Efficient Networks

Router Family

Command Line Interface Guide

Part No. 107-0001-000

Efficient Networks, Inc. – End User Software License and Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY EFFICIENT NETWORKS, INC. ("EFFICIENT") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS OF THE FOLLOWING SOFTWARE LICENSE AND LIMITED WARRENTY. IF YOU DO NOT ACCEPT THESE TERMS, PLEASE RETURN THE HARDWARE AND SOFTWARE AND SOFTWARE IN ITS ORIGINAL PACKAGING TO THE VENDOR FROM WHICH YOU PURCHASED IT FOR A FULL REFUND OF THE PURCHASE PRICE.

The following describes your license to use the software (the"Software") that has been provided with your EFFICIENT DSL customer premise equipment ("Hardware") and the limited warranty that EFFICIENT provides on its Software and Hardware. EFFICIENT reserves any right not expressly granted to the end user.

Software License

The Software is protected by copyright laws and international copyright treaties. The Software is licensed and not sold to you. The definition od Software includes, but not limited to, system and operating software marketed by EFFICIENT, including firmware, embedded software, software provided on media, downloadable software, software for configuration or programmable logic elements, and all EFFICIENT maintenance and diagnostic tools associated with the above mentioned software. Accordingly, while you own the media (such as CD ROM or floppy disk) on which the software is recorded, EFFICIENT or its licensors retains ownership of the Software itself.

1. **Grant of License.** You may install and use one (and only one) copy of the Software in conjunction with the EFFICIENT provided Hardware. You may make backup copies of the system configuration as required. If the Hardware is being installed on a network, you may install the Software on the network server or other server-side devise on which the Hardware is being installed and onto the client-side devices.

2. **Restrictions.** The license granted is a limited license. You may NOT:
- sublicense, assign, or distribute copies of the Software to others;
- decompile, reverse engineer, disassemble or otherwise reduce the Software or any part thereof to a human perceivable form;
- modify, adapt, translate or create derivative works based upon the Software or any part thereof; or
- rent, lease, loan or otherwise operate for profit the Software.

3. **Transfer.** You may transfer the Software only where you are also transferring the Hardware. In such cases, you must remove all copies of the Software from any devices onto which you have installed it, and must ensure that the party to whom you transfer the Hardware receives this License Agreement and Limited Warranty.

4. **Upgrades Covered.** This License covers the Software originally provided to you with the Hardware, and any additional software that you may receive from EFFICIENT, whether delivered via tangible media (CD ROM or floppy disk), down loaded from EFFICIENT, or delivered through customer support. Any such additional software shall be considered "Software" for all purposes under this License.

5. **Export Law Assurances.** You acknowledge that the Software may be subject to export control laws and regulations of the U.S.A. You confirm that you will not export or re-export the Software to any countries that are subject to export restrictions.

6. **No Other Rights Granted.** Other than the limited license expressly granted herein, no license, whether express or implied, by estoppel or otherwise, is granted to any copyright, patent, trademark, trade secret, or other proprietary rights of EFFICIENT or its licensors.

7. **Termination.** Without limiting EFFICIENT's other rights, EFFICIENT may terminate this license if you fail to comply with any of these provisions. Upon termination, you must return the Software and all copies thereof.

Limited Warranty

The following limited warranties provided by EFFICIENT extend to the original end user of the Hardware/licensee of the Software and are not assignable or transferable to any subsequent purchaser/licensee.

1. **Hardware.** EFFICIENT warrants that the Hardware will be free from defects in materials and workmanship and will perform substantially in compliance with the user documentation relating to the Hardware for a period of one year from the date the original end user received the Hardware.

2. **Software.** EFFICIENT warrants that the Software will perform substantially in compliance with the end user documentation provided with the Hardware and Software for a period of ninety days from the date the original end user received the Hardware and Software. The end user is responsible for the selection of Hardware and Software used in the end user's network. Given the wide range of third-party hardware and applications, EFFICIENT does not warrant the compatibility or uninterrupted or error free operation of our Software with the end user's systems or network.

3. **Exclusive Remedy.** Your exclusive remedy and EFFICIENT's exclusive obligation for breach of this limited warranty is, in EFFICIENT's sole option, either (a) a refund of the purchase price paid for the Hardware/Software or (b) repair or replacement of the Hardware/Software with new or remanufactured products. Any replacement Hardware or Software will be warranted for the remainder of the original warranty period or thirty days, which ever is longer.

4. **Warranty Procedures.** If a problem develops during the limited warranty period, the end user shall follow the procedure outlined below:

A. Prior to returning a product under this warranty, the end user must first call EFFICIENT at (888) 286-9375, or send an email to EFFICIENT at support@efficient.com to obtain a return materials authorization (RMA) number. RMAs are issued between 8:00 a.m. and 5:00 p.m. Central Time, excluding weekends and holidays. The end user must provide the serial number(s) of the products in order to obtain an RMA.

B. After receiving an RMA, the end user shall ship the product or defective component, including power supplies and cable, where applicable, freight or postage prepaid and insured, to EFFICIENT at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from EFFICIENT, the end user shall provide EFFICIENT with any missing items or, at EFFICIENT's sole option, EFFICIENT will either (a) replace missing items and charge the end user or (b) return the product to the end user freight collect. The end user shall include a return address, daytime phone number and/or fax. The RMA number must be clearly marked on the outside of the package.

C. Returned Products will be tested upon receipt by EFFICIENT. Products that pass all functional tests will be returned to the end user.

D. EFFICIENT will return the repaired or replacement Product to the end user at the address provided by the end user at EFFICIENT Network's expense. For Products shipped within the United States of America, EFFICIENT will use reasonable efforts to ensure delivery within five (5) business days from the date received by EFFICIENT. Expedited service is available at additional cost to the end user.

E. Upon request from EFFICIENT, the end user must prove the date of the original purchase of the product by a dated bill of sale or dated itemized receipt.

5. **Limitations.**

- The end user shall have no coverage or benefits under this limited warranty if the product has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other acts which are not the fault of EFFICIENT, including acts of nature and damage caused by shipping.
- EFFICIENT will not honor, and will not consider the warranty voided, if: (1) the seal or serial number on the Product have been tampered with or (2) there has been any attempted or actual repair or modification of the Product by anyone other than an EFFICIENT authorized service provider.
- The limited warranty does not cover defects in appearance, cosmetic, decorative or structural items, including framing, and any non-operative parts.
- EFFICIENT's limit of liability under the limited warranty shall be the actual cash value of the product at the time the end user returns the product for repair, determined by the price paid by the end user for the product less a reasonable amount for usage. EFFICIENT shall not be liable for any other losses or damages.
- The end user will be billed for any parts or labor charges not covered by this limited warranty. The end user will be responsible for any expenses related to reinstallation of the product.
- THIS LIMITED WARRENTY IS THE ONLY WARRENTY EFFICIENT MAKES FOR THE PRODUCT AND SOFTWARE. TO THE EXTENT ALLOWED BY LAW, NO OTHER WARRENTY APPLIES, WETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRENTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. **Out of Warranty Repair.** Out of warranty repair is available for a fixed fee. Please contact EFFICIENT at the numbers provided above to determine out of warranty repair rate. End users seeking out of warranty repair should contact EFFICIENT as described above to obtain an RMA and to arrange for payment of the repair charge. All shipping charges will be billed to the end-user.

General Provisions

The following general provisions apply to the foregoing Software License and Limited Warranty.

1. **No Modification.** The foregoing Limited Warranty is the end user's sole and exclusive remedy and is in lieu of all other warranties, express or implied. No oral or written information or advice given by EFFICIENT or tis dealers, distributors, employees or agents shall in any way extend, modify or add to the foregoing Software License and Limited Warranty. This Software License and Limited Warranty constitutes the entire agreement between EFFICIENT and the end user, and supersedes all prior and contemporaneous representation, agreements or understandings, oral or written. This Software License and Limited Warranty may not be changed or amended except by a written instrument executed by a duly authorized officer of EFFICIENT.

EFFICIENT neither assumes nor authorizes any authorized service center or any other person or entity to assume for it any other obligation or liability beyond that which is expressly provided for in this Limited Warranty including the provider or seller of any extended warranty or service agreement.

The Limited Warranty period for EFFICIENT supplied attachments and accessories is specifically defined within their own warranty cards and packaging.

2. **EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND OTHER DAMAGES.** TO THE FULL EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EFFICIENT OR ITS LICENSORS BE LIABLE, WHETHER UNDER CONTRACT, WARRENTY, TORT OR ANY OTHER THEORY OF LAW FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRPUTION, PERSONAL INJURY, LOSS OR IMPAIRMENT OF DATA OR BUSINESS INFORMATION, EVEN IF EFFICIENT HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. EFFICIENTS'S OR IT'S LICENSOR'S LIABILITY TO YOU (IF ANY) FOR ACTUAL DIRECT DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO, AND SHALL NOT EXCEED, THE AMOUNT PAID FOR THE HARDWARE/SOFTWARE.

3. **General.** This Software License and Limited Warranty will be covered by and construed in accordance with the laws of the State of Texas, United States (excluding conflicts of laws rules), and shall insure to the benefit of EFFICIENT and its successor, assignees and legal representatives. If any provision of this Software License and Limited Warranty is held by a court of competent jurisdiction to be a invalid or unenforceable to any extent under applicable law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this Software License and Limited Warranty will remain in full force and effect. Any notices or other communications to be sent to EFFICIENT must be mailed by certified mail to the following address:

Efficient Networks, Inc.
4849 Alpha Road
Dallas, TX 75244
U.S.A.
Attn: Customer Service

Revision History

Revision	Effective Date	Description Of Change
- 001	12 Feb 2002	Initial Release. Information provided to support software kernel release 6.0.0.

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

This page intentionally left blank.

CHAPTER 1

INTRODUCTION

This manual contains information on the syntax and use of the Command Line Interface for the Efficient Networks family of business-class DSL routers. This manual is intended for small and home office users, remote office users, and other networking professionals who are installing and maintaining bridged and routed networks.

It assumes that you have read the User Reference Guide that came with the router and have installed the router as described in that guide. If the configuration is to include advanced functionality, a Technical Reference Guide has also been supplied that provides essential information on the application, configuration, and management of these features.

Configuration of network connections, bridging, routing, and security features are essentially the same for all DSL routers, unless otherwise noted.

As described in the User Reference Guide, a graphical interface is also available for configuring the router. It provides many, but not all, of the capabilities of the Command Line Interface. Look for the User Reference Guide in the box in which your router was shipped or find it on the Technical Support web site (www.efficient.com).

How This Manual is Organized

This manual is organized in two parts:

- How to Access the Command Line. Describes how to access the router command line from a PC so you can enter router commands.
- Command Reference. Provides a description and syntax for each command.

Command Conventions

The Command Line Interface (CLI), unless noted otherwise, follows these conventions:

- Command line length may be up to 120 characters long unless otherwise noted. Input characteristics are footnoted throughout the manual.
- The Command Line Interface is not case-sensitive except for passwords and router names, and key strings.
- All parameters are positional; i.e., each keyword/parameter must be entered in the correct order, as shown in the command format in this manual.

The command formats shown in this manual follow these conventions:

- For each command, the input format is provided. Many command use additional parameters that allow
- Parameters enclosed in **<** and **>** are placeholders representing specific information that you supply or a list of defined parameters of which one must be entered.
- Parameters (may include more than one) enclosed in the characters **[** and **]** are optional.

Accessing the Command Line

To use the Command Line Interface, you must first access the router command line. To do this, perform the following steps:

Step 1 Connect a PC (or ASCII) terminal to a port of the router.
(The required cable and adapter are provided with the router. The connection procedure is described in detail in the User Reference Guide that came with the router.)

Step 2 Restart the PC and power on the router.

Step 3 Open a terminal window or start a terminal session on the PC.

Step 4 The router displays the login prompt. Login with the username **superuser**.

```
Username:
```

Step 5 The router displays the password prompt, enter the login password (default password is *admin*.

```
Password:
```

☞ **NOTE:**

The password will be displayed as *****

Step 6 A confirmation is returned; the command line interface is now available.

```
Logged in successfully!
```

Step 7 If the default login password (*admin*) was used a message will be displayed.

```
**************************************************************

WARNING: You must change your password from the default value!

**************************************************************
```

Step 8 Enter a new password at the prompt.

```
Enter New Password:
```

Step 9 Re-enter the new password at the prompt.

```
Enter New Password Again:
```

The password change will be confirmed:

```
Password changed.
```

The command line is now available for use.

Task Complete

Terminal Sessions

The router supports both local access and remote access. In step 3 above, the terminal session could be:

- Terminal Session under Windows (HyperTerminal) or Terminal Session for Macintosh or UNIX (for local access)
- Telnet Session for Remote Access

Terminal Session under Windows (HyperTerminal)

To open the HyperTerminal emulator available under the Windows operating system:

Step 1 Click **Start** on the Windows taskbar, then select:

> Programs

> Accessories

> Communications

> Hyperterminal

> Hyper Terminal

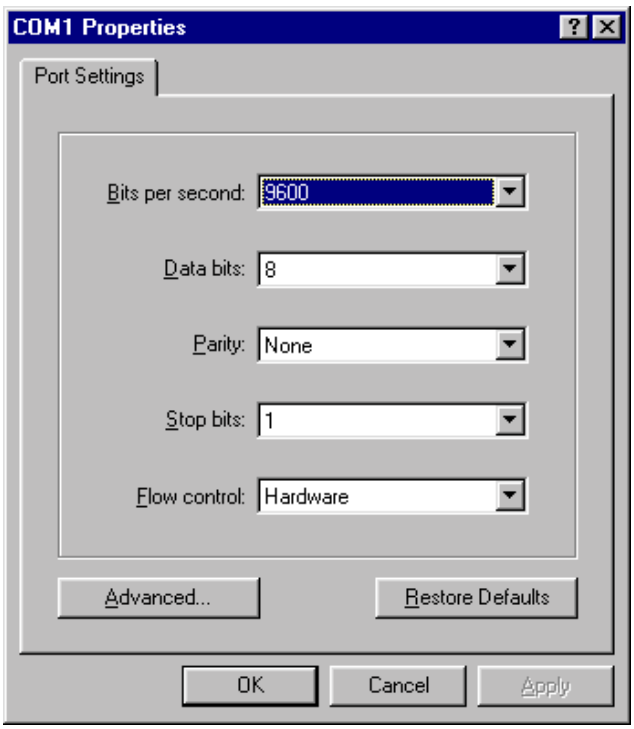
The HyperTerminal window will appear in the background and you will be prompted for configuration information.

Step 2 In the **Connection Description** window, enter a name for the connection and select **OK**.

Step 3 In the **Phone Number** window, under **Connect using**, select **Com 1** (or **2**).

Step 4 In the **Com 1** (or **2**) **Properties** page, enter the following port settings and select **OK**:

Bits per second: 9600[a]
Data bits: 8
Parity: None
Stop bits: 1
Flow control: Hardware



[a] To use a baud rate other than 9600, "Option 7: Set Console Baud Rate" on page 4-39 in the Technical Reference Guide.

Task Complete

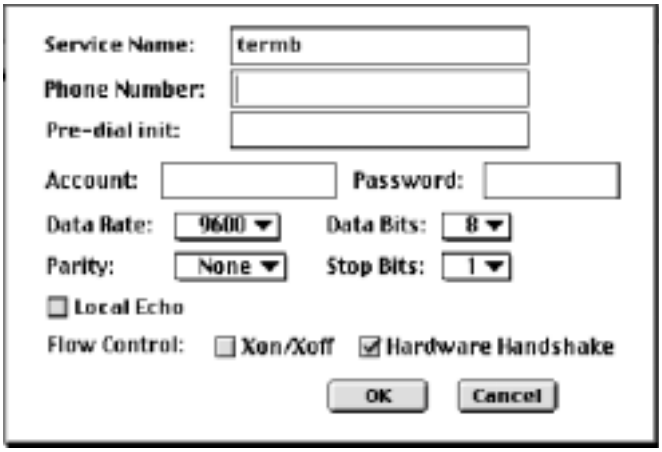
Terminal Session for Macintosh or UNIX

To open a terminal window emulation in a Macintosh or UNIX environment, a VT100 terminal emulation program is required.

Step 1 Start your VT100 terminal emulator.

Step 2 Configure the emulator with the following settings:

Bits per second: 9600[a]
Data bits: 8
Parity: None
Stop bits: 1
Flow control: Hardware



[a] To use a baud rate other than 9600, "Option 7: Set Console Baud Rate" on page 4-39 in the Technical Reference Guide.

Task Complete

Telnet Session for Remote Access

From the local area network you can use TELNET to login in using the Ethernet IP address. (For more information, see Telnet Remote Access.)

☞ **NOTE:**

Remote access to the router configuration can be disabled or restricted. For further information, see “Controlling Remote Management” on page 5-15.

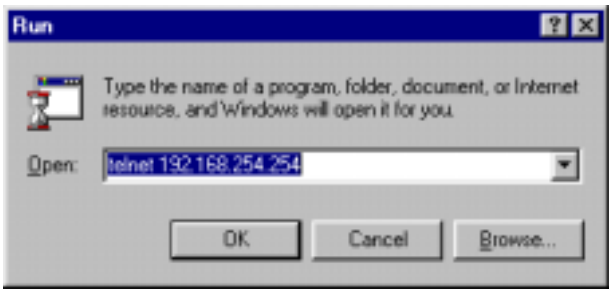
Step 1 Make sure that your PC and router addresses are in the same subnetwork. For example, the router address could be 192.168.254.254 and the PC address could be 192.168.254.253.

Step 2 Start a TELNET session.

a. If you are using a PC running Windows“ 95/98/NT“, select **Start > Run**. If on a UNIX system, bring up a shell window.

b. In the **Run** dialog box (or shell) window, enter:

```
telnet 192.168.254.254
```



c. Click **OK**, or press <Enter>.

Step 3 A TELNET window will be launched; a line identifying the router will be displayed, followed by the **Login:** prompt as shown below.

```
Efficient 5950 G.SHDSL [ATM] Router (5950-001)Ready
Username:
```

Task Complete

Command Line via the Web Management Interface

The Web Management interface provides a web gateway to the command line interface allowing command line syntax the be entered through a browser-based connection. For more information on connecting to the system via the Web Management Interface, refer to the User Reference Guide.

CHAPTER 2

STATUS COMMANDS

The commands in this section are online action and status commands. They facilitate the following functions:

- log into and log out of configuration update mode
- display the router's configuration, the version and level numbers
- list running tasks, memory, and communication interfaces
- dial a remote router to test the ISDN line
- connect to a remote router to test the line
- list IP routes, IPX routes and SAPs, and root bridge
- save the new configuration image
- reboot the system

The status commands found in this section include:

Table 2-1: Status Command Listing

Command	Function
? or help	Lists the top-level commands and keywords and a brief description of their function.
arp delete	Deletes the IP address of the entry in the Address Resolution Protocol (ARP) table.
arp list	Lists ARP table entries.
bi	Lists the root bridge, and indicates whether the mode is learning, listening, or forwarding.
bi list	Lists the contents of the bridge table.
call	Dials a remote router.
date	Displays or changes the current date on the router's clock.

Table 2-1: Status Command Listing (Cont.)

Command	Function
erase	Erases the entire router's configuration or parts of it from FLASH memory.
exit	Has the same function as logout, but will disconnect the Telnet session.
ifs	Lists the communication interfaces installed in the router and the status of the interfaces.
ipifs	Lists the system IP interface(s).
iproutes	Lists the current entries in the IP routing table.
ipxroutes	Lists the current entries in the IPX routing table.
ipxsaps	Lists the current services in the IPX SAPs table.
logout	Logs user out (to Login prompt ->) to reinstate administrative security.
mem	Reports the amount of RAM memory installed in the router and its current allocation.
mlp summary	Lists the status of the protocols negotiated for an active remote connection.
password	Changes the current user password.
ping	Transmits an echo message.
ps	Lists all of the tasks (processes) running in the system and the status of the tasks.
reboot	Initiates a reboot of the system.
save	Saves the entire router's configuration or parts of it to FLASH memory.
sntp active	Displays the active SNTP server.
sntp disable	Displays the active SNTP server.
sntp enable	Enables SNTP requests.
sntp offset	Specifies the SNTP offset from the Universal Time Coordinate (UTC).
sntp prefserver	Displays or changes the preferred SNTP server.
sntp request	Requests the time from an SNTP server.

Table 2-1: Status Command Listing (Cont.)

Command	Function
sntp server	Displays or changes the SNTP server list.
tcp stats	Displays the TCP statistics and open connections.
time	Displays or changes the current time on the router's clock.
traceroute	Traces the route taken by packets sent from the local router to the specified IP address or domain name.
vers	Displays the software version level, source, software options, and amount of elapsed time that the router has been running.

? or help

Lists the top-level commands and keywords and a brief description of their function.

Input Format

? or `help`

Parameters

None

Response

A listing of the top-level commands and keywords with a description of their function.

arp delete

Deletes the IP address of the entry in the ARP table. For additional information, see "ARP" on page 6-6.

Mgmt Class

Network (R/W)

Input Format

```
arp delete <ipaddr> | all
```

Parameters

`<ipaddr>`[a]	IP address of IP entry to delete from ARP table.
`all`	Deletes all existing are table entries.

[a] Dotted-decimal notation.

Example

```
arp delete 128.1.2.0
```

Response

Command prompt.

arp list

Lists Address Resolution Protocol (ARP) table entries in an IP routing environment. ARP is a tool used to find the appropriate MAC addresses of devices based on the destination IP addresses. For additional information, see "ARP" on page 6-6.

Mgmt Class

Network (R)

Input Format

```
arp list <ipaddr> <interfacename> <interfaceunit>
```

Parameters

`<ipaddr>`[a]	IP address associated with a MAC address for a device on the local interface
`<interfacename>`[b]	MAC address on the local network.
`<interfaceunit>`[c]	For an Ethernet interface, this can be a 1 or 0. For a DSL interface, this is a VPN number.

[a] Dotted-decimal notation.
[b] HEX notation
[c] Integer

Example

```
arp list
```

Response

```
-> arp list

IP Addr            Mac Address           Interface
192.84.210.148     00:05:02:00:80:A8     ETHERNET/0
```

bi

Lists the root bridge, and indicates whether the mode is learning, listening, or forwarding. For additional information, see ”Bridging” on page 2-2.

Mgmt Class

Voice (R)

Input Format

```
bi
```

Parameters

None

Response

```
-> bi
GROUP 0Our ID=8000+00206f0249fc Root ID=8000+00206f0249fc
Port ETHERNET/0           00+00 FORWARDING
```

bi list

Lists the contents of the bridge table. Each MAC address in the table is listed with its corresponding bridge port as learned by the bridge function. The line also shows the number of seconds elapsed since the last packet was received by the MAC address followed by flags. Possible flags include:

P	Permanent (This entry is not aged out of the table.)
FLD	Flood
US	This entry is for the target router.
A	Accept
FWD	Forward
BC	Broadcast
MC	Multicast

Mgmt Class

Voice (R)

Input Format

```
bi list
```

Parameters

None

Response

```
-> bi list
BRIDGE GROUP 0:
00206F024C34:                          P       US    SD   A
0180C2000000:                          P                  A      MC
FFFFFFFFFFFF:                          P FLD              A      BC MC
02206F02E70D:  ETHERNET/0      325                        FWD
00C04F2E1AEB:  ETHERNET/0      143                        FWD
0060081BD761:  ETHERNET/0       95                        FWD
```

call

Dials a remote router. This command can be used to test the ISDN link or L2TP secession and the configuration settings for the remote router.

Mgmt Class

Voice (R/W)

Input Format

```
call <remotename>
```

Parameters

`<remotename>`[a] Name of the target router.

[a] ASCII string.

Response

Normal response:

```
Request Queued
```

If an unknown target `<remotename>` is entered, the following is displayed:

```
unknown remotename <hq>
```

date

Displays or changes the current date on the router's clock. To change the current time, use the time command.

Automatic SNTP requests are generated if the system needs to get the time. You can specify an SNTP server using the command sntp server () and a UTC offset with the sntp offset command.

To see the current date and time on the router clock, enter date with no parameters:

Mgmt Class

All (R/W)

Input Format

```
date <mm/dd/yy>
```

Parameters

<mm>[a]	Month
<dd>[b]	Day
<yy>[c]	Year

[a] Integer 1-12
[b] Integer 1-31
[c] Integer, indicating a year from 1968 through 2034. Thus, 1/1/4 is January 1, 2004, 1/1/33 is January 1, 2033, and 1/1/78 is January 1, 1978.

Response

Display when date is entered with no parameters.

```
-> date
BootTime:       7/1/2001 at 15:42:42
Current time:   7/1/2001 at 15:49:16
```

Display when date is entered with parameters.

```
-> date 7/1/1
Time set to UTC-420, 7/1/2001 at 15:59:29
Time adjusted for (-) 0 days 0 hours 10 minutes 13 seconds
```

erase

Erases the entire router's configuration or parts of it from FLASH memory.

CAUTION:
You will need to completely reconfigure any part of the configuration that you erase.

NOTE:
An erase command does not take effect until after a reboot without a save command.

Mgmt Class

Admin (R/W)

Input Format

```
erase all | keys | dod | sys | eth | filter | ipsec | ike | atom
| sdsl | idsl | frame | dhcp | atm25 | l2tp | sntp
```

Parameters

`***`	When entered with no parameters, same as erase all.
`all`	Erases the entire router configuration from FLASH memory, including settings for the system, Ethernet LAN, DSL line, DHCP, and remote router database.
`atom`	Erases the ATM configuration settings.
`dhcp`	Erases the DHCP configuration settings from FLASH memory. To clear all DHCP information without erasing FLASH memory, use the command dhcp clear all records (xxx).
`dod`	Erases the current state of the remote router database.
`eth`	Erases the configuration settings for the Ethernet LAN from FLASH memory.
`filter`	Erases the current bridging filtering database from FLASH memory.When you issue this command you must reboot (without a save).
`keys`	Erases the software option keys from FLASH memory.
`sys`	Erases the name, message, and authentication password system settings from FLASH memory.

Example

```
# erase dod
```

Response

Command prompt.

☞ **NOTE:**

There is a time lag between the response issued by the erase command and the time that the data is actually deleted from FLASH memory. To commit the changes to FLASH memory, issue a sync command after an erase command before powering off the router.

exit

Has the same function as logout, but will disconnect an active Telnet session.

Mgmt Class

All (R)

Input Format

```
exit
```

Parameters

None

Response

Command prompt.

ifs

Lists the communication interfaces installed in the router and the status of the interfaces.

Mgmt Class

Voice (R), Network (R)

Input Format

```
ifs
```

Parameters

None

Response

A typical response is shown below.

```
Interface     Speed    In %     Out %    Protocol     State    Connection
ETHERNET/0    10.0mb   0%/0%    0%/0%    (Ethernet)   OPENED
SHDSL/0       384kb    50%/50%  50%/50%  (ATM)        OFF
ATM-VOICE/1   384kb    45/45%   0%/0%    (ATM)        OFF
BACKUP/0      57kb     0%/0%    0%/0%    (AHDLC/PPP)  OPENED   to backup
CONSOLE/0     9600 b   0/0%     0%/0%    (ATM)        OFF
VOX-STRM/0    0 b                        (CLEAR)      OFF
```

An example of additional interfaces that may be displayed.

```
FR/3          144kb    0%/0%    0%/0%    (HDLC/FR)    OPENED
FR-VC/1       144kb    0%/12%   0%/2%    (FR)         OPENED   to internet
DMT/0         0 b                        (ATM)        OFF
ATM-VC/1      0 b                        (ATM)        OFF
```

ipifs

Lists the system IP interface(s).

Mgmt Class

Network (R)

Input Format

```
ipifs
```

Parameters

None

Response

```
-> ipifs
ATM_VC/1          192.168.254.1 (FFFFFF00) dest 192.168.254.2 sub
                  192.168.254.0 net 192.168.254.0 (FFFFFF00) P-2-P
ETHERNET/0        192.84.210.12 (FFFFFF00) dest 0.0.0.0 sub
                  192.84.210.0 net 192.84.210.0 (FFFFFF00) BROAD-
                  CAST mtu 1500
```

iproutes

Lists the current entries in the IP routing table.

Mgmt Class

Network (R)

Input Format

```
iproutes
```

Parameters

None

Response

```
-> iproutes
IP route         /  Mask     -->   Gateway   Interface    Hops Flags

0.0.0.0          /ffffffff   -->   0.0.0.0   [none]       0 NW PRIV
192.84.210.0     /ffffff00   -->   0.0.0.0   ETHERNET/0   1 NW FW DIR PERM
192.84.210.12    /ffffffff   -->   0.0.0.0   ETHERNET/0   0 ME
192.168.254.0    /ffffff00   -->   0.0.0.0   [none]       0 NW PRIV
192.168.254.1    /ffffffff   -->   HQ        ATM_VC/1     0 ME
192.168.254.2    /ffffffff   -->   HQ        ATM_VC/1     1 FW DIR PRIV
224.0.0.9        /ffffffff   -->   0.0.0.0   [none]       0 ME
255.255.255.255  /ffffffff   -->   0.0.0.0   [none]       0 NW PERM
```

ipxroutes

Lists the current entries in the IPX routing table.

Mgmt Class

Network (R)

Input Format

```
ipxroutes
```

Parameters

None

Response

```
-> ipxroutes

Network   Gateway  Interface   Hops  Ticks Flags
00001001  HQ       [down]      1     4     STATIC FORWARD DOD
00000456  (DIRECT) ETHERNET/0  0     1     FORWARD
```

ipxsaps

Lists the current services in the IPX SAPs table.

Mgmt Class

Network (R)

Input Format

```
ipxsaps
```

Parameters

None

Response

```
-> ipxsaps

Service Name     Type   Node number Network   Skt     Hops
SERV312_FP       4      000000000001:00001001:045    1
```

logout

Logs user out (to login prompt) to reinstate administrative security.

Mgmt Class

All (R)

Input Format

```
logout
```

Parameters

None

Response

Command prompt.

mem

Reports the amount of RAM memory installed in the router and its current allocation.

Mgmt Class

System (R), Debug (R)

Input Format

```
mem
```

Parameters

None

Response

```
-> mem

Small buffers used.......18        (7% of 256 used)
Large buffers used.......41        (16% of 256 used)
Buffer descriptors used..59        (7% of 768 used)
Number of waiters s/1....0/0

Table memory allocation statistics:
Sizes   16     32     64     128    256    512    1024   2048
Used    34     18     12     3      8      9      8      7
Free    3      1      4      0      1      1      1      1

Sizes   4096   8192
Used    3      1
Free    1      0
```

mlp summary

Lists the status of the protocols negotiated for an active remote connection. The following are the most common protocols:

- MLP (Multilink Procedure)
- IPNCP (IP routing Network Protocol)
- CCP (Compression Control Protocol)
- BNCP (Bridging Network Protocol)
- IPXCP (IPX Network Protocol)

Mgmt Class

Network (R)

Input Format

```
mlp summary
```

Parameters

None

Response

Open - indicates that the protocol is in ready state.

Stopped - means that the protocol is defined, but did not successfully negotiate with the remote end.

No message (command prompt ->) indicates that the link is not active.

password

Changes the current user password.

Mgmt Class

All (R/W)

Input Format

```
password <old password> <new password>
```

Parameters

`<old password>`[a] User's current password.

`<new password>`[a] User's new password.

[a] ASCII string

Response

The follwoing example would change the password for user admin101 from *1675309* to *lobster*:

```
admin101@console-> password 1675309 lobster

Password changed for user "admin101"
```

ping

Transmits an echo message, available within the TCP/IP protocol suite. The echo message is sent to a remote node and returned; the echo tests connectivity to the remote node. It is particularly useful for locating connection problems on a network.

The remote node can be specified by IP address or by domain name. If a domain name is specified, the address of the domain is requested from the domain name server (DNS).

A status message is issued for each echo message sent.

☞ **NOTE:**

You cannot ping your own LAN address; you can ping your own WAN address.

To fit the echo message into one ATM cell in routing mode, set the length of user data down to 0 bytes (-s 0 or -l 0).

☞ **NOTE:**

To terminate the ping before it ends, press control-c.

Mgmt Class

Network (R/W)

Input Format

```
ping [-c <count>] [-i <wait>] [- s | -l <size>)] [-I
<srceaddr>] <ipaddr> | <domainname>
```

Parameters

`-c <count>`[a]	Number of packets sent.
`-i <wait>`[b]	Wait period between packets in seconds.
`-s | -l <size>`[c]	Packet data length in bytes.
`-I <scraddr>`[d]	Source IP address contained in the echo message. Use this option to force packets into a tunnel or to force use of the management address as the source address.
`<ipaddr>`[d]	Remote node to which the echo message is sent. It can be specified by its domain name or by its IP address.
`<domainname>`[e]	

[a] integer, 1 - 2000000000 (5)
[b] integer, 1 - 10 (1)
[c] integer, 0 - 1648 (56)
[d] Dotted-decimal notation
[e] ASCII string

Response

The following are application examples of the ping command and their typical responses.

Example

The following command will ping the domain name www.yahoo.com.

```
-> ping www.yahoo.com
```

The command attempts a DNS (domain name server) lookup to find the address of the domain. If the DNS server address is not known, it returns the following message:

```
ping: unknown host www.yahoo.com
```

If the DNS lookup is successful, the ping sends five packets, one second apart, with a packet length of 56 bytes.

```
ping: reply from 216.32.74.52: bytes=56 (data), icmp_seq=1, time=86 ms
ping: reply from 216.32.74.52: bytes=56 (data), icmp_seq=2, time=81 ms
ping: reply from 216.32.74.52: bytes=56 (data), icmp_seq=3, time=82 ms
ping: reply from 216.32.74.52: bytes=56 (data), icmp_seq=4, time=84 ms
ping: reply from 216.32.74.52: bytes=56 (data), icmp_seq=5, time=82 ms
ping: packets sent 5, packets received 5
```

Example

The following command requests 2 echo messages sent 7 seconds apart with a packet length of 34 bytes. The messages are sent to IP address 192.168.254.2.

```
-> ping -c 2 -i 7 -s 34 192.168.254.2
```

```
-ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: reply from 192.168.254.2: bytes=34 (data), time<5 ms
ping: packets sent 2, packets received 2
```

Example

The following command sends packets with the source IP address 192.168.254.254 to the IP address 192.4.210.122. Default values are used for the other options.

```
-> ping -I 192.168.254.254 192.4.210.122
```

Example

The following command uses management address 192.168.1.2 as the source address when pinging destination address 192.168.100.100.

```
-> ping -I 192.168.1.2 192.168.100.100
```

ps

Lists all of the tasks (processes) running in the system and the status of the tasks.

Mgmt Class

System (R), Debug (R)

Input Format

ps

Parameters

None

Response

```
-> ps

TID:              NAME    FL  P   BOTTOM   CURRENT SIZE
1:IDLE                    02  7   1208f0   121008  2032
3:MSFS_SYNC               03  6   1224a0   122ba8  2032
4:SYSTEM LOGGER           03  5   122cd0   1233d8  2032
5:LL_PPP                  03  5   126750   126e58  2032
6:NL_IP                   03  5   126fe0   1272e0  1000
7:TL_IP_UDP               03  3   127460   127768  1000
8:TL_IP_TCP               03  3   1278c0   127fd0  2032
9:IP_RIP                  03  4   128120   128420  1000
10:TELNETD                03  5   128550   128838  1000
11:DUM                    03  5   12b580   12bc88  2032
12:ATM25                  03  1   12c0a0   12c790  2032
13:SNMPD                  03  5   124b60   125a70  4080
14:BOOTP                  03  5   12e3d0   12e6c0  1000
15:CMD                    01  6   12cba0   12d9f8  4080
```

reboot

This command causes a reboot of the system.

CAUTION:
A reboot erases any configuration changes that have not been saved. If necessary, enter a save command before the reboot command.

Certain configuration settings require a reboot before the setting becomes effective, including:

- A change from IP routing to bridging or the reverse.
- The addition of IKE filters
- IPX changes
- Certain changes to Stateful Firewall rules

Other configuration changes become effective following either a reboot or a restart of the Ethernet or remote interface. These changes include:

- System settings
- Ethernet IP address
- TCP/IP routing
- Remote router default bridging destination
- TCP/IP route addresses
- SAPs and bridging
- Adding a new remote entry to the remote database.

A reboot also ensures that all file system updates are completed. There is a time lag between the entry of a save command and the safe storage of the data in FLASH memory. If the power goes off before the data is stored in memory, the data can be lost. Always reboot before powering off the router. Or, use the sync command to commit file changes to memory.

Mgmt Class

All (R/W)

Input Format

```
reboot <option>
```

Parameters

☞ **NOTE:**

The word *default* cannot be abbreviated in the command.

`***`	If no option is specified, the router is rebooted using the existing configuration file.
`factory`	This option deletes all files except AUTOEXEC.OLD if it exists. AUTOEXEC.OLD is renamed AUTOEXEC.BAT; it is re-executed by the reboot. This option also resets the non-volatile RAM; thus deleting the IP address of the router and the TFTP server during the boot process and also forcing the router to boot from FLASH instead of from the network.
`default`	This option deletes the system configuration file and restores the router to its original defaults (before any configuration was entered).

Response

User is prompted to verify the command.

save

The save command saves the entire router's configuration or parts of it to FLASH memory. The keyword in the command determines what is saved.

☞ **NOTE:**

There is a time lag between the response issued by the save command and the time when the data is actually stored in FLASH memory. Issue a sync command after a save command before powering off the router. This commits the changes to FLASH memory.

Mgmt Class

All (R/W)

Input Format

`save`

Parameters

None

Response

Command prompt.

sntp active

Displays the active SNTP server, that is, the server that last responded to an SNTP request.

Mgmt Class

Admin (R/W)

Input Format

```
sntp active
```

Parameters

None

Response

```
-> sntp active
Active SNTP server is 1 (192.6.38.127)
```

sntp disable

Disables SNTP requests.

Mgmt Class

Admin (R/W)

Input Format

```
sntp disable
```

Parameters

None

Response

```
-> sntp disable

Current offset from UTC is 0 minutes
Use <system sntp offset> to set time zone
```

sntp enable

Enables SNTP requests.

Mgmt Class

Admin (R/W)

Input Format

```
sntp enable
```

Parameters

None

Response

```
-> sntp enable

Current offset from UTC is 0 minutes
Use <system sntp offset> to set time zone
```

sntp offset

Specifies the SNTP offset from the Universal Time Coordinate (UTC). The offset is specified in minutes. A positive offset is an offset to the east of the Greenwich meridian; a negative offset is to the west of the Greenwich meridian.

Mgmt Class

Admin (R/W)

Input Format

```
sntp offset <minutes>
```

Parameters

`***`	When no parameter is entered, current offset is displayed.
`<minutes>`[a]	Number of minutes east or west of the Greenwich meridian. A positive number is east; a negative number is west.

[a] Integer 1 - 59

Response

```
-> sntp offset
Current offset from UTC is 0 minutes
Use <system sntp offset> to set time zone
usage: sntp offset <Minutes from UTC>
  (offset is negative for west, positive for east of Greenwich meridian)
-> sntp offset -360
```

sntp prefserver

Displays or changes the preferred SNTP server. (The preferred server is the server that should be attempted first when a request is made.)

To specify a server preference, specify the number of the preferred server within the SNTP server list. To see the SNTP server list, enter sntp server.

To see the active SNTP server (that is, the server that last responded to an SNTP request), use the command sntp active.

☞ **NOTE:**
To make this change permanent, a save must be performed before a reboot.

Mgmt Class

Admin (R/W)

Input Format

```
sntp prefserver <number>
```

Parameters

***	When no parameter is entered, current preferred server displayed.
<number>[a]	Number of a server within the SNTP server list.

[a] Integer

Response

When entered with no <number> parameter:

```
-> sntp prefserver
The preferred SNTP server is 1 (192.6.38.127)
```

When entered with a <number> parameter:

```
-> sntp prefserver 3
Preferred SNTP server is set to 3 (192.6.38.127)
```

sntp request

Requests the time from an SNTP server. (SNTP is the Simple Network Time Protocol defined by RFC 1769.)

☞ **NOTE:**
A request is performed only if SNTP is enabled (see sntp enable).

Mgmt Class

Admin (R/W)

Input Format

```
sntp request
```

Parameters

None

Response

When entered while sntp function is currently disabled:

```
-> sntp request

SNTP is currently disabled
```

When entered and no sntp preferred server is defined:

```
-> sntp request

Time server IP address not set, use "sntp server w.x.y.z"
```

When entered and an sntp preferred server has been defined:

```
-> sntp request

Time set to UTC-480, 5/7/2001 at 17:29:25.245
Time adjusted for (-) 0 days 1 hours 0 minutes 0 seconds
```

sntp server

Displays or changes the SNTP server list.

- To see the current SNTP server list, specify sntp server with no parameter.
- To specify the default server list, specify sntp server default.
- To add a server to the list, specify sntp server with the server IP address and a new number for the entry.
- To change the address of a server, specify sntp server with the server IP address and the existing entry number.
- To remove a server from the list, specify sntp server 0.0.0.0 and the number of the server to be removed.

☞ **NOTE:**
To make a change permanent, you must save the change before you reboot.

Mgmt Class

Admin (R/W)

Input Format

```
sntp server <ipaddress> | default [<number>]
```

Parameters

`<ipaddress>`[a]	IP address of an SNTP server.[b]
`default`	Requests the default server list.
`<number>`[c]	Number of the server in the list. If that server number is already in the list, the IP address is changed; otherwise, a new entry is added to the list. If you omit a number, the IP address of the active server is changed.

[a] Dotted-decimal notation
[b] To remove a server, specify 0.0.0.0 as the IP address.
[c] Integer

Response

When entered with the `<default>` parameter:

```
-> sntp server default

Current server (1) IP addr: 192.5.41.40
Current server (2) IP addr: 192.6.38.127
Current server (3) IP addr: 209.81.9.7
Current server (4) IP addr: 129.7.1.66
Current server (5) IP addr: 192.168.254.2
```

tcp stats

Displays the TCP statistics and open connections.

Mgmt Class

Network (R)

Input Format

```
tcp stats
```

Parameters

None

Response

Typical response:

```
-> tcp stats

TCP Statistics:
   Active Opens.............. 0
   Passive Opens............. 0
   Failed Connect Attempts... 0
   Connections Reset......... 0
   Current Connections....... 0
   Segments Received......... 0
   Segments Sent............. 0
   Segments Retransmitted.... 0
   Bad Checksums............. 0
   Bad Packet Lengths........ 0
   Segments with Reset Flag.. 0
   *:80              0.0.0.0:0          LISTEN       s=0 r=0 f=0
   *:23              0.0.0.0:0          LISTEN       s=0 r=0 f=0
```

time

Displays or changes the current time on the router's clock. To change the current date, use the command date.

Automatic SNTP requests are generated if the system needs to get the time. You can specify an SNTP server using the command sntp server and a UTC offset with the command sntp offset.

Mgmt Class

All (R/W)

Input Format

```
time <hh:mm:ss>
```

Parameters

***	When entered with no parameters, current time and date is displayed.
<hh>[a]	Hour parameter.
<mm>[b]	Minute parameter.
<ss>[b]	Second parameter.

[a] Integer, 1 - 23
[b] Integer, 0 - 59

Response

When entered with no parameters:

```
-> time

BootTime:      5/18/2001 at 11:57:12
Current time:  5/18/2001 at 12:00:01
```

When entered with parameters:

```
-> time 1:01:01

Time set to UTC-420, 5/18/2001 at 1:01:01.074
Time adjusted for (-) 0 days 11 hours 49 minutes 34 seconds
```

traceroute

Traces the route taken by packets sent from the local router to the specified IP address or domain name. A packet is sent for each hop in the route. The output lists the IP addresses of the hops that returned packets.

Unless the -n option is specified, traceroute also attempts to look up the name of each gateway in the route. If the DNS lookup is successful, the name is included in the output message.

