   DSP Silicon:75.4  AFE:0.8
                   Connected : FALSE
                 Modem State : In Progress

    Attributes Setting:
                      Action : Start
        Clocking Combination : remote_receiverecover
                    Terminal : remote
                  DSLRate TS : 36
                   Serial TS : ACCESS FAILED
                 Data Rate I : 0
                 Actual Rate : 2304
                   Interface : atm
                     PCMMode : Ethernet
                    Loopback : Off
                    Clocking : Internal
              TPClk Polarity : Normal
              RPClk Polarity : Normal
                   Ghs Annex : AnnexA
                   Cnt Clear : Normal
                  Line Probe : Disable
                   IBit Mask : 0
                  LPOpt Rate : 0
                 TPSTCConfig : DoNotModify
               Eth Link Kill : false

    Status Information:
                    LBStatus : Off
              Loss Of Signal : Signal Loss
           Loss Of Sync Word : Sync Word Loss
              Line Condition : Poor
                Noise Margin :  0.0
            Line Attenuation : 0
               DSLSync State : Out Of Sync
                Nb Dpll Lock : Not Locked
                   Dpll Lock : Not Locked
                 Rx Fifo Err : Normal
                 Tx Fifo Err : Normal
                Tx Stuff Err : Normal
                 Valid TPClk : Valid TX PCM Clock
```

gshdsl showTestMode

Display test mode information.

Table 54. gshdsl showTestMode

Command	Explanation
gshdsl showTestMode	Display Loopback and BERT counters.

Example Output: gshdsl showTestMode

```
--> gshdsl showTestMode

Test Mode:
                Loopback : Off
           BERMeter Mode : off

BERT Counters:
          BERMeter Error : 0
           BERMeter Time : 0
         BERMeter Status : Idle
         BERErr Overflow : 0
        Local Loop State : IDLE
        F11Pattern State : IDLE
```

gshdsl showc

Display error counters.

Table 55. gshdsl showc

Command	Explanation
gshdsl showc	Display error counters.

Example Output: gshdsl showc

```
--> gshdsl showc

Error Counters (FIFO):
         Cnt RPFifo Full : 0
        Cnt RPFifo Empty : 0
         Cnt RPFifo Slip : 0
         Cnt TPFifo Full : 0
        Cnt TPFifo Empty : 0
         Cnt TPFifo Slip : 0
             Cnt TXStuff : 0
             Cnt PCMDpll : 0

Error Counters (Signal):
                 Cnt CRC : 0
                Cnt SEGD : 0
                Cnt LOSW : 0
                Cnt SEGA : 0
                Cnt LOSD : 0

Error Counters (ATM):
          Cnt ATMTx Cell : 0
          Cnt ATMRx Cell : 0
     Cnt ATMTx Idle Cell : 0
     Cnt ATMRx Idle Cell : 0

Error Monitor Values:
        Err Mon Interval : 1
    Err Mon Interval Cnt : 3
       Err Mon Threshold : 3
 Err Mon Total Intervals : 10
   Err Mon Startup Delay : 5
```

Chapter 7 Help Commands

Chapter contents

help

Display help menu.

Table 56. help

Command	Explanation
help	Display top-level help menu.

Chapter 8 IP Commands

Chapter contents

ip add defaultroute

Configure default IP routes.

Table 57. ip add defaultroute

Command	Explanation
ip add defaultroute gateway <gatewayip>	Enter an IP address of the gateway that the route will use by default.
ip add defaultroute interface <interface>	Enter the name of the existing interface that the route will use.

ip add interface

Add an IP interface.

Table 58. ip add interface

Command	Explanation
ip add interface <name>	Add a named interface and set its IP address (optional).
ip add interface <name> <ipaddress>	
ip add interface <name> <ipaddress> <netmask>	

ip add route

Add an IP route.

Note Begin each top-level command in the table below with **`ip add route <name> <dest_ip> <netmask>`**.

Table 59. ip add route

Command	Explanation
gateway <gateway_ip>	Enter the IP address of the gateway that the route will use.
interface <interface>	Enter the name of the existing interface that the route will use.

ip attach

Add a transport to an IP interface.

Table 60. ip attach

Command	Explanation
ip attach <name> <transport>	Attach an existing transport to an existing IP interface.

ip attachbridge

Attach a bridge to the router.

Table 61. ip attachbridge

Command	Explanation
ip attachbridge <name>	Attach the bridge to the router via an existing IP interface.

ip attachvirtual

Create a virtual interface.

Table 62. ip attachvirtual

Command	Explanation
ip attachvirtual <name> <real_interface>	Create a virtual interface that is associated with a "real" IP interface that has already been atatched to a transport.

ip clear

Clear attributes from an IP interface.

Table 63. ip clear

Command	Explanation
ip clear arpentries	Clear all ARP entries listed in the IP ARP table.
ip clear interfaces	Clear all IP interfaces that were created.
ip clear riproutes	Delete all of the existing dynamic routes that have been obtained from RIP.
ip clear routes	Clear all static routes that were created.

ip delete

Delete an IP interface or route.

Table 64. ip delete

Command	Explanation
ip delete interface <name>	Delete a specific IP interface.
ip delete route <name>	Delete a specific route.

ip detach

Detach a transport from an IP interface.

Table 65. ip detach

Command	Explanation
ip detach <name>	Detach a transport from an IP interface.

ip interface

Configure an IP interface.

Note Begin each top-level command in the table below with **`ip interface <name>`**.

Table 66. ip interface <name>

Command				Explanation
add	**proxyarpentry**	**<ipaddress>**		Configure proxy ARP functionality on an existing IP interface.
	proxyarpentry	**<ipaddress>**	**<netmask>**	Enter the netmask address of the interface.
	proxyarpexclusion	**<ipaddress>**		Configure proxy ARP exclusion functionality on an existing IP interface.
	proxyarpexclusion	**<ipaddress>**	**<netmask>**	Enter the netmask address of the interface.
	secondaryipaddress	**<ipaddress>**		Add a secondary IP address to an existing IP interface.
	secondaryipaddress	**<ipaddress>**	**<netmask>**	Enter the netmask address of the interface.
clear	**proxyarpentries**			Clear all proxy ARP entries and exclusions.
	secondaryipaddresses			Delete all additional IP addresses that have been added to an existing IP interface.
delete	**proxyarpentry**	**<number>**		Delete a specific proxy ARP entry.
	proxyarpexclusion	**<number>**		Delete a specific proxy ARP exclusion entry.
	secondaryipaddress	**<number>**		Delete a specific secondary IP address.
list	**proxyarpentries**			Display information about proxy ARP entries and exclusions.
	secondaryipaddresses			Display a list of secondary IP addresses and netmasks that have been added to an existing IP interface.

Example Output: ip interface ip1 list proxyarpentries

```
--> ip interface ip1 list proxyarpentries

Proxy ARP entries for interface: ip1

 ID  |    IP Address    |    Netmask      | Exclude
-----|-----------------|-----------------|---------
   1 | 192.168.200.1   | 255.255.255.255 | false
   2 | 192.168.200.2   | 255.255.255.255 | true
---------------------------------------------------
```

Example Output: ip interface ip1 list secondaryipaddresses

```
--> ip interface ip1 list secondaryipaddresses

Secondary IP addresses for interface: ip1

 ID  |    IP Address     |    Netmask
-----|------------------|-----------------
   1 | 192.168.200.11   | 255.255.255.0
------------------------------------------
```

ip list

Display information for an IP address.

Table 67. ip list

Command	Explanation
ip list arpentries	Display ARP table information.
ip list connections	Display a list of active TCP/UDP connections in use by applications running on the device.
ip list interfaces	Display information about IP interfaces.
ip list riproutes	Display information about the routes that have been obtained from RIP.
ip list routes	Display information about existing routes.

Example Output: ip list arpentries