☞ **NOTE:**

To terminate the traceroute before it ends, press **control-c**.

Mgmt Class

Network (R/W), Debug (R)

Input Format

```
ping [-c count] [-i <wait>] [- s | -l <size>)] [-I <srceaddr>]
[-n] <ipaddr> | <domainname>
```

Parameters

`-c <count>`[a]	Number of packets sent.
`-i <wait>`[b]	Wait period between packets in seconds.
`-s <size>`[c]	Packet data length in bytes.
`-l <size>`[c]	Packet data length in bytes. Same as `-s`.
`-I <scrceaddr>`[d]	Source IP address contained in the echo message. Use this option to force packets into a tunnel or to force use of the management address as the source address.
`-n`	Eliminates the DNS lookup for each hop. Only the IP address of the hop is listed in the output message.
`<ipaddr>` `<domainname>`[e]	Remote node to which the echo message is sent. It can be specified by its domain name or by its IP address.

[a] Integer, 1 - 2000000000 (5)
[b] Integer, 1 - 10 (1)
[c] Integer, 0 - 1648 (56)
[d] Dotted-decimal notation
[e] ASCII string

Response

The following are application examples of the traceroute command and their responses.

Example

The following two commands trace the same route. The first specifies the domain name; the second specifies the IP address.

```
-> traceroute www.yahoo.com

-> traceroute 204.71.200.68
```

Both commands send up to thirty packets with a wait period of one second and a packet length of 56 bytes. The following is an example of the command output:

```
       1: 172.17.20.122      l2tp-router.flowpoint.com
       2: 172.17.20.1        checkpoint.flowpoint.com
       3: 12.39.98.136       csco2.efficient.com
       4: 12.124.40.65
       5: 12.123.13.166      gbr5-p56.sffca.ip.att.net
       6: 12.122.5.142       gbr3-p100.sffca.ip.att.net
       7: 12.122.5.253       gbr2-p60.sffca.ip.att.net
       8: 12.123.13.61       gar1-p370.sffca.ip.att.net
       10: 206.132.150.250
       11: 206.132.254.37    ge0-0-1000M.hr8.SNV.gblx.net
       12: 206.178.103.62    baslr-ge3-0-hr8.snv.yahoo.com
       13: reply from 204.71.200.68: bytes=56 (data), time=18 ms
traceroute: packets set 13, packets received 12
```

Example

For a faster route trace, specify the `-n` option to eliminate the domain name lookup.

```
-> traceroute -n  204.71.200.68
       1: 172.17.20.122
       2: 172.17.20.1
       3: 12.39.98.136
       4: 12.124.40.65
       5: 12.123.13.166
       6: 12.122.5.142
       7: 12.122.5.253
       8: 12.123.13.61
       10: 206.132.150.250
       11: 206.132.254.37
       12: 206.178.103.62
       13: reply from 204.71.200.68: bytes=56 (data), time=8 ms
traceroute: packets set 13, packets received 12
```

vers

Displays the software version level, source, software options, and amount of time elapsed since router has been running.

All software options are listed.

- If the option has no prefix, the option was enabled when the router was manufactured.
- If the option has a **+** prefix, the option was enabled using a key.
- If the option has a **~** prefix, the option is disabled in this router.

For more information, refer to the Technical Reference Guide and see "Key Enabled Features" on page 4-29.

Mgmt Class

All (R)

Input Format

```
vers
```

Parameters

None

Response

Typical response:

```
-> vers

Efficient 5950 G.SHDSL [ATM] Router (5950-001)
Efficient-5000 BOOT/POST V5.9.0 (25-Apr-00 16:19)
Software version v6.0.0 built Wed Jan 29 09:30:26 PDT 2002
Maximum users: unlimited
Options: SDSL, RFC1483, ipstack, ipcheck, ipfilter, WEB, ~HW-DES,
+ipsec, +3DES, ~l2tp, ~des, ~QoS, ~firewall, ~HWcrypt, ~radius,
+sshd, BRIDGE, IPX, DIAL-BACKUP, VRRP, ~IntModem
Up for 49 days 19 hours 57 minutes (started 12/20/2001 at 17:11)
```

CHAPTER 3

FILE SYSTEM COMMANDS

The file system commands allow you to perform maintenance and recovery on the device. These commands allow you to:

- Format the file system
- List the contents of the file system
- Copy, rename, and delete files

The router file system is DOS-compatible, and the file system commands are similar to the DOS commands of the same name.

The file system commands found in this section include:

Table 3-1: File System Command Listing

Command	Function
copy	Copies a file from the source to the destination.
delete	Deletes the specified file from the flash filesystem.
dir	Displays the directory of the file system. The size of each file is listed in bytes.
execute	This command loads batch files of configuration commands into the router.
format disk	Erases and reformats the device file system.
msfs	Checks and reports the structure of the file system.
rename	Renames a file in the file system.
sync	Commits the changes made to the file system to FLASH memory.

copy

Copies a file from the source to the destination. This command allows you to update the device software level or to write configuration files to a TFTP server

Issue a sync command after a copy command to commit the changes to FLASH memory.

CAUTION:
No warning message is issued if copying over an existing file.

Mgmt Class

All (R/W)

Input Format

```
copy <srcfile> <dstfile>
```

Parameters

`<srcfile>`	Filename of the source file to be copied.It can be either the name of a local file or a file accessed remotely via a TFTP server.
`<dstfile>`	Destination filename to which the file is copied.

A local filename is in the format: **name.ext**.

A remotely accessed filename is specified as: **tftp@serveraddr:filename.ext**. The TFTP server address is optional. If the TFTP server address is not specified, the address used is either the one from which the router booted or the one permanently configured in the boot system.

To force use of a specific source address when copying a file from a TFTP server, use this format: `tftp@serveraddr-sourceaddr:filename.ext`

Examples

The following command copies the file KERNELNW on TFTP server 128.1.210.66 to the local file KERNEL.F2K.

```
-> copy tftp@128.1.210.66:kernelnw kernel.f2k
Copying...
421888 bytes copied
```

The following command uses the source address 192.168.1.2 when copying the file KERNELNW on TFTP server 192.168.100.100 to the local file KERNEL.F2K.

```
-> copy tftp@192.168.100.100-192.168.1.2:kernelnw kernel.f2k
```

Response

Refer to examples for typical responses.

delete

Deletes the specified file from the flash filesystem.

Mgmt Class

Admin (R/W), System (R/W)

Input Format

```
delete <filename>
```

Parameters

`<filename>`[a]	Name of the file to be deleted.

[a] ASCII string

Response

A typical response is shown below.

```
-> delete kernel.f2k
kernel.f2k deleted
```

dir

Displays the directory of the file system. The size of each file is listed in bytes.

Mgmt Class

Admin (R/W), System (R/W)

Input Format

```
dir
```

Parameters

None

Response

A typical response is shown below.

```
-> dir

KEYFILE  DAT  768
SYSTEM   CNF  2816
ATOM     DAT  44
DHCP     DAT  1024
SDSL     DAT  32
FILTER   DAT  1284
KERNEL   F2K  682018
ASIC     AIC  15091
DSP      DAT  24
```

execute

This command loads batch files of configuration commands into the router. This allows for customization and simpler installation of the device. A script file can contain commands, comments (lines introduced by the # or ; characters), and blank lines.

There are two kinds of script files:

- A one-time script that is executed on startup (only once).
- A group of commands that can be executed at any time from the Command Line Interface with the `execute <filename>` command.

One-time scripts are useful to execute the complete configuration process from a default (unconfigured) state.

Mgmt Class

All (R/W)

Input Format

```
execute <filename>
```

Parameters

`<filename>`[a]	Name of the file to be executed.

[a] ASCII string

Response

Command prompt.

format disk

Erases and reformats the device file system. This command should only be used when the file system is unusable. If the device does not execute the POST test and software boot successfully, and the result of the dir command indicates the file system is corrupted, you may wish to reformat the disk, reboot the device, and recopy the system software.

Mgmt Class

System (R/W), Debug (R/W)

Input Format

```
format disk
```

Parameters

None

Response

The following is an example of the `format disk` command.

```
-> format disk

NEWFS: erasing disk..
NEWFS: fs is 381k and will have 762 sectors
NEWFS: 128 directory slots in 8 sectors
NEWFS: 747 fat entries in 3 sectors
NEWFS: writing boot block...done.
NEWFS: writing fat tables...done.
NEWFS: writing directory...done.
Filesystem formatted!
```

msfs

Checks the structure of the file system. This command performs a function similar to the DOS chkdsk command. The router analyzes the File Allocation Table (FAT) and produces a file system status report.

CAUTION:
When you specify <*fix*>, make sure that no other operation is being performed on the configuration files at the same time by another user.

Mgmt Class

System (R/W), Debug (R/W)

Input Format

```
msfs <fix>
```

Parameters

`<fix>` Optional - If fix is specified, errors are corrected in the FAT. [a]

[a] This option should only be used when an msfs command results in a recommendation to apply the fix option.

Response

The following is an example of a typical response without the `fix` parameter.

```
-> msfs

Filesystem 0, size=825k
Checking filesystem...
Checking file entries...
  SYSTEM    CNF ... 2304    bytes .. ok.
  ATM25     DAT ... 20      bytes .. ok.
  DHCP      DAT ... 1536    bytes .. ok.
  KERNEL    F2K ... 257014  bytes .. ok.
  IDL_7     AIC ... 14828   bytes .. ok.
  ASIC      AIC ... 14828   bytes .. ok.
  FILTER    DAT ... 1284    bytes .. ok.
  1097 fat(s) used, 0 fat(s) unused, 0 fat(s) unref, 534 fat(s) free
  561664 bytes used by files, 9728 bytes by tables, 273408 bytes free
```

rename

Renames a file in the file system.

Mgmt Class

All (R/W)

Input Format

```
rename <oldname> <newname>
```

Parameters

<oldname>[a]	Existing name of the file.
<newname>[a]	New name of the file.

[a] ASCII string

Response

The following is an example `rename` command.

```
-> rename ether.dat oldeth.dat
'ether.dat' renamed to 'oldeth.dat'
```

sync

Commits the changes made to the file system to FLASH memory.

Mgmt Class

All (R/W)

Input Format

```
sync
```

Parameters

None

Response

```
-> sync
Syncing file systems...done.
```

CHAPTER 4

SYSTEM COMMANDS

All commands in this section begin with the word *system*. The commands set basic router configuration information, such as the following:

- name of the router
- optional system message
- authentication password
- security authentication protocol
- management security
- system administration password
- IP address translation
- NAT configuration
- host mapping
- WAN-to-WAN forwarding
- filters
- Dial Backup configuration
- SNTP parameters

The system commands found in this section include:

Table 4-1: System Command Listing

Command	Function
system ?	Lists the supported keywords.
system addbootpserver	Adds an address to the BootP server list.
system addhostmapping	Remaps a range of local-LAN IP addresses to a range of public IP addresses on a system-wide basis.

Table 4-1: System Command Listing (Cont.)

Command	Function
system addhttpfilter	Enables blocking all devices except those within the defined IP address range from using the HTTP protocol
system addiproutingtable	Defines a new virtual routing table.
system addserver	Configures a local IP address as the selected server on the LAN (FTP, SMTP, etc.) for the global configuration.
system addsnmpfilter	Validates SNMP clients by defining a range of IP addresses that are allowed to access the router via SNMP.
system addsyslogfilter	Limits the Syslog server addresses that may be returned by DHCP.
system addsyslogserver	Adds an address to the list of Syslog servers.
system addtelnetfilter	Validates Telnet clients by defining a range of IP addresses that are allowed to access the router via Telnet.
system addudprelay	Create a UDP port range for packet forwarding.
system authen	Forces the target router authentication protocol that is used for security negotiation with the remote routers when the local side authentication is set.
system backup add	Adds an IP address to the list of addresses to be pinged for the Dial Backup option.
system backup delete	Deletes an IP address from the list of addresses to be pinged for the Dial Backup option.
system backup disable	Disables the Dial Backup option in the router.
system backup enable	Enables the Dial Backup option in the router.
system backup pinginterval	Changes the ping interval for a group, that is, the number of seconds between pings during a test of the addresses in the group.
system backup pingsamples	Changes the number of ping samples for a group, that is, the number of pings performed for each address in the group.
system backup retry	Changes the Dial Backup retry period.
system backup stability	Changes the Dial Backup stability period.

Table 4-1: System Command Listing (Cont.)

Command	Function
system backup successrate	Changes the minimum success rate required for a group of pinged addresses.
system blocknetbiosdefault	Sets the default value used when a remote router entry is defined.
system community	Enables changing the SNMP community name from its default value.
system default modem	Lists the default modem settings.
system delbootpserver	Removes an address from the BootP server list.
system delhostmapping	Undoes an IP address/host translation (remapping) range
system delhttpfilter	Deletes an http address filter.
system deliproutingtable	Deletes a range of addresses that reference a virtual routing table or deletes the entire virtual routing table.
system delserver	Deletes an server entry.
system delsnmpfilter	Deletes the SNMP client range.
system delsyslogfilter	Renames a file in the file system.
system delsyslogserver	Deletes the Syslog address filter.
system deltelnetfilter	Deletes the Telnet client range.
system deludprelay	Deletes the UDP port range.
system history	Displays the router's most recent console log.
system httpport	Manages the system HTTP port access.
system list	Lists the system settings for the target router.
system log	Allows logging of the device's activity in a Telnet session.
system modem	Changes the selected modem setting.
system moveiproutingtable	Moves a range of IP addresses to another virtual routing table.
system msg	Sets or changes the message saved in the local router you are configuring.

Table 4-1: System Command Listing (Cont.)

Command	Function
system name	Sets or changes the name of the local router being configured.
system onewandialup	Can force the router to have no more than one remote connection active at a time.
system passwd	Sets the system authentication password for the target router that is used when the router connects to other routers or is challenged by them.
system riptimer	Sets the duration for RIP information to be exchanged with remote routers.
system securemode list	Displays the current secure mode configuration values and the number of concurrent Telnet and SSH sessions allowed.
system securemode set	Enables and disables the secure mode function.
system securemode set cli	Sets the number of concurrent Telnet and SSH sessions the system will allow.
system securemode set lan	Allows discrete control of the secure mode for the LAN interface.
system securemode set wan	Allows discrete control of the secure mode for the WAN interface.
system securitytimer	Allows the user to change the 10-minute default security timer to another value.
system selnat addpolicy	Adds a Selective NAT policy.
system selnat delpolicy	Deletes a Selective NAT policy.
system selnat list	Lists the current Selective NAT policies.
system snmpport	Manages SNMP port access.
system sshport	Manages SSH port access.
system supporttrace	Provides the ability to capture all configuration data to a file for troubleshooting.
system syslogport	Manages Syslog port access.
system telnetport	Manages the built-in Telnet server port access.
system wan2wanforwarding	Allows management of WAN-to-WAN forwarding of data from one WAN link to another.

system ?

Lists the supported keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

All (R)

Input Format

```
system ?
```

Parameters

None

Response

A listing of all the supported system commands and keywords with a brief description of their function.

system addbootpserver

Adds an address to the BootP server list. (The BootP server list is also the DHCP relay list.)

While the BootP server list has at least one address, the router disables its own DHCP server and, instead, forwards all DHCP/BootP requests to all servers in the list. It forwards every reply received from any of the servers in the list to the appropriate LAN. To read about BootP service, see "BootP Service" on page 4-15 of the Technical Reference Guide.

Addresses can also be added to the list using the dhcp addrelay command. To remove an address from the list, use the dhcp delrelay command.

To see the current BootP server address, enter the command dhcp addrelay or system addbootpserver with no parameters. To remove a BootPserver address, use the command dhcp delrelay or system delbootpserver.

Mgmt Class

Network (R/W)

Input Format

```
system addbootpserver <ipaddr>
```

Parameters

`<ipaddr>`[a] IP address of the server.

[a] Dotted-decimal notation

Response

The following is an example of adding a server address then querying a response.

```
-> system addbootpserver 128.1.210.64

-> system addbootpserver
BOOTP/DHCP Server address: 128.1.210.64
```

system addhostmapping

Remaps a range of local-LAN IP addresses to a range of public IP addresses on a system-wide basis. These local addresses are mapped one-to-one to the public addresses.

☞ **NOTE:**

The range of public IP addresses is defined by `<first public addr>` only. The rest of the range is computed automatically (from `<first public addr>` to `<first public addr>` + number of addresses remapped - 1) inclusive.

Automatic SNTP requests are generated if the system needs to get the time. You can specify an SNTP server using the command sntp server and a UTC offset with the command sntp offset.

Mgmt Class

Network (R/W)

Input Format

```
system addhostmapping <first private addr>
<second private addr> <first public addr>
```

Parameters

`<first private addr>`[a]	First IP address in the range of IP addresses to be remapped.
`<second private addr>`[a]	Last address in the range of IP addresses to be remapped.
`<first public addr>`[a]	Last address in the range of IP addresses to be remapped.

[a] Dotted-decimal notation

Response

Command prompt.

system addhttpfilter

Enables blocking all devices except those within the defined IP address range from using the HTTP protocol (for example, to browse the Web). This command can block devices on the WAN from accessing the Web browser. This validation feature is off by default.

☞ **NOTE:**

This command does not require a reboot and is effective immediately.

☞ **NOTE:**

To list the range of allowed clients, use the command system list when you are logged in with read and write permission (be sure to log in with password). To delete addresses from the HTTP filter, use the system delhttpfilter command.

For more information, see "Controlling Remote Management" on page 5-15 of the Technical Reference Guide.

Mgmt Class

Security (R/W)

Input Format

```
system addhttpfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address in the range.
`<last ipaddr>`[a]	Last address in the range of IP addresses to be remapped.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system addiproutingtable

Defines a new virtual routing table. Once defined, you can add routes to the table using the commands eth ip bindroute and remote bindipvirtualroute.

The command specifies the name of the new routing table and the range of IP addresses that reference the table for their routing. When the router receives a packet, the source address of the packet determines which routing table is used. For example, if the range of addresses for the virtual routing table ROSA includes address 192.168.25.25, then every packet with the source address 192.168.25.25 is routed using virtual routing table ROSA.

If the source address of a packet is not within the address ranges for any virtual routing table, the default routing table is referenced to route the packet.

For more information, see ”Virtual Routing Tables” on page 6-2 of the Technical Reference Guide.

If an IP routing table has been defined, you can see its range of addresses using the system list command.

Mgmt Class

Network (R/W)

Input Format

```
system addiproutingtable <first ipaddr> [<last ipaddr>] <tablename>
```

Parameters

`<first ipaddr>`[a]	First IP address in the range.
`<last ipaddr>`[a]	Last IP address in the range of IP addresses to be remapped.[b]
`<tablename>`	Name of the virtual routing table to which the addresses are assigned.[c]

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.
[c] This parameter may be omitted if the range contains only one IP address. The specified address range may not overlap the address range defined for any other virtual routing table.

Response

Example

The following command defines a virtual routing table named ROSA (if it does not already exist) and assigns it the IP address range 192.168.1.5 through 192.168.1.12.

```
-> system addiproutingtable 192.168.1.5 192.168.1.12 ROSA
```

After routing table ROSA has been defined, the following line appears in the output for the command `system list`:

```
192.168.1.5 through 192.168.1.12 uses IP Routing Table <ROSA>
```

system addserver

This Network Address Translation (NAT) command is used to configure a local IP address as the selected server on the LAN (FTP, SMTP, etc.) for the global configuration. To learn more, see ”Network Address Translation (NAT)” on page 4-17 of the Technical Reference Guide.

Multiple system addserver, remote addserver, and eth ip addserver commands can designate different servers for different protocols, ports, and interfaces. When a request is received, the router searches the server list for the appropriate server. The order of search for a server is discussed in ”Server Request Hierarchy” on page 4-22 of the Technical Reference Guide.

To delete a server designation, use the system delserver command.

Mgmt Class

Network (R/W)

Input Format

```
system addserver <action> <protocol> <first port> [<last port>
[<first private port>]]
```

Response

Command prompt.

Parameters

`<action>`	One of the following command actions:	
	`<ipaddr>`[a]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.
`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[b]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the remote end. Port used by the selected server.	
	`<portid>`[c]	Numerical port value; a value of 0 matches any port.
	`dns`	Domain Name Server (DNS) port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypertext Transfer Protocol (HTTP) port.
	`login`	rlogin port (513).
	`rsh`	Remote shell port.
	`smtp`	Simple Mail Transfer Protocol (SMTP) port.
	`snmp`	Simple Network Management Protocol (SNMP) port.
	`t120`	T.120 port.
	`telnet`	Telnet port.
	`tftp`	Trivial File Transfer Protocol (TFTP) port.
	`all`	All ports.
`<last port>`	Optional last port in the range of ports as seen by the remote end for the server on the LAN.	
`<first private port>`[c]	If specified, this is a port remapping of the incoming requests from the remote end.	

[a] Dotted-decimal notation
[b] Integer
[c] Integer, 0 - 65,535

system addsnmpfilter

Validates SNMP clients by defining a range of IP addresses that are allowed to access the router via SNMP. This validation feature is *off* by default. This command is functionally equivalent to the snmp addsnmpfilter command.

☞ NOTE:

This command does not require a reboot and is effective immediately.

☞ NOTE:

To list the range of allowed clients, use the system list command. To delete addresses from the SNMP filter, use the system delsnmpfilter or snmp delsnmpfilter command.

For more information, see "Controlling Remote Management" on page 5-15 of the Technical Reference Guide.

Mgmt Class

Security (R/W)

Input Format

```
system addsnmpfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the client range.
`<last ipaddr>`[a]	Last IP address of the client range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system addsyslogfilter

Limits the Syslog server addresses that may be returned by DHCP. By default, this validation feature is off.

The Syslog filter can comprise one or more ranges of IP addresses that DHCP may return for Syslog servers. To delete addresses from the Syslog filter, use the system delsyslogfilter command.

This command does not affect the Syslog server addresses that you specify explicitly. For more information on the router as a Syslog client, see "Syslog Client" on page 7-1 of the Technical Reference Guide.

☞ **NOTE:**

This command does not require a reboot and is effective immediately.

☞ **NOTE:**

To list the range of allowed clients, use the system list command.

Mgmt Class

Security (R/W)

Input Format

```
system addsyslogfilter <firstipaddr> [<last ipaddr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the valid server range.
`<last ipaddr>`[a]	Last IP address of the valid server range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system addsyslogserver

Adds an address to the list of Syslog servers. The router sends system event messages to all Syslog servers in the list, unless the Syslog port has been disabled. For more information about the router as a Syslog client, refer to "Syslog Client" on page 7-1 of the Technical Reference Guide.

To see the server addresses, use the system list command. To remove a Syslog server address from the list, use the system delsyslogserver command.

☞ **NOTE:**

The new server address becomes effective after performing a save and a reboot.

Mgmt Class

System (R/W)

Input Format

```
system addsyslogserver <ipaddr>
```

Parameters

`<ipaddr>`[a]	IP address to be added to the Syslog server address list.

[a] Dotted-decimal notation

Response

Command prompt.

system addtelnetfilter

Validates Telnet clients by defining a range of IP addresses that are allowed to access the router via Telnet. The mode is off by default. For more information, refer to "Controlling Remote Management" on page 5-15 of the Technical Reference Guide.

☞ **NOTE:**

This command does not require a reboot and is effective immediately.

☞ **NOTE:**

To list the range of allowed clients, use the system list command. To delete addresses from the Telnet filter, use the system deltelnetfilter command.

Mgmt Class

Security (R/W)

Input Format

```
system addtelnetfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the client range.
`<last ipaddr>`[a]	Last IP address of the client range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system addudprelay

Create a UDP port range for packet forwarding. You can specify a port range from 0 to 65535; however, 137 to 139 are reserved for NetBIOS ports.

☞ **NOTE:**

Overlap of UDP ports is not allowed.

Mgmt Class

Network (R/W)

Input Format

```
system addudprelay <ipaddr> <first port>|all [<last port>]
```

Parameters

`<ipaddr>`[a]	IP address of the server to which the UDP packet will be forwarded.
`<first port>`[b]	First port in the UDP port range to be created.
`all`	Incorporates all the available UDP ports in the new range.
`<last port>`[b]	Last port in the UDP port range to be created.

[a] Dotted-decimal notation
[b] Integer, see description above for port range.

Response

Command prompt.

system authen

Forces the target router authentication protocol that is used for security negotiation with the remote routers when the local side authentication is set. You should not need to issue this command as the best security possible is provided with the *none* default. To read about PAP/CHAP, see "PAP/CHAP Security Authentication" on page 5-20 of the Technical Reference Guide.

Mgmt Class

Security (R/W)

Input Format

```
system authen none | pap | chap
```

Parameters

`***`	When the command is entered with no parameters, the current authentication override is displayed.
`none`	The authentication protocol is negotiated, with the minimum best security level as defined for each remote router in the database.
`pap`	Negotiation begins with PAP (instead of CHAP) for those entries that have PAP in the remote database and only when the call is initiated locally.
`chap`	Overrides all the remote database entries with CHAP, that is, only CHAP is performed.

Response

This following example illustrates setting the authentication level, then displaying the current setting.

```
-> system authen chap

-> system authen
Authentication needed.................CHAP
```

system backup add

Adds an IP address to the list of addresses to be pinged for the Dial Backup option. The command can specify an explicit address, or it can request that the router determine the gateway or DNS address and add that address to the list.

For additional information, see ”Dial Backup” on page 6-7 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system backup add <ipaddr> | gw | dns [<group>]
```

Parameters

`<ipaddr>`[a]	IP address to be added to the list.
`gw`	Gateway address. The router determines the actual gateway address.
`dns`	Domain Name Server address. The router determines the actual DNS address.
`<group>`[b]	Optional number of a group to which the address is assigned.

[a] Dotted-decimal notation
[b] integer, 0 - 65535 (0)

Examples

The following command adds the address 192.168.1.5 to group 0 of the addresses to be pinged.

```
-> system backup add 192.168.1.5
```

The following command adds the gateway address to group 1 of the addresses to be pinged.

```
-> system backup add GW 1
```

Response

Command prompt.

system backup delete

Deletes an IP address from the list of addresses to be pinged for the Dial Backup option. The command can:

- Specify an explicit address to be deleted.
- Request that the router delete the gateway or DNS address from the list.
- Delete all addresses in a group.
- Clear all addresses from the list.

To see the addresses in the current list, use the system list command. For more information, refer to "Dial Backup" on page 6-7 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system backup delete <ipaddr> | gw | dns | all [<group> | all ]
```

Parameters

`<ipaddr>`[a]	IP address to be deleted from the list.
`gw`	Gateway address. The router determines the actual gateway address.
`dns`	Domain Name Server address. The router determines the actual DNS address and deletes it.
`all <group>`[b]	Optional number of a group to which the specified address or all addresses are deleted.
`all`	Requests deletion of all addresses in all groups including group 0.

[a] Dotted-decimal notation
[b] integer, 0 - 65535 (0)

Examples

The following command deletes the address 192.168.1.5 from group 0.

```
-> system backup delete 192.168.1.5
```

The following command deletes the gateway address from group 1.

```
-> system backup delete  GW  1
```

The following command deletes all addresses from group 2.

```
-> system backup delete  all  2
```

The following command clears all addresses from the list.

```
-> system backup delete  all  all
```

Response

Command prompt.

system backup disable

Disables the Dial Backup option in the router.

☞ **NOTE:**

Because Dial Backup uses the console port, you cannot access the command line via the console port while Dial Backup is enabled. You must use the Web GUI interface or a Telnet session to disable Dial Backup.

☞ **NOTE:**

If you do not use the save command to save this change, Dial Backup is only temporarily disabled and it is re-enabled at the next reboot. Temporarily disabling Dial Backup stops Dial Backup, but it does not change the use of the console port. To disable Dial Backup across reboots, see ”Disabling and Re-Enabling Dial Backup” on page 6-15 of the Technical Reference Guide.

To re-enable the Dial Backup option, use the system backup enable command. For more information about Dial Backup, refer to ”Dial Backup” on page 6-7 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system backup disable
```

Parameters

None

Response

Command prompt.

system backup enable

Turns on the enable switch for the Dial Backup option in the router. To see the current setting of the Dial Backup switch, use the system list command. To disable Dial Backup, use the system backup disable command. For more information, see "Dial Backup" on page 6-7 of the Technical Reference Guide.

☞ **NOTE:**

Dial Backup cannot be enabled unless the remote containing its dialup parameters is also enabled. (Check this using the remote list command).

Mgmt Class

Network (R/W)

Input Format

```
system backup enable
```

Parameters

None

Response

Command prompt.

system backup pinginterval

Changes the ping interval for a group, that is, the number of seconds between pings during a test of the addresses in the group.

To see the current ping intervals, use the system list command. For more information about the ping interval and Dial Backup, see "Ping Interval, Number of Samples, and Success Rate" on page 6-13 of the Technical Reference Guide.

☞ **NOTE:**

If you change the ping interval to *0*, the group of addresses is disabled.

Mgmt Class

Network (R/W)

Input Format

```
system backup pinginterval <seconds> [<group>]
```

Parameters

`<seconds>`[a]	Number of seconds in the ping interval for the group.
`<group>`[b]	Optional, number of a group.

[a] Integer
[b] integer, 0 - 65535 (0)

Examples

The following command changes the ping interval to 10 seconds for group 0.

```
-> system backup pinginterval 10
```

The following command disables the pinging of addresses in group 1.

```
-> system backup pinginterval  0  1
```

Response

Command prompt.

system backup pingsamples

Changes the number of ping samples for a group, that is, the number of pings performed for each address in the group.

To see the current ping sample values, use the system list command. For more information about ping samples and Dial Backup, see ”Addresses to Ping” on page 6-12 of the Technical Reference Guide.

☞ **NOTE:**

If you change the ping samples value to *0*, you disable pinging for that group of addresses.

Mgmt Class

Network (R/W)

Input Format

```
system backup pingsamples <samples> [<group>]
```

Parameters

`<samples>`[a]	Number of times the addresses in the group are pinged.
`<group>`[b]	Optional, number of a group.

[a] Integer, (6)
[b] integer, 0 - 65535 (0)

Examples

The following command changes the number of ping samples to 10 for addresses in group 0.

```
-> system backup pingsamples  10
```

The following command disables the pinging of addresses in group 1.

```
-> system backup pingsamples  0  1
```

Response

Command prompt.

system backup retry

Changes the Dial Backup retry period. The retry period determines how often the router attempts to restore the DSL link. For more information about the Dial Backup retry period, see "Setting DSL Link Conditions" on page 6-11 of the Technical Reference Guide.

The default retry period is thirty minutes. The minimum retry period is two minutes. To see the current retry value, use the system list command.

☞ **NOTE:**

When the Dial Backup retry timer expires, the modem is disconnected even if there is traffic on the modem.

Mgmt Class

Network (R/W)

Input Format

```
system backup retry <minutes>
```

Parameters

`<minutes>`[a] Number of minutes in the retry period.

[a] Integer, 2 - 60 (20)

Examples

The following command changes the retry period to 60 minutes.

```
-> system backup retry 60
```

The following command changes the retry period to 2.

```
-> system backup retry 1
```

Response

Command prompt.

system backup stability

Changes the Dial Backup stability period. The stability period guards against frequent switching back and forth between the DSL link and the backup port. For more information about the Dial Backup stability period, see "Stability Period" on page 6-11 of the Technical Reference Guide.

To see the current stability value, use the system list command.

Mgmt Class

Network (R/W)

Input Format

```
system backup stability <minutes>
```

Parameters

`<minutes>`[a] Number of minutes in the stability period.

[a] Integer, 1 - 60 (3)

Examples

The following command changes the stability period to 5 minutes.

```
-> system backup stability 5
```

Response

Command prompt.

system backup successrate

Changes the minimum success rate required for a group of pinged addresses. If the success rate is less than the minimum, the DSL link is assumed to have failed and a switchover to the backup is performed.

☞ **NOTE:**
If you change the success rate to *0*, you disable pinging for that group of addresses.

☞ **NOTE:**
A minimum success rate of 100% is not recommended; this would require a reply from every ping sent.

To see the current success rate values, use the system list command. For more information about success rates and Dial Backup, see "Ping Interval, Number of Samples, and Success Rate" on page 6-13 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system backup successrate <percentage> [<group>]
```

Parameters

`<percentage>`[a]	Minimum success rate required during a ping test of the addresses in the group.
`<minutes>`[b]	Optional, number of a group.

[a] Integer, 0 - 99 (50)
[b] Integer, 0 - 65535 (0)

Examples

The following command changes the success rate to 75% for addresses in group 0.

```
-> system backup successrate 75
```

The following command disables the pinging of addresses in group 1.

```
-> system backup successrate  0  1
```

Response

Command prompt.

system blocknetbiosdefault

The router can block all NetBIOS and NetBUI requests from being sent over the WAN. This command sets the default value used when a remote router entry is defined.

The command remote blocknetbios can change the NetBIOS setting for a specific remote router. To see the current NetBIOS default, use the system list command.

Mgmt Class

Security (R/W)

Input Format

```
system blocknetbiosdefault  yes | no
```

Parameters

`yes`	Sets the default to block all NetBIOS and NetBUI requests.
`no`	Sets the default to *not* block all NetBIOS and NetBUI requests.

Examples

The following command will block all NetBIOS and Net BUI requests

```
-> system blocknetbiosdefault yes
```

Response

Command prompt.

system community

Enhances SNMP security by allowing the user to change the SNMP community name from its default value of "*public*" to a different value. Refer to "SNMP" on page 7-2 of the Technical Reference Guide for additional information.

☞ **NOTE:**
This command is functionally equivalent to the snmp community command.

Mgmt Class

Security (R/W)

Input Format

```
system community [<snmp community name>]
```

Parameters

`***`	When entered with no parameter the current community name is displayed.
`<snmp community name>`[a]	SNMP community name to which device is added.

[a] ASCII string, 40 characters maximum

Response

The following response is given when the system community is changed to 'fred':

```
-> system community fred
The community name fred will take effect at the next reboot
```

system default modem

Lists the default modem settings. The modem settings are for the backup V.90 modem connected to the console port.

To change the modem settings, use the command system modem. For more information on the Dial Backup option, refer to "Dial Backup" on page 6-7 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system defaultmodem
```

Parameters

None

Response

Command prompt.

system delbootpserver

Removes an address from the BootP server list. (The BootP server list is also the DHCP relay list.)

Addresses can also be removed from the list using the command dhcp delrelay. To add an address to the list, use the dhcp addrelay command.

Mgmt Class

Network (R/W)

Input Format

```
system delbootpserver <ipaddr> | all
```

Parameters

`<ipaddr>`[a]	IP address of the server to be deleted from the BootP server list.
`all`	Removes all addresses from the BootP server list.

[a] Dotted-decimal notation

Examples

The following command will remove only the address 128.1.210.64 from the bootP server list.

```
-> system delbootpserver 128.1.210.64
```

The following command will remove all addresses from the bootP server list.

```
-> system delbootpserver all
```

Response

Command prompt.

system delhostmapping

Undoes an IP address/host translation (remapping) range that was previously established with the command remote addhostmapping on a per-system-wide basis.

Mgmt Class

Network (R/W)

Input Format

```
system delhostmapping <first private addr> <second private
addr> <first public addr>
```

Parameters

`<first private addr>`[a]	First IP address in the range of IP address.
`<second private addr>`[a]	Last IP address in the range of IP address.
`<first public addr>`[a]	Defines the range of public IP addresses.[b]

[a] Dotted-decimal notation
[b] The rest of the range is computed automatically.

Response

Command prompt.

system delhttpfilter

Deletes an http address filter created by the system addhttpfilter command. To see the address range of the filter, use the system list command.

Mgmt Class

Security (R/W)

Input Format

```
system delhttpfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the range.
`<last ipaddr>`[a]	Last IP address of the range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system deliproutingtable

Deletes a range of addresses that reference a virtual routing table or deletes the entire virtual routing table. To list the virtual routing tables, use the iproutes command. For more information, see "Virtual Routing Tables" on page 6-2 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system addiproutingtable <first ip addr> [<last ip addr>]
<tablename>
```

Parameters

`all`	Deletes the virtual routing table. Both the table definition and all routes in the table are deleted.
`<first ipaddr>`[a]	First IP address of the range.
`<last ipaddr>`[a]	Last IP address of the range.[b]
`<tablename>`[c]	Name of the virtual routing table in which the addresses are assigned.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.
[c] ASCII string

Examples

The following command deletes two IP addresses from the address range that references routing table ROSA:

```
-> system deliproutingtable 192.168.1.5 192.168.1.6 ROSA
```

The following command deletes the virtual routing table ROSA:

```
-> system deliproutingtable all ROSA
```

Response

Command prompt.

system delserver

Deletes an entry created by the system addserver command.

Mgmt Class

Network (R/W)

Input Format

```
system addServer <action> <protocol> <first port> [<last port>
[<first private port>]]
```

Response

Command prompt.

Parameters

`<action>`	One of the following command actions:	
	`<ipaddr>`[a]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.
`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[b]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the remote end. Port used by the selected server.	
	`<portid>`[c]	Numerical port value; a value of 0 matches any port.
	`dns`	Domain Name Server (DNS) port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypertext Transfer Protocol (HTTP) port.
	`login`	rlogin port (513).
	`rsh`	Remote shell port.
	`smtp`	Simple Mail Transfer Protocol (SMTP) port.
	`snmp`	Simple Network Management Protocol (SNMP) port.
	`t120`	T.120 port.
	`telnet`	Telnet port.
	`tftp`	Trivial File Transfer Protocol (TFTP) port.
	`all`	All ports.
`<last port>`	Optional last port in the range of ports as seen by the remote end for the server on the LAN.	
`<first private port>`[c]	If specified, this is a port remapping of the incoming requests from the remote end.	

[a] Dotted-decimal notation
[b] Integer
[c] Integer, 0 - 65,535

system delsnmpfilter

Deletes the client range previously defined by the command system addsnmpfilter. This command is functionally equivalent to the snmp delsnmpfilter command.

☞ **NOTE:**

This command does not require a reboot and is effective immediately.

☞ **NOTE:**

To list the range of allowed clients, use the command system list.

For more information, see "Controlling Remote Management" on page 5-15 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system delsnmpfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the client range.
`<last ipaddr>`[a]	Last IP address of the client range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system delsyslogfilter

Deletes the Syslog address filter. To see the address range of the filter, use the command system list. To define a new Syslog address filter, use the command system system addsyslogfilter.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Security (R/W)

Input Format

```
system delsyslogfilter <firstipaddr> [<last ipaddr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the range.
`<last ipaddr>`[a]	Last IP address of the range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system delsyslogserver

Removes an address from the list of Syslog servers. To see the server addresses, use the command system list. To specify a new Syslog server address, use the command system system addsyslogserver.

☞ **NOTE:**
The new server address becomes effective after a save and a reboot command.

Mgmt Class

Network (R/W)

Input Format

```
system delsyslogserver <ipaddr>
```

Parameters

`<ipaddr>`[a]	IP address to be deleted from the Syslog server address list.

[a] Dotted-decimal notation

Response

Command prompt.

system deltelnetfilter

Deletes the client range previously defined by the command system system addtelnetfilter.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

☞ **NOTE:**
To list the range of allowed clients, use the command system list.

Mgmt Class

Security (R/W)

Input Format

```
system deltelnetfilter <first ipaddr> [<last ipaddr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the client range.
`<last ipaddr>`[a]	Last IP address of the client range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

system deludprelay

Deletes the port range that was previously enabled by the command system addudprelay.

Mgmt Class

Network (R/W)

Input Format

```
system deludprelay <ipaddr> <first port>|all [<last port>]
```

Parameters

`<ipaddr>`[a]	IP address of the server.
`<first port>`[b]	First port in the UDP port range to be deleted.
`all`	Deletes all existing UDP ports.
`<last port>`[b]	Last port in the UDP port range to be deleted.

[a] Dotted-decimal notation
[b] Integer

Response

Command prompt.

system history

Displays the router's most recent console log.

Mgmt Class

Admin (R/W)

Input Format

```
system history
```

Parameters

None

Response

The following is a typical response.

```
-> system history
Begin System History.

POST summary: successful

Initializing the system RAM ..... done

Hardware "IDSL" successfully initialized -- ID: 3000
Today is Tuesday May 15, 2001; the time is 10:40:30
My MAC address is: 00:20:6F:0B:67:A1
Reason for this reset: power up

Trying to boot from flash memory

loading ..............................................done.
Verifying CRC (77D79D92)..............................done.

Efficient Networks, Inc. SS5871 (P/N 120-5871-001), Rev 34-06
(S/N 747425)
Now 2769k free before buffers
Interfaces detected
LAN: Ethernet (10BASET HUB)   WAN: IDSL

SpeedStream 5871 IDSL Router (120-5871-001/2) v5.0.0
Copyright (c) 1999-2000 Efficient Networks, Inc.
All Rights Reserved

INIT: buffer pool is 1371632 bytes
ETHERNET/0 interface started, MAC=00:20:6F:0B:67:A1
05/15/2001-10:40:38:ETH: Obtaining an IP address for ETHERNET/
0:3 with DHCP

SpeedStream 5871 IDSL Router (120-5871-001/2) v5.0.0 Ready
Login:
Login: *****
Logged in successfully!
# system history

End System History.
->
```

system httpport

This command manages HTTP port access. It can:

- Disable HTTP for this router (sets the HTTP port to 0).
- Request the default HTTP port (80). This re-enables HTTP after it is disabled.
- Redefine the HTTP port.

☞ **NOTE:**
This command requires a save and reboot to take effect.

To see the current setting, use the command system list. For more information, see "Controlling Remote Management" on page 5-15 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system httpport  default | disabled | <port>
```

Parameters

`default`	Restores the port value to the default value (80) and re-enables the port.
`disabled`	Disables the existing HTTP port.
`<port>`[a]	Defines a new HTTP port number. Use this option to restrict remote access.

[a] Integer

Examples

This command sets the HTTP port to the default value (80).

```
-> system httpport default
```

This command disables the existing HTTP port.

```
-> system httpport disabled
```

This command remaps the HTTP port to port 3333.

```
-> system httpport 3333
```

Response

Command prompt.

system list

Lists the system settings for the target router.

Mgmt Class

Network (R)

Input Format

```
system list
```

Parameters

None

Response

The following is an example of a typical response.

```
-> system list
GENERAL INFORMATION FOR <SOHO>   file systems...done.
  System started on.............. 9/8/2000 at 13:29
  Authentication override........ none  file systems...done.
  WAN to WAN Forwarding.......... no  file systems...done.
  Block NetBIOS Default.......... no  file systems...done.
  BOOTP/DHCP Server address...... none
  Telnet Port.................... default (23)  file
  systems...done.
  Telnet Clients................. all
  SNMP Port...................... default (161)  file
  systems...done.
  SNMP Clients................... all  file systems...done.
  HTTP Port...................... default (80)
  HTTP Clients................... all
  Syslog Port.................... default (514)
  Allowed Syslog Servers......... all
  Default Syslog Servers......... none
  System message:
  Security timer................. 30 minutes
  One WAN Dial Up................ no
  Management feature............. 0
  Rip timer...................... 45
  Backup......................... no (no valid remote profile is
  enabled)
  Retry Interval In Minutes...... 30
      Stability Interval In Minutes.... 3
```

system log

Allows logging of the device's activity in a Telnet session.

Mgmt Class

Admin (R/W)

Input Format

```
system log start | stop | status
```

Parameters

`start`	Initiates monitoring activity.
`stop`	Discontinues monitoring activity.
`status`	Displays all users (yourself included) currently using this feature.

Response

Command prompt.

system modem

Changes the selected modem setting. The modem settings are for the backup asynchronous modem connected to the console port.