```
--> ip list arpentries

IP ARP table entries:

 IP address      | MAC address       | Interface    | Static
-----------------|-------------------|--------------|--------
 192.168.200.1   | 00:a0:c9:b7:fd:23 | ip1          | no
-------------------------------------------------------------
```

Example Output: ip list connections

```
--> ip list connections

Local TCP/UDP connections:

 Proto | Local address          | Remote address         | State
-------|------------------------|------------------------|--------------
 tcp   | *:53                   | *:*                    | LISTEN
 tcp   | *:23                   | *:*                    | LISTEN
 tcp   | *:80                   | *:*                    | LISTEN
 udp   | *:50003                | *:*                    |
 udp   | *:520                  | *:*                    |
 udp   | *:50002                | *:*                    |
 udp   | *:55003                | *:*                    |
 udp   | *:55002                | *:*                    |
 udp   | *:55001                | *:*                    |
 udp   | *:55000                | *:*                    |
 udp   | *:50001                | *:*                    |
 udp   | *:53                   | *:*                    |
 udp   | *:161                  | *:*                    |
 udp   | *:69                   | *:*                    |
 udp   | *:123                  | *:*                    |
------------------------------------------------------------------------
```

Example Output: ip list interfaces

```
--> ip list interfaces

IP Interfaces:

 ID  |    Name      |    IP Address    |   DHCP   |   Transport
-----|--------------|------------------|----------|----------------
   1 | ip1          | 192.168.200.10   | disabled | <BRIDGE>
-------------------------------------------------------------------
```

Example Output: ip list riproutes

```
--> ip list riproutes

IP RIP routes:

 Destination     | Mask            | Gateway         | Cost | Time | Source
-----------------|-----------------|-----------------|------|------|----------
------------------------------------------------------------------------------
```

Example Output: ip list routes

```
--> ip list routes

IP routes:

 ID  |    Name     | Destination      | Netmask          | Gateway / Interface
-----|------------|------------------|------------------|---------------------
   1 | default    | 0.0.0.0          | 0.0.0.0          | 192.168.200.1
   2 | item0      | 10.0.0.0         | 255.255.255.0    | ip1
------------------------------------------------------------------------------
```

ip ping

Ping an IP address.

Table 68. ip ping

Command	Explanation
ip ping <name>	Excute Ping command to specified IP address.

ip set interface

Configure specific settings for an IP interface.

Note Begin each top-level command in the table below with
`ip set interface <name>.`

Table 69. ip set interface <name>

Command			Explanation
dhcp	**disabled**		The interface does not use DHCP client information.
	enabled		The interface obtains its configuration information from the DHCP client.
ipaddress	**<ipaddress>**		Set the IP address for the existing IP interface.
	<ipaddress>	**<netmask>**	Set the netmask address of the interface.
mtu	**<mtu>**		Set the MTU (Maximum Transmission Unit) for an existing IP interface.
netmask	**<netmask>**		Set the netmask for an existing IP interface.
rip	**accept**	**all**	Set the interface to accept RIP version 1 and RIP version 2 messages.
		none	The interface does not accept RIP messages.
		v1	Set the interface to accept only RIP version 1 messages.
		v2	Set the interface to accept only RIP version 2 messages.
	multicast	**disabled**	Disable RIP version 2 messages from being sent via multicast.
		enabled	Allow RIP version 2 messages to be sent via multicast.
	send	**all**	Send RIP version 1 and RIP version 2 messages from the interface.
		none	The interface does not accept RIP messages.
		v1	Send only RIP version 1 messages from the interface.
		v2	Send only RIP version 2 messages from the interface.
tcpmssclamp	**disabled**		The IP stack will not examine or modify TCP traffic routed through the interface.
	enabled		Examine and modify TCP SYN packets that are routed through the interface.

ip set rip

Configure RIP settings for an IP interface.

Table 70. ip set rip

Command			Explanation
ip set rip	**advertisedefault**	**disabled**	Disable advertisement of a default route.
		enabled	Enable RIP to advertise a default route with the cost metric set.
	authentication	**disabled**	Reject RIP v2 packets containing an authentication entry.
		enabled	Accept RIP v2 packets that contain an authentication entry with the correct password.
	defaultroutecost	**<cost>**	Set the number of hops counted as the cost of a default route advertised via RIP.
	hostroutes	**disabled**	Set the hostroutes flag to OFF.
		enabled	Set the hostroutes flag to ON; Accept RIP routes to specific routes.
	password	**<password>**	Set an authentication string that is placed on RIP v2 packets.
	poison	**disabled**	Set the poisoned reverse flag to OFF.
		enabled	Set the poisoned reverse flag to ON; ATMOS TCP/IP performs poisoned reverse.

ip set route

Configure settings for an IP route.

Note Begin each top-level command in the table below with **`ip set route <name>.`**

Table 71. ip set route <name>

Command			Explanation
cost	**<cost>**		Set the number of hops counted as the cost of the route for a route previously created.
destination	**<dest_ip>**	**<netmask>**	Set the destination network address of a route previously created.
gateway	**<gateway_ip>**		Set the gateway address of a route previously created.
interface	**<interface>**		Set the interface used by a route previously created.

ip show

Display information for an IP interface.

Table 72. ip show

Command	Explanation
ip show	Display current RIP configuration and any other information global to the router.
ip show debuginfo	Display debugging information.
ip show interface <name>	Display information about a named interface.
ip show route <name>	Display information about a named route.

Example Output: ip show debuginfo

```
--> ip show debuginfo
Found IP stack.

Interfaces:
-----------
IfIndex:  1   Name: ip1          Addr: 192.168.200.10    Mask: 255.255.255.0
    All addresses:
        192.168.200.10   255.255.255.0
        192.168.200.11   0.0.0.0
    IGMP membership:
    DHCP: disabled         MSS Clamp: disabled
    Rx Filter: none        Tx Filter: none
    IfType: ETHER          MAC: 00:a0:ba:03:71:0e
    Virtual: No     Device: //bridge

IfIndex: 16   Name: loopback     Addr: 127.0.0.1         Mask: 255.0.0.0
    All addresses:
        127.0.0.1        255.0.0.0
    IGMP membership:
    DHCP: disabled         MSS Clamp: disabled
    Rx Filter: none        Tx Filter: none
    IfType: LOOP
    Virtual: No     Device: (null)


Routing table:
--------------
Dst:    0.  0.  0.  0 /  0   Gw: 192.168.200.  1   If:  1  Cost:  1
Dst:   10.  0.  0.  0 / 24   Gw:   0.  0.  0.  0   If:  1  Cost:  1
Dst: 192.168.200.  0 / 24   Gw:   0.  0.  0.  0   If:  1  Cost:  1
Dst: 127.  0.  0.  0 /  8   Gw:   0.  0.  0.  0   If: 16  Cost:  1

IGMP Proxy multicast forwarder:
-------------------------------
    Upstream interface: none
    Group address      Interfaces


Pending socket messages:
```

```
------------------------
Socket message pending queue count: 3


Compile time configuration:
---------------------------
    QOS support: disabled
    Checksum forwarded packets: no
    Validate source addresses: no
    ATIC Layer 2: not present
    IPv6 support: not present
```

Example Output: ip show interface ip1

```
--> ip show interface ip1

IP Interface: ip1

                  Ipaddr : 192.168.200.10
                    Mask : 255.255.255.0
                     MTU : 1500
                    Dhcp : false

           TCP MSS Clamp : false
               Accept V1 : false
                 Send V1 : false
               Accept V2 : false
                 Send V2 : false
          Send Multicast : false
```

Note See “ip interface” on page 88 for other interface addresses.

Example Output: ip show route default

```
--> ip show route default

IP route: default

   Destination: 0.0.0.0
       Netmask: 0.0.0.0
       Gateway: 192.168.200.1
          Cost: 1
     Interface:

   Route valid: true
```

ip traceroute

Start or stop a trace route process.

Table 73. ip traceroute

Command	Explanation
ip traceroute start	Start a trace route process.
ip traceroute start <name>	Input multiple parameters for a trace route as a string, i.e.: "-v 0.0.0.0".
ip traceroute stop	Cancel a route trace already in progress.

Chapter 9 Logger Commands

Chapter contents

logger set

Configure syslog.

Table 74. logger set

Command	Explanation
logger set facility	Set the "facility" attribute.
logger set facility <facility>	Set the new value of "facility".
logger set host	Set the log host.
logger set host <host>	Specify the host IP address.

logger show

Display syslog information.

Table 75. logger show

Command	Explanation
logger show	Show the syslog configuration.

Example Output: logger show

```
    --> logger show

    version                                            = 1.00
    host                                               = 0.0.0.0
    ident                                              =
    facility                                           = 0
```

Chapter 10 Port Commands

Chapter contents

port ethernet

Configure the Ethernet port.

Table 76. port ethernet

Command			Explanation
port ethernet set	**100BaseMode**	**false**	Use 10Mbps Ethernet operation.
		true	Use 100Mbps Ethernet operation.
	AutoNegotiation	**false**	Force operation specified by 100BaseMode and FullDuplexMode.
		true	Allow speed/duplex negotiation.
	FullDuplexMode	**false**	Use half duplex Ethernet operation.
		true	Use full duplex Ethernet operation.
	Reset	**false**	Do not reset the Ethernet chip.
		true	Perform a soft reset on the Ethernet chip.
port ethernet show			Display port attributes.
port ethernet status			Display port status.

port list

List ports and port types.

Table 77. port list

Command	Explanation
port list	List ports by type.
port list all	List all ports.
port list atm	List all ports using atm.
port list ethernet	List all ethernet ports.
port list hdlc	List all ports using hdlc.

Example Output: port list all

```
--> port list all

Valid port names in class 'all':
    ciao
    atm
    ethernet
    hdlc
```

Example Output: port list atm

```
--> port list atm

Valid port names in class 'atm':
    atm
```

Example Output: port list ethernet

```
--> port list ethernet

Valid port names in class 'ethernet':
    ethernet
```

Example Output: port list hdlc

```
--> port list hdlc

Valid port names in class 'hdlc':
    hdlc
```

Chapter 11 **PPP Commands**

Chapter contents

ppp add transport

Add a PPP over HDLC (PPPoH) transport.

Table 78. ppp add transport

Command	Explanation
ppp add transport <name>	Create PPPoH transport.
ppp add transport <name> dialin <iface> <port>	Create PPPoH transport that accepts dialin connections.
ppp add transport <name> dialout <iface> <port>	Create PPPoH transport that performs dialout.

ppp clear transports

Remove all PPPoH transports.

Table 79. ppp clear transports

Command	Explanation
ppp clear transports	Remove all PPPoH transports.

ppp delete transport

Remove a single PPPoH transport.

Table 80. ppp delete transport

Command	Explanation
ppp delete transport <name>	Remove a single PPPoH transport.

ppp list transports

List existing PPPoH transports.

Table 81. ppp list transports

Command	Explanation
ppp list transports	List existing PPPoH transports.

Example Output: ppp list transports

```
--> ppp list transports

PPP transports:

 ID  |    Name     | Port
-----|------------|-----------
   1 | ppp1        | hdlc
------------------------------
```

ppp set transport

Configure properties for a PPPoH transport.

Note Begin each top-level command in the table below with **`ppp set transport <name>`**.

Table 82. ppp set transport

Command			Explanation
dialin			Set an existing PPPoH transport to accept dialin connections.
dialout			Set a PPPoH transport to perform dialout.
disabled			Disable a PPPoH transport.
discoverdns	**primary**	**disabled**	Disable whether the primary DNS server address is requested from a remote PPP peer using IPCP.
		enabled	Request a primary DNS server IP address.
	secondary	**disabled**	Disable whether the secondary DNS server address is requested from a remote PPP peer using IPCP.
		enabled	Request a secondary DNS server IP address.
enabled			Enable a PPPoH transport.
givedns	**client**	**disabled**	IPCP cannot request a DNS server IP address and then give the address to the DNS client.
		enabled	Allow IPCP to request a DNS server IP address and then give the address to the DNS client.
	relay	**disabled**	IPCP cannot request a DNS server IP address and then give the address to DNS relay.
		enabled	Allow IPCP to request a DNS server IP address and then give the address to DNS relay.
headers	**hdlc**	**disabled**	Do not allow packets that have HDLC headers to be transmitted/received.
		enabled	Allow packets that have HDLC headers to be transmitted/received.
	llc	**disabled**	Do not allow packets that have LLC headers to be transmitted/received.
		enabled	Allow packets that have LLC headers to be transmitted/received.
interface	**<iface>**		Set the PPP interface for an existing transport.
lcpechoevery	**<lcpechoevery>**		Tell a specified PPP transport to send an LCP (Link Control Protocol) echo request frame at specified intervals (in seconds).
lcpmaxconf	**<lcpmaxconf>**		Set the LCP maximum configure number for an existing transport.

Table 82. ppp set transport

Command			Explanation
lcpmaxfail	**<lcpmaxfail>**		Set the LCP maximum fail number for an existing transport.
lcpmaxterm	**<lcpmaxterm>**		Set the LCP maximum terminate number for an existing transport.
localip	**<ipaddress>**		Only applies to dialin SVC or PVC transports that provide the server-end of a connection.
mru	**<mru>**		Set the interface's maximum receive unit (MRU) (in bytes).
password	**<password>**		Set a dial-out password on a named transport.
remotedns	**<ipaddress>**	**<ipaddress2>**	Set the primary and secondary local DNS server addresses that will be given to a remote PPP peer when the peer requests a primary or secondary DNS server IP address using IPCP.
remoteip	**<ipaddress>**		Set the remote end of the PPP connection during negotiation.
routemask	**<mask>**		Set the subnet mask used by the route that is created when a PPP link comes up.
specificroute	**disabled**		Create a default route to the subnet at the remote end of the PPP link.
	enabled		Allow the created route to apply to packets for the subnet at the remote end of the PPP link.
subnetmask	**<mask>**		Set the subnet mask used for the local IP interface connected to the PPP transport.
theylogin	**chap**		Set CHAP (Challenge Handshake Authentication Protocol) for the authentication method remote PPP clients must use to dialin to the server.
	none		No authentication method is used.
	pap		Set PAP (Password Authentication Protocol) for the authentication method remote PPP clients must use to dialin to the server.
username	**<username>**		Set a dial-out username on a named transport.
welogin	**auto**		The authentication protocol used by the remote PPP server is discovered and used.
	chap		Set CHAP (Challenge Handshake Authentication Protocol); Server sends an authentication request to the remote user dialing in.
	none		No authentication method is used.
	pap		Set PAP (Password Authentication Protocol); Server sends an authentication request to the remote user dialing in.

ppp show transport

Display properties for a specific PPPoH transport.

Table 83. ppp show transport

Command	Explanation
ppp show transport <name>	Show a single PPPoH transport's properties.

Example Output: ppp show transport ppp1

```
--> ppp show transport ppp1

PPP Transport: ppp1

             Description : ppp1
                 Summary : enabled, down
                  Server : false
                    Hdlc : true
                     LLC : false


          NCPRemote Addr : N/A
                Local Ip : N/A
             Subnet Mask : 0.0.0.0
               Remote Ip : N/A
    Discover Primary DNS : true
              Remote DNS : N/A
  Discover Secondary DNS : true
       Give DNSto Client : true
        Give DNSto Relay : true

            Create Route : true
          Specific Route : false
              Route Mask : 0.0.0.0