For more information on the Dial Backup option, ”Dial Backup” on page 6-7 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system modem reset | escape | init | offhook | dial | answer |
hangup  <string>
```

Parameters

`dial`	Enter one of the following options: `ATDT` ATDT for tone dialing, `ATDP` ATDP for pulse dialing.

`reset <string>`
`escape <string>`
`int <string>`
`offhook <string>`
`answer <string>`
`hangup <string>`
	Commands followed by an ASCII string configures a new setting for the option selected by the first parameter

Examples

The following command changes the string for the *init* setting:

```
-> system modem init  ATS0=0Q0V1&C2&D3&K1X4&H1&I0S12=20
```

The following command selects pulse dialing;

```
-> system modem dial ATDP
```

Response

Command prompt.

system moveiproutingtable

Moves a range of IP addresses to another virtual routing table. The command first looks at the address ranges defined for other virtual routing tables, searching for the addresses to be moved. If it finds addresses to be moved, it deletes them from the address ranges for the other virtual routing tables. The command then adds the specified address range to the virtual routing table named on the command.

To list the routes in the virtual routing tables, use the iproutes command or the remote listiproutes command. For more information, see"Virtual Routing Tables" on page 6-2 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
system moveiproutingtable <first ip addr> [<last ip addr>]
<tablename>
```

Parameters

`<first ipaddr>`[a]	First IP address of the range to be moved.
`<last ipaddr>`[a]	Last IP address of the range to be moved.[b]
`<tablename>`[c]	Name of the virtual routing table to be assigned the address range. The virtual routing table may be new or it may already exist.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.
[c] ASCII string

Examples

With this command, all packets with source addresses in the range 192.168.254.11 through 192.168.254.20 to be routed using virtual routing table MIGUEL. Addresses in that range may already be assigned to other virtual routing tables. Therefore, to delete the addresses from any other virtual routing tables and assign the address range to MIGUEL, enter this command:

```
-> system moveIPRoutingTable 192.168.254.11 192.168.254.20 MIGUEL
```

Response

Command prompt.

system msg

Sets or changes the message saved in the local router you are configuring.

Mgmt Class

System (R/W)

Input Format

```
system msg <message>
```

Parameters

***	Entering the command with no parameter will display the current message or use the command system list.
<message>[a,b]	New message.

[a] ASCII string
[b] Maximum of 255 characters. Space characters are not allowed; use underscore characters instead.

Response

The following is an example response of a message configuration and recall.

```
-> system msg Configured _on_10/21/98
-> system msg
System message: Configured _on_10/21/98
```

system name

Sets or changes the name of the local router being configured.

A name must be assigned to the local router. This name is sent to a remote router during PAP/CHAP Security Authentication.

Mgmt Class

Security (R/W)

Input Format

```
system name <name>
```

Parameters

***	Entering the command with no parameter will display the current router name.
<name>[a,b]	New name of the target router.

[a] ASCII string
[b] The system name is case-sensitive and may be no more than 50 characters.

Example

The following is an example response of name configuration and recall.

```
-> system name Router1
-> system name
System name: <Router1>
```

Response

Command prompt.

system onewandialup

This command can force the router to have no more than one remote connection active at a time. (Multiple links to the same remote are allowed.) To see the current setting, use the command system list and check the One WAN Dial Up line.

This command is useful when security concerns dictate that the router have only one connection active at a time. For example, if set to on, the router cannot connect to both the Internet and another location (such as your company) at the same time.

A connection is only generated when data is forwarded to the remote router (dial-on-demand); Permanent links cannot be automatically generated.

The command allows multiple connections to the SAME location and supports the PPP Multi-Link protocol. To do so, at system startup time, the router examines each remote entry. If it finds only one remote enabled, it leaves the remote enabled. If it finds more than one remote enabled, it disables every entry that does not have a protocol of PPP or PPPLLC. It sets the minimum number of active links (remote minLink) to 0 (zero) on the enabled entries; if the command did not perform this function, connections to multiple destinations would not be possible (since the link to the destination with minLink=non-zero would be active).

This system oneWANdialup command complements the system wan2wanforwarding command. That command allows multiple connections to different locations to be active at the same time but stops traffic from passing from one WAN connection to another.

Mgmt Class

Security (R/W)

Input Format

```
system onewandialup  on | off
```

Parameters

`on`	Enables only one active connection at a time to a remote entry.
`off`	Disables command, allowing WAN connections to multiple locations.

Response

Command prompt.

system passwd

Sets the system authentication password for the target router that is used when the router connects to other routers or is challenged by them. This password is a default password used for all remote sites unless a unique password is explicitly defined for connecting to a remote router with the remote setourpasswd command.

Mgmt Class

Security (R/W)

Input Format

```
system passwd <password>
```

Parameters

`<password>`[a,b] Authentication password of the target router.

[a] ASCII string
[b] The password is case-sensitive and should be no more than 40 characters.

Response

Command prompt.

system riptimer

Sets the duration, in seconds, for Routing Information Protocol (RIP) information to be exchanged with remote routers. For additional information on RIP, refer to the Technical Reference Guide and see “RIP Controls” on page 6-4.

Mgmt Class

Network (R/W)

Input Format

```
system riptimer <seconds>
```

Parameters

`***`	When entered with no parameter, the current setting is displayed.
`<seconds>`[a]	Timer value for RIP information exchange.

[a] Integer, minimum 15 (30)

Response

Command prompt.

system securemode list

Displays the current secure mode configuration values and the number of concurrent Telnet and SSH sessions allowed.

Mgmt Class

Security (R)

Input Format

```
system securemode list
```

Parameters

None

Response

A typical response is shown below.

```
Secure Mode is currently "ENABLED".
WAN interface is currently "UN-TRUSTED".
LAN interface is currently "TRUSTED".
System CLI limit set to 7.
```

system securemode set

Enables and disables secure mode. When secure mode is enabled, management access of the system is allowed only through secure channels for untrusted interfaces. For more information, refer to ”Secure Mode Access” on page 5-18 of the Technical Reference Guide.

Mgmt Class

Security (R/W)

Input Format

```
system securemode set <enable | disable>
```

Parameters

`enable`	Enables secure mode.
`disable`	Disables secure mode.

Response

Typical response indicating the curent mode is displayed.

```
System Secure Mode set to "ENABLED".
```

system securemode set cli

Sets the number of concurrent telnet and SSH sessions allowed by the system.

☞ **NOTE:**
The number of sessions allowed is a system setting and independent of the secure mode state (enabled or disabled).

☞ **NOTE:**
If the number of sessions allowed is set to <*0*>, access to the command line interface will be available only through the serial console connection.

Mgmt Class

Security (R/W)

Input Format

```
system securemode set cli <value>
```

Parameters

`<value>`[a]	Number of Telnet and SSH sessions allowed.

[a] Integer, 0 - 8 (8)

Response

Typical response:

```
System CLI limit set to 7.
```

system securemode set lan

Allows discrete control of the secure mode function on the LAN interface. When secure mode is enabled, the LAN interface can be set to *trusted* and unsecured sessions will still be allowed; *untrusted* will require a secure connection.

☞ **NOTE:**
Changes to this setting are persistent, but not effective unless the secure mode is enabled.

Mgmt Class

Security (R/W)

Input Format

```
system securemode set lan <trusted | untrusted>
```

Parameters

`trusted`[a]	Allows unsecure sessions from the LAN when secure mode is enabled.
`untrusted`	Only secure connections from the LAN are allowed when secure mode is enabled.

[a] Default value

Response

Typical response:

```
System LAN designation set to "TRUSTED".
```

system securemode set wan

Allows discrete control of the secure mode function on the WAN interface. When secure mode is enabled, the WAN interface can be set to *trusted* and unsecured sessions will still be allowed; *untrusted* will require a secure connection.

☞ **NOTE:**
Changes to this setting are persistent, but not effective unless the secure mode is enabled.

Mgmt Class

Security (R/W)

Input Format

```
system securemode set wan <trusted | untrusted>
```

Parameters

`trusted`	Allows unsecure sessions from the WAN when secure mode is enabled.
`untrusted`[a]	Only secure connections from the WAN are allowed when secure mode is enabled.

[a] Default value

Response

Typical response:

```
System WAN designation set to "UN-TRUSTED".
```

system securitytimer

Allows the user to change the 10-minute default security timer to another value. The router automatically logs out a Telnet or console user out of privileged mode when no typing has occurred for the length of time set for the security timer.

- To see the current security timer value, use the system list command.
- To disable the security timer, set the <minutes> value to 0.

Mgmt Class

Security (R/W)

Input Format

```
system securitytimer <minutes>
```

Parameters

`<minutes>`[a]	Timer length in minutes.

[a] Integer

Response

Command prompt.

system selnat addpolicy

Configures selective NAT policies. Selective NAT translation is performed based on destination address defined in the policy. For more information, refer to ”Selective NAT” on page 4-30 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

Two commands are used to create policies; the first (below) specifies translation of the private address, the second will specify no translation is performed.

```
system selnat addpolicy <remote addr> <remote addr mask> trans
<public addr>
```

```
system selnat addpolicy <remote addr><remote addr mask> notrans
```

Parameters

`<remote addr>`[a]	Specifies the destination IP address to which the policy will be applied.
`<remote addr mask>`[a]	Speficies the destination IP network mask to which the policy will be applied.
`<public addr>`[a]	Specifies the resulting public address to which private address will be translated.

[a] Dotted-decimal notation

Examples

This command will create a policy translating the source address to 64.35.6.1 for packets destined for any address in the 12.16.32.0 subnet.

```
-> system selnat addpolicy 12.16.32.0 255.255.255.0 trans
64.35.6.1
```

This command creates a policy that speficies no translation is performed for packets destined for the adress of 10.2.2.2.

```
-> system selnat addpolicy 10.2.2.2 255.255.255.0 notrans
```

Response

Command prompt.

system selnat delpolicy

Deletes an existing selective NAT policy. To view the existing policies, use the system selnat list command.

Mgmt Class

Network (R/W)

Input Format

```
system selnat delpolicy <policy number>
```

Parameters

<policy number>[a]	Number of the policy to be deleted.

[a] Integer

Response

Command prompt.

system selnat list

Lists the current selective NAT policies. Policies are sorted by subnet mask, then listed in ascending order from more-specific to general policies.

Mgmt Class

Network (R)

Input Format

```
system selnat list
```

Parameters

None

Response

Typical response:

```
-> system selnat list
    Remote address          Action
1. 10.2.2.2/255.255.255.255   No Translation
2. 12.16.32.0/255.255.255.0    Transle to 64.35.6.1
3. 0.0.0.0/0.0.0.0             Transle to 12.35.10.1
```

system snmpport

This command manages SNMP port access. It can:

- Disable SNMP for this router (sets the HTTP port to 0).
- Request the default SNMP port (161). This re-enables SNMP after it is disabled.
- Redefine the SNMP port.

☞ **NOTE:**

This command is functionally equivalent to the snmp snmpport command.

☞ **NOTE:**

This command requires a save and reboot to take effect.

To see the current setting, use the command system list. For more information, see "Controlling Remote Management" on page 5-15.

Mgmt Class

Network (R/W)

Input Format

```
system snmpport  default | disabled | <port>
```

Parameters

`default`	Restores the port value to the default value 161 and re-enables the port.
`disable`	Disables the existing SNMP port.
`<port>`[a]	Defines a new SNMP port number. Use this option to restrict remote access.

[a] Integer

Examples

This command sets the SNMP port to the default value (161)

```
-> system snmpport default
```

This command disables the existing SNMP port.

```
-> system snmpport disabled
```

This command remaps the SNMP port to port 1331.

```
-> system snmppport 1331
```

Response

Command prompt.

system sshport

Specifies the port that the SSH server listens on.

Mgmt Class

Security (R/W)

Input Format

```
system sshport <port>
```

Parameters

`default`	Restores the SSH port value to the default value 22 and re-enables the port.
`disable`	Disables the existing SSH port.
`<port>`[a]	Defines a new SNMP port number. Use this option to restrict remote access.

[a] Integer, 1 - 65525 (22)

Examples

This command sets the SSH port to the default value (22)

```
-> system sshport default
```

This command disables the existing SNMP port.

```
-> system sshport disabled
```

This command remaps the SSH port to port 1320.

```
-> system sshport 1320
```

system supporttrace

Provides the ability to capture to a file all the configuration data that Technical Support may need to investigate configuration problems. This exhaustive list command incorporates the following commands:

- system history
- vers
- mem
- system list
- eth list
- dhcp list (if DHCP is enabled)
- remote list
- ifs
- isdn list
- pots list (if this is a POTS device)
- bi (if bridging is enabled)
- ipifs
- iproutes
- ipxroutes

Mgmt Class

Debug (R/W)

Input Format

```
system supporttrace
```

Parameters

None

Response

The following is a typical response:

```
-> system supporttrace

=== HISTORY ===

End System History.

=== VERSION ===
Efficient 7851 SDSL [CM/FR] (120-7851-034) Router
Efficient-5000 BOOT/POST V7.0.101 (19-Apr-01 16:57)
Software version v5.X.Y(irislin).0 built Mon May 7 17:42:01 PDT 2001
Maximum users: unlimited
Options: FRAME RELAY, ASYNC, SDSL, VOICE-TOLLBRIDGE, RFC1483, IP ROUTING,
IP FILTERING, WEB, HW-DES, IPSEC, 3DES, L2TP, ENCRYPT, BRIDGE, IPX,

         CMMGMT, DIAL-BACKUP, VRRP

Up for 0 days 20 hours 53 minutes (started 5/17/2001 at 17:49)
=== MEMORY ===
Amount of RAM installed..  4096 Kbytes
Small buffers used.......  25 (3% of 656 used)
Large buffers used....... 161 (23% of 700 used)
Buffer descriptors used.. 186 (10% of 1695 used)
Number of waiters s/l....   0/0

Table memory allocation statistics:
Sizes      8    16    32    64   128   256   512  1024
Used       7   132    28    90     2    13     7     5
Free       1     1     2     2     1     2     1     1

Sizes   2048  4096  8192
Used      19     9     1
Free       0     1     0
```

```
Total in use: 105080, total free: 968952 (6488 + 962464)

=== PROCESSES ===
TID:          NAME               FL P BOTTOM CURRENT SIZE
  1:IDLE                         02 7 2f6974  2f7880 4080
 24:SENDSIG                      04 3 30ec84  30f368 2032
  3:MSFS_SYNC                    03 6 2f8a04  2f9100 2032
  4:SYSTEM LOGGER                03 5 2fc874  2fcf70 2032
  5:LL_PPP                       03 5 2fb844  2fc738 4080
  6:NL_IP                        03 5 2fddf4  2fe4f0 2032
  7:TL_IP_UDP                    03 3 2fe674  2fed78 2032
  8:TL_IP_TCP                    03 3 2feed4  2ff5d8 2032
  9:TELNETD                      03 5 2ff734  2ffe18 2032
 10:IKE                          03 4 301504  301be8 2000
 11:BOOTP                        03 5 303fd4  3046c0 2032
 12:DUM                          03 5 302964  303850 4080
 13:SDSL                         03 5 304d34  3053d8 2032
 14:CALLCTRL                     03 3 306624  306d18 2032
 15:DSP                          03 3 306e34  307520 2032
 16:SNMPD                        03 5 3055a4  3064a8 4080
 17:CAS                          03 3 3076d4  307dc0 2032
 18:HAPI                         04 2 307ff4  308ed8 4096
 19:HTTPD                        03 5 3090a4  309f58 4080
 20:DNS                          03 5 30a204  30b0b0 4000
 21:SNTP                         03 4 30e454  30eb38 2000
 22:CMD                          01 6 30cf54  30db58 4080
 25:IP_RIP                       03 4 310a94  311190 2032

=== FILE SYSTEM ===
Filesystem 0, size=1714k :
Checking filesystem...
Checking file entries...
  KERNEL   IRI ... 684629 bytes .. ok.
  ASIC     AIC ...  50847 bytes .. ok.
  KEYFILE  DAT ...    768 bytes .. ok.
  SYSTEM   CNF ...   2304 bytes .. ok.
  FRAME    DAT ...      0 bytes .. ok.
  ATOM     DAT ...      0 bytes .. ok.
  DHCP     DAT ...   1280 bytes .. ok.
  SDSL     DAT ...     28 bytes .. ok.
  41DB833E GAN ...    192 bytes .. ok.
  2BC5A0B4 GAN ...    192 bytes .. ok.
```

```
  2BC5A0B4 DHV ...    960 bytes .. ok.
  DSP      DAT ...     28 bytes .. ok.
  USER     BAT ...    462 bytes .. ok.
  41DB833E DHV ...    960 bytes .. ok.
  EF2E6B8F GAN ...    192 bytes .. ok.
  35B2A0B5 GAN ...    192 bytes .. ok.
  35B2A0B5 DHV ...    960 bytes .. ok.
  EF2E6B8F DHV ...    960 bytes .. ok.
  2D4E5524 GAN ...    192 bytes .. ok.
  2D4E5524 DHV ...    960 bytes .. ok.
  FILTER   DAT ...   1284 bytes .. ok.
  KERNEL   F2K ... 684629 bytes .. ok.
  2807 fat(s) used, 590 fat(s) free
  0 fat(s) unused, 0 fat(s) unreferenced, 2 fat(s) reserved
  1437184 bytes used by files, 14848 bytes by tables, 302080 bytes free

=== SYSTEM ===
GENERAL INFORMATION FOR <>
  System started on.................. 5/17/2001 at 17:49
  Authentication override............ none
  WAN to WAN Forwarding.............. yes
  Block NetBIOS Default.............. no
  BOOTP/DHCP Server address.......... none
  Telnet Port........................ default (23)
  Telnet Clients..................... all
  SNMP Port.......................... default (161)
  SNMP Clients....................... all
  HTTP Port.......................... default (80)
  HTTP Clients....................... all
  Syslog Port........................ default (514)
  Allowed Syslog Servers............. all
  Default Syslog Servers............. none
  System message:
  Security timer..................... 10 minutes
  One WAN Dial Up.................... no
  Management feature................. 0
  Rip timer.......................... 45
  Backup............................. no (no valid remote profile is enabled)
    Retry Interval In Minutes........ 30
    Stability Interval In Minutes.... 3

MODEM STRINGS:
```

```
  Reset:    ATZ
  Escape:   +++
  Init:     ATS0=0Q0V1&C1&D0X4S12=20
  Off-Hook: ATH1
  Dial:     ATDT
  Answer:   ATA
  Hangup:   ATH0


=== ETHERNET ===
GLOBAL BRIDGING/ROUTING SETTINGS:
  Bridging enabled..................... no
    Exchange spanning tree with dest... yes
    Bridge only PPPoE with dest........ no
  IP Routing enabled................... yes
    Multicast forwarding enabled....... no
    Firewall filter enabled ........... yes
    Directed Broadcasts Allowed........ no
    RIP Multicast address.............. default
    VRRP Multicast address............. default
  IPX Routing enabled.................. no

ETHERNET INFORMATION FOR <ETHERNET/0>
  Hardware MAC address................. 00:20:6F:09:0C:25
  Send IP RIP to the LAN............... rip-1 compatible
    Advertise me as default router..... yes
  Process IP RIP packets received...... rip-1 compatible
    Receive default route by RIP....... yes
  IP address translation............... no
  IP filters defined................... yes
  IP address/subnet mask............... 192.168.254.254/255.255.255.0
  Management IP address/subnet mask.... 0.0.0.0/0.0.0.0
  Static Ethernet routes defined....... none
  Virtual Ethernet routes defined...... none
  IPX External network number.......... 00000000
  IPX Frame type....................... 802.2
  MTU.................................. default


=== DHCP ===
       BOOTP/DHCP Relay address ..... none
       bootp tftpserver ............. none
       bootp file ................... n/a
```

```
Subnet 192.168.254.0, enabled
       When DHCP servers are active . stop
       Mask ......................... 255.255.255.0
       first ip address ............. 192.168.254.2
       last ip address .............. 192.168.254.20
       lease ........................ default
       bootp ........................ not allowed
       bootp server ................. none
       bootp file ................... n/a

       Client IP          State     Host Name            Expires
       192.168.254.2      enabled   QA-LABPC             Jun 24 2001

=== VOICE ===
VOICE DLCI is 22
Port  Pkts from Network/Dsp  VoiceRate   CallState              ChannelID
  1            0/         0  G711 uLaw   Inactive                    0
  2            0/         0  G711 uLaw   Inactive                    0
  3            0/         0  G711 uLaw   Inactive                    0
  4            0/         0  G711 uLaw   Inactive                    0
  5            0/         0  G711 uLaw   Inactive                    0
  6            0/         0  G711 uLaw   Inactive                    0
  7          198/       570  G711 uLaw   Inactive                    0
  8            0/         0  G711 uLaw   Inactive                    0

=== REMOTE DATABASE ===
INFORMATION FOR <configuredForCMPPlay>
  Status.............................. enabled
  Interface in use.................... FR
  Protocol in use..................... RFC1483 (SNAP) - MAC Encapsulated
Routing
  Data Link Connection Id (DLCI)....... 528
  IP address translation.............. on
  IP filters defined.................. yes
  Send/Receive Multicast.............. off
  Block NetBIOS Packets............... off
  Source IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Remote IP address/subnet mask........ 0.0.0.0/0.0.0.0
  Management IP address/subnet mask.... 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............. no
    Send IP default route if known..... no
  Receive IP RIP from this dest........ no
```

```
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes.............. 1
          0.0.0.0/0.0.0.0/1
  IPX network number.................. 00000000
  Use IPX RIP/SAP (negotiate with PPP): yes
  Total IPX remote routes.............. 0
  Total IPX SAPs...................... 0
  Bridging enabled.................... no
    Exchange spanning tree with dest... yes
    Bridge only PPPoE with dest........ no
  mtu................................. 1500

=== INTERFACES ===
Interface     Speed        In %     Out % Protocol     State
Connection
ETHERNET/0   10.0mb       0%/0%     0%/0% (Ethernet)   OPENED
FR/0          784kb       0%/0%     0%/0% (HDLC/FR)    OPENED
FR-VOICE/1    784kb       0%/0%     0%/0% (CLEAR)      OPENED
CONSOLE/0      57kb       0%/0%     0%/0% (TTY)        OPENED
FR-VC/2       784kb       0%/0%     0%/0% (FR)         OPENED       to
configuredForCMPPlay

=== PPP ===

=== BRIDGING ===
Bridging is disabled
Bridging is disabled

=== ARP TABLE ===
IP Addr              Mac Address             Interface
224.0.0.9            01:00:5E:00:00:09       ETHERNET/0
172.17.32.1          02:20:6F:09:0C:25       FR-VC/2

=== IP ROUTES ===
    IP route   /  Mask   --> Gateway         Interface    Hops Flags

0.0.0.0      /00000000 --> configuredForCMPPlay FR-VC/2 1 NW FW PRM
RP1 RP2
172.17.32.0  /ffffff00 --> configuredForCMPPlay FR-VC/2 1 NW FW DIR
PRM PRV
172.17.32.132  /ffffffff --> configuredForCMPPlay FR-VC/2 0 ME
192.168.254.0  /ffffff00 --> 0.0.0.0      ETHERNET/0   1 NW FW DIR PRM
RP1 RP2
```

```
192.168.254.254/ffffffff --> 0.0.0.0      ETHERNET/0   0 ME
224.0.0.9      /ffffffff --> 0.0.0.0      [none]       0 ME
224.0.0.18     /ffffffff --> 0.0.0.0      [none]       0 ME
255.255.255.255/ffffffff --> 0.0.0.0      [none]       0 NW PRM

=== IP IFS ===
FR-VC/2       172.17.32.132 (FFFFFF00) dest 0.0.0.0 sub 172.17.32.0
              net 172.17.0.0 (FFFF0000) BROADCAST  mtu 1500 mru 4096
              MAC address in use 02:20:6F:09:0C:25
              DHCP - lease good until Jul 24 2137 0:17:23
ETHERNET/0    192.168.254.254 (FFFFFF00) dest 0.0.0.0 sub 192.168.254.0
              net 192.168.254.0 (FFFFFF00) BROADCAST  mtu 1500 mru 1500
              MAC address in use 00:20:6F:09:0C:25

=== IPX ROUTES ===
No IPX sessions are active.

=== IPX SAPS ===
No IPX sessions are active.

=== L2TP TUNNELS ===

=== IP FILTERS ===

Begin IPFilters for configuredForCMPPlay
# watching for dropped/rejected packets is OFF

# Begin rules for input list
remote ipfilter flush  input configuredForCMPPlay
remote ipfilter insert 0 input accept -c 0 -p 50 -da 172.17.32.132 (IKE
Global Filter) configuredForCMPPlay
remote ipfilter insert 1 input accept -c 0 -p 51 -da 172.17.32.132 (IKE
Global Filter) configuredForCMPPlay
remote ipfilter insert 2 input accept -c 0 -p udp -sp 500 -da 172.17.32.132
-dp 500 (IKE Global Filter) configuredForCMPPlay
# End rules for input list

# Begin rules for receive list
remote ipfilter flush  receive configuredForCMPPlay
# End rules for receive list

# Begin rules for transmit list
remote ipfilter flush  transmit configuredForCMPPlay
remote ipfilter insert 0 transmit accept -c 0 -p udp -sa 172.17.32.132 -sp
500 -dp 500 (IKE Global Filter) configuredForCMPPlay
remote ipfilter insert 1 transmit accept -c 0 -p 50 -sa 172.17.32.132 (IKE
```

```
Global Filter) configuredForCMPPlay
remote ipfilter insert 2 transmit accept -c 0 -p 51 -sa 172.17.32.132 (IKE
Global Filter) configuredForCMPPlay
# End rules for transmit list

# Begin rules for output list
remote ipfilter flush  output configuredForCMPPlay
remote ipfilter insert 0 output accept -c 0 -p udp -sa 172.17.32.132 -sp 500
-dp 500 (IKE Global Filter) configuredForCMPPlay
# End rules for output list

End IPFilters for configuredForCMPPlay

Begin IPFilters for (ETHERNET/0)
# watching for dropped/rejected packets is OFF

# Begin rules for input list
eth ip filter flush  input 0
eth ip filter insert 0 input accept -c 0 -p 50 -da 192.168.254.254 (IKE
Global Filter) 0
eth ip filter insert 1 input accept -c 0 -p 51 -da 192.168.254.254 (IKE
Global Filter) 0
eth ip filter insert 2 input accept -c 0 -p udp -sp 500 -da 192.168.254.254
-dp 500 (IKE Global Filter) 0
# End rules for input list

# Begin rules for receive list
eth ip filter flush  receive 0
# End rules for receive list

# Begin rules for transmit list
eth ip filter flush  transmit 0
eth ip filter insert 0 transmit accept -c 0 -p udp -sa 192.168.254.254 -sp
500 -dp 500 (IKE Global Filter) 0
eth ip filter insert 1 transmit accept -c 0 -p 50 -sa 192.168.254.254 (IKE
Global Filter) 0
eth ip filter insert 2 transmit accept -c 0 -p 51 -sa 192.168.254.254 (IKE
Global Filter) 0
# End rules for transmit list

# Begin rules for output list
eth ip filter flush  output 0
eth ip filter insert 0 output accept -c 0 -p udp -sa 192.168.254.254 -sp 500
-dp 500 (IKE Global Filter) 0
# End rules for output list
```

```
End IPFilters for (ETHERNET/0)


=== IPSEC ===
There are no security associations.

=== IKE ===
There are no IKE peers.
There are no IKE proposals.
There are no IKE IPSec Proposals.
There are no IKE IPSec Policies.

=== END OF TECH SUPPORT DATA
```

system syslogport

This command manages Syslog port access. It can:

- Disable syslog port for this router (sets the syslog port to 0).
- Request the default syslog port (514). Re-enables Syslog after it is disabled.
- Redefine the syslog port.

☞ **NOTE:**

This command requires a save and reboot to take effect.

To see the current setting, use the command system list. For more information on configuring the router as a Syslog client, see “Syslog Client” on page 7-1. For more information on restricting port access, see “Controlling Remote Management” on page 5-15.

Mgmt Class

Network (R/W)

Input Format

```
system syslogport default | disabled | <port>
```

Parameters

`default`	Restores the port value to the default value 514 and re-enables the port.
`disable`	Disables the existing Syslog port.
`<port>`[a]	Defines a new Syslog port number. Use this option to restrict remote access.

[a] Integer

Examples

This command sets the Syslog port to the default value (514).

```
-> system syslogport default
```

This command disables the existing Syslog port.

```
-> system syslogport disabled
```

This command remaps the syslog port to port 154.

```
-> system syslogpport 154
```

Response

Command prompt.

system telnetport

This command manages the built-in Telnet server port access. It can:

- Disable Telnet port for this router (sets the Telnet port to 0).
- Request the default Telnet port (23). This re-enables Telnet port after it is disabled.
- Redefine the Telnet port.

☞ **NOTE:**
This command requires a save and reboot to take effect.

To see the current setting, use the system list command.

Mgmt Class

Network (R/W)

Input Format

```
system telnetport default | disabled | <port>
```

Parameters

`default`	Restores the port value to the default value 23 and re-enables the port.
`disabled`	Disables the existing Telnet port.
`<port>`[a]	Defines a new Telnet port number. Use this option to restrict remote access.

[a] Integer

Examples

This command sets the Telnet port to the default value (23).

```
-> system telnetport default
```

This command disables the existing telnet port.

```
-> system telnetport disabled
```

This command remaps the telnet port to port 188.

```
-> system telnetpport 154
```

Response

Command prompt.

system vpnpassthru

Enables and disables VPN pass-through mode. When enabled, multiple concurrent VPNs are allowed.

Mgmt Class

Network (R/W)

Input Format

```
system vpnpassthru enable | disable
```

Parameters

`enable`	Enables the VPN pass-through mode.
`disable`	Disables the VPN pass-through mode.

Response

Command prompt.

system wan2wanforwarding

Allows management of WAN-to-WAN forwarding of data from one WAN link to another.

For example, an employee uses the router at home to access both a company network and the Internet at the same time. To prevent the passing of company information to the Internet, WAN-to-WAN forwarding should be disabled.

To see the current setting for WAN to WAN forwarding, use the command system list.

This `system wan2wanforwarding` command complements the system onewandialup command. That command allows you to limit WAN connections to just one remote location at a time.

Mgmt Class

Network (R/W)

Input Format

```
system wan2wanforwarding on | of
```

Parameters

`on`	Allows data to be forwarded from one WAN link to another WAN link.
`off`	Stops data from being forwarded from one WAN link to another WAN link.

Response

Command prompt.

CHAPTER 5

ETHERNET INTERFACE COMMANDS

The commands in this section begin with the word eth. The commands configure the Ethernet interfaces in your router. You can:

- Set the Ethernet LAN IP address
- Define logical interfaces to provide service to multiple IP subnets
- Manage the contents of the default routing table and any virtual routing tables
- Enable and disable IP routing
- List the current configuration settings

☞ **NOTE:**

In general, these commands require a save and reboot before they take effect. However, changes made to IP filters and to virtual routing tables take effect immediately; the changes are lost, though, if they are not saved before the next reboot.

The Ethernet interface commands found in this section include:

Table 5-1: Ethernet Interface Command Listing

Command	Function
eth ?	Lists the supported keywords.
eth add	Adds a logical interface onto an Ethernet port so that the router can provide service to multiple IP subnets.
eth delete	Deletes a logical interface from an Ethernet port.
eth ip addhostmapping	Remaps a range of local LAN IP addresses to a range of public IP addresses on a per-interface basis.
eth ip addr	Defines the IP address and subnet mask for an Ethernet port or logical interface.

Table 5-1: Ethernet Interface Command Listing (Cont.)

Command	Function
eth ip addroute	Adds a route to the default routing table for the Ethernet interface.
eth ip addserver	This Network Address Translation (NAT) command adds a server's IP address (on the LAN) associated with this interface for a particular protocol.
eth ip bindroute	Adds an Ethernet route to the named IP virtual routing table.
eth ip defgateway	Assigns an Ethernet default gateway for packets whose destination address does not have a route defined.
eth ip delhostmapping	Undoes an IP address/ host translation (remapping) range.
eth ip delroute	Removes a route from the default routing table.
eth ip delserver	Deletes a server entry.
eth ip directbcast	Enables or disables the forwarding of broadcast packets directed to a specific network prefix.
eth ip disable	Disables IP routing across the Ethernet LAN.
eth ip enable	Enables IP routing across the Ethernet LAN.
eth ip filter	Manages the IP filters for the Ethernet interface(s).
eth ip firewall	Enables and disables Ethernet Firewall Filtering.
eth ip mgmt	Assigns to an Ethernet interface an IP address which is to be used for management purposes only and not for IP address translation.
eth ip options	Enables or disables an IP option for the specified Ethernet interface.
eth ip ripmulticast	Changes the multicast address for RIP-1 compatible and RIP-2 packets.
eth ip translate	Controls Network Address Translation on a per-interface basis.
eth ip unbindroute	Removes an Ethernet route from the named IP virtual routing table.
eth ip vrid	Assigns a virtual router ID (VRID) to an Ethernet interface.

Table 5-1: Ethernet Interface Command Listing (Cont.)

Command	Function
eth ipx addr	Sets the IPX network number for the Ethernet LAN connection.
eth ipx disable	Disables IPX routing across the Ethernet LAN.
eth ipx enable	Enables IPX routing across the Ethernet LAN.
eth ipx frame	Sets the frame encapsulation method.
eth list	Lists information about the Ethernet interfaces including the status of bridging and routing, IP protocol controls, and IP address and subnet mask.
eth mtu	Sets the maximum transfer unit for the Ethernet interface.
eth restart	Starts a stopped logical Ethernet interface.
eth start	Starts a stopped logical Ethernet interface.
eth stop	Stops a logical Ethernet interface.
eth vrrp add	Defines a VRRP attribute record for the VRID (virtual router ID).
eth vrrp clear password	Clears the password in a VRRP attribute record for the VRID.
eth vrrp delete	Deletes a VRRP attribute record for the VRID.
eth vrrp list	Lists the VRRP attribute records for the port and shows the status of the VRRP router.
eth vrrp set multicast	Changes the multicast address used for VRRP router announcements.
eth vrrp set option	Specifies the preemption option in a VRRP attribute record for the VRID.
eth vrrp set password	Specifies the password in a VRRP attribute record for the VRID.
eth vrrp set priority	Specifies the priority attribute in a VRRP attribute record for the VRID.
eth vrrp set timeinterval	Specifies the time interval attribute in a VRRP attribute record for the VRID.
eth ip remsrcrouteopt	Adds or removes the source routing option.

eth ?

Lists the supported keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

All (R)

Input Format

```
eth ?
```

Parameters

None

Response

A listing of all the supported Ethernet commands and keywords with a brief description of their function.

eth add

Adds a logical interface onto an Ethernet port so that the router can provide service to multiple IP subnets. The `eth add` command defines the port number and logical interface number. Next, use the eth ip addr command to define the IP subnet that uses the logical interface. For more information, see “IP Subnets” on page 6-1 of the Technical Reference Guide.

☞ **NOTE:**

A logical interface 0 always exists for Ethernet port 0 (and for port 1 in a dual-port router); logical interface 0 cannot be deleted.

Once defined, routes and filters can be created for the new logical interface using the other eth commands in this section. To list the currently defined logical interfaces, use the eth list command. To remove a logical interface, use an eth delete command.

☞ **NOTE:**

This command requires a save and reboot before it takes effect.

Mgmt Class

Network (R/W)

Input Format

```
eth add <port#>:<logical#>
```

Parameters

`<port#>`[a]	Ethernet interface to add logical port value.
`<logical#>`[b]	New logical interface number.

[a] 0 for a single-port router; 0 or 1 for a dual-port router.
[b] Integer, value cannot = 0; logical interface 0 always exists.

Example

In the following example, logical interface 1 is added to Ethernet port 0:

```
-> eth add 0:1
```

Response

Command prompt.

eth delete

Deletes a logical interface from an Ethernet port. For more information, see “IP Subnets” on page 6-1 of the Technical Reference Guide.

When a logical interface is deleted, all information defined for that interface, such as routes and filters, is deleted automatically.

☞ **NOTE:**

This command takes effect immediately; however, if the change is not saved before the next reboot, the deletion is lost and the deleted interface reappears after the reboot.

Once defined, routes and filters can be created for the new logical interface using the other eth commands in this section. To list the currently defined logical interfaces, use the eth list command. To remove a logical interface, use an eth delete command.

Mgmt Class

Network (R/W)

Input Format

```
eth delete <port#>:<logical#>
```

Parameters

`<port#>`[a]	Ethernet interface from which logical port will be deleted
`<logical#>`[b]	Logical interface number to be deleted.

[a] 0 for a single-port router; 0 or 1 for a dual-port router.
[b] Integer, value cannot = 0; logical interface 0 always exists.

Example

In the following example, logical interface 1 is deleted from Ethernet port 0:

```
-> eth delete 0:1
```

Response

Command prompt.

eth ip addhostmapping

Remaps a range of local LAN IP addresses to a range of public IP addresses on a per-interface basis. These local addresses are mapped one-to-one to the public addresses. For more information, see “Host Remapping” on page 4-23 of the Technical Reference Guide.

☞ **NOTE:**

The range of public IP addresses is defined by `<first public addr>` only. The rest of the range is computed automatically (from `<first public addr>` to `<first public addr>` + number of addresses remapped - 1) inclusive.

Mgmt Class

Network (R/W)

Input Format

```
eth ip addhosthapping <first private addr> <second private
addr> <first public addr> <interface>
```

Parameters

`<first public addr>`[a]	First IP address of the range of IP addresses.
`<second public addr>`[a]	Last IP address of the range of IP addresses.
`<first public addr>`[a]	Defines the range of public IP addresses. The rest of the range is computed automatically.
`<interface>`[b,c]	Defines the target Ethernet interface.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Example

Typical usage:

```
-> eth ip addHostMapping 192.168.207.40 192.168.207.49 10.0.20.11 1
```

Response

Command prompt.

eth ip addr

Defines the IP address and subnet mask for an Ethernet port or logical interface.

Mgmt Class

Network (R/W)

Input Format

```
eth ip addr <ipaddr> <ipnetmask> [<interface>]
```

Parameters

`<ip addr>`[a]	Ethernet LAN IP address.
`<ipnetmask>`[a]	IP network mask.
`<interface>`[b,c]	Ethernet interface.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Example

The following command sets the IP address and subnet mask for the default Ethernet interface (0:0):

```
-> eth ip addr 192.168.1.254 255.255.255.0
```

The following command sets the IP address and subnet mask for logical interface 1 on Ethernet port 0:

```
-> eth ip addr 10.0.27.1 255.255.255.0 0:1
```

Response

Command prompt.

eth ip addroute

Adds a route to the default routing table for the Ethernet interface. This command is needed only if the system does not support RIP (see “RIP Controls” on page 6-4 of the Technical Reference Guide and the eth ip options command).

☞ **NOTE:**

This command requires a save and reboot before it takes effect.

Mgmt Class

Network (R/W)

Input Format

```
eth ip addroute <ipaddr> <ipnetmask> <gateway> <hops>
[<interface>]
```

Parameters

`<ip addr>`[a]	Ethernet LAN IP address.
`<ipnetmask>`[a]	IP network mask.
`<gateway>`[a]	IP address of the IP gateway.
`<hops>`[b]	Number of routers the packet will pass to get to its destination.
`<interface>`[c,d]	Ethernet interface through which the packet is sent.

[a] Dotted-decimal notation
[b] Integer
[c] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[d] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Examples

The following command adds a route to the default routing table for the default Ethernet interface (0:0):

```
-> eth ip addRoute 10.1.2.0 255.255.255.0 192.168.1.17 1
```

The following command adds a route to the default routing table for logical interface 1 on Ethernet port 0:

```
-> eth ip addRoute 10.1.3.0 255.255.255.0 10.0.27.20 1 0:1
```

Response

Command prompt.

eth ip addserver

This Network Address Translation (NAT) command adds a server's IP address (on the LAN) associated with this interface for a particular protocol. For more information, see "Network Address Translation (NAT)" on page 4-17 of the Technical Reference Guide.

To delete a server designation, use the command eth ip delserver.

Mgmt Class

Network (R/W)

Input Format

```
eth ip addserver <action> <protocol> <first port> [<last port>
[<first private port>]] <interface>
```

Parameters

`<action>`	One of the following command actions:	
	`<ipaddr>`[a]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.
`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[b]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the Ethernet interface. Port used by the selected server.	
	`<portid>`[c]	Numerical port value; a value of 0 matches any port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypertext Transfer Protocol (HTTP) port.

[a] Dotted-decimal notation
[b] Integer
[c] Integer, 0 - 65,535

Parameters Cont.

`smtp`	Simple Mail Transfer Protocol (SMTP) port.
`snmp`	Simple Network Management Protocol (SNMP) port.
`t120`	T.120 port.
`telnet`	Telnet port.
`tftp`	Trivial File Transfer Protocol (TFTP) port.
`all`	All ports.

`<last port>` — Optional, last port in the range of ports as seen by the remote end for the server on the LAN.

`<first private port>`[c] — If specified, this is a port remapping of the incoming requests from the Ethernet interface.

`<interface>`[a,b,c] — Ethernet interface.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth ip bindroute

Adds an Ethernet route to the named IP virtual routing table.

Duplicate routes are not allowed within a routing table. However, identical routes may be added to different routing tables. For example, the same route may be added to a virtual routing table and to the default routing table.

To list the routes, use the iproutes command. To remove an Ethernet route from a virtual routing table, use the eth ip unbindroute command.

☞ **NOTE:**

A route change in an IP virtual routing table takes effect immediately. However, the change is lost if it is not saved before the next reboot.

Mgmt Class

Network (R/W)

Input Format

```
eth ip bindroute <ipaddr> <ipnetmask> <hops> [<gateway>]
<tablename> [<interface>]
```

Parameters

<ip addr>[a]	Ethernet LAN IP address.
<ipnetmask>[a]	IP network mask.
<hops>[b]	Number of routers through which the packet must go to get to its destination.
<gateway>[a]	IP address of the IP gateway.
<tablename>[c]	IP virtual routing table o which the route is added.
<interface>[d,e]	Ethernet interface through which the packet is sent.

[a] Dotted-decimal notation
[b] Integer
[c] ASCII string
[d] This parameter may be omitted if the router has only one Ethernet interface.
If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[e] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Example

The following commands add a route for IP address 10.1.2.0/255.255.255.0 to four routing tables: ROSA, MIGUEL, FRANCISCO, and the default routing table. The first two routes are for Ethernet interface 0:1 and use gateway 192.168.252.9; the second two are for the default Ethernet interface (0:0) and, therefore, specify another gateway (192.168.252.7):

```
-> eth ip bindroute 10.1.3.0 255.255.255.0 1 192.168.252.9 ROSA 0:1

-> eth ip bindroute 10.1.3.0 255.255.255.0 1 192.168.252.9 MIGUEL 0:1

-> eth ip bindroute 10.1.3.0 255.255.255.0 1 192.168.252.7 FRANCISCO

-> eth ip addroute 10.1.3.0 255.255.255.0 1 192.168.252.7
```

Response

Command prompt.

eth ip defgateway

Assigns an Ethernet default gateway for packets whose destination address does not have a route defined.

This setting is most useful when IP routing is not enabled, in which case the system acts as an IP host (i.e., an end system, as opposed to an IP router).

☞ **NOTE:**

This command requires a save and reboot before it takes effect.

☞ **NOTE:**

The following command is recommended instead of the eth ip defgateway command. It sends packets for all IP addresses to the specified gateway:

```
-> eth ip addRoute 0.0.0.0 255.255.255.0 <gateway> 1
```

Mgmt Class

Network (R/W)

Input Format

```
eth ip defgateway <ipaddr> [<interface>]
```

Parameters

`<ip addr>`[a]	Ethernet LAN IP address.
`<interface>`[b,c]	Ethernet interface through which the packet is sent.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth ip delhostmapping

Undoes an IP address/ host translation (remapping) range that was previously established with the command eth ip addhostmapping on a per-interface basis. For more information, see “Host Remapping” on page 4-23 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
eth ip delhostmapping <first private addr> <second private
addr> <first public addr> <interface>
```

Parameters

`<first public addr>`[a]	First IP address of the range of IP addresses.
`<second public addr>`[a]	Last IP address of the range of IP addresses.
`<first public addr>`[a]	Defines the range of public IP addresses. The rest of the range is computed automatically.
`<interface>`[b,c]	Defines the target Ethernet interface.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface.
If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Example

Typical usage:

```
-> eth ip delHostMapping 192.168.207.40 192.168.207.49 10.0.20.11 1
```

Response

Command prompt.

eth ip delroute

Removes a route from the default routing table that was added using the eth ip addroute command.

The route to be deleted is identified by its IP address and mask and its Ethernet interface. To see the remaining routes, use the iproutes command.

☞ **NOTE:**
This command requires a save and reboot before it takes effect.

Mgmt Class

Network (R/W)

Input Format

```
eth ip addroute <ipaddr> <ipnetmask> [<interface>]
```

Parameters

`<ip addr>`[a]	Ethernet LAN IP address.
`<ipnetmask>`[a]	IP network mask.
`<interface>`[b,c]	Ethernet interface.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Examples

The following command deletes the route for IP address 10.9.2.0/255.255.255.0 for the default Ethernet interface (0:0).

```
-> eth ip delroute 10.9.2.0 255.255.255.0
```

The following command deletes the route for IP address 10.1.3.0/255.255.255.0 for the Ethernet interface 0:1.

```
-> eth ip delroute 10.1.3.0 255.255.255.0 0:1
```

Response

Command prompt.

eth ip delserver

Deletes an entry created by the command eth ip addserver.

Mgmt Class

Network (R/W)

Input Format

```
eth ip delserver <action> <protocol> <first port> [<last port>
[<first private port>]] <interface>
```

Parameters

`<action>`	One of the following command actions:	
	`<ipaddr>`[a]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.
`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[b]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the Ethernet interface. Port used by the selected server.	
	`<portid>`[c]	Numerical port value; a value of 0 matches any port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypertext Transfer Protocol (HTTP) port.
`<action>`	One of the following command actions:	
	`<ipaddr>`[d]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.

[a] Dotted-decimal notation
[b] Integer
[c] Integer, 0 - 65,535
[d] Dotted-decimal notation

Parameters Cont.

`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[a]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the Ethernet interface. Port used by the selected server.	
	`<portid>`[b]	Numerical port value; a value of 0 matches any port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypettext Transfer Protocol (HTTP) port.
	`smtp`	Simple Mail Transfer Protocol (SMTP) port.
	`snmp`	Simple Network Management Protocol (SNMP) port.
	`t120`	T.120 port.
	`telnet`	Telnet port.
	`tftp`	Trivial File Transfer Protocol (TFTP) port.
	`all`	All ports.
`<last port>`	Optional, last port in the range of ports as seen by the remote end for the server on the LAN.	
`<first private port>`[c]	If specified, this is a port remapping of the incoming requests from the Ethernet interface.	
`<interface>`[a,c,d]	Ethernet interface.	

[a] Integer
[b] Integer, 0 - 65,535
[c] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[d] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth ip directbcast

Enables or disables the forwarding of broadcast packets directed to a specific network prefix. When forwarding is disabled, the router silently discards all packets broadcast to a subnet. The default is off; thus, by default, all network prefix-directed broadcast packets are discarded. This applies to all broadcast interfaces, including all Ethernet interfaces.

A network prefix-directed broadcast address is the broadcast address to a particular network. For example, if a network's IP address is 192.168.254.254 and its mask is 255.255.255.0, its network prefix-directed broadcast addresses are 192.168.254.0 and 192.168.254.255.

This feature is independent of the IP firewall and IP filtering features. However, it does require that IP routing be enabled (see eth ip enable). To see the current settings for IP routing and directed broadcasts, use the eth list command.

Mgmt Class

Network (R/W)

Input Format

```
eth ip directedbcast on | off
```

Parameters

`on`	Enables the forwarding of packets broadcast to a subnet.
`off`	Disables the forwarding of packets broadcast to a subnet.

Response

Command prompt.

eth ip disable

Disables IP routing across the Ethernet LAN. This commands acts as a master switch allowing you to disable all IP routing for testing or control purposes.

☞ **NOTE:**

This command requires a save and reboot before it takes effect.

Mgmt Class

Network (R/W)

Input Format

```
eth ip disable
```

Parameters

None

Response

Command prompt.

eth ip enable

Enables IP routing across the Ethernet LAN. This command acts as a master switch allowing you to re-enable all IP routing.

☞ **NOTE:**
This command requires a save and reboot before it takes effect.

Mgmt Class

Network (R/W)

Input Format

```
eth ip enable
```

Parameters

None

Response

Command prompt.

eth ip filter

Manages the IP filters for the Ethernet interface(s). The filters are used to screen IP packets.

Each Ethernet interface can have its own set of filters. The intended interface is designated at the end of the filter command. If the router has two physical Ethernet interfaces (an Ethernet hub router), the interface is designated by its port number (0 or 1). If logical interfaces have been defined to provide service to multiple IP subnets, the logical interface number is also specified (port #:<logical #, for example, 0:1).

Each interface can have filter lists that are applied at up to four points in the process: Input, Receive, Transmit, and Output. For more information on how and when the filter types are applied, refer to "IP Filtering" on page 5-23 of the Technical Reference Guide.

☞ **NOTE:**

IP filters take effect immediately upon entry. They can even affect the current connection that you are using to enter commands. Unlike other configuration changes, you do not need to save and reboot or restart.

Mgmt Class

Security (R/W)

Input Format

```
eth ip filter <command> <type> <action> [<parameters>]
[<interface>]
```

The following <commands> are provided for managing IP filters for an Ethernet interface:

eth ip filter append

eth ip filter append [<line number>] <type> <action> [<parameters>] [<interface>]

Appends a filter to the list of filters for this `<type>` and `<interface>`. The filter is specified by the `<action>` and optional `<parameters>`.

If no line number is specified, the filter is appended to the end of the list; otherwise, it is appended after the specified line. For example, "`append 0`" appends the filter after line 0. Filters are used in the order they appear in their list.

eth ip filter insert

```
eth ip filter insert [<line number>] <type> <action>
<parameters> [<interface>]
```

Inserts a filter in the list of filters for this <type> and <interface>. The filter is specified by the <action> and optional <parameters>.

If no line number is specified, the filter is inserted at the beginning of the list; otherwise, it is inserted before the specified line. For example, "*insert 0*" inserts the filter before line 0 so it is the first filter in the list. Filters are used in the order they appear in their list.

eth ip filter delete

```
eth ip filter delete <type> <action> <parameters> [<interface>]
```

Deletes the first filter that matches the filter specified on the command.

eth ip filter flush

```
eth ip filter flush [<first line> [<last line>]] <type>
[<interface>]
```

Deletes a range of filters from the list for this <type> and <interface>.

If no line numbers are specified, all filters in the list are deleted. If only the first line number is specified, all filters from that line to the end are deleted. To see the current filter list, use the eth ip filter list command. Filters are used in the order they appear in their list.

eth ip filter clear

```
eth ip filter clear [<first line> [<last line>]] [<type>]
<clear arg> [<interface>]
```

Resets the counters for the specified filters. A filter has a counter if the *-c* parameter was specified when the filter was defined.

You can specify the filters whose counters are to be reset by their line number range and type (input, output, or forward). If no <*type*> is specified, the counters for all filters for the interface are reset. If no line numbers are specified, the counters for all filters for that type and interface are reset. If only the first line number is specified, all counters for filters from that line to the end of the list are reset. To see the line numbers and counters, use the eth ip filter list command.

eth ip filter check

```
eth ip filter check <type> <parameters> [<interface>]
```

Checks the action that would be taken if a packet with the specified parameters was compared with the list of filters defined for the specified `<type>` and `<interface>`. For example, the command:

```
-> eth ip filter check input -p TCP 1
```

would check what action (accept, drop, reject, inipsec, outipsec) would be taken for a TCP packet after it was compared with the list of input filters defined for port 1.

eth ip filter list

```
eth ip filter list <type> [<interface>]
```

Lists all filters of the specified `<type>` defined for the specified `<interface>`.

eth ip filter watch

```
eth ip filter watch <on | off> [-q | -v] [<interface>]
```

Enables or disables the console watch for the interface. If the watch is on, a message is printed to the console serial port when a packet is dropped or rejected. (The message is also sent to any Syslog servers; see “Syslog Client” on page 7-1.)

However, if the parameter *-q* (quiet) was specified for a filter, no message is printed when that filter matches a packet. If the parameter *-v* (verbose) was specified for a filter, a message is printed whenever that filter matches a packet, regardless of the filter <*action*>.

To see the messages, Telnet to the router and enter system log start. The watch does not continue after a reboot; to resume the watch after a reboot, you must enter the eth ip filter watch *on* command again.

Parameters

The filter <*type*> specifies at which point the filter is compared to the IP packet (see the illustration under “Filters and Interfaces” on page 5-23 of the Technical Reference Guide.):

`input`	When the packet enters the interface, *before* any network address translation is performed.
`receive`	When the packet enters the interface, *after* any network address translation, but before routing table processing.
`transmit`	After routing table processing, *before* any network address translation before the packet is sent out.
`output`	After routing *and* network address translation, just before the packet is sent out.

If the packet matches the filter, the specified <*action*> is performed:

`accept`	The packet is allowed to proceed for further processing.
`drop`	The packet is discarded, without sending an ICMP (Internet Control Management Protocol) error message.
`reject`	The packet is discarded and an ICMP error message is returned to the sender.
`inipsec`	The packet is passed to IPSec for decrypting. The filter is intended to match packets coming from the other IPSec gateway. Although filters are the mechanism by which packets are passed to IPSec, it is recommended that you use IKE to manage your IP Security (see "IPSec (Internet Protocol Security)" on page 5-50.)
`outipsec`	The packet is passed to IPSec so it can be encrypted and sent to the other IPSec gateway. The filter is intended to match packets coming from the local protected network. Although filters are the mechanism by which packets are passed to IPSec, it is recommended that you use IKE to manage your IP Security (see "IPSec (Internet Protocol Security)" on page 5-50.)

The following parameters specify the characteristics that an IP packet must have in order to match the filter. A filter can require any or all of these characteristics.

`-p <protocol> | TCP | UDP | ICMP`

The packet must have the specified protocol. If no protocol is specified, the filter matches every protocol.

`-sa <first source ip addr>[:<last source ip addr>]`

The packet must have a source IP address within the specified address range. If only one address is specified, the packet must have that source IP address. If no source IP address is specified, the filter matches any address in the range 0.0.0.0:255.255.255.255.

`-sm <source ip mask>`

The filter uses the specified mask when comparing the <first source ip addr>...<last source ip addr> with the source IP address in the IP packet. If no source mask is specified, the mask used is 255.255.255.255.

`-sp <ICMP type> | <first source port>[:<last source port>]`

The packet must have a source port that matches the specified ICMP type or that is within the specified port range. If only one port is specified, the packet must have that source port. If no source port is specified, the filter matches any source port in the range 0:0xffff.

`-da <first dest ip addr>[:<last dest ip addr>]`

The packet must have a destination IP address within the specified address range. If only one address is specified, the packet must have that destination IP address. If no destination IP address is specified, the filter matches any address in the range 0.0.0.0:255.255.255.255.

`-dm <dest ip mask>`

The filter uses the specified mask when comparing the <first dest ip addr>...<last dest ip addr> with the destination IP address in the IP packet. If no destination mask is specified, the mask used is 255.255.255.255.

`-dp <ICMP type> | <first dest port>[:<last dest port>]`

The packet must have a destination port that matches the specified ICMP type or that is within the specified port range. If only one port is specified, the packet must have that destination port. If no destination port is specified, the filter matches any destination port in the range 0:0xffff.

`-tcp syn | ack | noflag | rst`

If the IP packet is a TCP packet, the filter matches the packet only if the packet flag settings are as specified. If no *-tcp* option is specified for the filter, flag settings are not checked.

☞ **NOTE:**

More than one -tcp option may be specified for the IP filter.

The syn, ack, and noflag settings work together as follows:

- Specify `-tcp syn` if the TCP SYN flag must be set.
- Specify `-tcp ack` if the TCP ACK flag must be set
- Specify `-tcp noflag` if neither the SYN flag nor the ACK flag can be set.

For example, for the IP filter to match the initiation of a TCP connection, specify *-tcp syn*. The filter will match TCP packets that have the TCP SYN flag set but not the TCP ACK flag set. For the filter to match the response to initiation of a TCP connection, specify *-tcp syn and -tcp ack*. The filter will match only TCP packets with both the TCP SYN and TCP ACK flags set.

The *-tcp rst* setting is independent of the others; if you specify *-tcp rst* for the filter, the filter matches every TCP packet with the TCP RESET flag set, regardless of the other flag settings. For example, for the filter to match packets for “established” connections, you would specify both *-tcp rst and -tcp ack* so that the filter is applied to every TCP packet that has either the RESET flag or the ACK flag set.

The following <*parameter*>s request additional filter options.

`-b`

This option requests that this filter be compared twice with each packet. The first time the source filter information is matched against the source information in the IP packet and the destination filter information is matched against the destination information in the IP packet. The second time the source filter information is matched against the destination information in the IP packet and the destination filter information is matched against the source information in the IP packet.

`-c <count of times rule used>`

This option requests a counter for this filter. If specified, a count is kept of how many IP packets have matched this filter since the router was rebooted. To see the current count for a filter, use the eth ip filter list command. To clear a counter, use the eth ip filter clear command.

`-ipsec <IPSec record name>`

Use this option when the action specified is inipsec or outipsec. It specifies the IPSec Security Association that uses the filter.

`- q` *or* `-v`

Specify one of these options to determine when watch messages are sent for this filter. The messages are sent to the console serial port (and to any Syslog servers; see "Syslog Client" on page 7-1.)
If neither `-q` or `-v` are specified for the filter, and an eth ip filter watch on command is entered for the interface, a message is sent each time this filter causes a packet to be dropped or rejected.

If *-q* (quiet) is specified, no messages are printed for this filter, even if the filter causes a packet to be dropped or rejected.

If *-v* (verbose) is specified, a message is printed every time this filter matches a packet, regardless of the filter action.

The optional <*interface*> determines which Ethernet interface the filter applies to.

If the router has only one Ethernet interface, <*interface*> may be omitted.

If the router has two physical Ethernet interfaces (that is, a dual-port router), you must specify the port by its number (*0* or *1*).

If logical interfaces have been defined for the physical Ethernet interface, the port number and the logical interface number are specified (<*port #*>:<*logical #*>, for example, *0:1*).

Examples

This command example clears all filters from the Input filter list for Ethernet interface 0. Use this command as the first command in a list of commands starting a new Input filter list.

```
-> eth ip filter flush input 0
```

This command example prevents the forwarding of all IP traffic. If you put these filters at the end of the filter lists, they will stop all packets that have not matched filters earlier in the lists.

```
-> eth ip filter append receive drop
-> eth ip filter append transmit drop
```

Response

Command prompt

eth ip firewall

The router supports IP Internet Firewall Filtering to prevent unauthorized access to your system and network resources from the Internet. This filter discards packets received from the WAN that have a source IP address recognized as a local LAN address. This command sets Ethernet Firewall Filtering *on* or *off* and allows you to list the active state.

This command requires a save and reboot before it takes effect.

To perform Firewall Filtering, IP routing must be *enabled*. For more information, see "IP Filtering" on page 5-23 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
eth ip firewall on | off | list
```

Parameters

`on`	Enables firewall filtering. IP routing must also be enabled for filtering to be performed.
`off`	Disables the firewall filtering feature.
`list`	Lists the current status of firewall filtering.

Response

The following is a typical response when the `list` parameter is entered:

```
-> eth ip firewall list
The Internet firewall filter is currently on.
0 offending packets were filtered out.
```

eth ip mgmt

Assigns to an Ethernet interface an IP address which is to be used for management purposes only and not for IP address translation. This management IP address is generally a private network address used solely by the ISP.

The management IP address is separate from the IP address used for IP address translation. The IP address used for address translation is generally a public IP address valid on the Internet. It is set by the eth ip addr command.

☞ **NOTE:**

The management address is not effective until after the next save and reboot.

☞ **NOTE:**

To use the management address as the source address for a ping, you must specify it using the *-I* option on the ping command. For example, to use management address 192.168.1.2 when pinging destination address 192.168.100.100, specify:

```
ping -I 192.168.1.2 192.168.100.100
```

☞ **NOTE:**

To use the management address as the source address for a copy, you must specify both the source and destination addresses on the copy command.

To list the current management address for the Ethernet interface, if any, use the eth list command. To set a management address for the WAN interface, see remote setmgmtipaddr.

Mgmt Class

Network (R/W)

Input Format

```
eth ip mgmt <ipaddr> <ipnetmask> [<interface>]
```

Parameters

`<ip addr>`[a]	Ethernet IP address.
`<ipnetmask>`[a]	IP subnet mask.
`<interface>`[b,c]	Ethernet interface.

[a] Dotted-decimal notation
[b] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[c] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Example

```
-> eth ip mgmt 10.0.0.1 255.255.255.0 0:1
-> save
-> reboot
```

Response

Command prompt.

eth ip options

Enables or disables an IP option for the specified Ethernet interface. The IP options include:

- Options to transmit or receive RIP-1 and/or RIP/2 packets. (see “RIP Controls” on page 6-4 of the Technical Reference Guide.)
- Option to advertise this router as the default router.
- Option to enable forwarding of IP multicast traffic.

☞ **NOTE:**
This command is not effective until after save and reboot commands have been performed.

Mgmt Class

Network (R/W)

Input Format

```
eth ip options <option> on | off [<interface>]
```

Parameters

`<option>`	Must be one of the following:.	
	`rxrip`	Receive and process IP RIP-1 compatible and RIP-2 broadcast packets from the Ethernet LAN. Also receive and process RIP-2 packets that are multicast as defined by the eth ip ripmulticast command. Set this option if the local router is to discover route information from the Ethernet LAN. The default is *on*.
	`rxrip1`	Receive and process RIP-1 packets only.
	`rxrip2`	Receive and process RIP-2 packets only.
	`rxdef`	Receive the default route address from the Ethernet LAN. The default is on. This option is useful if you do not want to configure your router with a default route.
	`txrip`	Transmit RIP-1 compatible broadcast packets and RIP-2 multicast packets over the Ethernet LAN. The default is *on*.
	`txrip1`	Transmit broadcast RIP-1 packets only.
	`txrip2`	Transmit broadcast RIP-2 packets only.
	`txdef` `advfr`	Advertise this router as the default router over the Ethernet LAN (provided it has a default route). The default is *on*. Set this to off if another router on the local LAN is the default router.
	`multicast`	Enables this Ethernet interface to forward IP multicast traffic.
`<interface>`[a,b]		Ethernet interface.

[a] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.

[b] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth ip ripmulticast

Changes the multicast address for RIP-1 compatible and RIP-2 packets. The default address is 224.0.0.9. For more information, see “RIP Controls” on page 6-4 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
eth ip ripmulticast <ipaddr>
```

Parameters

`<ip addr>`[a]	IP address of the remote network or station.

[a] Dotted-decimal notation

Response

Command prompt.

eth ip translate

Controls Network Address Translation on a per-interface basis; it allows several PCs to share a single IP address to the Internet. To read more about NAT, refer to "Network Address Translation (NAT)" on page 4-17 of the Technical Reference Guide.

Mgmt Class

Network (R/W)

Input Format

```
eth ip translate on | off | <interface>
```

Parameters

`on` `off`	Indicates whether Network Address Translation is on or off for this Ethernet interface.
`<interface>`[a,b]	Ethernet interface.

[a] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.

[b] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Examples

The following command enables Network Address Translation for port 0.

```
-> eth ip translate on
```

The following command disables Network Address Translation for logical interface 0:1.

```
-> eth ip translate off 0:1
```

Response

Command prompt.

eth ip unbindroute

Removes an Ethernet route from the named IP virtual routing table. To list the routes, use the command iproutes. To add an Ethernet route to a virtual routing table, use the command eth ip bindroute.

☞ **NOTE:**
A route change in an IP virtual routing table takes effect immediately. However, the change is lost if it is not saved before the next reboot.

To list the current management address for the Ethernet interface, if any, use the eth list command. To set a management address for the WAN interface, see remote setmgmtipaddr.

Mgmt Class

Network (R/W)

Input Format

```
eth ip unbindroute <ipaddr> <tablename> [<interface>]
```

Parameters

`<ip addr>`[a]	Ethernet LAN IP address.
`<tablename>`[b]	IP virtual routing table from which the route is removed.
`<interface>`[c,d]	Ethernet interface.

[a] Dotted-decimal notation
[b] ASCII string
[c] This parameter may be omitted if the router has only one Ethernet interface. If the router has two physical Ethernet interfaces (an Ethernet hub router), the port number (0 or 1) must be specified.
[d] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Example

The following commands remove Ethernet routes from virtual routing table ROSA. The first deleted route is for IP address 10.1.2.0 and the default Ethernet interface (0:0). The second deleted route is for IP address 10.1.3.0 and the logical Ethernet interface 0:1

```
-> eth ip unbindRoute 10.1.2.0 ROSA

-> eth ip unbindRoute 10.1.3.0 ROSA 0:1
```

Response

Command prompt.

eth ip vrid

Assigns a virtual router ID (VRID) to an Ethernet interface. The same VRID must be assigned to the master router and its backup routers. For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

This command designates the interface as the VRRP interface for the router. You must use another logical Ethernet interface as the management interface for the router. To create a new logical Ethernet interface, use the command eth add and then assign it an IP address with an eth ip addr command.

☞ **NOTE:**

The assignment takes effect after a save the change and restart the interface or reboot the router.

After assigning the VRID, its attributes may be specified with the *eth vrrp* commands (see eth vrrp add).

If you delete the VRID (eth vrrp delete), the VRRP interface designation is cleared. You can also clear the VRRP interface designation by entering the eth ip vrid command with *0* as the VRID.

Mgmt Class

Network (R/W)

Input Format

```
eth ip vrid <vrid> [<interface>]
```

Parameters

`<vrid>`[a]	Virtual route ID.
`<interface>`[b]	Ethernet interface. The default value is *0:0*.

[a] Integer, 1 - 255
[b] To specify a logical interface other than 0:0, specify both the port number (0 or 1) and the logical interface number using the format <port #>:<logical #> (for example, 0:1).

Example

This command example assigns VRID 7 to the logical Ethernet interface 0:1.

```
-> eth ip vrid 7 0:1
```

This command example clears the VRRP interface designation from interface 0:1.

```
-> eth ip vrid 0 0:1
```

Response

Command prompt.

eth ipx addr

Sets the IPX network number for the Ethernet LAN connection.

Mgmt Class

Network (R/W)

Input Format

```
eth ipx addr <ipxnet> [port#]
```

Parameters

`<ipxnet>`[a]	IPX network number.
`<port>`[b]	Port number of the Ethernet LAN.

[a] 8 hexadecimal characters.
[b] Integer, 0, 1 or it may be omitted.

Response

Command prompt.

eth ipx disable

Disables IPX routing across the Ethernet LAN. This acts as a master switch allowing you to disable IPX routing for testing or control purposes.

☞ **NOTE:**

This command requires a reboot.

Mgmt Class

Network (R/W)

Input Format

```
eth ipx disable [port#]
```

Parameters

`<port>`[a] Port number of the Ethernet LAN.

[a] Integer, 0, 1 or it may be omitted.

Response

Command prompt.

eth ipx enable

Enables IPX routing across the Ethernet LAN. This acts as a master switch allowing you to enable IPX routing.

☞ **NOTE:**

This command requires a reboot.

Mgmt Class

Network (R/W)

Input Format

```
eth ipx enable [port#]
```

Parameters

`<port>`[a] Port number of the Ethernet LAN.

[a] Integer, 0, 1 or it may be omitted.

Response

Command prompt.

eth ipx frame

Sets the frame encapsulation method.

Mgmt Class

Network (R/W)

Input Format

```
eth ipx enable <type>
```

Parameters

`<type>`	802.2 (DEC standard).[a]
	802.3 (Intel standard).
	dix (Xerox/Ethernet II standard).

[a] Default value

Response

Command prompt.

eth list

Lists information about the Ethernet interfaces including the status of bridging and routing, IP protocol controls, and IP address and subnet mask.

Mgmt Class

Network (R)

Input Format

```
eth list [<interface>]
```

Parameters

`***`	If the command is entered with no parameters, information is listed for all Ethernet interfaces in the router.
`<interface>`[a]	Ethernet interface for which information is listed.

[a] For a dual-port router, you may specify the port number(0 or 1).

Response

Typical response:

```
-> eth list
GLOBAL BRIDGING/ROUTING SETTINGS
  Bridging enabled ..........................  no
    Exchange spanning tree with dest.........  yes
  IP Routing enabled.........................  yes
    Multicast forwarding enabled.............  no
    Firewall filter enabled..................  yes
    Directed Broadcasts Allowed..............  no
    RIP Multicast address....................  default
  IPX Routing enabled........................  no

ETHERNET INFORMATION FOR <ETHERNET/0>
  Hardware MAC Address.......................  00:20:6F:02:98:04
  Send IP RIP to the LAN.....................  no
    Advertise me as default router...........  yes
  Process IP RIP packets received............  rip-1 compatible
    Receive default route by RIP.............  yes
  IP address translation.....................  no
  IP filters defined.........................  no
  IP address/subnet mask.....................  192.168.7.253/
                                               255.255.255.0
  Management IP address/subnet mask..........   0.0.0.0/0.0.0.0
  Static Ethernet routes defined.............  none
  Virtual Ethernet routes defined............  none
  IPX External network number................  00000000
  IPX Frame type.............................  802.2
  MTU........................................  default
```

eth mtu

Sets the maximum transfer unit for the Ethernet interface. The default is 1500 bytes.

You can set the MTU size to less than 1500 bytes, but you cannot set the MTU to greater than 1500 bytes, even if you specify a larger value on an eth mtu command. (RFC 1042 recommends 1500 bytes as the maximum MTU for an Ethernet network.)

To see the current MTU size for an interface that has IP enabled, use the ipifs command.

Mgmt Class

Network (R/W)

Input Format

```
eth mtu <size> [<interface>]
```

Parameters

`<size>`	Maximum number of bytes that can be transferred as a unit.
`<interface>`[a,b]	Ethernet interface.

[a] Integer, 0, 1 or it may be omitted if the router has only 1 Ethernet interface.
[b] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth restart

Stops and restarts a logical Ethernet interface. To read about logical Ethernet interfaces, see “IP Subnets” on page 6-1 of the Technical Reference Guide.

Certain configuration changes for a logical Ethernet interface become effective only after the logical interface is restarted or the router is rebooted. Remember to save the changes before the restart or reboot.

☞ **NOTE:**

Use restart instead of reboot whenever possible. A restart does not affect other interfaces, allowing their traffic to continue. For example, using restart, you can add an IP route without killing voice traffic.

To restart an remote interface, use remote restart.

Mgmt Class

Network (R/W)

Input Format

```
eth restart <interface>
```

Parameters

`<interface>`[a,b] Logical Ethernet interface.

[a] Integer, 0, 1 or it may be omitted if the router has only 1 Ethernet interface.
[b] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth start

Starts a stopped logical Ethernet interface. To read about logical Ethernet interfaces, see “IP Subnets” on page 6-1 of the Technical Reference Guide.

A logical Ethernet interface is stopped using the command eth stop. To stop and immediately restart a logical Ethernet interface, use the command eth restart.

Mgmt Class

Network (R/W)

Input Format

```
eth start <interface>
```

Parameters

`<interface>`[a,b] Logical Ethernet interface.

[a] Integer, 0, 1 or it may be omitted if the router has only 1 Ethernet interface.
[b] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth stop

Stops a logical Ethernet interface.

☞ **NOTE:**

To keep certain configuration changes, you must enter a save command before stopping the logical interface.

The stopped interface is disabled until it is started again. To start a logical Ethernet interface, use the command eth start. To stop and immediately restart a logical Ethernet interface, use the command eth restart.

Mgmt Class

Network (R/W)

Input Format

```
eth restart <interface>
```

Parameters

`<interface>`[a,b] Logical Ethernet interface.

[a] Integer, 0, 1 or it may be omitted if the router has only 1 Ethernet interface.
[b] To specify a logical interface other than logical interface 0, specify both the port number and the logical interface number (<port #>:<logical #>, for example, 0:1).

Response

Command prompt.

eth vrrp add

Defines a VRRP attribute record for the VRID (virtual router ID). Attribute records must be defined for the VRID in the master router and in each of its backup routers. For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

☞ **NOTE:**

This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

To see the contents of the VRRP attribute records, use the command eth vrrp list. You can change the attribute values using other `eth vrrp` commands (see “VRRP Configuration” on page 6-16 of the Technical Reference Guide.)

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp add <vrid> [<port#>]
```

Parameters

`<vrid>`[a]	Virtual router ID.
`<port#>`[b]	Physical Ethernet interface (port) number.

[a] Integer, 1 - 255
[b] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command example defines an attribute record for VRID 7 for the default port 0.

```
-> eth vrrp add 7
```

This command example defines an attribute record for VRID 2 for port 1.

```
-> eth vrrp add 2 1
```

Response

Command prompt.

eth vrrp clear password

Clears the password in a VRRP attribute record for the VRID (virtual router ID). To see the current password, use the command eth vrrp list. To set a new password, use the command eth vrrp set password. For more information,see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

☞ **NOTE:**
If the VRRP attribute record has no password, no VRRP authentication is performed.

☞ **NOTE:**
If you clear the password for one VRRP router, you must clear the password for every router for that VRID on the LAN. For example, if VRID 7 is defined in routers A, B, and C in the LAN and you clear the password for router A, you must clear the password for routers B and C as well.

☞ **NOTE:**
This command takes effect immediately, but changes must saved if it is to persist after a restart the interface or reboot of the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp clear password <vrid> [<port#>]
```

Parameters

`<vrid>`[a]	Virtual router ID.
`<port#>`[b]	Physical Ethernet interface (port) number.

[a] Integer, 1 - 255
[b] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command example clears the password for VRID 7 using default port 0.

```
-> eth clear password 7
```

Response

Command prompt.

eth vrrp delete

Deletes a VRRP attribute record for the VRID (virtual router ID). It also disassociates the VRRP IP and MAC addresses from the logical interface. For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

Use this command to disable VRRP. To re-instate a deleted VRID, you need to redefine both the VRID and the VRRP attribute record. For example, the following commands disable VRID 7 and then re-enable it for the logical interface 0:0:

```
-> eth vrrp delete 7
-> eth ip vrid 7
-> eth vrrp add 7
-> 04/16/2001-08:36:06:VRRP: VRRP 7 on Interface ETHERNET/0 now active
```

When removing a VRRP configuration from a router, you would delete both the VRRP attribute record and the extra logical interface. To do so, use the commands eth vrrp delete and eth delete.

☞ **NOTE:**
This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp delete <vrid> [<port#>]
```

Parameters

`<vrid>`[a]	Virtual router ID.
`<port#>`[b]	Physical Ethernet interface (port) number.

[a] Integer, 1 - 255
[b] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command example deletes the attribute record for VRID 7 for the default port 0.

```
-> eth vrrp delete 7
```

Response

Command prompt.

eth vrrp list

Lists the VRRP attribute records for the port and shows the status of the VRRP router. For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

Mgmt Class

Network (R)

Input Format

```
eth vrrp list [<port#>]
```

Parameters

<port#>[a]	Physical Ethernet interface (port) number.

[a] The default is 0; the parameter may be omitted if the router has only one port.

Response

Typical response listing the attribute records for the default port 0.

```
-> eth vrrp add 7
VRRP Records for Ethernet Port.   0
 VRRP Record...................   VRID 8, Priority 100, Interval 1
                                  Flags: preempt, No Authentication

                                  Interface: ETHERNET/0:3
                                  Primary WAN interface is down
```

eth vrrp set multicast

Changes the multicast address used for VRRP router announcements. This address is used by all VRRP announcements from this router, regardless of VRID or port. For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

☞ **NOTE:**

This command is not usually needed for VRRP configuration. Do not use this command unless you clearly understand its impact.

☞ **NOTE:**

This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp set multicast <ipaddr>
```

Parameters

`<ipaddr>`[a]	IP address that is to be the new multicast address.

[a] Dotted-decimal notation

Example

This command example specifies a new multicast address for VRRP.

```
-> eth vrrp multicast 192.168.255.255
```

Response

Command prompt.

eth vrrp set option

Specifies the preemption option in a VRRP attribute record for the VRID (virtual router ID).

The preemption option determines what the router does when it recovers from a failure, as follows:

- If the router is the master router for the IP address (it has priority 255), it always immediately preempts the backup router and resumes its function in the network.The preemption option cannot change this.
- However, if the router is a backup router for the IP address and it determines that a router with a lower priority is currently functioning as backup, the preemption option determines whether this router immediately preempts the router with lower priority or waits for the lower priority router to go away before becoming the active VRRP router.

To read more about VRRP Backup, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

The preemption setting may differ among the backup routers for a VRID.

☞ **NOTE:**

This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp set option preempt | nopreempt <vrid> [<port#>]
```

Parameters

`preempt`	Preempt immediately.
`nopreempt`	Do not preempt a router with lower priority.
`<vrid>`[a]	Virtual router ID of the VRRP attribute record (integer, 1-255). The attribute record was created by the command eth vrrp add.
`<port#>`[b]	Physical Ethernet interface (port) number (0 or 1).

[a] Integer, 1 - 255
[b] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command specifies no preemption for VRID 7 using default port 0.

```
-> eth vrrp set option nopreempt 7
```

Response

Command prompt.

eth vrrp set password

Specifies the password in a VRRP attribute record for the VRID (virtual router ID). The password is used to authenticate VRRP advertisement packets. It is sent as clear text on the LAN. For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

☞ **NOTE:**
If you do not specify a password, no authentication is performed.

To see the current password, use the command eth vrrp list. To clear a password, use the command eth vrrp clear password.

☞ **NOTE:**

The password must be the same for every router in the Virtual Router, that is, for every router in the LAN with the same VRID. For example, if a VRRP interface in routers A, B, and C has the VRID 7, routers A, B, and C must all specify the same password for VRID 7.

☞ **NOTE:**

This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp set password <password> <vrid> [<port#>]
```

Parameters

`preempt`	Preempt immediately.
`<password>`[a,b]	Password.
`<vrid>`[c]	Virtual router ID of the VRRP attribute record (integer, 1-255). The attribute record was created by the command eth vrrp add
`<port#>`[d]	Physical Ethernet interface (port) number (0 or 1).

[a] ASCII string, 1 - 8 characters.
[b] The password is case sensitive.
[c] Integer, 1 - 255
[d] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command example specifies the password “AbCdEfGh” for VRID 7 using default port 0.

```
-> eth vrrp set password AbCdEfGh 7
```

Response

Command prompt.

eth vrrp set priority

Specifies the priority attribute in a VRRP attribute record for the VRID (virtual router ID). The priority value determines which VRRP router in the LAN takes over when a VRRP router fails. For more information, see "VRRP Backup" on page 6-16 of the Technical Reference Guide.

☞ **NOTE:**

If you do not specify a priority value for a VRRP attribute record, the default priority, 100, is used.

The priority for the master router must be the maximum, 255; the priority for each backup router must be less than 255.

The priority values must differ for each router that uses the same VRID. For example, the master router for VRID 7 must have priority 255 while the first backup router for VRID 7 could have the default priority 100 and a second backup router for VRID 7 could have priority 50.

☞ **NOTE:**

This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp set priority <priority> <vrid> [<port#>]
```

Parameters

`<priority>`[a]	Priority value. The priority for the master router must be 255; the priority for each backup router must be less than 255.
`<vrid>`[a]	Virtual router ID of the VRRP attribute record (integer, 1-255). The attribute record was created by the command eth vrrp add
`<port#>`[b]	Physical Ethernet interface (port) number (0 or 1).

[a] Integer, 1 - 255
[b] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command example specifies the maximum priority for the master router for VRID 7 using default port 0.

```
-> eth vrrp set priority 255 7
```

This command example defines priority 50 for a backup router for VRID 7 using port 1.

```
-> eth vrrp set priority 50 7 1
```

Response

Command prompt.

eth vrrp set timeinterval

Specifies the time interval attribute in a VRRP attribute record for the VRID (virtual router ID). The time interval determines how often VRRP advertisement packets are sent, and thus, how quickly a backup router can recognize that another VRRP router is down.

☞ **NOTE:**
If you do not specify a time interval value for a VRRP attribute record, the default time interval, 1 second, is used.

If the backup does not receive a VRRP packet from another VRRP router during the master down interval, the backup assumes the other router is down. The master down interval is calculated as follows:

Master _Down_Interval = (3 * Time_Interval) + Skew_Time
Skew_Time = (256 - Priority) / 256

Thus, the default skew time is (256 - 100) / 256, or .609375. The default master down interval is (3 * 1) + .609375, or 3.609375 seconds.

For more information, see “VRRP Backup” on page 6-16 of the Technical Reference Guide.

☞ **NOTE:**
The time interval must be the same for every router in the Virtual Router, that is, for every router in the LAN with the same VRID. For example, if a VRRP interface in routers A, B, and C has the VRID 7, routers A, B, and C must all specify the same time interval for VRID 7.

☞ **NOTE:**
This command takes effect immediately, but you must save the change if it is to persist after you restart the interface or reboot the router.

Mgmt Class

Network (R/W)

Input Format

```
eth vrrp set timeinterval <seconds> <vrid> [<port#>]
```

Parameters

<seconds>[a]	Time interval value in seconds
<vrid>[b]	Virtual router ID of the VRRP attribute record.
<port#>[c]	Physical Ethernet interface (port) number (0 or 1).

[a] Integer, 0 - 60
[b] Integer, 1 - 255
[c] The default is 0; the parameter may be omitted if the router has only one port.

Example

This command example specifies two seconds as time interval for VRID 7 using default port 0.

```
-> eth vrrp set timeinterval 2 7
```

Response

Command prompt.

eth ip remsrcrouteopt

Adds or removes the source routing option.

Mgmt Class

Network (R/W)

Input Format

```
eth ip remsrcrouteopt <enable | disable>
```

Parameters

`enable`	Adds the source routing option.
`disable`	Removes the source routing option. (Default value)

Response

Command prompt.

CHAPTER 6

REMOTE COMMANDS

The commands in this section begin with the word remote. The commands allow you to add, delete, and modify remote routers to which the target router can connect. Remote router information that can be configured includes:

- PVC numbers
- Phone numbers
- CallerID phone numbers
- Call management
- Bandwidth management
- Security authentication protocols and passwords
- WAN IP/ IPX addresses
- IP routes
- IPX routes and SAPS
- Remote bridging addresses and bridging control
- Host mapping

The remote commands found in this section include:

Table 6-1: Remote Command Listing

Command	Function
remote ?	Lists the supported remote keywords.
remote add	Adds a remote router entry into the remote router database.
remote addbridge	Defines the remote router entry as the default bridging destination for outbound bridging.
remote addhostmapping	Remaps a range of local LAN IP addresses to a range of public IP addresses on a per-remote-router basis.

Table 6-1: Remote Command Listing (Cont.)

Command	Function
remote addiproute	Adds an IP address route to a network or station on the LAN connected beyond the remote router.
remote addipxroute	Adds an IPX route for a network or station on the LAN network connected beyond the remote router.
remote addipxsap	Adds an IPX SAP to the server information table for a service on the LAN network connected beyond the remote router.
remote addserver	Adds a server's IP address (on the LAN) associated with this remote router for a particular protocol.
remote bindipvirtualroute	Adds a remote route to the named IP virtual routing table.
remote blocknetbios	Enables or disables a filter that blocks all NetBIOS packets over this WAN connection.
remote del	Deletes a remote router entry from the remote router database.
remote delatmsnap	Deletes an ATM mapping entry.
remote delbridge	Removes the designation of the remote router entry as the default bridging destination.
remote delencryption	Deletes encryption files associated with a remote router.
remote delhostmapping	Undoes an IP address/host translation (remapping) range on a per-remote-router basis.
remote deliproute	Deletes an IP address route for a network or station on the LAN connected beyond the remote router.
remote delipxroute	Deletes an IPX address for a network on the LAN connected beyond the remote router.
remote delipxsap	Deletes an IPX service on the LAN network connected beyond the remote router.
remote delourpasswd	Removes the unique CHAP or PAP authentication password entries.
remote deloursysname	Removes the unique CHAP or PAP authentication system name entries.
remote delphone	Deletes a phone number.
remote delserver	Deletes a server entry.
remote disable	Disables the remote.

Table 6-1: Remote Command Listing (Cont.)

Command	Function
remote disauthen	This command is intended for situations where third-party routers cannot be authenticated; the target router will not attempt to authenticate the remote router.
remote disbridge	Disables bridging from the target router to the remote router.
remote enaauthen	Initiates the target router authentication negotiation as defined in the remote router's database.
remote enable	Enables use of an entry in the remote router database.
remote enabridge	Enables bridging from the target router to the remote router.
remote ipfilter	Manages the IP filters on the WAN interface.
remote list	Lists the remote router entry (or all the entries) in the remote router database.
remote listbridge	Lists the current bridge settings for the specified remote router entry.
remote listiproutes	Lists IP information for a remote router or, if the router name is omitted, for all routers in the remote router database.
remote listipxroutes	Lists all network IPX route addresses defined for the LAN connected beyond the remote router.
remote listipxsaps	Lists all services defined for the LAN connected beyond the remote router.
remote listphones	Lists the PVC numbers available for connecting to the remote router.
remote restart	Stops the current active session and starts a new active session for a remote.
remote setatmnsap	RFC1577 (Classical IP over ATM) specifies a mechanism to map an ATM Name (called an SNAP) to a PVC.
remote setauthen	Sets the authentication protocol used communicate with the remote router.
remote setbod	Sets the bandwidth on demand (BOD) management option for a DOD (dial on demand) connection, that is, a connection where the link goes up and down.
remote setbroptions	Sets controls on bridging for the remote router entry.
remote setbwthresh	Sets the bandwidth threshold for a DOD (dial on demand) connection, that is, a connection where the link goes up and down.

Table 6-1: Remote Command Listing (Cont.)

Command	Function
remote setcompression	Enables or disables negotiation of the Stac LZS compression of the payload (RFC 1974).
remote setencryption	RFC 1969 encryption. Specifies a PPP DES (Data Encryption Standard) 56-bit key with fixed transmit and receive keys.
remote setencryption	Diffie-Hellman Encryption. Specifies encryption based on the Diffie-Hellman key-exchange protocol.
remote setipoptions	Enables or disables the selected IP option for the WAN interface.
remote setipslaveppp	Sets the IP Slave PPP mode.
remote setiptranslate	Controls Network Address Translation on a per remote router basis.
remote setipxaddr	Sets the IPX network number for the remote WAN connection.
remote setipxoptions	Enables or disables the IPX option RIPSAP for the remote WAN connection.
remote setmaxline	Sets the maximum links (1 or 2) for a DOD (dial on demand) connection, that is, a connection where the link goes up and down.
remote setmgmtipaddr	Assigns to the remote router entry, an IP address which is to be used for management purposes only and not for IP address translation.
remote setminline	Sets the minimum number of channels to be continually allocated to the connection.
remote setmtu	Sets the maximum transfer unit for the remote interface.
remote setourpasswd	Sets a unique CHAP or PAP authentication password for the local router that is used for authentication when the local router connects to the specified remote router.
remote setoursysname	Sets a unique CHAP or PAP authentication system name for the local router that is used for authentication when the local router connects to the specified remote router.
remote setpasswd	Sets the CHAP or PAP authentication password that is used when the remote router establishes a connection or is challenged by the target router.
remote setphone	Specifies the phone number to be used for the dial on demand (DOD) connection, that is, a connection where the link goes up and down.
remote setpppoptions	Enables and disables a PPP option.