        Dialout Username :
        Dialout Password :
            Dialout Auth : none
             Dialin Auth : none

       Lcp Max Configure : 10
         Lcp Max Failure : 10
       Lcp Max Terminate : 10
          Lcp Echo Every : 10
```

Chapter 12 PPPoA Commands

Chapter contents

pppoa add transport

Add a PPP over ATM (PPPoA) transport.

Note Begin each top-level command in the table below with `pppoa add transport <name>`.

Table 84. pppoa add transport

Command	Explanation
dialin pvc <iface> <port> <vpi> <vci>	Create PPPoA transport that accepts dialin connections.
dialout pvc <iface> <port> <vpi> <vci>	Create PPPoA transport that performs dialout.

pppoa clear transports

Remove all PPPoA transports.

Table 85. pppoa clear transports

Command	Explanation
pppoa clear transports	Remove all PPPoA transports.

pppoa delete

Remove a single PPPoA transport.

Table 86. pppoa delete

Command	Explanation
pppoa delete <name>	Remove a single PPPoA transport.

pppoa list transports

List existing PPPoA transports.

Table 87. pppoa list transports

Command	Explanation
pppoa list transports	List existing PPPoA transports.

Example Output: pppoa list transports

```
--> pppoa list transports

PPPoA transports:

 ID  |    Name     | Port       | Vci        | Vpi
-----|------------|-----------|-----------|-----------
   1 | ppp1        | hdlc       | N/A        | N/A
------------------------------------------------------
```

pppoa set transport

Configure properties for a PPPoA transport.

Note Begin each top-level command in the table below with **`pppoa set transport <name>`**.

Table 88. pppoa set transport

Command			Explanation
atmaddress	**<atmaddr>**		Set the ATM address for use in an ATM network.
autoconnect	**disabled**		Disable autoconnect function.
	enabled		Connect automatically to TCP/IP whenever a user requests TCP/IP packets from a public destination.
bt	**<bt>**		Set the burst tolerance for an existing PPPoA transport (PVC transports only).
createroute	**disabled**		No route is added to the system after IPCP negotiation.
	enabled		Add a route to the system after IPCP negotiation
dialin	**pvc**	**<port><vpi><vci>**	Create a PPPoA transport that accepts dialin connections over a PVC (Permanent Virtual Circuit).
dialout	**pvc**	**<port><vpi><vci>**	Create a PPPoA transport that performs dialout over a PVC (Permanent Virtual Circuit).
disabled			Disable PPPoA transport.
discoverdns	**primary**	**disabled**	Disable whether the primary DNS server address is requested from a remote PPP peer using IPCP.
		enabled	Request a primary DNS server IP address.
	secondary	**disabled**	Disable whether the secondary DNS server address is requested from a remote PPP peer using IPCP.
		enabled	Request a secondary DNS server IP address.
enabled			Enables PPPoA transport.
givedns	**client**	**disabled**	IPCP cannot request a DNS server IP address and then give the address to the DNS client.
		enabled	Allow IPCP to request a DNS server IP address and then give the address to the DNS client.
	relay	**disabled**	IPCP cannot request a DNS server IP address and then give the address to DNS relay.
		enabled	Allow IPCP to request a DNS server IP address and then give the address to DNS relay.

Table 88. pppoa set transport

Command			Explanation
headers	**hdlc**	**disabled**	Do not allow packets that have HDLC headers to be transmitted/received.
		enabled	Allow packets that have HDLC headers to be transmitted/received.
	llc	**disabled**	Do not allow packets that have LLC headers to be transmitted/received.
		enabled	Allow packets that have LLC headers to be transmitted/received.
idletimeout	**<idletimeout>**		Set an idle time out for your LAN connection.
interface	**<iface>**		Set the PPP interface for an existing PPPoA transport.
lcpechoevery	**<lcpechoevery>**		Tell a specified PPP transport to send an LCP (Link Control Protocol) echo request frame at specified intervals (in seconds).
lcpmaxconf	**<lcpmaxconf>**		Set the LCP maximum configure number for an existing transport.
lcpmaxfail	**<lcpmaxfail>**		Set the LCP maximum fail number for an existing transport.
lcpmaxterm	**<lcpmaxterm>**		Set the LCP maximum terminate number for an existing transport.
localip	**<ipaddress>**		Only applies to dialin SVC or PVC transports that provide the server-end of a connection.
mbs	**<mbs>**		Set the maximum burst size for PPPoA transport (Applies only to existing PVC transports).
mcr	**<mcr>**		Set the minimum cell rate for an existing PPPoA transport (Applies only to existing PVC transports).
mru	**<mru>**		Set the interface's maximum receive unit (MRU) (in bytes).
password	**<password>**		Set a dial-out password on a named transport.
pcr	**<pcr>**		Set the peak cell rate for an existing PPPoA transport (Applies only to existing PVC transports).
port	**<port>**		Set the port that an existing transport uses to transport PPPoA data (Applies only to existing PVC transports).
pvc	**<port>**	**<vpi><vci>**	Set PVC (Permanent Virtual Circuit) for PPPoA data.

Table 88. pppoa set transport

Command			Explanation
qosclass	**abr**		Set quality of service class as abr (Available Bit Rate) for the transport.
	cbr		Set quality of service class as cbr (Constant Bit Rate) for the transport.
	qfc		Set quality of service class as qfc for the transport.
	ubr		Set quality of service class as ubr (Unspecified Bit Rate) for the transport.
	vbr		Set quality of service class as vbr (Variable Bit Rate) for the transport.
	vbrrt		Set quality of service class as vbrrt (Variable Bit Rate Real-Time) for the transport.
remotedns	**<ipaddress>**	**<ipaddress2>**	Set the primary and secondary local DNS server addresses that will be given to a remote PPP peer when the peer requests a primary or secondary DNS server IP address usig IPCP.
remoteip	**<ipaddress>**		Set the IP address supplied to the remote end of the PPP connection during negotiation.
routemask	**<mask>**		Set the subnet mask used by the route that is created when a PPP link comes up.
scr	**<scr>**		Set scr (Sustainable Cell Rate); Valid only if you set VBR or VBRRT as the qosclass; Applies only to existing PVC transports.
specificroute	**disabled**		Create a default route to the subnet at the remote end of the PPP link.
	enabled		Allow the created route to apply to packets for the subnet at the remote end of the PPP link.
subnetmask	**<mask>**		Set the subnet mask used for the local IP interface connected to the PPP transport.
theylogin	**chap**		Set CHAP (Challenge Handshake Authentication Protocol) for the authentication method remote PPP clients must use to dialin to the server.
	none		No authentication method is used.
	pap		Set PAP (Password Authentication Protocol) for the authentication method remote PPP clients must use to dialin to the server.
username	**<username>**		Set a dial-out username on a named transport.
vci	**<vci>**		Set the Virtual Circuit Identifier (Applies only to existing PVC transports).
vpi	**<vpi>**		Set the Virtual Path Identifier (Applies only to existing PVC transports).

Table 88. pppoa set transport

Command		Explanation
welogin	**auto**	The authentication protocol used by the remote PPP server is discovered and used.
	chap	Set CHAP (Challenge Handshake Authentication Protocol); Server sends an authentication request to the remote user dialing in.
	none	No authentication method is used.
	pap	Set PAP (Password Authentication Protocol); Server sends an authentication request to the remote user dialing in.

pppoa show transport

Display properties for a specific PPPoA transport.

Table 89. pppoa show transport

Command	Explanation
pppoa show transport <name>	Show a single PPPoA transport's properties.

Example Output: pppoa show transport ppp1

```
--> pppoa show transport ppp1

PPP Transport: ppp1

             Description : ppp1
                 Summary : enabled, down
                  Server : false
          NCPRemote Addr : N/A
                    Hdlc : true
                     LLC : false