Table 6-1: Remote Command Listing (Cont.)

Command	Function
remote setpppppretrytimer	Enables or disables the PPP retry timer for a remote session.
remote setprefer	Changes the interface for the remote entry.
remote setprotocol	Sets the link protocol for the remote router.
remote setpvc	Specifies the PVC number for connecting to the remote router.
remote setrmtipaddr	Sets the WAN IP address for the remote router.
remote setspeed	Specifies the speed to be used when dialing out using the backup V.90 modem connected to the console port.
remote setsrcipaddr	Sets the IP address for the target WAN connection to the remote router.
remote settimer	Sets the length of the timeout period before disconnection.
remote start	If the remote is not currently active, this command attempts to start an active session.
remote stats	Shows the current status of the connection to the remote router, including the bandwidth and data transfer rate.
remote stop	If the remote is active, this command stops the active session.
remote unbindipvirtual-route	Removes a remote route from the named IP virtual routing table.

remote ?

Lists the supported remote keywords. The list will vary depending on the router model.

Mgmt Class

Network (R)

Input Format

```
remote ?
```

Parameters

None

Response

A listing of the remote commands and keywords with a brief description of their function.

remote add

Adds a remote router entry into the remote router database.

Mgmt Class

Network (R/W)

Input Format

```
remote add <remotename>
```

Parameters

`<remotename>`[a] Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

remote addbridge

Defines the remote router entry as the default bridging destination for outbound bridging. The command can define either the default bridging destination for all MAC addresses or the default bridging destination for a specific MAC address.

When you specify a MAC address on this command, a permanent entry for that address is created in the bridging table. Thereafter, packets that contain that MAC address are bridged using the specified remote router entry. (To see the entries in the bridging table, use the bi list command.)

☞ **NOTE:**

Bridging using the specified remote is effective only after it has been enabled using the remote enabridge command. To see the current bridge settings for a remote, use the remote listbridge command. To remove the default designation from a remote, use the remote delbridge command.

If IP and IPX routing are disabled, all packets, with an unknown destination, are bridged to the default bridging destination. If IP and/or IPX routing is enabled, bridging occurs only for packets that are not routed.

Mgmt Class

Network (R/W)

Input Format

```
remote addbridge  * | <mac_addr> <remotename>
```

Parameters

*	All MAC addresses
<mac_addr>[a]	MAC address
<remotename>[b]	Name of the remote router. [c]

[a] HEX-decimal notation
[b] ASCII string
[c] The name is case sensitive.

Response

Command prompt.

remote addhostmapping

Remaps a range of local LAN IP addresses to a range of public IP addresses on a per-remote-router basis. These local addresses are mapped one-to-one to the public addresses.

☞ **NOTE:**

The range of public IP addresses is defined by <*first public addr*> only. The rest of the range is computed automatically (from <*first public addr*> to <*first public addr*> + number of addresses remapped - 1) inclusive.

Mgmt Class

Network (R/W)

Input Format

```
remote addhostmapping <first private addr> <second private
addr> <first public addr> <remoteName>
```

Parameters

`<first private addr>`[a]	First IP address in the range of local IP address to be remapped.
`<second private addr>`[a]	Last IP address in the range of local IP address to be remapped.
`<first public addr>`[a]	Defines the range of public IP addresses.
`<remotename>`[b]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Response

Command prompt.

remote addiproute

Adds an IP address route to a network or station on the LAN connected beyond the remote router. The route is added to the default routing table.

The local router's routing table must be seeded statically to access networks and stations beyond this remote router. After the connection is established, standard RIP update packets can dynamically add routes to the routing table. Setting this address is not required if the local router never connects to the remote router and the remote router supports RIP.

☞ **NOTE:**

Changes to the default routing table require a save and a remote restart or reboot before they take effect.

Mgmt Class

Network (R/W)

Input Format

```
remote addIpRoute <ipaddr> <ipnetmask> <hops> [<ipgateway>]
<remotename>
```

Parameters

`<ipaddr>`[a]	IP address of the remote network or station.
`<ipnetmask>`[a]	IP network mask of the remote network or station.
`<hops>`[b]	Perceived cost to reach the remote network or station by this route.
`<ipgateway>`[a]	Address of a router on the remote LAN. Enter a gateway only if configuring a MER interface. Check with your system administrator for details
`<remotename>`[c]	Name of the remote router.

[a] Dotted-decimal notation
[b] Integer, 1 - 15
[c] ASCII string

Examples

The first two addresses in the list represent subnetworks, the third is a class B network, the fourth is a host, and the fifth address is the default route. The fifth command adds the default route when the WAN interface is a point-to-point interface; the sixth command adds the default route when the WAN interface is a broadcast interface.

```
-> remote addIpRoute 10.1.210.64 255.255.255.192 1 HQ
-> remote addIpRoute 10.1.210.032 255.255.255.224 1 HQ
-> remote addIpRoute 172.17.0.0 255.255.0.0 2 HQ
-> remote addIpRoute 10.1.210.072 255.255.255.255 1 HQ
-> remote addIpRoute 0.0.0.0 0.0.0.0 1 HQ
-> remote addIproute 0.0.0.0 0.0.0.0 1 172.16.10.1 HQ
```

Response

Command prompt.

remote addipxroute

Adds an IPX route for a network or station on the LAN network connected beyond the remote router. The target router's routing information table must be seeded statically to access networks and stations beyond this remote router. After the connection is established, standard RIP update packets will dynamically add to the routing table. (Setting this address is not required if a target router never connects to the remote router and the remote router supports RIP.)

☞ **NOTE:**

A reboot command must be performed on the target router for the addition of a static route to take effect.

Mgmt Class

Network (R/W)

Input Format

```
remote addIpxRoute <ipxne#> <metric> <ticks> <remotename>
```

Parameters

`<ipne#>`[a]	IPX network number.
`<metric>`[b]	Number of routers through which the packet must go to get to the network/station.
`<ticks>`[b]	Number in 1/8 seconds which is the estimated time delay in reaching the remote network or station.
`<remotename>`[c]	Name of the remote router.

[a] Hexadecimal notation
[b] Integer
[c] ASCII string

Response

Command prompt.

remote addipxsap

Adds an IPX SAP to the server information table for a service on the LAN network connected beyond the remote router. The target router's SAP table must be seeded statically to access services beyond this remote router. After the connection is established, standard SAP broadcast packets will dynamically add to the table.

☞ **NOTE:**

A reboot must be performed on the target router for the addition of a SAP to take effect.

Mgmt Class

Network (R/W)

Input Format

```
remote addipxsap <servicename> <ipxnet> <ipxnode> <socket>
<type> <hops> <remotename>
```

Parameters

`<servicename>`	Name of service.
`<ipxnet>`[a]	IPX network number.
`<ipxnode>`[a]	IPX node address.
`<socket>`	Socket address of the destination process within the destination node. The processes include services such as file and print servers.
`<type>`	Number representing the type of server.
`<hops>`[b]	Number of routers through which the packet must go to get to the network/station.
`<remotename>`[c]	Name of the remote router.

[a] Hexadecimal notation
[b] Integer
[c] ASCII string

Response

Command prompt.

remote addserver

This Network Address Translation (NAT) command is used to add a server's IP address (on the LAN) associated with this remote router for a particular protocol. To learn more, see "Network Address Translation (NAT)" on page 4-17.

Multiple system addserver and remote addserver commands can designate different servers for different protocols, ports, and interfaces. When a request is received, the router searches the server list for the appropriate server. The order of search for a server is discussed in "Server Request Hierarchy" on page 4-22

To delete a server designation, use the remote delserver command.

Mgmt Class

Network (R/W)

Input Format

```
remote addserver  <action> <protocol>  <first port>  [<last
port> [<first private port>]] <remotename>
```

Parameters

`<action>`	One of the following command actions:	
	`<ipaddr>`[a]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.
`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[b]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the remote end. Port used by the selected server.	
	`<portid>`[c]	Numerical port value; a value of 0 matches any port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypertext Transfer Protocol (HTTP) port.

[a] Dotted-decimal notation
[b] Integer
[c] Integer, 0 - 65,535

Parameters Cont.

`smtp`	Simple Mail Transfer Protocol (SMTP) port.
`sntp`	Simple Network Management Protocol (SNMP) port.
`t120`	T.120 port.
`telnet`	Telnet port.
`tftp`	Trivial File Transfer Protocol (TFTP) port.
`all`	All ports.

`<last port>` Optional last port in the range of ports as seen by the remote end for the server on the LAN.

`<first private port>`[c] If specified, this is a port remapping of the incoming requests from the remote end.

Example

```
-> remote addserver 192.168.1.5 tcp smtp
```

Response

Command prompt.

remote bindipvirtualroute

Adds a remote route to the named IP virtual routing table.

To list the remote routes, use the remote listiproutes command. To remove a route from a virtual routing table, use the remote unbindipvirtualroute command.

☞ **NOTE:**
A route change in an IP virtual routing table takes effect immediately. However, the change is lost if it is not saved before the next remote restart or reboot

Mgmt Class

Network (R/W)

Input Format

```
remote bindipvirtualroute <ipaddr> <ipnetmask> <hops>
[<ipgateway>] <tablename> <remotename>
```

Parameters

`<ipaddr>`[a]	IP address of the remote network or station.
`<ipnetmask>`[a]	IP network mask of the remote network or station.
`<hops>`[b]	Perceived cost in reaching the remote network or station by this route.
`<ipgateway>`[a]	Address of a router on the remote LAN. Enter a gateway only if you are configuring a MER interface.
`<tablename>`[c]	IP virtual routing table to which the route is added.
`<remotename>`[c]	Name of the remote router.

[a] Dotted-decimal notation
[b] Integer, 1 - 15
[c] ASCII string

Example

The following command adds a route to virtual routing table FRANCISCO. The route is to IP address 10.1.2.0/255.255.255.0 and goes through remote router HQ.

```
-> remote bindIPVirtualRoute 10.1.2.0 255.255.255.0 1 francisco HQ
```

Response

Command prompt.

remote blocknetbios

This command enables or disables a filter that blocks all NetBIOS packets over this WAN connection.

Mgmt Class

Security (R/W)

Input Format

```
remote blocktetbios on | off <remotename>
```

Parameters

`on`	Enables NetBIOS filtering.
`off`	Disables NetBIOS filtering.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote del

Deletes a remote router entry from the remote router database.

Input Format

```
remote del <remotename>
```

Mgmt Class

Network (R/W)

Parameters

`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote delatmsnap

This command deletes an ATM mapping set by the remote setatmnsap command, page 40.

Mgmt Class

Network (R/W)

Input Format

```
remote delatmfasp  atmf | e164  partial | full  <nsap>
<remotename>
```

Parameters

`atmf`	ATM forum encoding.
`E164`	ITU E164 encoding.
`partial`	The MAC address of the router is substituted for octets 2-7 of the NSAP.
`full`	No change is made to the specified NSAP.
`<nsnap>`[a]	NSAP

[a] specified as 40 hex digits or 20 octets (2-digit pairs separated by colons

Response

Command prompt.

remote delbridge

Removes the designation of the remote router entry as the default bridging destination. (Default bridging destinations are defined using the remote addbridge command.) To see the bridge settings for a remote entry, use the remote listbridge command.

To remove a designation as the default bridging destination for a specific MAC address, specify that address on the command. The entry is then removed from the bridging table. To see the entries in the bridging table, use the bi list command.

Mgmt Class

Network (R/W)

Input Format

```
remote delbridge  * | <mac_addr>  <remotename>
```

Parameters

*	All MAC addresses
<mac_addr>[a]	MAC address
<remotename>[b]	Name of the remote router. [c]

[a] HEX-decimal notation
[b] ASCII string
[c] The name is case sensitive.

Response

Command prompt.

remote delencryption

Deletes encryption files associated with a remote router.

Mgmt Class

Security (R/W)

Input Format

```
remote delencryption <remotename>
```

Parameters

<remotename>[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote delhostmapping

Undoes an IP address/host translation (remapping) range that was previously established with the command remote addhostmapping on a per-remote-router basis.

Mgmt Class

Network (R/W)

Input Format

```
remote delhostmapping <first private addr> <second private
addr> <first public addr> <remotename>
```

Parameters

`<first private addr>`[a]	First IP address in the range of local IP address to be remapped.
`<second private addr>`[a]	Last IP address in the range of local IP address to be remapped.
`<first public addr>`[a]	Defines the range of public IP addresses.
`<remotename>`[b]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Response

Command prompt.

remote deliproute

Deletes an IP address route for a network or station on the LAN connected beyond the remote router. The route is deleted from the default routing table.

☞ **NOTE:**
Changes to the default routing table require a save and a remote restart or reboot before they take effect.

Mgmt Class

Network (R/W)

Input Format

```
remote deliproute <ipaddr> <remotename>
```

Parameters

`<ipaddr>`[a]	IP address of the remote network or station.
`<remotename>`[b]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Response

Command prompt.

remote delipxroute

Deletes an IPX address for a network on the LAN connected beyond the remote router.

☞ **NOTE:**
A reboot command must be performed on the target router for the deletion of a static route to take effect.

Mgmt Class

Network (R/W)

Input Format

```
remote delIpxRoute <ipxnet> <remotename>
```

Parameters

`<ipnet>`[a]	IPX network number.
`<remotename>`[b]	Name of the remote router.

[a] Hexadecimal notation
[b] ASCII string

Response

Command prompt.

remote delipxsap

Deletes an IPX service on the LAN network connected beyond the remote router.

☞ **NOTE:**

A reboot must be performed on the target router for a deleted service to take effect.

Mgmt Class

Network (R/W)

Input Format

```
remote delipxSap <servicename> <remotename>
```

Parameters

`<servicename>`	Name of service.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote delourpasswd

Removes the unique CHAP or PAP authentication password entries established by the remote setourpasswd command.

Mgmt Class

Network (R/W)

Input Format

```
remote delourpasswd <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote deloursysname

Removes the unique CHAP or PAP authentication system name entries established by the command remote setoursysname.

Mgmt Class

Security (R/W)

Input Format

```
remote deloursysname <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote delphone

Deletes a phone number that was specified by the command remote setphone.

Mgmt Class

Network (R/W)

Input Format

```
remote delphone async | isdn  1 | 2  <phone#> <remotename>
```

Parameters

`async`	Asynchronous connection.
`isdn`	ISDN connection.
`1`	Primary phone number or first ISDN channel.
`2`	Alternative phone number or first ISDN channel.
`<phone#>`[a]	Decimal number representing the exact digits to be dialed.
`<remotename>`[b]	Name of the remote router.

[a] Digits, the asterisk, and the # characters are accepted; use a comma to specify a 2-second pause.
[b] ASCII string

Response

Command prompt.

remote delserver

Deletes a server entry created by the remote addserver command.

Mgmt Class

Network (R/W)

Input Format

```
remote delserver <action> <protocol> <first port> [<last port>
[<first private port>]]
```

Parameters

`<action>`	One of the following command actions:	
	`<ipaddr>`[a]	Selects the host with this IP address as server.
	`discard`	Discards the incoming server request.
	`me`	Sends the incoming server requests to the local router, regardless of the IP address.
`<protocol>`	Protocol used by the selected server.	
	`<protocolid>`[b]	Numerical protocol ID.
	`tcp`	TCP only.
	`udp`	UDP only.
	`all`	All protocols.
`<first port>`	First or only port as seen by the remote end. Port used by the selected server.	
	`<portid>`[c]	Numerical port value; a value of 0 matches any port.
	`ftp`	File Transfer Protocol (FTP) port.
	`h323`	H.323 port.
	`http`	Hypertext Transfer Protocol (HTTP) port.
	`smtp`	Simple Mail Transfer Protocol (SMTP) port.
	`sntp`	Simple Network Management Protocol (SNMP) port.
	`t120`	T.120 port.
	`telnet`	Telnet port.
	`tftp`	Trivial File Transfer Protocol (TFTP) port.
	`all`	All ports.
`<last port>`	Optional last port in the range of ports as seen by the remote end for the server on the LAN.	
`<first private port>`[c]	If specified, this is a port remapping of the incoming requests from the remote end.	

[a] Dotted-decimal notation
[b] Integer
[c] Integer, 0 - 65,535

Response

Command prompt.

remote disable

Disables the remote. The remote remains disabled even after a reboot. To enable the remote, the command remote enable must be entered.

☞ **NOTE:**

You may enter and save information and settings for a disabled remote entry. However, the remote entry cannot be used until it is enabled.

☞ **NOTE:**

If the remote is currently active when the remote is disabled, the active session is not stopped. To stop the active session, use the remote stop command.

Mgmt Class

Network (R/W)

Input Format

```
remote disable <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote disauthen

This command is intended for situations where third-party routers cannot be authenticated; the target router will not attempt to authenticate the remote router.

Mgmt Class

Security (R/W)

Input Format

```
remote disauthen <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote disbridge

Disables bridging from the target router to the remote router.

☞ **NOTE:**
This command requires a reboot of the target system for the change to take effect.

Mgmt Class

Security (R/W)

Input Format

```
remote disbridge <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote enaauthen

Initiates the target router authentication negotiation as defined in the remote router's database.

Mgmt Class

Security (R/W)

Input Format

```
remote enaAuthen <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote enable

Enables use of an entry in the remote router database. Although the command makes it possible to use the remote entry, it does not start an active session for the remote.

☞ **NOTE:**

The entry remains enabled across reboots. The entry remains enabled until it is disabled by a remote disable command.

Mgmt Class

Network (R/W)

Input Format

```
remote enable <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote enabridge

Enables bridging from the target router to the remote router.

☞ **NOTE:**
This command requires a reboot of the target system for the change to take effect.

Mgmt Class

Security (R/W)

Input Format

```
remote enablebridge <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote ipfilter

Manages the IP filters on the WAN interface. The filters screen IP packets at the interface level.

You can define filters for any entry in the remote router database. To see the names of the remote entries, use the command remote list.

A remote entry can have up to four lists of filters; the list types are Input, Receive, Transmit, and Output. For more information on how these filter types are applied, see "IP Filtering" on page 5-23.

☞ **NOTE:**

IP filters take effect immediately upon entry. They can even affect the current connection that you are using to enter commands. Unlike other configuration changes, you do not need to save and restart or reboot

Mgmt Class

Security (R/W)

Input Format

```
remote ipfilter <command> <type> <action> <parameters>
<remotename>
```

The following <command>s are provided for managing IP filters for the WAN interface:

remote ipfilter append

```
eth ip filter append [<line number>] <type> <action>
[<parameters>] [<remotename>]
```

Appends a filter to the list of filters for this <type> (Input, Receive, Transmit, or Output) for this remote entry.

If no line number is specified, the filter is appended to the end of the list; otherwise, it is appended after the specified line. For example, "`append 0`" appends the filter after line 0. Filters are used in the order they appear in their list.

remote ipfilter insert

```
remote ipfilter insert <type> <action> <parameters>
<remotename>
```

Inserts a filter in the list of filters for this <type> (Input, Receive, Transmit, or Output) for this remote entry.

If no line number is specified, the filter is inserted at the beginning of the list; otherwise, it is inserted before the specified line. For example, "`insert 0`" inserts the filter before line 0 so it is the first filter in the list. Filters are used in the order they appear in their list.

remote ipfilter delete

```
remote ipfilter delete <type> <action> <parameters>
<remotename>
```

Deletes the first filter that matches the filter specified on the command.

remote ipfilter flush

```
remote ipfilter flush [<first line> [<last line>]] <type>
<remotename>
```

Deletes a range of filters of this `<type>` (Input, Receive, Transmit, or Output) for this remote entry.

If no line numbers are specified, all filters in the list are deleted. If only the first line number is specified, all filters from that line to the end are deleted. To see the current filter list, use the remote ipfilter list list command. Filters are used in the order they appear in their list.

remote ipfilter clear

```
remote ipfilter clear [<first line> [<last line>]] [<type>]
<clear arg> <remotename>
```

Resets the counters for the specified filters. A filter has a counter if the `-c` parameter was specified for the filter.

You can specify the filters whose counters are to be reset by their line number range and type (input, receive, transmit, or output). If no `<type>` is specified, the counters for all filters for the interface are reset. If no line numbers are specified, the counters for all filters for that type and interface are reset. If only the first line number is specified, all counters for filters from that line to the end are reset. To see the filter lists and counters, use the remote ipfilter list command.

remote ipfilter check

```
remote ipfilter check <type> <parameters> <remotename>
```

Checks the action that would be taken if a packet with the specified parameters was compared with the list of filters defined for the specified type and remote entry.

For example, the command

```
-> remote ipfilter check input -p TCP branch1
```

would check what action (accept, drop, reject, inipsec, outipsec) would be taken for a TCP packet after it was compared with the list of input filters defined for remote entry branch1.

remote ipfilter list

```
remote ipfilter list <type> <remotename>
```

Lists all filters of the specified <type> (input, receive, transmit, or output) for this remote entry.

remote ipfilter watch

```
remote ipfilter watch <on | off> [-q | -v] <remotename>
```

Turns on or turns off the console watch for this remote router entry. If the watch is on, a message is printed to the console serial port when a packet is dropped or rejected. (The message is also sent to any Syslog servers; see “Syslog Client” on page 7-1.)

However, if the parameter -q (quiet) was specified for a filter, no message is printed when that filter matches a packet. If the parameter -v (verbose) was specified for a filter, a message is printed whenever that filter matches a packet, regardless of the filter action.

To see the messages, Telnet to the router and enter system log. The watch does not continue after a remote restart or save; to resume the watch, you must enter the remote ipfilter watch <*on*> command again.

Parameters

The filter <type> specifies at which point the filter is compared to the IP packet (see the illustration under “Filters and Interfaces” on page 5-23):

`input`	When the packet enters the interface, *before* any network address translation is performed.
`receive`	When the packet enters the interface, *after* any network address translation, but before routing table processing.
`transmit`	After routing table processing, *before* any network address translation before the packet is sent out.
`output`	After routing *and* network address translation, just before the packet is sent out.

If the packet matches the filter, the specified action is performed:

`accept`	The packet is allowed to proceed for further processing.
`drop`	The packet is discarded, without sending an ICMP (Internet Control Management Protocol) error message.

`reject`	The packet is discarded and an ICMP error message is returned to the sender.
`inipsec`	The packet is passed to IPSec for decrypting. The filter is intended to match packets coming from the other IPSec gateway. Although filters are the mechanism by which packets are passed to IPSec, it is recommended that you use IKE to manage your IP Security (see "IPSec (Internet Protocol Security)" on page 5-50.)
`outipsec`	The packet is passed to IPSec so it can be encrypted and sent to the other IPSec gateway. The filter is intended to match packets coming from the local protected network. Although filters are the mechanism by which packets are passed to IPSec, it is recommended that you use IKE to manage your IP Security (see IPSec "IPSec (Internet Protocol Security)" on page 5-50).

The following parameters specify the characteristics that an IP packet must have in order to match the filter. A filter can require any or all of these characteristics.

`-p <protocol> | TCP | UDP | ICMP`

The packet must have the specified protocol. If no protocol is specified, the filter matches *every* protocol.

`-sa <first source ip addr>[:<last source ip addr>]`

The packet must have a source IP address within the specified address range. If only one address is specified, the packet must have that source IP address. If no source IP address is specified, the filter matches any address in the range 0.0.0.0:255.255.255.255.

`-sm <source ip mask>`

The filter uses the specified mask when comparing the <first source ip addr>...<last source ip addr> with the source IP address in the IP packet. If no source mask is specified, the mask used is 255.255.255.255.

`-sp <ICMP type> | <first source port>[:<last source port>]`

The packet must have a source port that matches the specified ICMP type or that is within the specified port range. If only one port is specified, the packet must have that source port. If no source port is specified, the filter matches any source port in the range 0:0xffff.

`-da <first dest ip addr>[:<last dest ip addr>]`

The packet must have a destination IP address within the specified address range. If only one address is specified, the packet must have that destination IP address. If no destination IP address is specified, the filter matches any address in the range 0.0.0.0:255.255.255.255.

`-dm <dest ip mask>`

The filter uses the specified mask when comparing the <first dest ip addr>...<last dest ip addr> with the destination IP address in the IP packet. If no destination mask is specified, the mask used is 255.255.255.255.

`-dp  <ICMP type> | <first dest port>[:<last dest port>]`

The packet must have a destination port that matches the specified ICMP type or that is within the specified port range. If only one port is specified, the packet must have that destination port. If no destination port is specified, the filter matches any destination port in the range 0:0xffff.

`-tcp syn | ack | noflag | rst`

If the IP packet is a TCP packet, the filter matches the packet only if the packet flag settings are as specified. If no -tcp option is specified for the filter, flag settings are not checked.

☞ **NOTE:**

More than one -tcp option may be specified for the IP filter.

The syn, ack, and noflag settings work together as follows:

- Specify `-tcp syn` if the TCP SYN flag must be set.
- Specify `-tcp ack` if the TCP ACK flag must be set
- Specify `-tcp noflag` if neither the SYN flag nor the ACK flag can be set.

For example, for the IP filter to match the initiation of a TCP connection, specify `-tcp syn`. The filter will match TCP packets that have the TCP SYN flag set but *not* the TCP ACK flag set. For the filter to match the response to initiation of a TCP connection, specify `-tcp syn` *and* `-tcp ack`. The filter will match only TCP packets with both the TCP SYN and TCP ACK flags set.

The `-tcp rst` setting is independent of the others; if you specify `-tcp rst` for the filter, the filter matches every TCP packet with the TCP RESET flag set, regardless of the other flag settings. For example, for the filter to match packets for “established” connections, you would specify both `-tcp rst` *and* `-tcp ack` so that the filter is applied to every TCP packet that has either the RESET flag or the ACK flag set.

The following `<parameter>`s request additional filter options.

`-b`

This option requests that this filter be compared *twice* with each packet. The first time the source filter information is matched against the source information in the IP packet and the destination filter information is matched against the destination information in the IP packet. The second time the source filter information is matched against the destination information in the IP packet and the destination filter information is matched against the source information in the IP packet.

`-c <count of times rule used>`

This option requests a counter for this filter. If specified, a count is kept of how many IP packets have matched this filter since the router was rebooted. To see the current count for a filter, use the remote ipfilter list command. To clear a counter, use the remote ipfilter clear command.

`-ipsec <IPSec record name>`

Use this option when the `<action>` specified is *inipsec* or *outipsec*. It specifies the IPSec Security Association that uses the filter.

`q` *or* `-v`

Specify one of these options to determine when watch messages are sent for this filter. The messages are sent to the console serial port (and to any Syslog servers; see see “Syslog Client” on page 7-1.)
If neither `-q` or `-v` are specified for the filter, and a remote ipfilter watch <on> command is entered for the interface, a message is sent each time this filter causes a packet to be dropped or rejected.
If `-q` (quiet) is specified, no messages are printed for this filter, even if the filter causes a packet to be dropped or rejected.
If `-v` (verbose) is specified, a message is printed every time this filter matches a packet, regardless of the filter action.

The `<remotename>` specifies the entry in the remote router database that the command applies to. To see the remote names, use the remote list command.

Examples

This command example deletes all IP filters of type Receive for the remote interface internet.

```
-> remote ipfilter flush receive internet
```

The following two command examples have the same effect: they deny all IP traffic for the remote interface internet from the specified destination addresses. The addresses can be specified as 192.168.0.0 masked with 255.255.0.0 or as the range 192.168.0.0 through 192.168.255.255.

```
-> remote ipfilter append receive drop -da 192.168.0.0 -dm
255.255.0.0 internet
-> remote ipfilter append receive drop -da 192.168.0.0:192.168.
255.255 internet
```

This command example lists all IP filters of type Input for the remote interface internet.

```
-> remote ipfilter list input internet
```

Response

Command prompt.

remote list

Lists the remote router entry (or all the entries) in the remote router database. The result is a complete display of the current configuration settings for the remote router(s), except for the authentication password/secret.

Mgmt Class

Network (R)

Input Format

```
remote list <remotename>
```

Parameters

`***`	If entered with no parameters, all remote router entries are listed.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Typical response:

```
-> rem list internet

INFORMATION FOR <internet>
  Status.............................. enabled
  Our System Name when dialing out.....
  Our Password used when dialing out... no
  Protocol in use..................... PPP
  ATM traffic shaping................. no
  Authentication...................... disabled
  Authentication level required........ PAP
  Use periodic LCP pings.............. yes
  Connection Identifier (VPI*VCI)..... 0*38
  IP address translation.............. off
  IP filters defined.................. no
  Send/Receive Multicast.............. off
  Block NetBIOS Packets............... off
  Compression Negotiation............. off
  IP slave mode (PPP)................. no
  Try to reacquire IP addr (PPP)...... yes
  Source IP address/subnet mask....... 0.0.0.0/0.0.0.0
  Remote IP address/subnet mask....... 0.0.0.0/0.0.0.0
  Send IP RIP to this dest............ no
    Send IP default route if known..... no
  Receive IP RIP from this dest....... no
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes.............. 1
    10.0.0.0/255.255.0.0/1
  IPX network number.................. 00000000
  Use IPX RIP/SAP (negotiate with PPP): yes
  Total IPX remote routes............. 0
  Total IPX SAPs...................... 0
  Bridging enabled.................... no
```

```
    Exchange spanning tree with dest... no
  TX Encryption..................... unknown
  RX Encryption..................... unknown
  mtu............................... 1500
```

remote listbridge

Lists the current bridge settings for the specified remote router entry.

Mgmt Class

Network (R/W)

Input Format

```
remote listbridge <remotename>
```

Parameters

`***`	If entered with no parameters, bridge settings for all remote routers entries are listed.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Typical response when entered with no `<remotename>` parameter:

```
-> rem listbridge

BRIDGING INFORMATION FOR <internet>
  Bridging enabled..................... yes
    Exchange spanning tree with dest... no
    Bridge only PPPoE with dest........ no

BRIDGING INFORMATION FOR <efficient>
  Bridging enabled..................... yes
    Exchange spanning tree with dest... no
    Bridge only PPPoE with dest........ no
    Mac addresses that dial remote..... none
```

remote listiproutes

Lists IP information for a remote router or, if the router name is omitted, for all routers in the remote router database. The IP information includes all network or station IP addresses defined for the LAN connected beyond the remote router.

This command lists all routes defined for the remote router, including those defined in the default routing table and in any virtual routing tables.

Mgmt Class

Network (R)

Input Format

```
remote listiproutes <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

The following example command response lists routing information for remote router HQ. It lists five routes that use HQ, the first four are in the default routing table and the fifth is in virtual routing table FRANCISCO.`<remotename>` parameter:

```
-> rem listiproutes hq

IP INFORMATION FOR <HQ>
  Send IP RIP to this dest.............. no
    Send IP default route if known..... no
  Receive IP RIP from this dest........ rip-1 compatible
    Receive IP default route by RIP.... no
  Keep this IP destination private..... yes
  Total IP remote routes............... 5
           192.168.210.0/255.255.255.0/1
           10.0.0.0/255.0.0.0/1
           172.16.0.0/255.240.0.0/1
           192.168.0.0/255.255.0.0/1
           10.1.2.0/255.255.255.0/1 through <FRANCISCO>
```

remote listipxroutes

Lists all network IPX route addresses defined for the LAN connected beyond the remote router. The network number, hop count, and ticks are displayed. If the remote name is not specified, a list of IPX routes is displayed for each remote router in the database.

Mgmt Class

Network (R)

Input Format

```
remote listipxroutes <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Typical response.:

```
-> rem listipxroutes

IPX ROUTE INFORMATION FOR <HQ>
Total IPX remote routes.............1    00001001/1/4
```

remote listipxsaps

Lists all services defined for the LAN connected beyond the remote router. Each service includes the server name, network number, node number, socket number, server type, and hop count. If the remote name is not specified, a list of IPX SAPs is displayed for each remote router in the database.

Mgmt Class

Network (R)

Input Format

```
remote listipxsaps <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Typical response:

```
-> rem listipxsaps hq

IPX SAP INFORMATION FOR <HQ>...   1
Total IPX SAPs
SERV312_FP 00001001 00:00:00:00:00:01 0451 0004 1

IPX SAP INFORMATION FOR <ISP>
Total IPX SAPs.............    1
    SERV312_FP 00001001 00:00:00:00:00:01 0451 0004 1
```

remote listphones

Lists the PVC numbers available for connecting to the remote router.

Mgmt Class

Network (R)

Input Format

```
remote listphones <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Typical response:

```
-> rem listphones hq

PHONE NUMBER(s) FOR <HQ>
Connection Identifier (VPI*VCI)..... 0*38
```

remote restart

Stops the current active session and starts a new active session for a remote.

Certain configuration changes for a remote become effective only after the remote is restarted or the router is rebooted. Remember to save the changes before the restart or reboot.

☞ **NOTE:**

Use restart instead of reboot whenever possible. A restart does not affect other interfaces, allowing their traffic to continue. For example, using restart, you can add an IP route without killing voice traffic.

To restart an Ethernet interface, use the eth restart command.

Mgmt Class

Network (R/W)

Input Format

```
remote restart <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setatmnsap

RFC1577 (Classical IP over ATM) specifies a mechanism to map an ATM Name (called an NSAP) to a PVC. NSAP's are normally not needed, but if they are used, they have a syntax defined by using either the ATM or E164 encodings. By convention, octets 2-7 contain a unique identifier for the router, such as a MAC address.

In the command remote setATMnsap, the complete 20 octets of the NSAP are specified. If Partial mode is selected, the router substitutes the MAC address of the router for octets 2-7. In Full mode, no change is made to the NSAP.

To see an ATM NSAP that has been set, use the remote list command.

Mgmt Class

Network (R/W)

Input Format

```
remote setatmnasp  atmf | e164  partial | full  <nsap>
<remotename>
```

Parameters

`atmf`	ATM forum encoding.
`E164`	ITU E164 encoding.
`partial`	The MAC address of the router is substituted for octets 2-7 of the NSAP.
`full`	No change is made to the specified NSAP.
`<nsnap>`[a]	NSAP

[a] specified as 40 hex digits or 20 octets (2-digit pairs separated by colons

Response

Command prompt.

remote setauthen

Sets the authentication protocol used communicate with the remote router. The authentication protocol is the minimum security level that the target router must use with the remote router; this level is verified during security negotiation. The router will always attempt to negotiate the highest level of security possible (CHAP). The router will not accept a negotiated security level less than this minimum authentication method.

The parameter in the remote router database is used for the local side of the authentication process; this is the minimum security level used by the target router when it challenges or authenticates the remote router.

Mgmt Class

Security (R/W)

Input Format

```
remote setauthen <protocol> <remotename>
```

Parameters

`<protocol>`	chap, pap, or none. The default is *pap*.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setbod

Sets the bandwidth on demand (BOD) management option for a DOD (dial on demand) connection, that is, a connection where the link goes up and down. These links include those for ISDN, L2TP tunnels, IPSec tunnels, and dial backup.

The bandwidth on demand management option can be set to apply to incoming, outgoing, or both incoming and outgoing traffic. The bandwidth threshold set by the remote setbwthresh command applies to the direction of traffic set by this command.

Mgmt Class

Security (R/W)

Input Format

```
remote setBOD  in | out | both  <remotename>
```

Parameters

`in | out | both`	Incoming traffic, outgoing traffic, or both. The default is *both*.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setbroptions

Sets controls on bridging for the remote router entry. To see the current bridging settings for remote router entries, use the remote listbridge command.

CAUTION:
Do not change the <stp> setting without approval from your system administrator.

Mgmt Class

Network (R/W)

Input Format

```
remote setBrOptions <option> on | off <remotename>
```

Parameters

`option` |

`stp`	Set this option to on to use the Spanning Tree Protocol (STP). The default is *on*.
`pppoe`[a]	Set this option to on to limit this remote router entry to bridging PPPoE traffic only. If the option is set to off, then the entry can bridge any traffic, including PPPoE traffic. The default is *off*.
`<routername>`[b]	Name of the remote router

[a] The Spanning Tree Protocol adds a 40-second delay each time the ADSL or ATM link comes up while the interface determines if there is a bridging loop.
[b] ASCII string

Examples

The following example command requests the spanning tree protocol for remote router HQ.

```
-> remote setBrOptions stp on HQ
```

The following example command configures remote router PPPoEbridge as the remote through which only PPPoE traffic is bridged.

```
-> remote setBrOptions pppoeonly on PPPoEbridge
```

Response

Command prompt.

remote setbwthresh

Sets the bandwidth threshold for a DOD (dial on demand) connection, that is, a connection where the link goes up and down. These links include those for ISDN, L2TP tunnels, IPSec tunnels, and dial backup.

The threshold is used in bandwidth on demand management. Initially, a call is activated on one B-channel. When bandwidth utilization reaches the bandwidth threshold, the second B-channel is activated. (The additional channel is available if the maximum links was set to 2 by a remote setmaxline command.)

Both channel are utilized until the bandwidth utilization drops below the threshold. The default is 0% utilization, in which case, both channels are always used for data transmission.

If you wish, you can have the bandwidth threshold apply only to incoming or outgoing traffic; see the remote setbod command.

Mgmt Class

Voice (R/W)

Input Format

```
remote setBWthresh <threshold> <remotename>
```

Parameters

`<threshold>`	Percentage of bandwidth utilization (0 through 100). The default is *0*, in which case, whenever data transmission occurs, the maximum number of links is allocated.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setcompression

Enables or disables negotiation of the Stac LZS compression of the payload (RFC 1974). The CCP (Compression Control Protocol, RFC 1962) negotiates and handles any compression between the local router and the remote router.

The default setting is off because LZS compression has a negative effect with high bit rates (greater than 768 Kb/s).

To see the current setting for payload compression, enter remote list and check the Compression Negotiation line. If desired, you can follow the negotiation of the Stac LZS compression within CCP using the debug command mlp debug ccp.

Mgmt Class

Network (R/W)

Input Format

```
remote setCompression on | off <remotename>
```

Parameters

`on`	Enables compression negotiation between the local and the remote router if both routers are set to perform compression and if they both share a common compression protocol.
`off`	Disables compression negotiation. The default is *off*.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setencryption

RFC 1969 encryption. Specifies a PPP DES (Data Encryption Standard) 56-bit key with fixed transmit and receive keys.

Mgmt Class

Security (R/W)

Input Format

```
remote setEncryption DESE RX|TX <key> <remotename>
```

Parameters

`rx`	Recieve key
`tx`	Transmit key
`key`[a]	Key
`<remotename>`[b]	Name of the remote router.

[a] Hexadecimal notation
[b] ASCII string

Response

Command prompt.

remote setencryption

Diffie-Hellman Encryption. Specifies encryption based on the Diffie-Hellman key-exchange protocol. Each router possesses an internal encryption file that is associated with a public key providing 768-bit security. The predefined keys can be replaced by the user. The configuration file on the router must have a “num” suffix (e.g., dh96.num).

Mgmt Class

Security (R/W)

Input Format

```
remote setEncryption DESE_1_KEY|DESE_2_KEY [<filename>]
<remoteName>
```

Parameters

`dese_1_key`	Specifies that the same key is used in both directions.
`dese_2_key`	Specifies that the keys are different.
`<filename>`	Name of the file containing the Diffie-Hellman values. If the file is not specified, default values built into the router’s kernel are automatically selected.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setipoptions

Enables or disables the selected IP option for the WAN interface. To select IP options for the Ethernet interface, use the command eth ip options.

Several RIP options are available. RIP is a protocol used for exchanging IP routing information among routers. The RIP options allow you to set IP routing information protocol controls over a point-to-point WAN. For more information, see "RIP Controls" on page 6-4.

Mgmt Class

Network (R/W)

Input Format

```
remote setipoptions <option> on | off <remotename>
```

Parameters

`<option>` Specify one of the following options:

`rxrip`	Receive and process IP RIP-1 compatible packets and RIP-2 broadcast packets from the remote site. Also receive and process RIP-2 multicast packets. Set this option if the local router is to discover route information from other sites connected to the remote router. This is useful for hierarchical organizations. If you are connecting to another company or an Internet Service Provider, you may wish to set this option off. The default is *off*.
`rxrip1`	Receive and process RIP-1 packets only.
`rxrip2`	Receive and process RIP-2 packets only.
`rxdef`	Receive default IP route address. When this option is set on, the local router receives the remote site's default IP route. The default is *off*.
`txrip`	Transmit IP RIP-1 compatible broadcast packets and RIP-2 multicast packets to the remote site. When this option is set on, the local router sends routing information packets to the remote site. The default is *off*.
`txrip1`	Transmit broadcast RIP-1 packets only.
`txrip2`	Transmit broadcast RIP-2 packets only.
`txdef`	Transmit the local router's default IP route. When this option is set to on, the local router sends the default route to the remote site. The default is *off*.
`private`	Keep IP routes private. Used to prevent advertisement of this route to other sites by the remote router. Used as a security mechanism when the remote site is outside your company (an Internet Service Provider, for example), or whenever you want to keep the identity of the site private. The default is *on*.

Parameters Cont.

`multicast`	Allows the remote router to forward IP multicast traffic.
`lanconfig`	Accept LAN configuration information. Indicates that this PPP remote can receive IPCP information for dynamically reconfiguring the Ethernet interface.
`lcpecho`	Use periodic echo.
`<routername>`[a]	Name of the remote router

[a] ASCII string

Response

Command prompt.

remote setipslaveppp

Sets the IP Slave PPP mode. If the slave mode is yes, the router accepts the IP address that the remote end informs the router that it has; the router disregards any IP address specified in its own configuration. If the mode is no, the router tries to use the address in its configuration.

Normally there is no need to change the default (no) value of this option. However, in certain situations where the router is managed by another party, (as part of a managed service), you could set this value to yes to ensure that the central management site always specifies the IP address of the router.

Mgmt Class

Network (R/W)

Input Format

```
remote setipslaveppp  yes | no  <remotename>
```

Parameters

`yes | no`	Slave mode setting. The default is *no*.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setiptranslate

Controls Network Address Translation on a per remote router basis. It allows several PCs to share a single IP address to the Internet. The remote router must assign the source WAN IP address to the routers' local WAN port. This command requires that you define a Source WAN IP Address with the remote setsrcipaddr command.

Mgmt Class

Network (R/W)

Input Format

```
remote setiptranslate on | off <remotename>
```

Parameters

`on | off`	Enables or disables NAT.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setipxaddr

Sets the IPX network number for the remote WAN connection. For more information about IPX configuration, see IPX Routing Concepts.

Mgmt Class

Network (R/W)

Input Format

```
remote setIpxaddr <ipxNet> <remotename>
```

Parameters

`<ipxnet>`[a]	IPX network number.
`<remotename>`[b]	Name of the remote router.

[a] Hexadecimal notation
[b] ASCII string

Response

Command prompt.

remote setipxoptions

Enables or disables the IPX option RIPSAP for the remote WAN connection.

Mgmt Class

Network (R/W)

Input Format

```
remote setIpxOptions ripsap on | off <remotename>
```

Parameters

`on | off`	Enables or disables option.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setmaxline

Sets the maximum links (1 or 2) for a DOD (dial on demand) connection, that is, a connection where the link goes up and down. These links include those for ISDN, L2TP tunnels, IPSec tunnels, and dial backup.

If you set the maximum links to 2, bandwidth on demand management determines their actual usage; see the remote setbwthresh command.

Mgmt Class

Network (R/W)

Input Format

```
remote setMaxLine  1 | 2 remotename>
```

Parameters

`1 | 2`	Maximum number of links to be used for the connection (1 or 2). The default is 1.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setmgmtipaddr

Assigns to the remote router entry, an IP address which is to be used for management purposes only and not for IP address translation. This management IP address is generally a private network address used solely by the ISP.

The management IP address is separate from the IP address used for IP address translation. The IP address used for address translation is generally a public IP address valid on the Internet. It is set by the remote setsrcipaddr command.

☞ **NOTE:**

The management address is not effective until after the next save and remote restart or reboot.

NOTE:

To use the management address as the source address for a ping, you must specify it using the -I option on the ping command. For example, to use management address 192.168.1.2 when pinging destination address 192.168.100.100, specify:

ping -I 192.168.1.2 192.168.100.100

NOTE:

To use the management address as the source address for a copy, you must specify both the source and destination addresses on the copy command.

To list the current management address for the remote router, if any, use the remote list. To set a management address for an Ethernet interface, see eth ip mgmt.

Mgmt Class

Network (R/W)

Input Format

```
remote setmgmtipaddr <ipaddr> <mask> <remotename>
```

Parameters

`<ipaddr>`[a]	IP address.
`<mask>`[a]	IP sub-network mask.
`<remotename>`[b]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Response

Command prompt.

remote setminline

This command is used for dial-up connections and other connections that behave like dial-up connections, such as L2TP and PPPoE sessions. The command sets the minimum number of channels to be continually allocated to the connection. The default is 0, in which case a channel is allocated only when needed.

For example, if your service provider charges by the hour, you might prefer the minlines default value (0) so that a channel is allocated only when needed. However, if you are not charged by the hour, then having a channel allocated continually would save you the 2-3 second wait time required for each channel re-allocation.

Mgmt Class

Network (R/W)

Input Format

```
remote setminline <minlines> <remotename>
```

Parameters

`<minlines>`	Minimum number of channels to be continually allocated for the connection (0, 1, or 2). If you specify 0, a channel is allocated for the connection only when needed. The default is *0*.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Examples

The following command keeps a channel allocated for the session even when there is no traffic.