                Local Ip : N/A
             Subnet Mask : 0.0.0.0
               Remote Ip : N/A
    Discover Primary DNS : true
              Remote DNS : N/A
  Discover Secondary DNS : true
    Remote Secondary DNS : N/A
       Give DNSto Client : true
        Give DNSto Relay : true

            Create Route : true
          Specific Route : false
              Route Mask : 0.0.0.0

        Dialout Username :
        Dialout Password :
            Dialout Auth : none
             Dialin Auth : none

       Lcp Max Configure : 5
         Lcp Max Failure : 10
       Lcp Max Terminate : 10
          Lcp Echo Every : 10
            Auto Connect : false
            Idle Timeout : 0



                    Port : hdlc
                     VPI :
                     VCI :
```

Chapter 13 PPPoE Commands

Chapter contents

pppoe add transport

Add a PPP over Ethernet (PPPoE) transport.

Note Begin each top-level command in the table below with **`pppoe add transport <name> dialout`**.

Table 90. pppoe add transport

Command				Explanation
eth <ifc><port>				Create a PPPoE transport that performs dialout over Ethernet.
	accessconcentrator <concentrator>			Connect only to the named access concentrator or to the first access concentrator that responds.
		servicename <servicename>		Connect to the specified service on the named concentrator.
	servicename <servicename>			Connect to the first access concentrator that uses this service.
pvc <ifc> <port>	**<vpi><vci>**			Create a PPPoE transport that performs dialout over a PVC (Permanent Virtual Circuit).
		accessconcentrator <concentrator>		Connect only to the named access concentrator or to the first access concentrator that responds.
			servicename <servicename>	Connect to the specified service on the named concentrator.
		servicename <servicename>		Connect to the first access concentrator that uses this service.

pppoe clear transports

Remove all PPPoE transports.

Table 91. pppoe clear transports

Command	Explanation
pppoe clear transports	Remove all PPPoE transports.

pppoe delete transport

Remove a single PPPoE transport.

Table 92. pppoe delete

Command	Explanation
pppoe delete transport <name>	Remove a single PPPoE transport.

pppoe list transports

List existing PPPoE transports.

Table 93. pppoe list transports

Command	Explanation
pppoe list transports	List existing PPPoE transports.

Example Output: pppoe list transports

```
--> pppoe list transports

PPPoE transports:

 ID  |    Name    | Port      | Vci       | Vpi
-----|------------|-----------|-----------|-----------
------------------------------------------------------
```

pppoe set transport

Configure properties for a PPPoE transport.

Note Begin each top-level command in the table below with **`pppoe set transport <name>`**.

Table 94. pppoe set transport

Command				Explanation
accessconcentrator	**<concentrator>**			Specify the access concentrator that you want PPPoE to connect to.
atmaddress	**<atmaddr>**			Set the ATM address for use in an ATM network.
autoconnect	**disabled**			Disable autoconnect function.
	enabled			Connect automatically to TCP/IP whenever a user requests TCP/IP packets from a public destination.
	filter	**add**	**tcpport**	Add TCP port filter.
			udpport	Add UDP port filter.
		delete	**tcpport**	Delete TCP port filter.
			udpport	Delete UDP port filter.
bt	**<bt>**			Set the burst tolerance for an existing PPPoE transport (PVC transports only).
createroute	**disabled**			No route is added to the system after IPCP negotiation.
	enabled			Add a route to the system after IPCP negotiation
dialout				Create a PPPoE transport that performs dialout.
disabled				Disable PPPoE transport.
discoverdns	**primary**	**disabled**		Disable whether the primary DNS server address is requested from a remote PPP peer using IPCP.
		enabled		Request a primary DNS server IP address.
	secondary	**disabled**		Disable whether the secondary DNS server address is requested from a remote PPP peer using IPCP.
		enabled		Request a secondary DNS server IP address.
enabled				Enables PPPoE transport.

Table 94. pppoe set transport

Command			Explanation
eth	**<port>**		Set the ethernet port that an existing PPPoE transport uses to transport PPPoE data.
givedns	**client**	**disabled**	IPCP cannot request a DNS server IP address and then give the address to the DNS client.
		enabled	Allow IPCP to request a DNS server IP address and then give the address to the DNS client.
	relay	**disabled**	IPCP cannot request a DNS server IP address and then give the address to DNS relay.
		enabled	Allow IPCP to request a DNS server IP address and then give the address to DNS relay.
headers	**hdlc**	**disabled**	Do not allow packets that have HDLC headers to be transmitted/received.
		enabled	Allow packets that have HDLC headers to be transmitted/received.
	llc	**disabled**	Do not allow packets that have LLC headers to be transmitted/received.
		enabled	Allow packets that have LLC headers to be transmitted/received.
idletimeout	**<idletimeout>**		Set an idle time out for your LAN connection.
interface	**<iface>**		Set the PPP interface for an existing PPPoE transport.
lcpechoevery	**<lcpechoevery>**		Tell a specified PPP transport to send an LCP (Link Control Protocol) echo request frame at specified intervals (in seconds).
lcpmaxconf	**<lcpmaxconf>**		Set the LCP maximum configure number for an existing transport.
lcpmaxfail	**<lcpmaxfail>**		Set the LCP maximum fail number for an existing transport.
lcpmaxterm	**<lcpmaxterm>**		Set the LCP maximum terminate number for an existing transport.
localip	**<ipaddress>**		Only applies to dialin SVC or PVC transports that provide the server-end of a connection.
mbs	**<mbs>**		Set the maximum burst size for PPPoE transport (Applies only to existing PVC transports).

Table 94. pppoe set transport

Command			Explanation
mcr	**<mcr>**		Set the minimum cell rate for an existing PPPoE transport (Applies only to existing PVC transports).
password	**<password>**		Set a dial-out password on a named transport.
pcr	**<pcr>**		Set the peak cell rate for an existing PPPoE transport (Applies only to existing PVC transports).
port	**<port>**		Set the port that an existing transport uses to transport PPPoE data (Applies only to existing PVC transports).
pvc	**<port><vpi><vci>**		Set PVC (Permanent Virtual Circuit) for PPPoE data.
qosclass	**abr**		Set quality of service class as abr (Available Bit Rate) for the transport.
	cbr		Set quality of service class as cbr (Constant Bit Rate) for the transport.
	qfc		Set quality of service class as qfc for the transport.
	ubr		Set quality of service class as ubr (Unspecified Bit Rate) for the transport.
	vbr		Set quality of service class as vbr (Variable Bit Rate) for the transport.
	vbrrt		Set quality of service class as vbrrt (Variable Bit Rate Real-Time) for the transport.
remotedns	**<ipaddress>**	**<ipaddress2>**	Set the primary and secondary local DNS server addresses that will be given to a remote PPP peer when the peer requests a primary or secondary DNS server IP address usig IPCP.
remoteip	**<ipaddress>**		Set the IP address supplied to the remote end of the PPP connection during negotiation.
routemask	**<mask>**		Set the subnet mask used by the route that is created when a PPP link comes up.
scr	**<scr>**		Set scr (Sustainable Cell Rate); Valid only if you set VBR or VBRRT as the qosclass; Applies only to existing PVC transports.

Table 94. pppoe set transport

Command		Explanation
specificroute	**disabled**	Create a default route to the subnet at the remote end of the PPP link.
	enabled	Allow the created route to apply to packets for the subnet at the remote end of the PPP link.
subnetmask	**<mask>**	Set the subnet mask used for the local IP interface connected to the PPP transport.
theylogin	**chap**	Set CHAP (Challenge Handshake Authentication Protocol) for the authentication method remote PPP clients must use to dialin to the server.
	none	No authentication method is used.
	pap	Set PAP (Password Authentication Protocol) for the authentication method remote PPP clients must use to dialin to the server.
username	**<username>**	Set a dial-out username on a named transport.
vci	**<vci>**	Set the Virtual Circuit Identifier (Applies only to existing PVC transports).
vpi	**<vpi>**	Set the Virtual Path Identifier (Applies only to existing PVC transports).
welogin	**auto**	The authentication protocol used by the remote PPP server is discovered and used.
	chap	Set CHAP (Challenge Handshake Authentication Protocol); Server sends an authentication request to the remote user dialing in.
	none	No authentication method is used.
	pap	Set PAP (Password Authentication Protocol); Server sends an authentication request to the remote user dialing in.

pppoe show transport

Display properties for a specific PPPoE transport.

Table 95. pppoe show transport

Command	Explanation
pppoe show transport <name>	Show a single PPPoE transport's properties.

Chapter 14 RFC1483 Commands

Chapter contents

rfc1483 add transport

Create a new transport.

Note Begin each top-level command in the table below with `rfc1483 add transport <name>`.

Table 96. rfc1483 add transport

Command			Explanation
<port> <vpi> <vci>			Create a named RFC1483 transport and specify the virtual path and virtual channel.
	llc		Create a named RFC1483 transport that uses the Logical Link Control (LLC) encapsulation method.
		bridged	Traffic type that is going to be transmitted/received.
		routed	Traffic type that is going to be transmitted/received.
	vcmux		Create a named RFC1483 transport that uses the VC Multiplexing (VCMUX) encapsulation method.
		bridged	Traffic type that is going to be transmitted/received.
		routed	Traffic type that is going to be transmitted/received.

rfc1483 clear transports

Remove all RFC1483 transports.

Table 97. rfc1483 clear transports

Command	Explanation
rfc1483 clear transports	Remove all RFC1483 transports.

rfc1483 delete transport

Remove a single RFC1483 transport.

Table 98. rfc1483 delete

Command	Explanation
rfc1483 delete transport <name>	Remove a specified transport.

rfc1483 list transports

List existing RFC1483 transports.

Table 99. rfc1483 list transports

Command	Explanation
rfc1483 list transports	List existing RFC1483 transports.

Example Output: rfc1483 list transports