```
-> remote setMinLine 1 PPPoEuser
```

The following commands set up a timeout period so that, if there is no traffic for 10 minutes (600 seconds), the channel is de-allocated.

```
-> remote setMinLine 0 PPPoEuser
-> remote settimer 600 PPPoEuser
```

Response

Command prompt.

remote setmtu

Sets the maximum transfer unit for the remote interface.

To see the current MTU size for an active remote that is doing IP routing, use the ipifs command. To change the MTU for an Ethernet interface, use the command eth mtu.

If the protocol in use is PPP, you can see the MRU and MTU sizes using the command mlp show. The MRU is the maximum receive unit. Other information in the mlp show output includes the maxtu (the maximum packet size that can be sent; it is based on the peer's MRU size), the ourmru (the maximum PPP packet size that can be received if multilink is not running), and ourmrru (the maximum PPP packet size that can be received if multilink is running).

Input Format

```
remote setmtu <size> <remotename>
```

Parameters

`<size>`[a]	Maximum number of bytes that can be transferred as a unit.
`<remotename>`[b]	Name of the remote router.

[a] Integer
[b] ASCII string

Example

The following command decreases the MTU size for remote interface HQ to 1400 bytes.

```
-> remote setmtu 1400 HQ
```

Response

Command prompt.

remote setourpasswd

Sets a unique CHAP or PAP authentication password for the local router that is used for authentication when the local router connects to the specified remote router. This password overrides the password set in the system passwd command. A common use is to set a password assigned by the Internet Service Providers.

Mgmt Class

Security (R/W)

Input Format

```
remote setourpasswd <password> <remotename>
```

Parameters

`<password>`[a,b]	Authentication password of the local router for use in connecting to the remote router.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string
[b] The password is case-sensitive and its maximum length is 39 characters.

Response

Command prompt.

remote setoursysname

Sets a unique CHAP or PAP authentication system name for the local router that is used for authentication when the local router connects to the specified remote router. This system name overrides the system name set in the system name command. A common use is to set a password assigned by the Internet Service Providers.

Mgmt Class

Security (R/W)

Input Format

```
remote setoursysname <name> <remotename>
```

Parameters

<password>[a,b]	System name of the target router.
<remotename>[a]	Name of the remote router.

[a] ASCII string
[b] The name is case-sensitive and its maximum length is 255 characters.

Response

Command prompt.

remote setpasswd

Sets the CHAP or PAP authentication password that is used when the remote router establishes a connection or is challenged by the target router.

Mgmt Class

Security (R/W)

Input Format

```
remote setpasswd <password> <remotename>
```

Parameters

<password>[a,b]	Authentication password of the remote router.
<remotename>[a]	Name of the remote router.

[a] ASCII string
[b] The password is case-sensitive and its maximum length is 40 characters.

Response

Command prompt.

remote setphone

Specifies the phone number to be used for the dial on demand (DOD) connection, that is, a connection where the link goes up and down. These links include those for ISDN, L2TP tunnels, IPSec tunnels, and dial backup.

For dial backup, the phone number is used when dialing out using the backup V.90 modem connected to the console port. You may specify both a primary number and an alternative phone number. For more information on the Dial Backup option, see “Dial Backup” on page 6-7.

Mgmt Class

Network (R/W)

Input Format

```
remote setPhone  async | isdn  1 | 2  <phone#> <remotename>
```

Parameters

`async`	Asynchronous connection.
`isdn`	ISDN connection.
`1`	Primary phone number or first ISDN channel.
`2`	Alternative phone number or first ISDN channel.
`<phone#>`[a]	Decimal number representing the exact digits to be dialed.
`<remotename>`[b]	Name of the remote router.

[a] Digits, the asterisk, and the # characters are accepted; use a comma to specify a 2-second pause.
[b] ASCII string

Example

The following is an example of phone numbers and bit rates for an asynchronous interface used for Dial Backup.

```
-> The phone number begins with 9 (to get an outside line), a comma
(for a 2-second
-> pause), and finally the 7-digit local number.
remote setphone async 1 9,3801100 backup
remote setspeed 115200 async 1 backup
-> Specifies the alternative phone number to use and it's bit rate.
remote setphone async 2 9,3801101 backup
remote setspeed 115200 async 2 backup
```

The following is an example of a command specifying two ISDN phone numbers, 555-2000 and 555-4000.

```
-> remote setphone async 1 5552000&5554000 backup
```

Response

Command prompt.

remote setpppoptions

Enables and disables a PPP option.

The default settings vary with the option. To see the current settings of the PPP options, use the command remote list.

Mgmt Class

Network (R/W)

Input Format

```
remote setpppoptions <option> on | off <remotename>
```

Parameters

`<option>`	Specify one of the following options:	
	`compression`	Van Jacobson compression of TCP/IP headers (RFC 1144), also known as IPCP compression.
	`ipslavemode`	Always accept peer proposal for our WAN IP address.
	`lcpecho`	Use periodic echo (if permanent interface or PPPoE).
	`reacqipaddr`	Try to reacquire the IP address. Turn this option off if the router should always request a new IP address when the PPP session is terminated.
	`ripsap`	Use IPX RIP/SAP protocols.
`on | off`		Desired setting for the option.
`<routername>`[a]		Name of the remote router

[a] ASCII string

Example

The following command forces the router to always request a new IP address whenever the PPP session is terminated. (This could be useful if the other PPP system does not completely support IP address negotiation.)

```
-> remote setpppoptions reacqipaddr off HQ
```

Response

Command prompt.

remote setpppretrytimer

Enables or disables the PPP retry timer for a remote. The default is off (0).

The PPP retry timer is useful in a network where several routers are connected to the same PPP server. If the link to the PPP server goes down, all PPP sessions on the connected routers go down. Then, when the link comes back up, all routers attempt reconnection at the same time and this could crash the PPP server. To solve this problem, turn on the PPP retry timer for each remote. Then, when the link comes back up, each router waits a random time before attempting reconnection.

To see the current setting of the retry timer for a remote, use the remote list command and check the output line:

```
Retry Timer (PPP) ..................... 0
```

Mgmt Class

Network (R/W)

Input Format

```
remote setpppretrytimer <timervalue> <remotename>
```

Parameters

`<timervalue>`[a]	Timer value. The value is the maximum number of seconds before the router attempts reconnection. To disable the timer, set the value to 0.
`<remotename>`[b]	Name of the remote router.

[a] Integer, 0 - 240, (0)
[b] ASCII string

Response

Command prompt.

remote setprefer

Changes the interface for the remote entry. Normally, a new remote profile defaults to the type of the WAN port present in the router: FR for Frame-Relay WANs (IDSL and some SDSL routers) or HSD for all ATM routers.

Use this command when defining the remote profile for Dial Backup. Dial Backup uses the console port as a serial port connected to an asynchronous modem; its interface must be asynchronous (see Specifying the dial backup parameters).

To see the current setting for a remote profile, use the remote list command and check the Interface in use line. Changing the interface preference changes the lines presented in the display; phone numbers are displayed only for asynchronous. See the example below.

Mgmt Class

Network (R/W)

Input Format

```
remote setprefer  < async  | fr  | hsd >  <remotename>
```

Parameters

`async`	Asynchronous. This preference allows you to specify phone numbers and bit rates in the remote profile.
`fr`	Frame Relay
`hsd`	High-Speed Data. Use this option for ATM virtual circuits; in this case, phone numbers take the form <VPI>*<VCI>.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Example

The information displayed by a remote list command changes depending on the interface preference. The following example shows how the information displayed changes from asynchronous to frame relay:

```
-> remote setprefer fr backup
-> remote list backup
INFORMATION FOR <backup>
     Status.............................. enabled
     Our System Name when dialing out..... gwbush
     Our Password used when dialing out... yes
     Interface in use.................... FR
     Protocol in use..................... PPP
     Authentication...................... disabled
```

```
     Authentication level required........ PAP
     . . . (subsequent lines same as for async) . . .
-> remote setPrefer async backup
-> remote list backup
     INFORMATION FOR <backup>
     Status.............................. enabled
     Our System Name when dialing out..... gwbush
     Our Password used when dialing out... yes
     Disconnect timeout (in seconds)...... 60
     Min/max channels..................... 0/1
     Interface in use..................... ASYNC
     Protocol in use...................... PPP
     Authentication....................... disabled
     Authentication level required........ PAP
     Bandwidth management criteria........ both
     Use periodic LCP pings............... yes
     1. ASYNC telephone number, speed 115200 9,5554218
     2. ASYNC telephone number, speed 115200 9,5554219
     1. HSD telephone number, speed auto
     2. HSD telephone number, speed auto
     Dial Back.............................off
     Request PPP Call Back.................no
```

Response

Command prompt.

remote setprotocol

Sets the link protocol for the remote router.

☞ **NOTE:**

The link protocol and encapsulation option must match those at the other end of the connection (the settings in the DSLAM).

The encapsulation options are described in "Encapsulation Options" in Chapter 2 of the Technical Reference manual.

Mgmt Class

Network (R/W)

Input Format

```
remote setProtocol  PPP | PPPLLC | RFC1483 | RFC1483MER | FRF8
| RAWIP  <remotename>
```

Parameters

`ppp`	PPP protocol with VC multiplexing encapsulation.
`ppplc`	PPP protocol with LLC SNAP encapsulation (used with frame relay internetworking units).
`rfc1483`	RFC 1483 protocol.
`rfc1483mer`	RFC 1483MER (MAC Encapsulated Routing) protocol.
`fr8`	This protocol implements ATM to frame relay as defined in the Frame Relay Forum FRF.8 Interworking Agreement.
`rawip`	RawIP protocol.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setpvc

Specifies the PVC number for connecting to the remote router.

Mgmt Class

Network (R/W)

Input Format

```
remote setpvc <vpi number>*<vci number> <remotename>
```

Parameters

`<vpi number>`	Virtual Path ID - number that identifies the link formed by the virtual path.
`<vci number>`	Virtual Circuit ID - number that identifies a channel within a virtual path in a DSL/ATM environment.
`rfc1483`	RFC 1483 protocol.
`rfc1483mer`	RFC 1483MER (MAC Encapsulated Routing) protocol.
`fr8`	This protocol implements ATM to frame relay as defined in the Frame Relay Forum FRF.8 Interworking Agreement.
`rawip`	RawIP protocol.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote setrmtipaddr

Sets the WAN IP address for the remote router. This address is required only if the remote router does not support IP address negotiation under PPP (i.e., numbered mode is required, and the remote router cannot specify a WAN IP address for use during the negotiation process).

Mgmt Class

Network (R/W)

Input Format

```
remote setrmtipaddr <ipaddr> <mask> <remotename>
```

Parameters

`<ipaddr>`[a]	IP address of the remote router.
`<mask>`[a]	IP network mask of the remote router.
`<remotename>`[b]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Response

Command prompt.

remote setspeed

Specifies the speed to be used when dialing out using the backup V.90 modem connected to the console port. Specify a speed for each phone number you provide (primary and alternative).

For more information specifying phone numbers for the Dial Backup feature, see "Specifying the Dialup Parameters" on page 6-9.

Mgmt Class

Network (R/W)

Input Format

```
remote setspeed <bitrate> | default  async  1 | 2  <remotename>
```

Parameters

`<bitrate>`[a]	Bit rate to be used for the phone number.
`default`	Use the default speed.
`1`	Primary phone number.
`2`	Alternative phone number.
`<remotename>`[b]	Name of the remote router.

[a] Range - possible speeds are 38400, 57600, 115200, or 230400.
[b] ASCII string

Examples

The following command specifies the primary phone number and its bit rate.

```
-> remote setphone async 1 9,5551288 backup
-> remote setspeed 115200 async 1 backup
```

The following commands specifies the alternative phone number to be used and its bit rate.

```
-> remote setphone async 2 9,5551289 backup
-> remote setspeed 115200 async 2 backup
```

Response

Command prompt.

remote setsrcipaddr

Sets the IP address for the target WAN connection to the remote router. You may set this address when the remote router requires the target and the remote WAN IP addresses to be on the same subnetwork. Another instance is to force numbered mode and to prevent the remote router from changing the target WAN IP address through IPCP address negotiation. The target WAN IP address defaults to the Ethernet LAN IP address.

Mgmt Class

Network (R/W)

Input Format

```
remote setsrcipaddr <ipaddr> <mask> <remotename>
```

Parameters

`<ipaddr>`[a]	Target IP address of the WAN connection to the remote router.
`<mask>`[a]	IP network mask of the remote router.
`<remotename>`[b]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Response

Command prompt.

remote settimer

This command is used for dial-up connections and other connections that behave like dial-up connections, such as L2TP and PPPoE sessions. The command sets the length of the timeout period before disconnection.

When the connection has had no traffic for the timeout period, the channel is deallocated. A channel is re-allocated when it is needed.

A timeout period is desirable if your service provider charges by the hour. However, the connection has to wait a few seconds each time a channel is re-allocated.

☞ **NOTE:**

The timeout period set by this command is not effective if a remote setMinLines command has changed the minlines value from its default (0) to 1 or 2

Mgmt Class

Network (R/W)

Input Format

```
remote settimer <seconds> <remotename>
```

Parameters

`<seconds>`[a]	Number of seconds in the timeout period.
`<remotename>`[b]	Name of the remote router.

[a] Integer, 0 - 60 (60)
[b] ASCII string

Example

set up a timeout period so that, if there is no traffic for 10 minutes (600 seconds), the channel is de-allocated

```
-> remote setMinLine 0 PPPoEuser
-> remote settimer 600 PPPoEuser
```

Response

Command prompt.

remote start

If the remote is not currently active, this command attempts to start an active session.

☞ **NOTE:**

A reboot ends the active session; to start a session after the reboot, you must enter another remote start command.

To stop an active session for the remote, use the remote stop command. To stop and immediately restart a session for the remote, use the remote restart command.

Mgmt Class

Network (R/W)

Input Format

```
remote start <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote stats

Shows the current status of the connection to the remote router, including the bandwidth and data transfer rate.

Mgmt Class

Network (R)

Input Format

```
remote stats <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Typical response:

```
-> remote setprefer fr backup
-> remote list backup
   Current state                Currently connected
   Current output bandwidth     0 bps
   Current input bandwidth      0 bps
   Current bandwidth allocated  25600000 bps
   On port ATM_VC/1             0+01:02:36 (0%/0% of 25600000
                                bps)
   Total connect time           0+01:11:48
   Total bytes out              15896
   Total bytes in               0

STATISTICS FOR <internet>:
   Current state                Not connected
   Current output bandwidth     0 bps
   Current input bandwidth\     0 bps
   Current bandwidth allocated  0 bps
   Total connect time           0+00:00:00
   Total bytes out              0
   Total bytes in               0
```

remote stop

If the remote is active, this command stops the active session.

☞ **NOTE:**

To keep certain configuration changes, you must enter a save command before stopping the remote interface.

☞ **NOTE:**

The stop command does not disable the remote entry so another session can be started for the remote.To start an active session for the remote, use the remote start commad. To stop and immediately restart a session for a remote, use the remote restart command.

Mgmt Class

Network (R/W)

Input Format

```
remote stop <remotename>
```

Parameters

`<remotename>`[a] Name of the remote router.

[a] ASCII string

Response

Command prompt.

remote unbindipvirtualroute

Removes a remote route from the named IP virtual routing table.

To list the remote routes, use the remote listiproutes command. To add a remote route, use the remote remote bindipvirtualroute command.

☞ **NOTE:**
A route change in an IP virtual routing table takes effect immediately. However, the change is lost if it is not saved before the next remote restart or reboot.

Mgmt Class

Network (R/W)

Input Format

```
remote unbindipvirtualroute <ipaddr> <tablename> <remotename>
```

Parameters

`<ipaddr>`[a]	IP address of the remote network or station.
`<tablename>`[b]	IP virtual routing table to which the route is removed.
`<remotename>`[a]	Name of the remote router.

[a] Dotted-decimal notation
[b] ASCII string

Example

The following command removes a route from virtual routing table FRANCISCO. The route removed is for IP address 10.1.2.0 and remote router HQ.

```
-> remote unbindIPVirtualRoute 10.1.2.0 FRANCISCO HQ
```

Response

Command prompt.

This page intentionally left blank.

CHAPTER 7

WAN INTERFACE COMMANDS

This chapter contains subsections of commands applicable to specific WAN interfaces. The subsections are:

- ADSL (Asymmetric Digital Subscriber Line) commands, see ADSL Commands.
- ADSL, Annex B commands, see GTI Commands.
- ATM (Asynchronous Transfer Mode) commands, see ATM Commands.
- DMT (Discrete Multi-Tone) commands, see DMT Commands.
- Dual-Ethernet commands, see Dual-Ethernet Router (ETH) Commands.
- Frame Relay commands, see Frame Commands.
- HDSL (High-speed Digital Subscriber Line) commands, see HDSL Commands.
- IDSL (ISDN Digital Subscriber Line) commands, see IDSL Commands.
- SDSL (Symmetric Digital Subscriber Line) commands, see SDSL Commands.
- G.shdsl commands, see SHDSL Commands.

☞ **NOTE:**

If you are unsure which set of commands is applicable to your system, enter a ? at the command prompt and look for one of the WAN interface key words listed in the top-level command listing. The response, for example *sdsl* or *adsl*, indicates the appropriate command set to use.

ADSL Commands

This section provides the commands to manage the ADSL (Asymmetric Digital Subscriber Line) link for an ADSL router. These commands include:

Table 7-1: ADSL Command Listing

Command	Function
adsl ?	Lists the supported ADSL keywords.
adsl restart	Re synchronizes the modem with the CO (Central Office) equipment.
adsl speed	Displays the current downstream and upstream rates.
adsl stats	Shows the current error status for the ADSL connection.

adsl ?

Lists the supported ADSL keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
adsl ?
```

Parameters

None

Response

A listing of the ADSL commands and keywords with a brief description of their function.

adsl restart

Re synchronizes the modem with the CO (Central Office) equipment.

Mgmt Class

Network (R/W)

Input Format

```
adsl restart
```

Parameters

None

Response

```
-> adsl restart

# 12/02/1997-12:47:46:ADSL: Idle
12/02/1997-12:47:46:ADSL: Startup initiated
12/02/1997-12:47:48:ADSL: Startup training in progress
12/02/1997-12:47:54:ADSL: Modem started successfully
12/02/1997-12:47:54:ADSL: Near Avg SQ #: 44 dB [   3]
12/02/1997-12:47:54:ADSL: Far  Avg SQ #: 44 dB [   3]
12/02/1997-12:47:54:ADSL: Downstream rate: 6272 Kb/s, Upstream
rate: 1088 Kb/s
12/02/1997-12:47:54:DOD: connecting to internet @ 0*38 over ATM_VC/1
12/02/1997-12:47:56:ADSL: Data Mode
DUM: BR CHG ATM_VC/1 - to internet now forwarding
```

adsl speed

Displays the current downstream and upstream rates.The actual speed is set by the DSLAM.

Mgmt Class

Network (R)

Input Format

```
adsl speed
```

Parameters

None

Response

```
-> adsl speed
downstream rate: 6272 Kb/s, upstream rate: 1088 Kb/s
```

adsl stats

Shows the current error status for the ADSL connection.

Mgmt Class

Network (R/W)

Input Format

```
adsl stats [clear]
```

Parameters

***	When entered with no parameters, the current ADSL statistics are displayed.
clear	Optional, resets the statistical counters.

Response

Statistical information displayed.

```
-> adsl stats
  Out of frame errors....   0
  HEC errors received....   0
  CRC errors received....   0
  FEBE errors received...   0
Remote Out-of-frame.......  0
Remote HEC errors.........  0
```

ATM Commands

The following commands are used to manage the ATM-25 (Asynchronous Transfer Mode) link for an ATM router. The commands include:

Table 7-2: ATM Command Listing

Command	Function
atm ?	Lists the supported ATM keywords.
atm pcr	Sets the speed of the ATM link in cells per second.
atm save	Saves the ATM configuration settings.
atm speed	Sets the speed of the ATM link in kilobits per second.
remote setatmtraffic	Sets ATM traffic-shaping on a remote router.

atm ?

Lists the supported ATM keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
atm ?
```

Parameters

None

Response

Lists the supported ATM commands and keywords and a brief description of their function. inconsistent

atm pcr

Sets the speed of the ATM link in cells per second.

The default upstream speed is 768 cells/second. Generally, your Network Service Provider should provide you with your speed value. If your service provider states your speed value in kilobits per second, enter the value using the atm speed command.

☞ **NOTE:**
The speed value entered may not be the actual upstream speed attained. When the command changes the processor clocks, only certain discrete values are allowed. The speed achieved is the allowed speed value that is equal to or the next lower value to the value entered (see the example below).

Mgmt Class

Network (R/W)

Input Format

```
atm pcr [cells/second]
```

Parameters

`***`	When entered with no parameters, the current upstream speed is displayed.
`<cells/second>`[a]	Upstream speed requested in cells/second.

[a] Integer, 294-18867

Example

The following command requests the current speed.

```
-> atm pcr 1200
ATM Upstream Rate:   500 Kb/sec or  1179 cells/sec
```

Response

Typical response when entered with no parameter.

```
-> atm pcr
ATM Upstream Rate:   326 Kb/sec or   768 cells/sec
```

atm save

Saves the ATM configuration settings.

Mgmt Class

Network (R/W)

Input Format

```
atm save
```

Parameters

None

Response

Command prompt.

atm speed

Sets the speed of the ATM link in kilobits per second.

The default upstream speed is 326 Kb/s. Generally, your Network Service Provider should provide you with your speed value. If your service provider states your speed value in cells per second, enter the value using the command atm pcr.

☞ **NOTE:**

The speed value entered may not be the actual upstream speed attained. When the command changes the processor clocks, only certain discrete values are allowed. The speed achieved is the allowed speed value that is equal to or the next lower value to the value entered.

Mgmt Class

Network (R/W)

Input Format

```
atm speed [Kb/s]
```

Parameters

`***`	When entered with no parameters, the current upstream speed is displayed.
`<kb/s>`[a]	Upstream speed requested in kilobits/second.

[a] Integer, 125-8000

Example

The following command example requests a speed of 512 kilobits/second. However, 512 is not one of the discrete speed values allowed, so the next lower value, 500 kilobits/second, is set, as indicated by the message.

```
-> atm speed 512

ATM Upstream Rate:   500 Kb/sec or  1179 cells/sec
```

Response

The following is a typical response from a request for the current speed.

```
-> atm speed

ATM Upstream Rate:   326 Kb/sec or   768 cells/sec
```

remote setatmtraffic

Sets ATM traffic-shaping on a remote router. ATM traffic-shaping allows the user to set the average rate at which cells are sent, that is, the Sustained Cell Rate (SCR), to a value lower than the ATM link speed, the Peak Cell Rate (PCR).

ATM traffic-shaping should be used to allocate bandwidth whenever more than one remote router is defined. Enter a remote setATMTraffic command for each remote. For example, if you have five remotes, enter five commands to allocate the bandwidth.

If no ATM traffic values are set, ATM traffic for the remote is shaped using UBR (unspecified bit rate).

If a CBR (constant bit rate) is required, then specify 1 as the Maximum Burst Size (MBS). If a VBR (Variable Bit Rate) is required, specify a value greater than 1 as the Maximum Burst Size (MBS).

Mgmt Class

Network (R/W)

Input Format

```
remote setATMTraffic <scr> <mbs> <remoteName>
```

Parameters

<scr>[a]	Sustained Cell Rate (cells per second).
<mbs>	Maximum Burst Size (cells). For a constant bit rate (CBR), specify 1; for a variable bit rate (VBR), specify a value greater than 1.
<remotename>[b]	Name of the remote router.

[a] Integer
[b] ASCII string

Examples

The following command disables ATM traffic-shaping remote router HQ.

```
-> remote setATMTraffic 0 0 HQ
```

Assuming that the ATM link speed (upstream) is 200 Kb/s 471 cells/s and an average upstream data rate of 20 Kbps (47 cells/s) is desired, you would issue the following command:

```
-> remote setATMtraffic 47 31 HQ
```

If a constant bit rate (CBR) is required, use the following command:

```
-> remote setATMtraffic 47 1 HQ
```

Response

Command prompt.

DMT Commands

These commands contained in this section are used manage the ADSL DMT (Discrete MultiTone) router; they include

Table 7-3: DMT Command Listing

Command	Function
dmt ?	Lists the supported DMT keywords.
dmt link	Selects the link type for the ADSL DMT router.
dmt mode	Sets DMT operational mode.

dmt ?

Lists the supported DMT keywords. To see the syntax for a command, enter the command followed by a ?.

Input Format

```
dmt ?
```

Mgmt Class

Network (R)

Parameters

None

Response

Lists the supported DMT commands and keywords and a brief description of their function.

dmt link

Selects the link type for the ADSL DMT router. The link type is persistent across reboots.

Normally, the CO and CPE negotiate the link type to be used. Use the dmt link command when you do not want the CO and CPE to negotiate the link type, but instead want to specify the type of data link required.

CAUTION:
This command forces the CPE into the specified mode. It is not for normal use.

Mgmt Class

Network (R/W)

Input Format

```
dmt  link  DEFAULT | T1_413 | G_DMT | G_LITE | MULTIMODE
```

Parameters

`default`	Default value. The CO and CPE negotiate the link type used.
`T1_413`	ANSI standard T1.413
`G_DMT`	G.dmt standard
`G_LITE`	ITU G.Lite standard
`MULTIMODE`	The CO and CPE negotiate the link type used.

Response

Command prompt.

dmt mode

Sets DMT operational mode. The dmt mode command can request one of three modes: ANSI, no_Trellis_ANSI, and UAWG.

☞ **NOTE:**

UAWG mode is becoming obsolete.

No Trellis encoding for T1.413 ANSI ADSL is only needed where auto-negotiation is not supported for Trellis.

Mgmt Class

Network (R/W)

Input Format

```
dmt mode ansi | no_trellis_ansi | uawg
```

Parameters

`ansi | no_trellis_ansi` Selects the DMT mode used.

Response

Command prompt.

Dual-Ethernet Router (ETH) Commands

The following Ethernet commands are used to manage the Ethernet interfaces of the Dual-Ethernet (Ethernet-to-Ethernet) router and thus are specific to that type of router only. For the other Ethernet commands, see Chapter 5, Ethernet Interface Commands.

The Dual-Ethernet router has two interfaces:

- ETH/0Hub with four 10Base-T connectors
- ETH/1Single 10Base-T connector

This Dual-Ethernet router may be configured via the Web Browser GUI or from the Command Line Interface (CLI). To set up any DHCP options and to configure optional features like IP filtering, you must use the CLI.

If using the ***Boot from Network option*** from the ***boot menu*** to perform a boot code update, the boot request is sent from the ETH/0 interface only.

The Dual-Ethernet Router commands found in this section include:

Table 7-4: Dual Ethernet Router Command Listing

Command	Function
eth br enable	Enables bridging in a Dual-Ethernet environment.
eth br disable	Disables bridging in a Dual-Ethernet environment.
eth br options	Sets controls on bridging for the Ethernet interface.

eth br enable

Enables bridging in a Dual-Ethernet environment. This command requires a reboot of the router for the change to take effect.

Mgmt Class

Network (R/W)

Input Format

```
eth br enable
```

Parameters

None

Response

Command prompt.

eth br disable

Disables bridging in a Dual-Ethernet environment.

☞ **NOTE:**
This command requires a reboot of the router for the change to take effect.

Mgmt Class

Network (R/W)

Input Format

```
eth br disable
```

Parameters

None

Response

Command prompt.

eth br options

Sets controls on bridging for the Ethernet interface. To see the current bridge settings for the Ethernet interface, use the eth list command.

Spanning Tree Protocol (STP) is used to detect bridging loops. Set this option to off only if the bridging peers do not support the Spanning Tree Protocol or if you are certain that no bridging loops could exist. When STP is disabled on an interface, any STP packets received on that interface are ignored.

CAUTION:

Warning: Do not change the Spanning Tree Protocol (stp) setting without approval from your system administrator.

The PPPoESet option limit this Ethernet port to bridging PPPoE traffic only. If the option is set to off, then the port can bridge any traffic, including PPPoE traffic. The default is off.

Mgmt Class

Network (R/W)

Input Format

```
eth br options <option> on | off [<port#>]
```

Parameters

`option` |

`stp`	Set this option to *on* to use the Spanning Tree Protocol (STP). The default is *on*.
`pppoe`[a]	Set this option to on to limit this remote router entry to bridging PPPoE traffic only. If the option is set to off, then the entry can bridge any traffic, including PPPoE traffic. The default is *off*.
`<port#>`[b]	Ethernet port number.

[a] The Spanning Tree Protocol adds a 40-second delay each time the ADSL or ATM link comes up while the interface determines if there is a bridging loop.
[b] Integer, 0 - 1 (0)

Examples

The following command turns off the spanning tree protocol for Ethernet port 0.

```
-> eth br options stp off
```

The following command configures Ethernet port 1 so that only PPPoE traffic is bridged through it.

```
-> eth br options pppoeonly on 1
```

Response

Command prompt.

Frame Commands

The following commands are used to manage a frame relay router's WAN interface. The Frame Relay commands found in this section include:

Table 7-5: Frame Relay Command Listing

Command	Function
frame ?	Lists the supported frame keywords.
frame cmpplay	Selects activation in routing or bridge mode. This command is applicable only when the router is configured using Copper Mountain Plug & Play.
frame lmi	Turns frame LMI either on or off.
frame stats	Displays frame relay statistics.
frame voice	Displays the voice DLCI for voice routers.

frame ?

Lists the supported frame keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
frame ?
```

Parameters

None

Response

Lists the supported frame relay commands and keywords and a brief description of their function.

frame cmpplay

Selects activation in routing or bridge mode. This command is applicable only when the router is configured using Copper Mountain Plug & Play (see Chapter 3 of the Technical Reference manual).

Mgmt Class

Network (R/W)

Input Format

```
frame cmpplay  < router | bridge >
```

Parameters

`bridge`	Selects bridging mode.
`router`	Selects bridging mode, default value.

Response

Command prompt.

frame lmi

Turns frame LMI either on or off.

Mgmt Class

Network (R/W)

Input Format

```
frame lmi  on | off
```

Parameters

`on`	Enables LMI.
`off`	Disables LMI.

Response

Command prompt.

frame stats

Displays frame relay statistics.

Mgmt Class

Network (R)

Input Format

```
frame stats
```

Parameters

None

Response

Although it is not an end-to-end loopback test, the command output does show counters for data sent and received as well as LMI events.

```
-> frame stats

FR/0 Frame Relay Statistics
ANSI LMI:
Protocol Errors..................... 0
Unknown Msg Recv.................... 0
T391 Timeouts....................... 0
PVC Status Changes.................. 0
StatusEnq Sent...................... 0
Status Recv......................... 0
StatusEnq Recv...................... 0
Unconfigured DLCIs recv in Status Msgs. 0
    LMI Stats for DLCI.............. 22
    LMI State....................... UNKNOWN
    Status State Changes............ 0
    Active to Not Active Changes.... 0
    Not Active to Active Changes.... 0
    Data Packets In................. 0
    Data Packets Out................ 0
    Data Packets Out Queued......... 0
    Data Packets Out (dropped Q Full).. 0
    Voice Cells In.................. 0
    Voice Cells In (with errors).... 0
    Voice Cells Out................. 0

    LMI Stats for DLCI.............. 16
```

```
LMI State.......................... UNKNOWN
Status State Changes............... 0
Active to Not Active Changes....... 0
Not Active to Active Changes....... 0
Data Packets In.................... 0
Data Packets Out................... 0
Data Packets Out Queued............ 0
Data Packets Out (dropped Q Full).. 0
Voice Cells In..................... 0
Voice Cells In (with errors)....... 0
Voice Cells Out.................... 0

Data Out (Delayed by Voice)........ 0
```

frame voice

Displays the voice DLCI for voice routers.

Mgmt Class

Voice (R)

Input Format

```
frame voice
```

Parameters

None

Response

Command prompt.

GTI Commands

This section provides the commands to manage the GTI - ADSL, Annex B (Asymmetric Digital Subscriber Line) link for an ADSL router. These commands include:

Table 7-6: GTI Command Listing

Command	Function
gti ?	Lists the supported GTI keywords.
gti speed	Displays the current downstream and upstream rates.
gti stats	Shows the operational time for the system and ADSL connection.
gti version	Displays GTI ADSL version information.

gti ?

Lists the supported GTI keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
gti ?
```

Parameters

None

Response

A listing of the gti commands and keywords with a brief description of their function.

gti speed

Displays the current downstream and upstream rates.The actual speed is set by the DSLAM.

Mgmt Class

Network (R)

Input Format

```
gti speed
```

Parameters

None

Response

```
-> gti speed
ATM Downstream: 6088 Kb/s    Upstream: 1021 Kb/s
```

gti stats

Shows the operational time for the system and ADSL connection.

Mgmt Class

Network (R)

Input Format

```
gti stats
```

Parameters

None

Response

Statistical information displayed.

```
-> gti stats
 System up:    12 days 16 hours 48 minutes
 Line up:      12 days 16 hours 47 minutes
```

gti version

Displays GTI ADSL version information.

Mgmt Class

Network (R)

Input Format

```
gti speed
```

Parameters

None

Response

GTI ADSL Version information is displayed.

```
-> gti version

   Firmware: P11
   DSP Version: 0
```

HDSL Commands

Use the following commands to manage the HDSL (High-Speed Digital Subscriber Line) link for an HDSL router.

The HDSL commands found in this section include:

Table 7-7: HDSL Command Listing

Command	Function
hdsl ?	Lists the supported HDSL keywords.
hdsl save	Saves the HDSL-related changes across restarts and reboots.
hdsl speed	Manages the line speed for the HDSL interface.
hdsl terminal	Defines router terminal operational mode as Central Office (CO) or Customer Premises Equipment (CPE).

hdsl ?

Lists the supported HDSL keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
hdsl ?
```

Parameters

None

Response

Lists the supported HDSL commands and keywords and a brief description of their function.

hdsl save

Saves the HDSL-related changes across restarts and reboots.

Mgmt Class

Network (R/W)

Input Format

```
hdsl save
```

Parameters

None

Response

Command prompt.

hdsl speed

Manages the line speed for the HDSL interface, as follows:

- CO end: Sets the speed manually on the Central Office (CO) end only.
- CPE end: The router on the Customer Premises End (CPE) is always in auto-speed mode: it uses an auto-speed algorithm to attempt to match the CO speed. The command hdsl speed noauto is used to override auto-speed.

Mgmt Class

Network (R/W)

Input Format

```
hdsl speed [384 | 1168 | noauto]
```

Parameters

`***`	When entered with no parameters, the current speed is dispaly-ed. [a]
`384`	Authorized non-default speed for the CO in Mbps.
`1168`	Authorized non-default speed for the CO in Mbps.
`noauto`[b]	Used to override auto-speed on the CPE.

[a] Available only if the modem has activated successfully.
[b] *hdsl speed noauto* should be followed by the command hdsl save to be persistent across restarts and reboots.

Response

Command prompt:

hdsl terminal

The router is by default configured as the Customer Premises Equipment (CPE). Use this command if you intend to configure the router as the Central Office equipment (CO).

- `hdsl terminal cpe` defines the CPE end (default configuration)
- `hdsl terminal co` defines the CO end.
- `hdsl terminal` displays the current settings.

Mgmt Class

Network (R/W)

Input Format

```
hdsl terminal [cpe | co]
```

Parameters

`***`	When entered with no parameters, the current mode is displayed.
`cpe`	Sets the terminal operation mode to CPE.
`co`	Sets the terminal operation mode to CO.

Response

Command example displaying current mode:

```
-> hdsl terminal
Customer Premise
```

IDSL Commands

This section describes the following commands used to manage an IDSL interface. The IDSL commands found in this section include:

Table 7-8: IDSL Command Listing

Command	Function
idsl list	Lists the current switch type.
idsl save	Saves the IDSL-related changes across restarts and reboots.
idsl set speed	Specifies the speed of the IDSL connection.
idsl set switch	Specifies link speeds of 64, 128, or 144 Kbps for the IDSL connection.
remote setdlci	Sets the DLCI for the remote router entry.
remote setprotocol	Specifies the appropriate link protocol for the IDSL connection.

idsl list

Lists the current switch type. To change the switch type, use the idsl set switch command.

Mgmt Class

Network (R)

Input Format

```
idsl list
```

Parameters

None

Response

```
Typical response:
  -> idsl list
  Switch type is FR128
```

idsl save

Saves IDSL-related changes across restarts and reboots. Changes that are not saved are discarded.

Mgmt Class

Network (R/W)

Input Format

```
idsl save
```

Parameters

None

Response

Command prompt.

idsl set speed

Specifies the speed of the IDSL connection. The IDSL bandwidth is composed of two 64 Kbps B channels, plus one 16 Kbps D channel. Your speed setting indicates the channels that you are using.

Mgmt Class

Network (R/W)

Input Format

```
idsl set speed 64 | 128 | 144
```

Parameters

`64`	64 Kbps (one channel)
`128`	128 Kbps (two channels)
`144`	144 Kbps (three channels)

Response

Command prompt.

idsl set switch

Specifies link speeds of 64, 128, or 144 Kbps for the IDSL connection.

Mgmt Class

Network (R/W)

Input Format

```
idsl set switch FR64 | FR128 | FR144
```

Parameters

`FR64`	Link speed of 64 Kbps
`FR128`	Link speed of 128 Kbps
`FR144`	Link speed of 144 Kbps

Response

Command prompt.

remote setdlci

This command sets the DLCI for the remote router entry. The DLCI (Data Link Connection Identifier) is an address identifying a logical connection in a Frame Relay environment. The DLCI is generally provided by the Network Service Provider.

The IDSL router can support several DLCI virtual circuits over a Frame-Relay IDSL link. However, a typical connection to the Internet requires only one DLCI. The DLCI number must match the DLCI of the remote end.

Mgmt Class

Network (R/W)

Input Format

```
remote setdlci <dlcinumber> <remotename>
```

Parameters

`<dlcinumber>`[a]	Frame Relay number identifying the data-link connection.
`<remotename>`[b]	Name of the remote router.

[a] Integer
[b] ASCII string

Response

Command prompt.

remote setprotocol

This IDSL-specific command is used to select the appropriate link protocol for the IDSL connection. The Network Service Provider should provide which link protocol to use.

Mgmt Class

Network (R/W)

Input Format

```
remote setProtocol ppp | fr | mer  <remotename>
```

Parameters

`ppp`	PPP protocol with no encapsulation.
`fr`	RFC 1490 protocol (Multiprotocol encapsulation over Frame Relay).
`mer`	RFC 1490 protocol with MAC Encapsulated Routing.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string

Response

Command prompt.

SDSL Commands

The commands in this section are used to manage the Symmetric Digital Subscriber Line (SDSL) link for an SDSL router. The SDSL commands found in this section include:

Table 7-9: SDSL Command Listing

Command	Function
sdsl ?	Lists the supported SDSL keywords.
sdsl preact	Displays and/or changes the autobaud pre-activation status.
sdsl save	Saves SDSL configuration changes across restarts and reboots.
sdsl speed	Manages the speed of the SDSL line.
sdsl terminal	Displays and/or changes the router's status as CO or CPE.

sdsl ?

Lists the supported SDSL keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
sdsl ?
```

Parameters

None

Response

Lists the supported SDSL commands and keywords and a brief description of their function.

sdsl preact

Displays and/or changes the autobaud pre-activation status.The default status is on. However, to be effective, autobaud pre-activation must also be enabled at the Central Office (CO) end of the connection.

☞ **NOTE:**

Remember to enter an sdsl save or save command to save SDSL changes across restarts and reboots.

For more information on the autobaud feature, see Auto-baud preactivation.

Mgmt Class

Network (R/W)

Input Format

```
sdsl preact [on | off]
```

Parameters

`on`	Enables pre-activation at the customer premises equipment (CPE) end.[a]
`off`	Disables pre-activation.

[a] To be effective, pre-activation must also be enabled at the CO end.

Response

SDSL preactivation status is displayed.

```
Preactivation enabled
```

```
Preactivation disabled
```

sdsl save

Saves SDSL configuration changes across restarts and reboots.

Mgmt Class

Network (R/W)

Input Format

```
sdsl save
```

Parameters

None

Response

Command prompt.

sdsl speed

Manages the speed of the SDSL line.

- At the Central Office (CO) end, the command sets the speed manually only.
- At the Customer Premises Equipment (CPE) end, the command can:
  - Display the current speed setting and list the available speeds (sdsl speed)
  - Manually set the speed (`sdsl speed <speed>`)
  - Override auto-speed detection (`sdsl speed noauto`)

☞ **NOTE:**
To re-instate auto-speed detection, enter an `sdsl speed <speed>` command.

Mgmt Class

Network (R/W)

Input Format

```
sdsl speed [<speed> | noauto]
```

☞ **NOTE:**

Enter an sdsl save or reboot command to save SDSL changes across restarts and reboots.

Parameters

`***`	When entered with no parameters, the current speed is displayed.
`<speed>`	Speed in kbps.[a]
`noauto`	Overrides auto-speed detection.[b]

[a] If the auto-speed search is in progress, this command stops the search and sets the line speed as specified on the command. Auto-speed detection is reinstated if an sdsl speed <*speed*> command is entered.

[b] If auto-speed detection is disabled, the Link light on the front panel is amber when the line tries to activate.

Examples

This command example displays the current line speed, indicates that the line speed is set by auto-speed detection [*AUTO*], and lists the available speed options.

```
-> sdsl speed

SDSL Current Speed: [AUTO] 768 Kb/s

usage: sdsl speed <value in Kb/s> [ 192 384 768 1152 1536 ] | noauto
```

This command example requests a line speed of 1152 Kb/s.

```
-> sdsl speed 1152
```

This command example shows that the line speed has been changed to 1151 Kb/s and that auto-speed detection is no longer in effect (the [AUTO] indicator is not displayed).

```
-> sdsl speed

SDSL Current Speed: 1152 Kb/s

usage: sdsl speed <value in Kb/s> [ 192 384 768 1152 1536 ] | noauto
```

Response

See examples above.

sdsl terminal

Displays and/or changes the router's status as CO or CPE. The router is, by default, configured as Customer Premises Equipment (CPE). Use this command if to configure the router as Central Office equipment (CO).

Mgmt Class

Network (R/W)

Input Format

```
sdsl terminal [cpe | co]
```

Parameters

`***`	When entered with no parameters, the current mode is displayed.
`cpe`	Sets the terminal operation mode to CPE.
`co`	Sets the terminal operation mode to CO.

Response

Terminal operation is displayed:

```
-> sdsl terminal
Customer Premises
```

SHDSL Commands

The commands in this section are used to manage the WAN link for a G.shdsl router. The SHDSL commands found in this section include:

Table 7-10: SHDSL Command Listing

Command	Function
shdsl ?	Lists the supported SHDSL keywords.
shdsl annex	Selects annex A or annex B of the G.shdsl standard.
shdsl list	Lists the current configuration of the G.shdsl interface.
shdsl margin	Specifies the acceptable noise margin in decibels.
shdsl ratemode	Selects adaptive or fixed rate mode.
shdsl restart	Restarts the G.shdsl WAN interface.
shdsl save	Saves SHDSL configuration changes across restarts and reboots.
shdsl speed	Manages the speed of the SHDSL line.
shdsl stats	Displays and/or clears SHDSL statistics.
shdsl terminal	Displays and/or changes the router's status as CO or CPE.
shdsl ver	Displays the G.shdsl version level of the modem firmware.

shdsl ?

Lists the supported SHDSL keywords.

Input Format

```
shdsl ? | help
```

Parameters

None

Response

Lists the supported SHDSL commands and keywords and a brief description of their function.

shdsl annex

Selects annex A or annex B of the G.shdsl standard. The annex used depends on the DSLAM the router is to connect to. In general, annex B is used in Europe and annex A is used in the rest of the world.

Mgmt Class

Network (R/W)

Input Format

```
shdsl annex [ A | B]
```

To see the current annex selection, enter `shdsl annex` without a parameter.

Parameters

`a | b`	Enables the selected annex.
`off`	Disables pre-activation.

Response

Selected annex is displayed.

```
-> shdsl annex
Annex A
```

shdsl list

Lists the current configuration of the G.shdsl interface.

Mgmt Class

Network (R)

Input Format

```
shdsl list
```

Parameters

None

Response

The following is a typical response.

```
-> shdsl list

G.SHDSL INTERFACE CONFIGURATION:
   Terminal ..................... CPE
   GTI SHDSL version ............ R1.2
   Requested speed .............. 2312 Kb/s
   Actual speed ................. 0 Kb/s
   Startup margin ............... 6 dB
   Rate mode .................... Adaptive
   Annex ........................ B
```

shdsl margin

Specifies the acceptable noise margin in decibels. If the connection is unstable, you may need to increase the margin.

Mgmt Class

Network (R/W)

Input Format

```
shdsl margin [dB]
```

Parameters

***	Enter the command with no parameter to display the current margin value.
<db>[a]	Noise margin in decibels.

[a] integer, -10 - 10, (6)

Response

Current margin is displayed.

```
-> shdsl margin
Margin = 6
```

shdsl ratemode

Selects adaptive or fixed rate mode.

Mgmt Class

Network (R/W)

Input Format

```
shdsl ratemode [adaptive | fixed]
```

Parameters

`***`	Enter the command with no parameter to display the current rate mode.
`adaptive`	Selects adaptive mode.
`fixed`	Selects fixed mode.

Response

Current ratemode is displayed.

```
-> shdsl ratemode
Adaptive
```

shdsl restart

Restarts the G.shdsl WAN interface.

☞ **NOTE:**
Unlike a reboot, a restart does not discard unsaved changes.

Mgmt Class

Network (R/W)

Input Format

```
shdsl restart
```

Parameters

None

Response

Command prompt.

shdsl save

Saves SHDSL configuration changes across restarts and reboots.

Mgmt Class

Network (R/W)

Input Format

```
shdsl save
```

Parameters

None

Response

Command prompt.

shdsl speed

Manages the speed of the SHDSL line.

☞ **NOTE:**
By default, it is assumed that the router is Customer Premises Equipment (CPE) and the line speed desired is the maximum allowed by the central office (CO).

This command can:

- Display the current requested speed and actual speed (shdsl speed with no parameter).
- If the actual speed shown is 0 (zero), the line is down.
- Manually set the speed (shdsl speed <speed>) (You might request a lower speed to improve stability.)
- Select auto-speed detection (shdsl speed auto). You should then restart the WAN interface with the command shdsl restart.

☞ **NOTE:**
A speed change automatically restarts the G.shdsl WAN interface. To make any changes persistent, perform a save command.

Mgmt Class

Network (R/W)

Input Format

```
shdsl speed [<speed> | auto]
```

Parameters

`***`	Enter the command with no parameter to display the current speed.
`speed` [a,b]	Speed in Kbps.
`auto` [c]	Selects auto-speed detection.

[a] Integer, 72 - 2312 in increments of 64 kbps
[b] If a value is specified falling between steps, the speed is set to the next lower step.
[c] Enter the command shdsl restart to carry out this change.

Examples

Example command with no parameter; the command returns the requested and actual shdsl rates.

```
-> shdsl speed

Requested speed: 2312 Kb/s
Actual speed:    2312 Kb/s
```

This command usage requests a line speed of 1096 Kb/s.

```
-> shdsl speed 1096
```

Response

See examples above.

shdsl stats

Displays SHDSL statistics. The statistics are kept for 24 hours and then automatically cleared. The statistics can also be cleared manually with the clear option.

Mgmt Class

Network (R/W)

Input Format

```
shdsl stats [clear]
```

Parameters

`***`	Enter the command with no parameter to display the current speed.
`clear`	Option used to reset the statistical counters.

Response

Statistical information displayed.

```
-> shdsl stats

SHDSL 24hr statistics displayed in time period of 15 minutes:

System up:   0 days 2 hours 9 minutes
Line up:     0 days 2 hours 9 minutes
Line SQ:     38 38 38 40 40 39 39 39 40
CRC Errors:  2 0 0 0 0 0 0 0 0
LOSW Errors: 0 0 0 0 0 0 0 0 0
FEBE Errors: 0 0 0 0 0 0 0 0 0
Loop Attn:   -2 -2 -2 -2 -2 -2 -2 -2 -2
```

Statistical information displayed after command entered with `clear` parameter.

```
-> shdsl stats clear

-> shdsl stats

SHDSL 24hr statistics displayed in time period of 15 minutes:

System up:   0 days 2 hours 9 minutes
Line up:     0 days 2 hours 9 minutes
Line SQ:     40
CRC Errors:  0
LOSW Errors: 0
FEBE Errors: 0
Loop Attn:   0
```

shdsl terminal

Displays and/or changes the router's designation as CO (Central Office) or CPE (Customer Premises Equipment).

By default, the router is assumed to be CPE. Use this command if the router is to be used as CO.

Mgmt Class

Network (R/W)

Input Format

```
sdsl terminal [cpe | co]
```

☞ **NOTE:**
To determine the current CO/CPE setting, enter `shdsl terminal` with no parameters.

Parameters

`***`	Enter the command with no parameter to display the current terminal mode.
`cpe`	Sets the terminal operation mode to CPE.
`co`	Sets the terminal operation mode to CO.

Response

Terminal operation is displayed:

```
-> shdsl terminal
Customer Premises
```

shdsl ver

Displays the G.shdsl version level of the modem firmware.

Mgmt Class

Network (R/W)

Input Format

```
shdsl ver
```

Parameters

None

Response

Typical response:

```
-> shdsl ver
GTI SHDSL Version R1.2
```

This page intentionally left blank.

CHAPTER 8

DHCP COMMANDS

The following DHCP (Dynamic Host Configuration Protocol) commands allow you to:

- Enable and disable subnetworks and client leases.
- Add subnetworks and client leases.
- Set the lease time.
- Change client leases manually.
- Set option values globally, for a subnetwork, or for a client lease.
- Enable/disable BootP.
- Use BootP to specify the boot server.
- Define option types.

The DHCP commands described in this section are included in Table 8-1, "DHCP Command Listing". To read about DHCP concepts and the DHCP configuration process, see "DHCP (Dynamic Host Configuration Protocol)" on page 4-2 of the Technical Reference Guide.

Table 8-1: DHCP Command Listing

Command	Function
dhcp ?	Lists the supported DHCP keywords.
dhcp add	Provides one of three types of DHCP definitions: subnetwork, client lease, or option type.
dhcp addrelay	Adds an address to the DHCP relay list.
dhcp bootp allow	Allows a BootP request to be processed for a particular client or subnet.
dhcp bootp disallow	Denies processing of a BootP request for a particular client or subnet.
dhcp bootp file	Specifies the boot file name (kernel) and the subnet to which it applies.

Table 8-1: DHCP Command Listing (Cont.)

Command	Function
dhcp bootp tftpserver	Specifies the TFTP server (boot server).
dhcp clear addresses	Clears the values from a pool of addresses.
dhcp clear all records	Clears all DHCP information, including all leases and all global DHCP information.
dhcp clear expire	Releases a client lease.
dhcp clear valueoption	Clears the value for a global option, for an option associated with a subnetwork, or with a specific client.
dhcp del	Deletes a subnetwork lease, a specific client lease, or a code.
dhcp delrelay	Removes a single (or all) address from the DHCP relay list.
dhcp disable	Disables a subnetwork or a client lease.
dhcp enable	Enables a subnetwork or a client lease.
dhcp list	Lists global, subnetwork, and client lease information.
dhcp list definedoptions	Lists all available predefined and user-defined options.
dhcp list lease	Lists the lease time.
dhcp set addresses	Creates or changes a pool of IP addresses that are associated with a subnetwork.
dhcp set expire	Allows manual changing of a client lease expiration time to a certain value.
dhcp set lease	Controls DHCP lease time.
dhcp set mask	Changes the mask of a DHCP subnet.
dhcp set otherserver	Instructs the router's DHCP server to either continue or stop sending DHCP requests when another DHCP server is detected on the LAN.
dhcp set valueoption	Sets values for global options, options specific to a subnetwork, or options specific to a client lease.

dhcp ?

Lists the supported DHCP keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
dhcp ?
```

Parameters

None

Response

List of the supported DHCP commands and keywords and a brief description of their function.

dhcp add

Provides one of three types of DHCP definitions: subnetwork, client lease, or option type. To delete any of these DHCP definitions, use the dhcp del command.

Mgmt Class

Network (R/W)

Input Format

To define a subnetwork:

```
dhcp add <net> <mask>
```

To define a client lease:

```
dhcp add <ipaddr>
```

To define an option type:

```
dhcp add <code> <min> <max> <type>
```

Parameters

<net>[a]	IP address of the subnetwork lease
<mask>[a]	IP network mask
<ipaddr>[a]	IP address of the subnetwork lease
<code>	User-defined code (128 - 254, or a keyword).
<min>	Minimum number of values.
<max>	Maximum number of values.
<type>	Byte | word | long | longint | binary | ipaddress | string

[a] Dotted-decimal notation

Examples

Command usage defining a subnetwork:

```
-> dhcp add 192.168.254.0.255.255.255.0
```

Command usage defining a client lease:

```
-> dhcp add 192.168.254.31
```

Command usage defining an option type. The code, 128, allows IP addresses, the server has a minimum of one, up to a maximum of four, IP addresses, and the type is “ipaddress”:

```
-> dhcp add 128 1 4 ipAddress
```

Response

Command prompt.

dhcp addrelay

Adds an address to the DHCP relay list. (This list is also the BootP server list.)

While the relay list contains at least one address, the DHCP server in the router is disabled, and the router forwards all DHCP requests and BootP requests to all servers in the relay list. (A DHCP request is issued whenever a device attempts to acquire an IP address). It forwards every reply received from any of the servers in the relay list to the appropriate LAN.

To remove an address from the list, use the dhcp delrelay command. For further discussion, see “Managing BootP” on page 4-10.

Mgmt Class

Network (R/W)

Input Format

```
dhcp addrelay <ipaddr>
```

Parameters

`***`	Displays the current address server.
`<ipaddr>`[a]	IP address of the DHCP relay server.

[a] Dotted-decimal notation

Response

Command usage defining, then listing a DHCP relay server:

```
-> dhcp addrelay 128.1.210.64

-> dhcp addrelay
BOOTP/DHCP Server address: 128.1.210.64
```

dhcp bootp allow

Allows a BootP request to be processed for a particular client or subnet.

Mgmt Class

Network (R/W)

Input Format

```
dhcp bootp allow <net> | <ipaddr>
```

Parameters

<net>[a]	IP address of the subnetwork lease.
<ipaddr>[a]	IP address of the client lease.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp bootp disallow

Denies processing of a BootP request for a particular client or subnet.

Mgmt Class

Network (R/W)

Input Format

```
dhcp bootp disallow <net> | <ipaddr>
```

Parameters

<net>[a]	IP address of the subnetwork lease.
<ipaddr>[a]	IP address of the client lease.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp bootp file

Specifies the boot file name (kernel) and the subnet to which it applies.

☞ **NOTE:**

The TFTP server IP address must be specified when specifying the file using the command dhcp bootp tftpserver.

Mgmt Class

Network (R/W)

Input Format

```
dhcp bootp file [<net> | <ipaddr>] <name>
```

Parameters

`<net>`[a]	IP address of the subnetwork lease.
`<ipaddr>`[a]	IP address of the client lease.
`<name>`[b]	Name of the file to boot from.

[a] Dotted-decimal notation.
[b] Default name for this file is KERNEL.F2K.

Response

Command prompt.

dhcp bootp tftpserver

Specifies the TFTP server (boot server).

Mgmt Class

Admin (R/W)

Input Format

```
dhcp bootp tftpserver [<net> |  <ipaddr] <tftpserver ipaddr>
```

Parameters

`<net>`[a]	IP address of the subnetwork lease.
`<ipaddr>`[a]	IP address of the client lease.
`<tftpserver ipaddr>`[a]	IP address of the TFTP server

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp clear addresses

Clears the values from a pool of addresses.

Mgmt Class

Network (R/W)

Input Format

```
dhcp clear addresses <net>
```

Parameters

`<net>`[a]	IP address of the subnetwork lease.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp clear all records

Clears all DHCP information, including all leases and all global DHCP information.

Unlike the erase *<dhcp>* command, this command clears all DHCP information from memory, but leaves the DHCP.DAT file intact. If you want to clear the information in the DHCP.DAT file as well, enter a save command after dhcp clear all records.

Mgmt Class

Network (R/W)

Input Format

```
dhcp clear all records
```

☞ **NOTE:**
The word `records` cannot be abbreviated in the command.

Parameters

None

Response

Command prompt.

dhcp clear expire

Releases a client lease. It then becomes available for other assignments.

☞ **NOTE:**
The client is not updated; it maintains the old value.

Mgmt Class

Network (R/W)

Input Format

```
dhcp clear expire <ipaddr>
```

Parameters

`<ipaddr>`[a]	IP address of the subnetwork lease.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp clear valueoption

Clears the value for a global option, for an option associated with a subnetwork, or with a specific client.

Mgmt Class

Network (R/W)

Input Format

```
dhcp clear valueoption [<net> | <ipaddr>] <code>
```

Parameters

`<net>`[a]	IP address of the subnetwork lease.
`<ipaddr>`[a]	IP address of the client lease.
`<code>`[b]	User defined code[c]

[a] Dotted-decimal notation.
[b] Integer, 1 - 61, or a keyword
[c] Use the command dhcp list definedoptions to list the codes and keywords.

Response

Command prompt.

dhcp del

Deletes a subnetwork lease, a specific client lease, or a code.

Mgmt Class

Network (R/W)

Input Format

```
dhcp del <net> | <ipaddr> | <code>
```

Parameters

`<net>`[a]	IP address of the subnetwork lease.
`<ipaddr>`[a]	IP address of the client lease.
`<code>`[b]	User defined code[c]

[a] Dotted-decimal notation.
[b] Integer, 128 - 245, or a keyword
[c] Use the command dhcp list definedoptions to list the codes and keywords.

Examples

Example command to delete the defined subnetwork:

```
-> dhcp del 192.168.254.0
```

Example command usage deleting a client lease:

```
-> dhcp del 192.168.254.31
```

Example command deleting the user-defined option with code 128:

```
-> dhcp del 128
```

Response

Command prompt.

dhcp delrelay

Removes an address from the DHCP relay list. (This list is also the BootP server list.)

To remove all addresses from the list, use dhcp delRelay all. If you remove all addresses from the DHCP relay list, the DHCP server is re-enabled and resumes processing DHCP requests and also BootP requests (if BootP processing is enabled).

To add an address to the list, use the command dhcp addrelay command. For further discussion, see “Configuring BootP/DHCP Relays” on page 4-12.

Mgmt Class

Network (R/W)

Input Format

```
dhcp delrelay <ipaddr> | all
```

Parameters

`<ipaddr>`[a]	IP address to be deleted from the list.
`all`	Removes all addresses from the list.

[a] Dotted-decimal notation

Response

Command prompt.

dhcp disable

Disables a subnetwork or a client lease.

Mgmt Class

Network (R/W)

Input Format

```
dhcp disable all | <net> | <ipaddr>
```

Parameters

`all`	Disables all subnets.
`<net>`[a]	IIP address of the subnetwork lease.
`<ipaddr>`[a]	IIP address of the client lease.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp enable

Enables a subnetwork or a client lease.

Mgmt Class

Network (R/W)

Input Format

```
dhcp enable all | <net> | <ipaddr>
```

Parameters

`all`	Enables all subnets.
`<net>`[a]	IIP address of the subnetwork lease.
`<ipaddr>`[a]	IIP address of the client lease.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp list

Lists global, subnetwork, and client lease information.

Mgmt Class

Network (R)

Input Format

```
dhcp list <net> | <ipaddr>
```

Parameters

`***`	When entered with no parameter, displays global DHCP information.
`<net>`[a]	IIP address of the subnetwork lease.
`<ipaddr>`[a]	IIP address of the client lease.

[a] Dotted-decimal notation.

Examples

The following example command lists global information:

```
-> dhcp list
     bootp server..............    none
     bootp file................
     DOMAINNAMESERVER (6).......    192.168.210.20 192.84.210.21
     DOMAINNAME (15)............    efficient.com
     WINSSERVER (44)............    192.168.254.73
Subnet 192.168.254.0, Enabled
     Mask......................    255.255.255.0
     first ip address..........    192.168.254.2
     last ip address...........    192.168.254.253
     lease.....................    Default
     bootp.....................    not allowed
     bootp file................
GATEWAY (3)192.168.254.254
client 192.168.254.2, Ena, jo-computer, Expired
client 192.168.254.3, Ena, Jo, 1999/5/16 11:31:33
```

The following example command lists information for client 192.168.254.3:

```
-> dhcp list 192.168.254.3

Client 192.168.254.3, Enabled
     lease.....................   Default
     expires...................   1998/5/16 11:31:33
     bootp.....................   not allowed
     bootp server..............   none
     bootp file................
HOSTNAME (12)..................   JO
CLIENTIDENTIFIER (61)..........   1 2 96 140 76 149 180
```

The following example command lists information for the subnetwork 192.168.254.0:

```
-> dhcp list 192.168.254.0

Subnet 192.168.254.0, Enabled
     Mask                         255.255.255.0
     first ip address             192.168.254.2
     last ip address              192.168.254.253
     lease                        Default
     bootp                        none
     bootp server                 not allowed
     bootp file
     GATEWAY (3)                  192.168.254.254
client 192.168.254.2, Ena, Jo-computer, Expired
client 192.168.254.3, Ena, Jo, 1998/5/16 11:31:33
```

Response

See examples above.

dhcp list definedoptions

Lists all available predefined and user-defined options.

☞ **NOTE:**

For description of the predefined options listed below, refer to RFC 1533. A predefined code can be a number between 1 and 61 or a keyword. A user-defined code can be a number between 128 and 254 or a keyword.

Mgmt Class

Network (R)

Input Format

```
dhcp list definedoptions | <code> | <string>
```

Parameters

`***`	When command is entered with no parameters all available options are listed.[a]
`<code>`	Predefined or user-defined number or keyword.
`<net>`[b]	Character string.

[a] Options may be predefined and/or user-defined
[b] Dotted-decimal notation.

Examples

The following example command lists all available options (predefined and user-defined):

```
-> dhcp list definedoptions

code TIMEOFFSET (2), 1 occurrence, type LONG
code GATEWAY (3), 1 to 63 occurrences, type IPADDRESS
code TIMESERVER (4), 1 to 63 occurrences, type IPADDRESS
code NAMESERVER (5), 1 to 63 occurrences, type IPADDRESS
code DOMAINNAMESERVER code SUBNETMASK (1), 1 occurrence, type
     IPADDRESS-RESERVED (6), 1 to 63 occurrences, type IPADDRESS
code LOGSERVER (7), 1 to 63 occurrences, type IPADDRESS
code COOKIESERVER (8), 1 to 63 occurrences, type IPADDRESS
code LPRSERVER (9), 1 to 63 occurrences, type IPADDRESS
code IMPRESSSERVER (10), 1 to 63 occurrences, type IPADDRESS
code RESOURCELOCATION (11), 1 to 63 occurrences, type IPADDRESS
code HOSTNAME (12), 1 to 255 characters, type STRING
code BOOTFILESIZE (13), 1 occurrence, type WORD
```

```
code MERITDUMPFILE (14), 1 to 255 characters, type STRING
code DOMAINNAME (15), 1 to 255 characters, type STRING
code SWAPSERVER (16), 1 occurrence, type IPADDRESS
code ROOTPATH (17), 1 to 255 characters, type STRING
code EXTENSIONSPATH (18), 1 to 255 characters, type STRING
code IPFORWARDING (19), 1 occurrence, type BINARY
code NONCALSOURCERTE (20), 1 occurrence, type BINARY
code POLICYFILTER (21), 1 to 31 occurrences, type IPADDRESS
code MAXDGMREASSEMBLY (22), 1 occurrence, type WORD
code DEFAULTIPTTL (23), 1 occurrence, type BYTE
code PATHMTUAGETMOUT (24), 1 occurrence, type LONGINT
code PATHMTUPLATEAUTBL (25), 1 to 127 occurrences, type WORD
code INTERFACEMTU (26), 1 occurrence, type WORD
code ALLSUBNETSLOCAL (27), 1 occurrence, type BINARY
code BROADCASTADDRESS (28), 1 occurrence, type IPADDRESS
code PERFORMMASKDSCVR (29), 1 occurrence, type BINARY
code MASKSUPPLIER (30), 1 occurrence, type BINARY
code PERFORMRTRDSCVR (31), 1 occurrence, type BINARY
code RTRSOLICITADDR (32), 1 occurrence, type IPADDRESS
code STATICROUTE (33), 1 to 31 occurrences, type IPADDRESS
code TRAILERENCAP (34), 1 occurrence, type BINARY
code ARPCACHETIMEOUT (35), 1 occurrence, type LONGINT
code ETHERNETENCAP (36), 1 occurrence, type BINARY
code TCPDEFAULTTTL (37), 1 occurrence, type BYTE
code TCPKEEPALIVEINTVL (38), 1 occurrence, type LONGINT
code TCPKEEPALIVEGARBG (39), 1 occurrence, type BINARY
code NETINFOSVCDOMAIN (40), 1 to 255 characters, type STRING
code NETINFOSERVERS (41), 1 occurrence, type IPADDRESS
code NETTIMEPROTOSRVRS (42), 1 occurrence, type IPADDRESS
code VENDORSPECIFIC (43), 1 to 255 occurrences, type BYTE
code WINSSERVER (44), 1 to 63 occurrences, type IPADDRESS
code NETBIOSTCPDGMDIST (45), 1 to 63 occurrences, type IPADDRESS
code NETBIOSTCPNODETYP (46), 1 occurrence, type BYTE
code NETBIOSTCPSCOPE (47), 1 to 255 characters, type STRING
code XWSFONTSERVER (48), 1 to 63 occurrences, type IPADDRESS
code XWSDISPLAYMANAGER (49), 1 to 63 occurrences, type IPADDRESS
code REQUESTEDIPADDR (50), 1 occurrence, type IPADDRESS-RESERVED
code IPADDRLEASETIME (51), 1 occurrence, type LONGINT-RESERVED
code OPTIONOVERLOAD (52), 1 occurrence, type BYTE-RESERVED
code MESSAGETYPE (53), 1 occurrence, type BYTE-RESERVED
code SERVERIDENTIFIER (54), 1 occurrence, type IPADDRESS-RESERVED
code PARAMREQUESTLIST (55), 1 to 255 occurrences, type BYTE-RESERVED
code MESSAGE (56), 1 to 255 characters, type STRING-RESERVED
code MAXDHCPMSGSIZE (57), 1 occurrence, type WORD-RESERVED
code RENEWALTIME (58), 1 occurrence, type LONGINT
```

```
code REBINDTIME (59), 1 occurrence, type LONGINT
code CLASSIDENTIFIER (60), 1 to 255 occurrences, type BYTE
code CLIENTIDENTIFIER (61), 2 to 255 occurrences, type BYTE
code NOTDEFINED62 (62), 1 to 255 occurrences, type BYTE
code NOTDEFINED63 (63), 1 to 255 occurrences, type BYTE
code NISDOMAIN (64), 1 to 255 characters, type STRING
code NISSERVERS (65), 1 to 63 occurrences, type IPADDRESS
code TFTPSERVERNAME (66), 4 to 255 characters, type STRING
code BOOTFILENAME (67), 1 to 255 characters, type STRING
code MOBILEIPHOMEAGNT (68), 0 to 63 occurrences, type IPADDRESS
code SMTPSERVERS (69), 1 to 63 occurrences, type IPADDRESS
code POP3SERVERS (70), 1 to 63 occurrences, type IPADDRESS
code NNTPSERVERS (71), 1 to 63 occurrences, type IPADDRESS
code WWWSERVERS (72), 1 to 63 occurrences, type IPADDRESS
code FINGERSERVERS (73), 1 to 63 occurrences, type IPADDRESS
code IRCSERVERS (74), 1 to 63 occurrences, type IPADDRESS
code STREETTALKSERVERS (75), 1 to 63 occurrences, type IPADDRESS
code STREETTALKDASRVRS (76), 1 to 63 occurrences, type IPADDRESS
```

The following example command lists options starting with the <string> “ga”:

```
-> dhcp list definedoptions ga

code,          number of values,      type of value
code GATEWAY (3), occurrence 1, type IPADDRESS
```

Response

See examples above.

dhcp list lease

Lists the lease time.

Mgmt Class

Network (R/W)

Input Format

```
dhcp list lease
```

Parameters

None

Response

Default lease duration is displayed.

```
-> dhcp list lease
Default lease time ......... 168 hours
```

dhcp set addresses

Creates or changes a pool of IP addresses that are associated with a subnetwork.

Mgmt Class

Network (R/W)

Input Format

```
dhcp set addresses <first ipaddr> <last ipaddr>
```

Parameters

`<first ipaddr>`[a]	First address in a pool of addresses for a particular subnetwork.
`<last ipaddr>`[a]	Last address in a pool of addresses for a particular subnetwork.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp set expire

Allows manual changing of a client lease expiration time to a certain value.

☞ **NOTE:**
The client information does not get updated; it will still have the old value.

Mgmt Class

Network (R/W)

Input Format

```
dhcp set expire <ipaddr> <hours> | default | infinite
```

Parameters

`<first ipaddr>`[a]	P address of the client lease.
`<hours>`[b]	Lease time.
`default`	Lease time that has been specified at the subnetwork or global level.
`infinite`	No lease time limit; the lease becomes permanent.

[a] Dotted-decimal notation.
[b] Integer, minimum 1 (168)

Response

Command prompt.

dhcp set lease

Controls DHCP lease time.

Mgmt Class

Network (R/W)

Input Format

```
dhcp set lease [<net> | <ipaddr>] <hours> | default | infinite
```

Parameters

`<Net>`[a]	IP address of the subnetwork lease.
`<ipaddr>`[a]	P address of the client lease.
`<hours>`[b]	Lease time.
`default`	Lease time that has been specified at the subnetwork or global level.
`infinite`	No lease time limit; the lease becomes permanent.

[a] Dotted-decimal notation.
[b] Integer, minimum 1 (168)

Examples

Example command sets client lease time to the default value:

```
-> dhcp set lease 192.168.254.17 default
```

Example command sets lease time to infinite for this subnet:

```
-> dhcp set lease 192.168.254.0 infinite
```

Response

Command prompt.

dhcp set mask

Used to conveniently change the mask of a DHCP subnet without having to delete and recreate the subnet and all its entries

Mgmt Class

Network (R/W)

Input Format

```
dhcp set mask <net> <mask>
```

Parameters

<Net>[a]	IP address of the subnetwork lease.
<mask>[a]	P network mask.

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp set otherserver

Instructs the router's DHCP server to either continue or stop sending DHCP requests when another DHCP server is detected on the LAN.

Mgmt Class

Network (R/W)

Input Format

```
dhcp set otherserver <net> continue | stop
```

Parameters

`<net>`[a]	IP address of the subnetwork lease.
`continue`	The router's DHCP server continues sending DHCP requests, even if another DHCP server is detected on the LAN.
`stop`	The router's DHCP server stops sending DHCP requests when another DHCP server is detected on the LAN. (This is the default value.)

[a] Dotted-decimal notation.

Response

Command prompt.

dhcp set valueoption

Sets values for global options, options specific to a subnetwork, or options specific to a client lease. For more information, see “Setting Option Values” on page 4-8.

Mgmt Class

Network (R/W)

Input Format

```
dhcp set valueoption [<ipaddr>|<net>] <code> <value>....
```

Parameters

`<ipaddr>`[a]	Specify the client IP address if the option value applies only to the client lease.
`<Net>`[a]	Specify the subnetwork IP address if the option value applies only to the subnetwork lease.
`<code>`[b]	Code specifying the option to be set.
`<value>`	Value to be assigned to the specified option. It could be a byte, word, signed long, unsigned long, binary, IP address, or string depending on the option.

[a] Dotted-decimal notation.
[b] number between 1 and 61 or a keyword. Use the command dhcp list definedoptions to list the codes and keywords,

Example

This example command does not specify an client or subnetwork address, and thus sets a global value for the *domainnameserver* option:

```
-> dhcp set valueoption domainnameserver 192.168.254.2 192.168.254.3
```

Response

Command prompt.

This page intentionally left blank.

CHAPTER 9

L2TP COMMANDS

This section contains L2TP command descriptions. For a complete discussion of L2TP tunneling, see “L2TP Tunneling — Virtual Dial-Up” on page 6-26 of the Technical Reference Guide. The L2TP commands allow you to:

- Add, delete, and modify tunnels
- Configure L2TP router information including:
- Names
- Security authentication protocols and passwords
- Addresses
- Management of traffic performance
- Restrict a tunnel so it can be established only with a specific remote interface (l2tp set wanif).

The L2TP commands found in this section include:

Table 9-1: L2TP Command Listing

Command	Function
l2tp ?	Lists the supported L2TP keywords.
l2tp add	Creates a tunnel entry.
l2tp call	Establishes a tunnel without creating a session.
l2tp close	Closes an L2TP tunnel and/or session.
l2tp del	Selects adaptive or fixed rate mode.
l2tp forward	Configures the router to forward all incoming calls to an LNS without answering the incoming call.
l2tp list	Display of the current configuration settings for tunnel(s), except for the authentication password/secret.

Table 9-1: L2TP Command Listing (Cont.)

Command	Function
l2tp set address	Defines the IP address of the other end of the tunnel, either the remote L2TP Access Concentrator (LAC) or remote L2TP Network Server (LNS).
l2tp set authen	Enables or disables authentication of the remote router during tunnel establishment using the CHAP secret.
l2tp set chapsecret	Creates a CHAP secret.
l2tp set dialout	Allows the LNS instruct the L2TP client to use an ISDN phone line to place a call on its behalf.
l2tp set hiddenavp	Configures the router to protect some L2TP control information using hidden AVPs.
l2tp set ouraddress	Specifies the source IP address used when the tunnel is originated.
l2tp set ourpassword	Specifies the router's secret/password for PPP authentication on a per-tunnel basis.
l2tp set oursysname	Specifies the router's name for PPP authentication on a per-tunnel basis.
l2tp set ourtunnelname	Creates local router's host name.
l2tp set remotename	Creates the host name of the remote tunnel.
l2tp set type	Defines the type of L2TP support for the tunnel.
l2tp set wanif	Restricts the remote interface with which the L2TP tunnel can be established.
l2tp set window	Controls options that enhance traffic performance in a tunneling environment.

l2tp ?

Lists the supported L2TP keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Security (R)

Input Format

```
l2tp ?
```

Parameters

None

Response

Lists the supported L2TP commands and keywords and a brief description of their function.

l2tp add

Creates a tunnel entry.

Mgmt Class

Security (R/W)

Input Format

```
l2tp add <tunnelname>
```

Parameters

`<tunnelname>`[a] Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Example

Example command adding the tunnel named *PacingAtWork*.

```
-> l2tp add PacingAtWork
```

Response

Command prompt.

l2tp call

This command is primarily used for debugging purposes and it establishes a tunnel without creating a session.

Mgmt Class

Security (R/W)

Input Format

```
l2tp call <tunnelname>
```

Parameters

`<tunnelname>`[a] Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Example

Example command adding the tunnel named *PacingAtWork*.

```
-> l2tp call PacingAtWork
```

Response

Command prompt.

l2tp close

Closes an L2TP tunnel and/or session.

Mgmt Class

Security (R/W)

Input Format

```
l2tp close <l2tp unit number>|-n<tunnelname>|-t<tunnelid>
|-s<serialnum>|-c<callid>
```

Parameters

`<L2TP unit number>`[a]	IP address of the subnetwork lease.
`-n<tunnelname>`[b]	Name of the tunnel.[c]
`-t<tunnelid>`	Local tunnel id.
`-s<serialnum>`	Serial number of the call within the tunnel.
`-c<callid>`	ID of the local call for the session.

[a] Integer
[b] ASCII string
[c] The tunnel name is case sensitive.

Response

Command prompt.

l2tp del

Deletes a tunnel entry.

Mgmt Class

Security (R/W)

Input Format

```
l2tp del <tunnelname>
```

Parameters

`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Example

Example command deletes the tunnel named *PacingAtWork*

```
-> l2tp del PacingAtWork
```

Response

Command prompt.

l2tp forward

The router can be configured to forward all incoming calls to an LNS without answering the incoming call. This feature is normally used when the router is acting as a LAC or both a LAC and LNS.

☞ **NOTE:**

Only one tunnel entry can have this option set.

Mgmt Class

Security (R/W)

Input Format

```
l2tp forward all | none <tunnelname>
```

Parameters

`all`	Forward all incoming calls through the tunnel to an LNS
`none`	No incoming calls are allowed to be forwarded through the tunnel to an LNS.
`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp list

Provides a complete display of the current configuration settings for tunnel(s), except for the authentication password/secret.

Mgmt Class

Security (R)

Input Format

```
l2tp list |<tunnelname>|
```

Parameters

`<tunnelname>`[a] Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Typical response:

```
-> l2tp list
INFORMATION FOR <pacingAtWork>
  type ..............................   L2TPClient (LAC-will not dial)/LNS
All Incoming Calls Tunneled here.....   no
  CHAP challenge issued..............   yes
  hidden AVPs used...................   yes
  sequencing/pacing..................   window pacing
    sequencing/pacing is.............   required
    window size for sequencing/pacing.  10
  ip address.........................   10.0.0.1
  Our host name......................   pacingAtHome

  ACTIVE TUNNEL......................   UNKNOWN
    current state....................   CLOSED
    LOCAL TUNNEL ID..................   1
    REMOTE TUNNEL ID.................   0
    remote firmware..................   0
    remote ip address................   10.0.0.1
    LAC SESSION serial number........   0
     current state...................   CLOSED
     LOCAL CALL ID...................   1
      local window size..............   10
      sequencing/pacing..............   WINDOW/PACING
       sequencing/pacing is..........   required
     REMOTE CALL ID..................   0
      remote window size.............   0
```

l2tp set address

Defines the IP address of the other end of the tunnel, either the remote L2TP Access Concentrator (LAC) or remote L2TP Network Server (LNS).

CAUTION:

If the IP address of the remote tunnel is part of a subnet that is also reached through the tunnel, a routing table entry for this address must be explicitly added. Normally, this routing entry will be added to remote entry, which has the default route.

NOTE:

When a remote router tries to create a tunnel, the remote router's IP address is not authenticated.

NOTE:

If this command is not used, then <ipaddr> defaults to 0.0.0.0, and this end cannot initiate the tunnel.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set address <ipaddr> <tunnelname>
```

Parameters

`<ipaddr>`[a]	IP address of the remote LAC or LNS.
`<tunnelname>`[b]	Name of the tunnel. [c]

[a] Dotted-decimal notation.
[b] ASCII string
[c] The name is case sensitive.

Response

Command prompt.

l2tp set authen

Enables or disables authentication of the remote router during tunnel establishment using the CHAP secret, if it exists. If the remote router tries to authenticate the local end during tunnel authentication, the local router will always attempt to respond, provided a CHAP secret has been configured.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set authen on | off  <tunnelname>
```

Parameters

`on`	Enables authentication.
`off`	Disables authentication.
`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set chapsecret

Creates a CHAP secret. This CHAP secret is used to authenticate the creation of the tunnel and is used for hiding certain control packet information. The LAC and the LNS can share a single CHAP secret for a given tunnel.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set CHAPSecret <secret> <tunnelname>
```

Parameters

`secret`[a]	CHAP secret used to authenticate the creation of the tunnel.
`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set dialout

Allows the LNS instruct the L2TP client to use an ISDN phone line to place a call on its behalf.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set dialout yes | no <tunnelname>
```

Parameters

`yes`	Allows the router to place outgoing calls.
`no`	Prevents the router from placing outgoing calls. Default value.
`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set hiddenavp

Configures the router to protect some L2TP control information (such as names and passwords for a PPP session) using hidden AVPs. This command is often used to turn off hidden AVPs (no option), in cases where the other end of the tunnel does not support hidden AVPs.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set hiddenAVP yes | no <tunnelname>
```

Parameters

`yes`	Allows the router hide AVPs. Default value.
`no`	Disables hidden AVPs.
`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set ouraddress

Specifies the source IP address used when the tunnel is originated.

Use this command when you want to specify a source IP address other than the WAN interface IP address. For example, if NAT (network address translation) is not being used, all IP addresses on the Ethernet LAN would be visible. You could then specify, as the source IP address, the Ethernet IP address of the router (which would be visible) instead of the WAN interface IP address.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set ouraddress <ipaddr> <tunnelname>
```

Parameters

`<ipaddr>`[a]	Source IP address used for this tunnel.
`<tunnelname>`[b]	Name of the tunnel. [c]

[a] Dotted-decimal notation.
[b] ASCII string
[c] The name is case sensitive.

Response

Command prompt.

l2tp set ourpassword

Specifies the router's secret/password for PPP authentication on a per-tunnel basis.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set ourpassword <password> <tunnelname>
```

Parameters

`<password>`[a]	Router's secret/password used for authentication when challenged by another router.
`<tunnelname>`[a]	Name of the tunnel. [b]

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set oursysname

Specifies the router's name for PPP authentication on a per-tunnel basis.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set oursysname <name> <tunnelname>
```

Parameters

`<name>`[a]	Name of the router that is used for authentication when challenged by another router.
`<tunnelname>`[a,b]	Name of the tunnel.

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set ourtunnelname

Creates local router's host name.

☞ **NOTE:**

If this command is not used, then, if it has been specified, the <name> from the l2tp set oursysname command or the <name> from the command system name <name> is used.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set ourTunnelName  <name> <tunnelname>
```

Parameters

<name>[a,b]	Host name of the local router. This is the fully qualified domain name of the local router.
<tunnelname>[a,b]	Name of the tunnel.

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set remotename

Creates the host name of the remote tunnel.

☞ **NOTE:**

If this command is not used, then <TunnelName> of the tunnel entry is used.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set remoteName <name> <tunnelname>
```

Parameters

`<name>`[a,b]	Host name of the remote tunnel. This is the fully qualified domain name of the remote host.
`<tunnelname>`[a,b]	Name of the tunnel.

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set type

Defines the type of L2TP support for the tunnel. The router's role is defined on a per-tunnel basis.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set type all|lac|lns|l2tpclient|disabled <tunnelname>
```

Parameters

`all`	The router is configured to act as both a LAC/L2TP client and an LNS server.
`lac`	The router is configured to act as a LAC for this tunnel.
`lns`	The router is configured to act as an LNS for this tunnel.
`l2tpclient`	The router is configured to act as an L2TP client for this tunnel.
`disabled`	The tunnel entry is disabled.
`<tunnelname>`[a,b]	Host name of the remote tunnel. This is the fully qualified domain name of the remote host.

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

l2tp set wanif

Restricts the remote interface with which the L2TP tunnel can be established.

If this command is not used, no remote interface restriction is enforced. For example, no restriction would be enforced when the Dial Backup feature is used (see "Dial Backup" on page 6-7.) Thus, the tunnel would be terminated and re-established when switching back and forth between the primary interface and the backup interface. If the tunnel is to established only with the primary interface or only with the backup interface, you must specify that restriction with this command.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set wanif  <remote> <tunnelname>
```

Parameters

`<remote>`	Name of the remote router profile that must be used when establishing the L2TP tunnel. To list the remote routers, use the command remote list. [a, b]
`<tunnelname>`[c,d]	Host name of the remote tunnel. This is the fully qualified domain name of the remote host.

[a] For the dual-Ethernet router, specify the physical interface name, that is, either ETHERNET/0 or ETHERNET/1.
[b] To clear the remote restriction for a tunnel, enter a hyphen (-) as the remote name.
[c] ASCII string
[d] The name is case sensitive.

Examples

This command example restricts the tunnel named *OfficeTunnel* to the remote interface named *officertr*.

```
-> l2tp set wanif officertr OfficeTunnel
```

This command example clears the remote interface restriction for the tunnel named *OfficeTunnel*.

```
-> l2tp set wanif - OfficeTunnel
```

This command example restricts the tunnel named *OfficeTunnel* to the physical interface ETHERNET/1.

```
-> l2tp set wanif ETHERNET/1 OfficeTunnel
```

Response

Command prompt.

l2tp set window

Enhances traffic performance in a tunneling environment. The command's options affect the way incoming payload packets are processed. The router is configured with the following default options: sequencing, required, and size 10.

Mgmt Class

Security (R/W)

Input Format

```
l2tp set window sequencing|pacing|nosequencing|optional|
required|size <tunnelname>
```

Parameters

`sequencing`	Sequence numbers are placed in the L2TP payload packets. With this option, one end instructs the other end to send sequence packets. No acknowledgments are issued for received packets.
`pacing`	Sequence numbers are placed in the L2TP payload packets. When a session is created, the router specifies a window size. Acknowledgments for received packets are issued.
`nosequencing`	No sequence numbers are placed in the L2TP payload packets carrying the PPP packets. If the remote end carries out sequencing or pacing, the router can still send and receive sequenced packets.
`optional`	Allows dynamic switching of a session from pacing or sequencing to nosequencing.
`required`	Disables dynamic switching from pacing or sequencing to nosequencing.
`size`[a]	Controls the size of the receive window for receiving packets for sequencing or pacing, when a session is created.
`<tunnelname>`[b,c]	Host name of the remote tunnel. This is the fully qualified domain name of the remote host.

[a] Size can be 0 for packet sequencing. Must be a non-zero value for window pacing. Size must be less than or equal to 30.
[b] ASCII string
[c] The name is case sensitive.

Response

Command prompt.

remote setl2tpclient

With this command, this remote is the path to the L2TP client and accepts tunnel calls. Use this command if your router acts as an LNS. You must also specify PPP authentication and IP routes for this remote.

Mgmt Class

Security (R/W)

Input Format

```
remote setl2tpclient <tunnelname><remotename>
```

Parameters

`<tunnelname>`[a,b]	Host name of the remote tunnel associated with the remote LAC.
`<remotename>`[a,b]	Name of the remote entry.

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

remote setlns

With this command, this remote is the path to the LNS, and it will forward the incoming call (which matches this remote entry) through the tunnel named <TunnelName> if your router is the client.

☞ **NOTE:**

The remote entry must also have appropriate information such as PPP authentication, IP routing, IPX routing, bridging, or Caller ID.