```
--> rfc1483 list transports

RFC1483 transports:

 ID  |    Name     | Port       | TxVci      | RxVci      | TxVpi      | RxVpi
-----|------------|-----------|-----------|-----------|-----------|-----------
   1 | rfc1        | atm        | 600        | 600        | 0          | 0
------------------------------------------------------------------------------
```

rfc1483 set transport

Configure properties for an RFC1483 transport.

Note Begin each top-level command in the table below with `rfc1483 set transport <name>`.

Table 100. rfc1483 set transport

Command			Explanation
bt	**<bt>**		Set burst tolerance.
mbs	**<mbs>**		Set max. burst size.
mcr	**<mcr>**		Set minimum cell rate.
mode	**llc**		Set RFC1483 transport mode to use the Logical Link Control (LLC) encapsulation method.
		bridged	Traffic type that is going to be transmitted/received.
		routed	Traffic type that is going to be transmitted/received.
	vcmux		Set RFC1483 transport mode to use the VC Multiplexing (VCMUX) encapsulation method.
		bridged	Traffic type that is going to be transmitted/received.
		routed	Traffic type that is going to be transmitted/received.
pcr	**<pcr>**		Set peak cell rate.
port	**<port>**		Set ATM port.
qosclass	**abr**		Set quality of service class as abr (Available Bit Rate) for the transport.
	cbr		Set quality of service class as cbr (Constant Bit Rate) for the transport.
	qfc		Set quality of service class as qfc for the transport.
	ubr		Set quality of service class as ubr (Unspecified Bit Rate) for the transport.
	vbr		Set quality of service class as vbr (Variable Bit Rate) for the transport.
	vbrrt		Set quality of service class as vbrrt (Variable Bit Rate Real-Time) for the transport.
rxvci	**<vci>**		Set Rx VCI.
rxvpi	**<vpi>**		Set Rx VPI.
scr	**<scr>**		Set sustainable cell rate.
txvci	**<vci>**		Set Tx VCI
txvpi	**<vpi>**		Set Tx VPI
vci	**<vci>**		Set VCI
vpi	**<vpi>**		Set VPI.

rfc1483 show transport

Display properties for a specific RFC1483 transport.

Table 101. rfc1483 show transport

Command	Explanation
rfc1483 show transport <name>	Show a single RFC1483 transport's properties.

Example Output: rfc1483 show transport rfc1

```
--> rfc1483 show transport rfc1

RFC1483 Transport: rfc1

    Description: rfc1
  Encapsulation: LlcBridged

       ATM port: atm
         Tx VPI: 0
         Rx VPI: 0
         Tx VCI: 600
         Rx VCI: 600

      QOS class: UBR
           Peak cell rate: 12000     Burst tolerance: 0
    Sustainable cell rate: 0         Max. burst size: 0
        Minimum cell rate: 0
```

Chapter 15 Security Commands

Chapter contents

security add

Add security interfaces and triggers.

Table 102. security add

Command			Explanation
security add interface <name>	**dmz**		Add DMZ interface.
	external		Add external interface.
	internal		Add internal interface.
security add trigger <name>	**netmeeting**		Add a trigger to allow Netmeeting to transport through the security package.
	tcp	**<startport> <endport> <maxactinterval>**	Add a trigger for a TCP application to the security package.
	udp	**<startport> <endport> <maxactinterval>**	Add a trigger for a UDP application to the security package.

security clear

Clear interfaces and triggers.

Table 103. security clear

Command	Explanation
security clear interfaces	Clear all interfaces.
security clear triggers	Clear all triggers.

security delete

Delete a specified interface or trigger.

Table 104. security delete

Command	Explanation
security delete interface <name>	Delete specified interface.
security delete trigger <name>	Delete specified trigger.

security disable

Disable security features.

Table 105. security disable

Command	Explanation
security disable	Disable security.

security enable

Enable security features.

Table 106. security enable

Command	Explanation
security enable	Enable security.

security list

List interfaces and triggers.

Table 107. security list

Command	Explanation
security list interfaces	List all interfaces.
security list triggers	List all triggers.

Example Output: security list interfaces

```
--> security list interfaces

Security Interfaces:

  ID |    Name    |   Type
----------------------------
   1 | ip1        | internal
----------------------------
```

Example Output: security list triggers

```
--> security list triggers

Security Triggers:

  ID |    Name    |Type |  Port Range   |Interval
-------------------------------------------------
   1 | t2_h323    | tcp | 1720  - 1720  | 30000
   2 | t3_dpudp   | udp | 51200 - 51201 | 3000
   3 | t4_dptcp   | tcp | 51210 - 51210 | 3000
-------------------------------------------------
```

security set trigger

Configure settings for security triggers.

Note Begin each top-level command in the table below with **`security set trigger <name>`**.

Table 108. security set trigger <name>

Command		Explanation
UDPsessionchaining	**disable**	Disable UDP session chaining on an existing trigger.
	enable	Enable UDP session chaining on an existing trigger.
addressreplacement	**both**	Set address replacement on TCP and UDP packets for an existing trigger.
	none	Disable address replacement.
	tcp	Set address replacement on TCP packets for an existing trigger.
	udp	Set address replacement on UDP packets for an existing trigger.
binaryaddressreplacement	**disable**	Disable the use of binary address replacement on an existing trigger.
	enable	Enable the use of binary address replacement on an existing trigger.
endport	**<portnumber>**	Set the end of the port number range for an existing trigger.
maxactinterval	**<interval>**	Set the maximum activity interval limit on existing session entries for an existing trigger.
multihost	**disable**	A secondary session can only be initiated to/from the same remote host.
	enable	A secondary session can be initiated to/from different remote hosts.
sessionchaining	**disable**	Disable all session chaining (TCP and UDP) on an existing trigger.
	enable	Enable TCP session chaining on an existing trigger.
startport	**<portnumber>**	Set the start of the port number range for an existing trigger.

security show

Display information about a specific interface or trigger.

Table 109. security show

Command	Explanation
security show interface <name>	Display information about a specific interface that was added to the Security module.
security show trigger <name>	Display information about a specific trigger that was added to the Security module.

Example Output: security show interface ip1

```
--> security show interface ip1


Interface name: ip1
Interface type: internal
```

Example Output: security show trigger t2_h323

```
--> security show trigger t2_h323

Security Trigger: t2_h323

                   Transport Type: tcp
             Starting port number: 1720
               Ending port number: 1720
             Allow multiple hosts: false
            Max activity interval: 30000
                 Session chaining: true
          Session chaining on UDP: false
       Binary address replacement: true
         Address translation type: tcp
```

security status

Display information about all security features.

Table 110. security status

Command	Explanation
security status	Display information about the security package including security status, firewall status, NAT status, and firewall logging.

Example Output: security status

```
--> security status

Security enabled.
Firewall enabled.
Firewall security level: high.
Firewall session logging enabled.
Firewall blocking logging enabled.
Firewall intrusion logging disabled.
NAT disabled
```

Chapter 16 SNMP Commands

Chapter contents

snmp add

Add community and trap entries.

Table 111. snmp add

Command				Explanation
snmp add community	**<community>**	**<ipaddress>**		Add an entry to the Community Table.
			read <id>	Add an SNMP version 1 or 2 read-only community. The IP address can be used to limit access to a single host or it can be 0.0.0.0 to allow access from any host.
			write <id>	Add an SNMP version 1 or 2 read-write community. The IP address can be used to limit access to a single host or it can be 0.0.0.0 to allow access from any host.
snmp add trap	**<community>**	**<ipaddress>**		Add an entry to the Trap Table.

snmp delete

Delete community and trap entries.

Table 112. snmp delete

Command		Explanation
snmp delete community		Delete an entry from the Community Table.
	<index>	Index of the row to delete.
snmp delete trap		Delete an entry from the Trap Table.
	<index>	Index of the row to delete.

snmp save

Save configuration.

Note System Save is still required.

Table 113. snmp save

Command	Explanation
snmp save	Save configuration.

snmp set

Configure SNMP properties.

Note Begin each top-level command in the table below with **`snmp set`**.

Table 114. snmp set

Command					Explanation
community	**<index>**	**<community>**	**<ipaddress>**		Add an entry to the Community Table.
				read<id>	Add an SNMP version 1 or 2 read-only community. The IP address can be used to limit access to a single host or it can be 0.0.0.0 to allow access from any host.
				write <id>	Add an SNMP version 1 or 2 read-write community. The IP address can be used to limit access to a single host or it can be 0.0.0.0 to allow access from any host.
sysContact	**<contact>**				Set system contact.
sysDescr	**<description>**				Set system description.
sysLocation	**<location>**				Set system location.
sysName	**<name>**				Set system name.
trap	**<index>**	**<community>**	**<ipaddress>**		Set trap.

snmp show

Display information for an SNMP configuration.

Table 115. snmp show

Command	Explanation
snmp show	Show SNMP configuration.

Example Output: snmp show

```
--> snmp show

Static Variables
               Sys Descr : "not set"
           Sys Object ID : 1.3.6.1.4.1.1768.200
            Sys Location : "not set"
             Sys Contact : "not set"
                Sys Name : "not set"
Snmp Enable Authen Traps : 1

Community Table

 Index | Community     | Management IP     | Access    | ID
-------|--------------|-------------------|----------|------
 1     | public        | 0.0.0.0           | read      | 1
-------------------------------------------------------------

Trap Table

 Index | Community     | Management IP
-------|--------------|-------------------
 1     | trap          | 192.168.200.1
-------------------------------------------------------------
```

Chapter 17 Source Commands

Chapter contents

source <filename>

Read a file of commands.

Table 116. source <filename>

Command	Explanation
source <filename>	Read a file of commands.

Chapter 18 System Commands

Chapter contents

system add

Add a user to the system.

Table 117. system add

Command			Explanation
system add login	**<name>**		Add Local user – Authenticate is Disabled.
		<comment>	Add an optional comment about the user that us displayed when you type the commands system list users and system list logins.
system add user	**<name>**		Add Dialin user – Authenticate is Enabled.
		<comment>	Add an optional comment about the user that us displayed when you type the commands system list users and system list logins.

system config

Manage the system configuration.

Table 118. system config

Command			Explanation
system config backup			Save system config as a backup file.
	<filename>		Save the backup configuration on a webserver.
system config clear			Clear all configuration, only leaves superuser login.
system config restore			Revert to saved configuration.
	backup		Restore the backup configuration from the file: //isfs/im.conf.backup.
		<filename>	Specify the name of a file containing an alernative backup configuration.
	factory		Restore the factory default configuration from the //isfs/im.conf.factory file.
	minimal		Clear the current configuration by resetting attributes to their defaults and deleting interfaces and transports.
system config save			Save to main boot configuration file.

system cpu

Manage CPU usage statistics.

Table 119. system cpu

Command			Explanation
system cpu npOverThreshold			Report if the current usage is at or above the NP (network processor) threshold.
system cpu npThreshold	**get**		Report NP (network processor) usage.
	set	**<val>**	Set the percent usage at which the system will declare an alarm condition.
system cpu npUsage			Display information about what percentage of the CPU’s cycles are actually being used.
system cpu ppOverThreshold			Report if the current usage is at or above the PP (protocol processor) threshold.
system cpu ppThreshold	**get**		Report PP (protocol processor) usage.
	set	**<val>**	Set the percent usage at which the system will declare an alarm condition.
system cpu ppUsage			Display information about what percentage of the CPU’s cycles are actually being used.

Example Output: system cpu npOverThreshold

```
--> system cpu npOverThreshold

NP Usage NOT Over Threshold
```

Example Output: system cpu npThreshold get

```
--> system cpu npThreshold get

NP Usage Threshold: 90%
```

Example Output: system cpu npUsage

```
--> system cpu npUsage

NP Usage: 1%
```

Example Output: system cpu ppOverThreshold

```
--> system cpu ppOverThreshold

PP Usage NOT Over Threshold
```

Example Output: system cpu ppThreshold get

```
--> system cpu ppThreshold get

PP Usage Threshold: 90%
```

Example Output: system cpu ppUsage

```
--> system cpu ppUsage

PP Usage: 1%
```

system delete

Remove system users.

Table 120. system delete

Command	Explanation
system delete login <name>	Remove local user.
system delete user <name>	Remove dialin user.

system ifTable reset

Reset packet counters.

Table 121. system ifTable reset

Command	Explanation
system ifTable reset all	Reset the packet counters for all interfaces.
system ifTable reset index <index>	Reset the packet counters for a particular interface.

system info

Display hardware/software information.

Table 122. system info

Command	Explanation
system info	Display hardware/software information.

Example Output: system info

```
--> system info

Global System Configuration:

 Model Code   : 3231 G.SHDSL Access Device
 Software ver: 2.8.18
 Hardware ver: BSP Rev.B  BSP:1.0 / He100/2xx CSP v2.3
 Kernal ver   : 8.2.0.37
 Key ver      : 4
 Build type   : RELEASE

 Product code: 20010307
 MAC address : 00:A0:BA:03:71:0E


 Vendor       :
 URL          :
```

system legal

Show copyright information.

Table 123. system info

Command	Explanation
system legal	Show copyright information.

Example Output: system legal

```
--> system legal

Copyright (c) 2007
```

system list

List system information.

Table 124. system list

Command	Explanation
system list errors	Display system error log.
system list logins	Display system users.
system list openfiles <name>	List open file handles.
system list users	Display system users.

Example Output: system list errors

```
--> system list errors

Errors:
  When    |    What
----------|----------------------------------------------------------------------
Thu, 01 Jan 2004 - 00:00:00| webserver:Invalid argument:failed to set the SNTP host to
Thu, 01 Jan 2004 - 00:27:38| webserver:Failed to add new secondary address

-------------------------------------------------------------------------------
```

Example Output: system list logins

```
--> system list logins

Users:
                      May    Authenticate   Access
 ID  |    Name     |  Conf.   |  Remote   |   Level     |  Comment
-----|------------|----------|----------|------------|-------------
   1 | superuser   | ENABLED  | ENABLED  | superuser   | Default Superuser
   2 | monitor     | ENABLED  | disabled | default     | Default monitor user
-------------------------------------------------------------------
```

Example Output: system list openfiles bun

```
--> system list openfiles bun

qid        devuse   appuse   colour   flags    lasterrno
console    00000059 00000000 00400000 3        0
console    0000002f 00000000 00400000 5        0
console    00000005 00000000 00400000 5        0
```

Example Output: system list users

```
--> system list users

Users:
                      May    Authenticate   Access
 ID  |   Name     |  Conf.   |  Remote  |   Level    |  Comment
-----|------------|----------|----------|------------|-------------
   1 | superuser  | ENABLED  | ENABLED  | superuser  | Default Superuser
   2 | monitor    | ENABLED  | disabled | default    | Default monitor user
-------------------------------------------------------------------
```

system log

Set system logging options.

Table 125. system log

Command	Explanation
system log all	Display all output.
system log disable <module> <category>	Disable module: upload/webserver/ip/rip
system log enable <module> <category>	Enable module: upload/webserver/ip/rip
system log entryexit	Display a message every time a function call is entered or left.
system log info	Show system information.
system log list	List the available debug logs and their enabled/disabled status.
system log nothing	No extra output is displayed.
system log trace	Display detailed trace output.
system log warnings	Display non-fatal errors.

Example Output: system log list

```
--> system log list

upload    info      (disabled)
upload    preserve  (disabled)
upload    get       (disabled)
webserver access    (disabled)
webserver file      (disabled)
webserver trace     (disabled)
ip        socket    (disabled)
ip        config    (disabled)
ip        arp       (disabled)
ip        rawip     (disabled)
ip        icmp      (disabled)
ip        udp       (disabled)
ip        tcp       (disabled)
rip       tx        (disabled)
rip       rx        (disabled)
rip       errors    (disabled)
ip        l2cyan    (disabled)
```

Example Output: system log list op

```
--> system log list ip

ip        socket    (disabled)
ip        config    (disabled)
ip        arp       (disabled)
ip        rawip     (disabled)
ip        icmp      (disabled)
ip        udp       (disabled)
ip        tcp       (disabled)
ip        l2cyan    (disabled)
```

system restart

Restart the system. This function acts the same as pressing the reset button.

Table 126. system restart

Command	Explanation
system restart	Restart the system.

system set

Set user privileges.

Note Begin each top-level command in the table below with **`system set`**.

Table 127. system set

Command				Explanation
baudrate	**<value>**			Set the baud rate.
firmware	**update**	**protection**	**disabled**	Disable checks that are performed on the software image during software upgrades in order to prevent accidentally overwriting the unit's flash with an invalid image.
			enabled	Enable checks that are performed on the software image during software upgrades in order to prevent accidentally overwriting the unit's flash with an invalid image
login	**<name>**	**access**	**default**	Set access permission for the user.
			engineer	
			superuser	
		authenremote	**disabled**	Disable user from dialing into the system.
			enabled	Allow user to dial into the system.
		mayconfigure	**disabled**	Disable user from configuring the system.
			enabled	Allow user to dial into the system.
user	**<name>**	**access**	**default**	Set access permission for the user.
			engineer	
			superuser	
		authenremote	**disabled**	Disable user from dialing into the system.
			enabled	Allow user to dial into the system.
		mayconfigure	**disabled**	Disable user from configuring the system.
			enabled	Allow user to configure the system.
		password	**<password>**	Set password to specified user.

system show

Display system information.

Table 128. system show

Command			Explanation
system show aticmem			Show memory in use by ATIC global pool – ATIC Memory diagnostics.
system show firmware	**update**	**protection**	Show Image Validation.

Example Output: system show aticmem

```
--> system show aticmem

ATIC Memory diagnostics not available
```

Example Output: system show firmware update protection

```
--> system show firmware update protection

Is Image Validation Enabled: enabled
```

Chapter 19 Transport Commands

Chapter contents

transports clear

Clear all transports.

Table 129. transports clear

Command	Explanation
transports clear	Clear all transports.

transports delete

Delete a specific transport.

Table 130. transports delete

Command	Explanation
transports delete <name>	Delete a specified transport.

transports list

List all transports.

Table 131. transports list

Command	Explanation
transports list	List all transports.

Example Output: transports list

```
--> transports list

Services:

 ID  |     Name      | Type
-----|--------------|-------------------------------------------------------------------------
-
   1 | eth1          | Ethernet  | TxPkts:       278/0    RxPkts:        477/0
   2 | ppp1          | PPP       | TxPkts:         0/0    RxPkts:          0/0
   3 | rfc1          | RFC1483   | TxPkts:       292/0    RxPkts:          0/0    VPI/VCI: 0/600
----------------------------------------------------------------------------------------------
-
```

transports show

Display information about a specific transport.

Table 132. transports show

Command	Explanation
transports show <name>	Show a specified transport.

Example Output: transports show eth1

```
--> transports show eth1

Ethernet Status

Service
Creator              : CLI
Description          : eth1

Ethernet
If In Octets         : 68976
If Out Octets        : 125008
If In Errors         : 0
If Out Errors        : 0
Packets Sent         : 278

Good Packets         : 477
Reset Counters       : 0
Enabled              : true

Termination          : Bridge Interface: br1


Ether Channel
Port                 : ethernet
```

Chapter 20 User Commands

Chapter contents

user change

Switch users.

Table 133. user change

Command	Explanation
user change <name>	Switch user.

user logout

Log out from the system.

Table 134. user logout

Command	Explanation
user logout	Log out from system.

user password

Change a user’s password.

Table 135. user password

Command	Explanation
user password	Change a current user's password.

Chapter 21 Webserver Commands

Chapter contents

webserver clear

Clear Web Server statistics.

Table 136. webserver clear

Command	Explanation
webserver clear statistics	Clear Web Server statistics.
webserver clear stats	

webserver disable

Disable the Web Server process.

Table 137. webserver disable

Command	Explanation
webserver disable	Disable the Web Server process.

webserver enable

Enable the Web Server process.

Table 138. webserver enable

Command	Explanation
webserver enable	Enable the Web Server process.

webserver load

Load derived archive for static content.

Table 139. webserver load

Command	Explanation
webserver load <archive-name>	Load derived archive for static content.

webserver set

Configure the Web Server settings.

Table 140. webserver set

Command			Explanation
webserver set	**interface**	**<interface>**	Existing IP interface over which to communicate.
	managementip	**<ipaddress>**	Restrict webserver access to a single IP (0.0.0.0 for any IP).
	port	**<port>**	Set an HTTP port.
	upnpport	**<port>**	Set a Universal Plug and Play port.

webserver show

Display information about the Web Server.

Table 141. webserver show

Command	Explanation
webserver show info	Display information about the Web Server process.
webserver show stats	Display information about how many bytes have been transmitted and received by the Web Server.

Example Output: webserver show info

```
--> webserver show info

Web server configuration:

          EmWeb release: R6_1_0
                Enabled: true
              Interface: eth1
              HTTP port: 80
              UPnP port: 280
  Management IP address: 0.0.0.0
```

Example Output: webserver show stats

```
--> webserver show stats

Web Server statistics:
Bytes transmitted:       201878
Bytes received:          27136
```