Mgmt Class

Security (R/W)

Input Format

```
remote setLNS <tunnelname> <remotename>
```

Parameters

<tunnelname>[a,b]	Name of the tunnel.
<remotename>[a,b]	Name of the remote entry.

[a] ASCII string
[b] The name is case sensitive.

Response

Command prompt.

CHAPTER 10

BRIDGE FILTERING COMMANDS

Bridge Filtering allows you to control the packets transferred across the router. This feature can be used to enhance security or improve performance. Filtering is based on matched patterns within the packet at a specified offset. Two filtering modes are available:

- Deny mode will discard any packet that matches the deny filter database and let all other packets pass.
- Allow mode will only pass the packets that match the allow filter database and discard all others.

Up to 40 deny and 40 allow filters can be activated from the filter database.

The Bridge Filtering commands found in this section include:

Table 10-1: Bridge Filtering Command Listing

Command	Function
filter br ?	Lists the supported bridge filtering keywords.
filter br add	Adds a bridging filter to the filtering database.
filter br del	Deletes a bridging filter from the filtering database.
filter br list	Lists the bridging filters in the filtering database.
filter br use	Sets the filtering mode.

filter br ?

Lists the supported Bridge Filtering keywords.

Mgmt Class

Security (R/W)

Input Format

```
filter br ?
```

Parameters

None

Response

Lists the supported bridge filtering commands and keywords and a brief description of their function.

filter br add

Adds a bridging filter to the filtering database. The filter can allow or deny the forwarding of packets based on the contents of the packets. The command specifies the position within the packet that is checked and the data that must appear in that location in order for the packet to match this filter.

Mgmt Class

Security (R/W)

Input Format

```
filter br add [pos] [data] allow | deny
```

Parameters

`<pos>`[a]	Byte offset within a packet.
`<byte>`	Hexadecimal number up to 6 bytes.
`allow`	Allows forwarding of the packet(s).
`deny`	Denies forwarding of the packet(s).

[a] Integer, 0 - 127

Example

Example command prevents forwarding of RARP packets across the bridge. The data at byte offset 12 in each packet is checked and, if the data is hex 8035, the packet is denied forwarding.

```
-> filter br add 12 8035 deny
```

Response

Command prompt.

filter br del

Deletes a bridging filter from the filtering database. The parameters on the command identify the filter to be deleted.

Mgmt Class

Security (R/W)

Input Format

```
filter br del [pos] [data] allow | deny
```

Parameters

<pos>[a]	Byte offset within a packet.
<byte>	Hexadecimal number up to 6 bytes.
allow	Allows forwarding of the packet(s).
deny	Denies forwarding of the packet(s).

[a] Integer, 0 - 127

Example

This command deletes the filter which denies the forwarding of packets that have the hex value 8035 at byte offset 12.

```
-> filter br del 12 8035 deny
```

Response

Command prompt.

filter br list

Lists the bridging filters in the filtering database.

Mgmt Class

Security (R/W)

Input Format

```
filter br list
```

Parameters

None

Response

Typical response:

```
-> filter br list
  Allow Filter:

  Deny Filter:
  pos:12, len=2, <80><35>
```

filter br use

Sets the mode of filtering to either deny, allow, or none.

Mgmt Class

Security (R/W)

Input Format

```
filter br use none | deny | allow
```

Parameters

`none`	Disables all filtering.
`deny`	Enables deny filtering.
`allow`	Enables allow filtering.

Example

This command enables allow filtering.

```
-> filter br use allow
```

Response

Command prompt.

This page intentionally left blank.

CHAPTER 11

PPPOE COMMANDS

This section contains the commands that are specific to PPPoE (PPP over Ethernet). To learn more about PPPoE configuration and management, see “PPPoE (PPP over Ethernet)” on page 6-41.

The PPPoE commands found in this section include:

Table 11-1: Bridge Filtering Command Listing

Command	Function
remote setpppoeservice	Defines the remote router entry as a PPPoE remote entry.
pppoe close	Closes a currently active PPPoE session.
pppoe list	Lists information about the currently active PPPoE sessions.

remote setpppoeservice

Defines the remote router entry as a PPPoE remote entry. It also specifies the service to which PPPoE users connect through this remote entry.

☞ **NOTE:**

Enter this command immediately after the remote add command that defines the remote router entry.

Mgmt Class

Data (R/W)

Input Format

```
remote setPPPoEservice <service> | * | -  <remotename>
```

Parameters

`<service>`[a]	Name of the PPPoE service to which this remote connects PPPoE users. The service provider defines the name of its service.[b]
`*`	Specify * if the router can be used to connect to any PPPoE service.
`-`	Specify - to clear the setting.
`<remotename>`[a]	Name of the remote router.

[a] ASCII string
[b] Name is case-sensitive

Example

The following commands define the remote router used to connect to the PPPoE service DialUpPPP.net. Note that the remote setPPPoEservice command is entered immediately after the remote add command.

```
-> remote add pppoeremote
-> remote setpppoeservice dialupppp.net pppoeremote
```

Response

Command prompt.

pppoe close

Closes a currently active PPPoE session. To see the currently active PPPoE sessions, use the command pppoe list.

Mgmt Class

Security (R/W)

Input Format

```
pppoe close <ifsnumber>
```

Parameters

`<ifsnumber>`	Session to be closed.[a]

[a] Specify the PPPoE/Ifs number for the session as shown in the ifs or pppoe list command output.

Response

Command prompt.

pppoe list

Lists information about the currently active PPPoE sessions.

Mgmt Class

Security (R/W)

Input Format

```
pppoe list
```

Parameters

None

Response

Typical response:

```
-> pppoe list
PPPoE Client Session......  DialUpPPP.net
     PPPoE/IFs number.....  1
     Access Concentrator..  15021109931568-efficient
     Peer MAC Address ....  00:10:67:00:66:E2
     Session ID...........  2
     State................  2
     Flags................  1
```

This page intentionally left blank.

CHAPTER 12

IKE/IPSEC COMMANDS

The commands in this section are used to manage the security features Internet Key Exchange (IKE) and Internet Protocol Security IPSec). For additional information on IKE and IPSec, see Chapter 5, System Security.

The commands found in this section include:

Table 12-1: Internet Key Exchange Command Listing

Command	Function
ike ipsec ?	List the supported IKE, IPSEC and IKE IPSEC keywords.
ike commit	Defines the remote router entry as a PPPoE remote entry.
ike flush	Closes a currently active PPPoE session.
ike ipsec policies add	Lists information about the currently active PPPoE sessions.
ike ipsec policies delete	Deletes an existing IPSec policy.
ike ipsec policies disable	Disables an IPSec policy.
ike ipsec policies enable	Enables an IPSec policy.
ike ipsec policies list	List the IPSec policies.
ike ipsec policies set dest	Defines a destination address filtering parameter value for an IPSec policy.
ike ipsec policies set dest-port	Defines a destination port filtering parameter value for an IPSec policy.
ike ipsec policies set interface	Defines an interface filtering parameter value for an IPSec policy
ike ipsec policies set mode	Defines the mode filtering parameter value for an IPSec policy

Table 12-1: Internet Key Exchange Command Listing (Cont.)

Command	Function
ike ipsec policies set peer	Defines a peer filtering parameter value for the policy.
ike ipsec policies set pfs	Defines the pfs filtering parameter value for the policy.
ike ipsec policies set proposal	Defines a proposal filtering parameter value for the policy.
ike ipsec policies set protocol	Defines a protocol filtering parameter value for the policy.
ike ipsec policies set source	Defines a source filtering parameter value for the policy.
ike ipsec policies set sourceport	Defines a source port filtering parameter value for the policy.
ike ipsec policies set translate	Defines a translate filtering parameter value for the policy.
ike ipsec proposals add	Defines the name of an IKE IPSec proposal.
ike ipsec proposals delete	Deletes an existing IKE IPSec proposal.
ike ipsec proposals list	Lists the IPSec proposals.
ike ipsec proposals set ahauth	Sets the proposal parameter that determines whether AH message authentication is requested and, if it is requested, the hash algorithm used.
ike ipsec proposals set espauth	Sets the proposal parameter that determines whether ESP message authentication is requested and, if it is requested, the hash algorithm used.
ike ipsec proposals set espenc	Sets the proposal parameter that determines whether ESP encryption is requested and, if it is requested, the encryption method used.
ike ipsec proposals set ipcomp	Sets the proposal parameter that requests either no compression or LZS compression.
ike ipsec proposals set lifedata	Sets the proposal parameter that specifies the maximum number of kilobytes for the IPSec Security Authentication (SA).
ike ipsec proposals set lifetime	Sets the proposal parameter that specifies the length of time (in seconds) before the IPSec Security Authentication (SA) expires.
ike peers add	Defines the name of a new IKE peer.
ike peers delete	Deletes an existing IKE peer entry.

Table 12-1: Internet Key Exchange Command Listing (Cont.)

Command	Function
ike peers list	Lists the defined IKE peers.
ike peers set address	Sets the IP address of the other endpoint of the secure IKE peer connection.
ike peers set localid	Sets the local ID for the IKE peer connection.
ike peers set localidtype	Sets the type of the local ID for the IKE peer connection.
ike peers set mode	Sets the IKE peer connection mode to either main mode or aggressive mode.
ike peers set peerid	Sets the peer ID for the IKE peer connection.
ike peers set peeridtype	Sets the type of the peer ID for the IKE peer connection.
ike peers set secret	Sets the shared secret for the IKE peer connection.
ike proposals add	Defines the name of a new IKE proposal.
ike proposals delete	Deletes an existing IKE proposal.
ike proposals list	Lists the IKE proposals.
ike proposals set dh_group	Sets the IKE proposal parameter that specifies the Diffie-Hellman (DH) key generation group used (no group or group 1 or 2).
ike proposals set encryption	Sets the IKE proposal parameter that requests ESP encryption and specifies the encryption method used.
ike proposals set lifetime	Sets the IKE proposal parameter that specifies the length of time (in seconds) before the Phase 1 Security Authentication (SA) expires.
ike proposals set message_auth	Sets the IKE proposal parameter that specifies the message authentication done.
ike proposals set session_auth	Sets the IKE proposal parameter that specifies the session authentication; pre-shared key is currently the only option.
ipsec add	Defines an IPSec security association (SA) name.
ipsec delete	Deletes an existing IPSec security association (SA) name.
ipsec disable	Disables a defined IPSec security association (SA) entry.

Table 12-1: Internet Key Exchange Command Listing (Cont.)

Command	Function
ipsec enable	Enables a defined IPSec security association entry.
ipsec flush	Clears all IPSec definitions.
ipsec list	Lists one or all of the IPSec security association (SA) entries.
ipsec set authentication	Selects authentication for the IPSec SA using either SHA-1 (Secure Hashing Algorithm 1) or MD5 (Message Digest 5).
ipsec set authkey	Specifies the authentication key for the IPSec security authentication (SA).
ipsec set direction	Defines the direction of the IPSec security authentication (SA).
ipsec set compression	Selects either LZ compression or no compression for the IPSec security authentication (SA).
ipsec set enckey	Specifies the encryption key for the IPSec security authentication (SA).
ipsec set encryption	Selects the method of encryption used for the IPSec security authentication (SA): no encryption, DES (56-bit) encryption, or 3DES (168-bit) encryption.
ipsec set gateway	Defines the IP address of the IP gateway of the IPSec security authentication (SA).
ipsec set ident	Specifies the identifier (SPID) for the IPSec tunnel.
ipsec set mode	Selects the encapsulation mode (tunnel or transport) for the SA.
ipsec set service	Selects the authentication and/or encryption services used for the IPSec SA.

ike ipsec ?

Three commands are used to list the supported IKE, IPSEC and IKE IPSEC keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Security (R)

Input Format

`ike ipsec ?` for IKE IPSec sub-commands.

`ike ?` for IKE sub-commands

`ipsec ?` for IPSec sub-commands

Parameters

None

Response

Lists the supported commands and keywords and a brief description of their functions.

ike commit

Determines whether the IKE commit bit is set. By default, the commit bit is not set (*off*).

If packets are not being processed correctly across an IPSec tunnel, try the command `ike commit on` so that the commit bit is set. Setting the commit bit makes sure that no IPSec traffic arrives at the router before the router is ready for it.

Mgmt Class

Security (R/W)

Input Format

```
ike commit [ on | off | help]
```

Parameters

`***`	When entered with no parameter, the current value is displayed.
`on`	Commit bit is set.
`off`	Commit bit is not set. (Default value)
`help`	Displays help message.

Response

Command prompt.

ike flush

Clears all IKE configuration information from the router. For more information about IKE, see “IPSec (Internet Protocol Security)” on page 5-50.

Mgmt Class

Debug (R/W)

Input Format

```
ike flush
```

Parameters

None

Response

Command prompt.

ike ipsec policies add

Defines the name of an IPsec policy to be used for filtering. Other IPSec Policy commands define the filtering parameters (see “IKE IPSec Policy Commands” on page 5-61.)

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies add <policyname>
```

Parameters

`<policyname>`[a] New name for an IPsec policy.[b]

[a] ASCII string
[b] To see the policy names in use, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies add mypolicy
```

Response

Command prompt.

ike ipsec policies delete

Deletes an existing IPSec policy. To define IPSec Policies, see see “IKE IPSec Policy Commands” on page 5-61.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies delete <policyname>
```

Parameters

`<policyname>`[a]	Name of an existing IPsec policy.[b]

[a] ASCII string
[b] To see the policy names in use, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies delete yourpolicy
```

Response

Command prompt.

ike ipsec policies disable

Disables an IPSec policy. The policy can be re-enabled using the ike ipsec policies enable command.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies disable <policyname>
```

Parameters

`<policyname>`[a]	Name of an existing IPsec policy.[b]

[a] ASCII string
[b] To see the policy names in use, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies disable mypolicy
```

Response

Command prompt.

ike ipsec policies enable

Enables an IPSec policy. An enable command is required for each new policy; the enable command indicates that the specification of the policy is complete and the policy is ready to be used. The enable command can also be used to re-enable a disabled policy. For more information, see “IKE IPSec Policy Commands” on page 5-61.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies enable <policyname>
```

Parameters

`<policyname>`[a] Name of an existing IPsec policy.[b]

[a] ASCII string
[b] To see the policy names in use, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies enable mypolicy
```

Response

Command prompt.

ike ipsec policies list

Lists the IPSec policies. For more information, see “IKE IPSec Policy Commands” on page 5-61.

Mgmt Class

Security (R)

Input Format

```
ike ipsec policies list
```

Parameters

None

Response

Typical response:

```
-> ike ipsec policies list
IKE IPSec policies:
mypolicy (enabled)
    Source address/mask: 192.168.16.0/255.255.255.0
    Destination address/mask: 192.168.23.0/255.255.255.0
    Protocol: *
    Source port: *
    Destination port: *
    Tunnel mode
    Peer: my_aggressive_peer (0.0.0.0)
    Proposals: myproposal
```

ike ipsec policies set dest

Defines a destination filtering parameter value for the policy. The destination parameter requires that the data be intended for the specified destination IP address and mask. The destination is the device or network that finally receives the packet, not the router that routes the packet.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set dest <ipaddress> <ipmask> <policyname>
```

Parameters

`<ipaddress>`[a]	IP address allowed to be the destination of the data.
`<ipmask>`[a]	IP network mask.
`<policyname>`[b]	Name of the IPsec policy to which the destination parameter value is added.[c]

[a] Dotted-decimal notation
[b] ASCII string
[c] To see the policy names, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies set dest 192.168.16.0 255.255.255.0 mypolicy
```

Response

Command prompt.

ike ipsec policies set destport

Defines a destination port filtering parameter value for the policy. The destination port parameter requires a specific destination port for the data or allows any destination port (*). (Because port numbers are TCP and UDP specific, a port filter is effective only when the protocol filter is TCP or UDP.)

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set destport <portnumber | telnet | http |
smtp | tftp | *>  <policyname>
```

Parameters

`<portnumber>`
`telnet`
`http`
`snmp`
`tftp`
`*`
	Destination port whose data is allowed by the policy. The port can be specified by one of the listed names or by its number. To allow data through for any destination port, specify an asterisk (*).

`<policyname>`[a]	Name of the IPsec policy to which the destination port parameter value is added.[b]

[a] ASCII string
[b] To see the policy names, use the ike ipsec policies list command.

Examples

```
-> ike ipsec policies set destport * mypolicy
-> ike ipsec policies set destport http webpolicy
```

Response

Command prompt.

ike ipsec policies set interface

Defines an interface filtering parameter value for the policy. The policy is only used when the specified interface is connected. For example, if the policy is to be used only when the Dial Backup remote is connected, you would specify the remote name as the interface for the policy. Otherwise, if the policy can be used regardless of the connected interface, specify the string `none`. (To read about Dial Backup, see "Dial Backup" on page 6-7.)

☞ **NOTE:**

The specified interface must be the interface to the IKE peer.

This command is intended to allow the user to choose when to apply IPSec/IKE filters and incur the resulting encryption and authentication costs. With this command, you can limit a policy to a specific interface.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set interface <interface | all >
<policyname>
```

Parameters

`<interface>`[a]	Interface that must be connected when the policy is used. This is usually referenced by a remote name, although it could be another interface such as “ethernet/0”. If no interface restriction is to be set for this policy, specify the string `all`.
`<policyname>`[a]	Name of the IPsec policy to which the interface parameter value is added.[b]

[a] ASCII string
[b] To see the policy names, use the ike ipsec policies list command.

Examples

This command requires that, when the remote interface backup comes up, IKE is enabled for packets described by policy corporate. The specified interface (back-up) must be the interface to the IKE peer.

```
-> ike ipsec policies set interface backup corporate
```

This command specifies that IKE is enabled for packets described by policy my-policy regardless of the interface the peer is on.

```
-> ike ipsec policies set interface all mypolicy
```

Response

Command prompt.

ike ipsec policies set mode

Defines the mode filtering parameter value for the policy. The mode parameter specifies the encapsulation mode (tunnel or transport) that may be used for the connection (see “Transport and Tunnel Encapsulation Modes” on page 5-50.) If no value is set for the mode parameter, tunnel mode is assumed.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set mode <tunnel | transport> <policyname>
```

Parameters

`tunnel | transport`	Encapsulation method required for the connection. The default value is TUNNEL.
`<policyname>`[a]	Name of the IPsec policy to which the encapsulation mode parameter value is added.[a]

[a] To see the policy names, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies set mode transport rtr2rtrpolicy
```

Response

Command prompt.

ike ipsec policies set peer

Defines a peer filtering parameter value for the policy. The peer parameter specifies an IKE peer that may be used for the connection. (The peer must have been defined by IKE peer commands; see “IKE Peer Commands” on page 5-56.)

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set peer <peerpame> <policyname>
```

Parameters

`<peername>`	Name of an IKE peer.[a]
`<policyname>`[a]	Name of the IPsec policy to which the encapsulation mode parameter value is added.[b]

[a] Name of an IKE peer. To see the IKE peer names, use the ike peers list command.
[b] To see the policy names, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies set peer my_aggressive_peer mypolicy
```

Response

Command prompt.

ike ipsec policies set pfs

Defines the pfs filtering parameter value for the policy. The pfs parameter specifies the Perfect Forward Secrecy negotiation used for the connection.

If you specify 1 or 2, Perfect Forward Secrecy is performed using the specified Diffie-Hellman group (1 or 2). If you specify none, then Perfect Forward Secrecy is not required for this connection and no Diffie-Hellman group is used to encrypt the keys during rekey. To read more about PFS, see "IKE Management" on page 5-52.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set pfs <1 | 2 | none > <policyname>
```

Parameters

`1`	Use Diffie-Hellman group 1 for the Perfect Forward Secrecy negotiation.
`2`	Use Diffie-Hellman group 2 for the Perfect Forward Secrecy negotiation.
`none`	Perfect Forward Secrecy negotiation is not required for this connection.
`<policyname>`[a]	Name of the IPsec policy to which the pfs parameter value is added.[b]

[a] ASCII string
[b] To see the policy names, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies set pfs 2 mypolicy
```

Response

Command prompt.

ike ipsec policies set proposal

Defines a proposal filtering parameter value for the policy. The proposal parameter specifies an IKE IPSec proposal that may be used for the connection. (It must have been defined by IKE IPSec proposal commands; see “IKE IPSec Proposal Commands” on page 5-58.)

Unlike the other filtering parameters, the policy may allow more than one value for the proposal parameter. For example, two set proposal commands could specify two proposals, either of which could be used by the connection; see “IKE IPSec Policy Commands” on page 5-61.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set proposal <proposalname> <policyname>
```

Parameters

`<proposalname>`[a]	Name of an IKE proposal.[b]
`<policyname>`[a]	Name of the IPsec policy to which the proposal parameter value is added.[c]

[a] ASCII string
[b] To see the IKE proposal names, use the ike ipsec proposals list command.
[c] To see the policy names, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies set proposal myproposal mypolicy
```

Response

Command prompt.

ike ipsec policies set protocol

Defines a protocol filtering parameter value for the policy. The protocol parameter requires a specific protocol that must be used or allows any protocol (*).

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set protocol <protocolnumber | tcp | udp |
*> <policyname>
```

Parameters

`<protocolnumber>`	Protocol required by the policy. The protocol can be specified by number or by name (TCP or UDP). To allow data through for any protocol, specify an asterisk (*).
`tcp`	
`udp`	
`*`	
`<policyname>`[a]	Name of the IPsec policy to which the protocol parameter value is added.[b]

[a] ASCII string
[b] To see the policy names, use the ike ipsec policies list command.

Examples

```
-> ike ipsec policies set protocol * mypolicy
-> ike ipsec policies set protocol tcp webpolicy
```

Response

Command prompt.

ike ipsec policies set source

Defines a source filtering parameter value for the policy. The source parameter requires the data come from the specified source IP address and mask. The source is the device or network that sent the packet, not the router that routes the packet.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set source <ipaddress> <ipmask>
<policyname>
```

Parameters

`<ipaddress>`[a]	IP address allowed to be the source of the data
`<ipmask>`[a]	IP network mask.
`<policyname>`[b]	Name of the IPsec policy to which the source parameter value is added.[c]

[a] Dotted-decimal notation
[b] ASCII string
[c] To see the policy names, use the ike ipsec policies list command.

Example

```
-> ike ipsec policies set source 192.168.16.0 255.255.255.0 mypolicy
```

Response

Command prompt.

ike ipsec policies set sourceport

Defines a source port filtering parameter value for the policy. The source port parameter requires a specific source port for the data or allows any source port (*) (Because port numbers are TCP and UDP specific, a port filter is effective only when the protocol filter is TCP or UDP.)

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set sourceport <portnumber | telnet | http |
smtp | tftp | *> <policyname>
```

Parameters

`<portnumber>`
`telnet`
`http`
`snmp`
`tftp`
`*`
	Source port whose data is allowed by the policy. The port can be specified by one of the listed names or by its number. To allow data through for any source port, specify an asterisk (*).

`<policyname>`[a]	Name of the IPsec policy to which the source port parameter value is added.[b]

[a] ASCII string
[b] To see the policy names, use the ike ipsec policies list command.

Examples

```
-> ike ipsec policies set sourceport * mypolicy
-> ike ipsec policies set sourceport http webpolicy
```

Response

Command prompt.

ike ipsec policies set translate

Defines a translate filtering parameter value for the policy. The translate option determines whether the router applies NAT (network address translation) before the packets are encrypted by IPSec.

☞ **NOTE:**

The remote must have IP address translation enabled (see "Network Address Translation (NAT)" on page 4-17. Or, the remote setiptranslate command).

☞ **NOTE:**

The address that NAT translates to should be the source or destination address for the policy (use the ike ipsec policies set source or ike ipsec policies set dest command).

Use this option when several remote sites have the same IP subnet, making it impossible to tunnel those sites unchanged to the corporate network.

When the router's public IP address is not the desired choice for the network address translation, you can define a virtual Ethernet interface. A virtual Ethernet interface can be created to translate to an arbitrary IP address (see "IP Subnets" on page 6-1.). Again, be sure that the virtual Ethernet interface has IP address translation enabled (eth ip translate), and use the virtual Ethernet interface as the gateway to the other end of the protected network. (See the example below.) You can use the eth ip addhostmapping command to map a range of NAT addresses to private addresses so the IKE tunnel can be initiated from either end.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec policies set translate  on | off <policyname>
```

Parameters

`on | off`	Sets the translate option on or off. If translate is set to on, translation is applied before encryption, and the packets are sent using the host router's public IP address.
`<policyname>`[a]	Name of the IPsec policy to which the source port parameter value is added.[b]

[a] ASCII string
[b] To see the policy names, use the ike ipsec policies list command.

Example

The following commands suggest how a virtual interface could be defined for use with Network Address Translation and an IPSec tunnel.

```
# The address of the corporate LAN is 192.168.0.0, but the desired
# NAT address is 10.0.0.1 so you create a virtual interface (0:99),
# turn off RIP for the interface, and assign it the address 10.0.0.1/24.
-> eth add 0:99
-> eth ip opt txrip off 0:99
-> eth ip opt rxrip off 0:99
-> eth ip addr 10.0.0.1 255.255.255.0 0:99
#
#Next, enable NAT for the virtual interface and route traffic to the
# the corporate backbone (192.168.0.0/16) through the virtual interface.
-> eth ip translate on 0:99
-> eth ip addroute 192.168.0.0 255.255.0.0 10.0.0.0.1 0:99

# Later, when you set up the IKE tunnel, include these commands
# when defining a policy. (The policy name is corporate.)
# The source address must be the virtual interface address.
# The destination address must be the corporate backbone address.
# ike ipsec policies set source 10.0.0.1 255.255.255.255 corporate
# ike ipsec policies set dest 192.168.0.0 255.255.0.0 corporate
# ike ipsec policies set translate on corporate
```

Response

Command prompt.

ike ipsec proposals add

Defines the name of an IKE IPSec proposal. The proposal commands define the proposals exchanged to set up an IPSec security association (SA), that is, an SA to be used for the user data transfer. (see “IKE IPSec Proposal Commands” on page 5-58.)

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals add <proposalname>
```

Parameters

`<proposalname>`[a] New name for an IPsec proposal.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals add myproposal
```

Response

Command prompt.

ike ipsec proposals delete

Deletes an existing IKE IPSec proposal. For more information, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals delete <proposalname>
```

Parameters

`<proposalname>`[a] Name of an existing IPsec proposal.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals delete yourproposal
```

Response

Command prompt.

ike ipsec proposals list

Lists the IPSec proposals. For more information, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals list
```

Parameters

None

Response

Typical response:

```
-> ike ipsec proposals list
IKE IPSec proposals:
myproposal
    ESP encryption: 3DES
    ESP authentication: SHA1
    IPComp: None
    Lifetime 600
    Lifedata 50000
```

ike ipsec proposals set ahauth

Sets the proposal parameter that determines whether AH message authentication is requested and, if it is requested, the hash algorithm used.

☞ **NOTE:**

The proposal must select either the AH or ESP encapsulation methods. It cannot request AH authentication if it requests ESP encryption and/or ESP authentication.

For more information, see "ESP and AH Security Protocols" on page 5-51. Or, see "IKE IPSec Proposal Commands" on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals set ahauth <md5 | sha1 | none>
<proposalname>
```

Parameters

`md5`	Use AH encapsulation and authenticate using hash algorithm Message Digest 5.
`sha1`	Use AH encapsulation and authenticate using hash algorithm Secure Hash Algorithm-1.
`none`	No AH encapsulation and no AH message authentication. (If you select this option, ESP encapsulation must be requested by a ike ipsec proposals set espenc or ike ipsec proposals set espauth.)
`<proposalname>`[a]	Name of the IPsec proposal to which the AH authentication parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals set ahauth sha1 myproposal
```

Response

Command prompt.

ike ipsec proposals set espauth

Sets the proposal parameter that determines whether ESP message authentication is requested and, if it is requested, the hash algorithm used.

For more information, see “ESP and AH Security Protocols” on page 5-51. Or, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals set espauth <md5 | sha1 | none>
<proposalname>
```

Parameters

`md5`	Use ESP encapsulation and authenticate using hash algorithm Message Digest 5.
`sha1`	Use ESP encapsulation and authenticate using hash algorithm Secure Hash Algorithm-1.
`none`	No ESP encapsulation and no ESP message authentication. (If you select this option, the encapsulation method must be requested by a ike ipsec proposals set espenc or ike ipsec proposals set espauth command.)
`<proposalname>`[a]	Name of the IPsec proposal to which the ESP authentication parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals set espauth sha1 myproposal
```

Response

Command prompt.

ike ipsec proposals set espenc

Sets the proposal parameter that determines whether ESP encryption is requested and, if it is requested, the encryption method used.

For more information, see “ESP and AH Security Protocols” on page 5-51. Or, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals set espenc <des | 3des | null | none>
<proposalname>
```

Parameters

`des`	Use ESP encapsulation and 56-bit encryption.
`3des`	Use ESP encapsulation and 168-bit encryption (if 3DES is enabled in the router)
`null`	No encryption, but use ESP encapsulation. Headers are inserted as though the data was encrypted. This allows verification of the source, but sends the data in the clear, increasing throughput.
`none`	No encryption and no ESP encapsulation. (If you select this option, the encapsulation method must be requested by a ike ipsec proposals set espauth or ike ipsec proposals set ahauth command.)
`<proposalname>`[a]	Name of the IPsec proposal to which the ESP encryption parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals set espenc 3des myproposal
```

Response

Command prompt.

ike ipsec proposals set ipcomp

Sets the proposal parameter that requests either no compression or LZS compression. For more information, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals set ipcomp <none | lzs> <proposalname>
```

Parameters

Choose one of the following:

`none`	No compression.
`lzs`	Compress using the LZS algorithm.
`<proposalname>`[a]	Name of the IPsec proposal to which the compression parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals set ipcomp none myproposal
```

Response

Command prompt.

ike ipsec proposals set lifedata

Sets the proposal parameter that specifies the maximum number of kilobytes for the IPSec SA; 0 means unlimited. After the maximum data is transferred, IKE renegotiates the connection. By limiting the amount of data that can be transferred, you reduce the likelihood of the key being broken.

For more information on proposal parameters, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals set lifedata <kbytes> <proposalname>
```

Parameters

<kbytes>[a]	Maximum number of kilobytes transferred before renegotiation; 0 means unlimited.
<proposalname>[b]	Name of the IPsec proposal to which the lifedata parameter is added.[c]

[a] Integer
[b] ASCII string
[c] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals set lifedata 50000 myproposal
```

Response

Command prompt.

ike ipsec proposals set lifetime

Sets the proposal parameter that specifies the length of time (in seconds) before the IPSec SA expires; the recommended value is 86400 (24 hours). When the time limit expires, IKE renegotiates the connection.

For more information on proposal parameters, see “IKE IPSec Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike ipsec proposals set lifetime <seconds> <proposalname>
```

Parameters

<seconds>[a]	Maximum number of seconds before renegotiation; 0 means unlimited.
<proposalname>[b]	Name of the IPsec proposal to which the lifetime parameter is added.[c]

[a] Integer
[b] ASCII string
[c] To see the proposal names in use, use the ike ipsec proposals list command.

Example

```
-> ike ipsec proposals set lifetime 600 myproposal
```

Response

Command prompt.

ike peers add

Defines the name of a new IKE peer. Other commands specify the address, secret, and mode of the peer connection; see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers add <peername>
```

Parameters

<peername>[a]	New name for an IKE peer.[b]

[a] ASCII string
[b] To see the peer names in use, use the ike peers list command.

Example

```
-> ike peers add my_aggressive_peer
```

Response

Command prompt.

ike peers delete

Deletes an existing IKE peer entry. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers delete <peername>
```

Parameters

`<peername>`[a] Name of the IKE peer to delete.[b]

[a] ASCII string
[b] To see the peer names in use, use the ike peers list command.

Example

```
-> ike peers delete my_aggressive_peer
```

Response

Command prompt.

ike peers list

Lists the defined IKE peers. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers list
```

Parameters

None

Response

Typical response:

```
-> ike peers list
IKE Peers:
IKE Peers:
my_aggresive_peer
    IP address = 0.0.0.0
    preshared secret = "confidential_hushhush"
    aggressive, peer id = example.efficient.com (Domain name)
          local peer id = test.efficient.com (Domain name)
my_main_peer
    TP address = 1.2.3.4
    preshared secret = "Shipsailsatmidnight"
    main mode
```

ike peers set address

Sets the IP address of the other endpoint of the secure IKE peer connection. The address specified depends on the mode of the peer connection, which can be either main mode or aggressive mode. (see “IKE Management” on page 5-52.)

If the mode is main mode, the other endpoint of the peer connection is constant, and you specify its IP address.

If the mode is aggressive mode, one end of the connection, the gateway, has a fixed IP address. The other end, the client, has a changing address. When configuring the client, set the peer IP address to the fixed gateway address. When configuring the gateway for an aggressive mode connection, set the peer IP address to 0.0.0.0.

Mgmt Class

Security (R/W)

Input Format

```
ike peers set address <ipaddress> <peername>
```

Parameters

`<ipaddress>`[a]	IP address.
`<peername>`[b]	Name of the IKE peer whose address is specified. [c]

[a] Dotted-decimal notation
[b] ASCII string
[c] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set address 0.0.0.0 my_aggressive_peer
```

Response

Command prompt.

ike peers set localid

Sets the local ID for the IKE peer connection. This command is used when aggressive mode has been selected by the ike peers set mode command for this peer name.

The local ID must match the peer ID on the other end of the connection. The local ID can be an IP address, domain name, or e-mail address as specified by the ike peers set localidtype command. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers set localid <aggressivemodeid> <peername>
```

Parameters

`<aggressivemodeid>` IP address[a], domain name[b], or e-mail address.

`<peername>`[b] Name of the IKE peer whose local ID is specified. [c]

[a] Dotted-decimal notation, ASCII string
[b] ASCII string
[c] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set localid test.efficient.com my_aggressive_peer
```

Response

Command prompt.

ike peers set localidtype

Sets the type of the local ID for the IKE peer connection. This command is used only when aggressive mode has been selected by the ike peers set mode command for this peer name.

The local ID type must match the peer ID type on the other end of the connection. The possible ID types are IP address, domain name, or e-mail address. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers set localidtype <ipaddr | domainname | email>
<peername>
```

Parameters

Choose one of the following:

`ipaddr`	The local ID must be an IP address.
`domainname`	The local ID must be a domain name.
`email`	The local ID must be an e-mail address.
`<peername>`[a]	Name of the IKE peer whose local ID type is specified.[b]

[a] ASCII string
[b] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set localidtype domainname my_aggressive_peer
```

Response

Command prompt.

ike peers set mode

Sets the IKE peer connection mode to either main mode or aggressive mode. Main mode is used when the IP addresses of both ends are known and constant. Aggressive mode is used when the address of one end can change, as with a typical modem or DSL connection. (See “Main Mode and Aggressive Mode” on page 5-54.)

Mgmt Class

Security (R/W)

Input Format

```
ike peers set mode <main | aggressive> <peername>
```

Parameters

Choose one of the following:

`main`	Select main mode (both ends constant).
`aggressive`	Selects aggressive mode (one end can change).
`<peername>`[a]	Name of the IKE peer whose mode is specified.[b]

[a] ASCII string
[b] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set mode aggressive my_aggressive_peer
```

Response

Command prompt.

ike peers set peerid

Sets the peer ID for the IKE peer connection. This command is used only when aggressive mode has been selected by the ike peers set mode command for this peer name.

The peer ID must match the local ID on the other end of the connection. The peer ID can be an IP address, domain name, or e-mail address as specified by the ike peers set peeridtype command. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers set peerid <aggressivemodeid> <peername>
```

Parameters

`<AggressiveModeID>` IP address[a], domain name[b], or e-mail address.

`<peername>`[b] Name of the IKE peer whose peer ID is specified. [c]

[a] Dotted-decimal notation, ASCII string
[b] ASCII string
[c] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set peerid example.efficient.com my_aggressive_peer
```

Response

Command prompt.

ike peers set peeridtype

Sets the type of the peer ID for the IKE peer connection. This command is used only when aggressive mode has been selected by the ike peers set mode command for this peer name.

The local peer type must match the local ID type on the other end of the connection. The possible ID types are IP address, domain name, or e-mail address. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers set peeridtype <ipaddr | domainname | email>
<peername>
```

Parameters

Choose one of the following:

`ipaddr`	The peer ID must be an IP address.
`domainname`	The peer ID must be a domain name.
`email`	The peer ID must be an e-mail address.
`<peername>`[a]	Name of the IKE peer whose peer ID type is specified.[b]

[a] ASCII string
[b] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set peeridtype domainname my_aggressive_peer
```

Response

Command prompt.

ike peers set secret

Sets the shared secret for the IKE peer connection. The secret must be identical for both ends. For more information, see “IKE Peer Commands” on page 5-56.

Mgmt Class

Security (R/W)

Input Format

```
ike peers set secret <secret> <peername>
```

Parameters

`<secret>`[a]	Secret.
`<peername>`[b]	Name of the IKE peer whose peer ID is specified. [c]

[a] ASCII string 1 - 256 characters; do not use spaces or non-printable characters.
[b] ASCII string
[c] To see the peer names, use the ike peers list command.

Example

```
-> ike peers set secret confidential_hushhush my_aggressive_peer
```

Response

Command prompt.

ike proposals add

Defines the name of a new IKE proposal. The IKE proposal commands define the proposals exchanged during the Phase 1 SA. For more information, see “IKE Management” on page 5-52.

Mgmt Class

Security (R/W)

Input Format

```
ike proposals add <ProposalName>
```

Parameters

`<proposalname>`[a] New name for an IKE proposal.[b]

[a] ASCII string
[b] To see the peer names in use, use the ike peers list command.

Example

```
-> ike proposals add my_ike_proposal
```

Response

Command prompt.

ike proposals delete

Deletes an existing IKE proposal. For more information, see “IKE Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike proposals delete <proposalname>
```

Parameters

`<proposalname>`[a] Name of the IKE proposal to delete.[b]

[a] ASCII string
[b] To see the peer names in use, use the ike proposals list command.

Example

```
-> ike proposals delete my_ike_proposal
```

Response

Command prompt.

ike proposals list

Lists the IKE proposals. For more information, see “IKE Proposal Commands” on page 5-58.

Mgmt Class

Security (R)

Input Format

```
ike proposals list
```

Parameters

None

Response

Typical response:

```
-> ike proposals list
IKE proposals:
my_ike_proposal
    Session Authentication: Preshared key
    Encryption: DES
    Message Authentication: MD5
    DH Group 2
    Lifetime 86400
    Lifedata 0
```

ike proposals set dh_group

Sets the IKE proposal parameter that specifies the Diffie-Hellman (DH) key generation group used (no group or group 1 or 2). See “IKE Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike proposals set dh_group <none | 1 | 2> <proposalname>
```

Parameters

Choose one of the following:

`none`	No DH group is used.
`1`	Use DH group 1.
`2`	Use DH group 2.
`<proposalname>`[a]	Name of the IKE proposal to which the DH group parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike proposals list command.

Example

```
-> ike proposals set dh_group 2 my_ike_proposal
```

Response

Command prompt.

ike proposals set encryption

Sets the IKE proposal parameter that requests ESP encryption and specifies the encryption method used. See “IKE Proposal Commands” on page 5-58.

Mgmt Class

Security (R/W)

Input Format

```
ike proposals set encryption <des | 3des> <proposalname>
```

Parameters

Choose one of the following:

`des`	Use DES (56-bit) encryption.
`3des`[a]	Use 3DES (168-bit) encryption (if 3DES encryption is enabled).
`<proposalname>`[b]	Name of the IKE proposal to which the encryption parameter is added.[c]

[a] Software Option Key enabled feature
[b] ASCII string
[c] To see the proposal names in use, use the ike proposals list command.

Example

```
-> ike proposals set encryption des my_ike_proposal
```

Response

Command prompt.

ike proposals set lifetime

Sets the IKE proposal parameter that specifies the length of time (in seconds) before the Phase 1 SA expires; the recommended value is 86400 (24 hours). When the time limit expires, IKE renegotiates the connection. See “IKE Management” on page 5-52.

Mgmt Class

Security (R/W)

Input Format

```
ike proposals set lifetime <seconds> <proposalname>
```

Parameters

`<seconds>`[a]	Maximum number of seconds before renegotiation; `0` means unlimited.
`<proposalname>`[b]	Name of the IKE proposal to which the lifetime parameter is added.[c]

[a] Integer
[b] ASCII string
[c] To see the proposal names in use, use the ike proposals list command.

Example

```
-> ike proposals set lifetime 86400 my_ike_proposal
```

Response

Command prompt.

ike proposals set message_auth

Sets the IKE proposal parameter that specifies the message authentication done. It can propose no message authentication, or it can propose authentication using the hash algorithm Message Digest 5 (MD5) or Secure Hash Algorithm-1 (SHA1).

Mgmt Class

Security (R/W)

Input Format

```
ike proposals set message_auth <none | md5 | sha1>
<proposalName>
```

Parameters

`none`	No authentication.
`md5`	Authentication using the Message Digest 5 algorithm.
`sha1`	Authentication using algorithm Secure Hash Algorithm-1.
`<proposalname>`[a]	Name of the IKE proposal to which the authentication parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike proposals list command.

Example

```
-> ike proposals set message_auth sha1 my_ike_proposal
```

Response

Command prompt.

ike proposals set session_auth

Sets the IKE proposal parameter that specifies the session authentication; preshared key is currently the only option. For more information on IKE proposals, see “IKE Management” on page 5-52.

Mgmt Class

Security (R/W)

Input Format

```
ike proposals set session_auth <preshare> <proposalname>
```

Parameters

`preshare`	Preshare key.
`<proposalname>`[a]	Name of the IKE proposal to which the session authentication parameter is added.[b]

[a] ASCII string
[b] To see the proposal names in use, use the ike proposals list command.

Example

```
-> ike proposals set session_auth sha1 my_ike_proposal
```

Response

Command prompt.

IPSec Commands

The following commands allow you to define an IPSec connection without IKE. To read about IPSec Security, see “IPSec (Internet Protocol Security)” on page 5-50.

☞ **NOTE:**

If you define a tunnel using IPSec commands, the keys will remain static. This could pose a security risk and is not recommended. Use of IKE for key management is recommended.

ipsec add

Defines an IPSec security association (SA) name.

Mgmt Class

Security (R/W)

Input Format

```
ipsec add <saname>
```

Parameters

`<saname>`[a] Name for the new IPSec SA.[b]

[a] ASCII string
[b] To see the SA names in use, use the ipsec list command.

Example

```
-> ipsec add show_rx
```

Response

Command prompt.

ipsec delete

Deletes an existing IPSec security association (SA) name.

Mgmt Class

Security (R/W)

Input Format

```
ipsec delete <saname>
```

Parameters

`<saname>`[a] Name of the IPSec SA to be deleted.[b]

[a] ASCII string
[b] To see the SA names in use, use the ipsec list command.

Example

```
-> ipsec delete show_rx
```

Response

Command prompt.

ipsec disable

Disables a defined IPSec security association entry.

Mgmt Class

Security (R/W)

Input Format

```
ipsec disable <saname>
```

Parameters

`<saname>`[a] Name of the IPSec SA to be disabled.[b]

[a] ASCII string
[b] To see the SA names in use, use the ipsec list command.

Example

```
-> ipsec disable show_rx
```

Response

Command prompt.

ipsec enable

Enables a defined IPSec security association entry, indicating it is complete and ready to be used.

Mgmt Class

Security (R/W)

Input Format

```
ipsec enable <saname>
```

Parameters

<saname>[a]	Name of the IPSec SA to be enabled.[b]

[a] ASCII string
[b] To see the SA names in use, use the ipsec list command.

Example

```
-> ipsec enable show_rx
```

Response

Command prompt.

ipsec flush

Clears all IPSec definitions.

Mgmt Class

Debug (R/W)

Input Format

```
ipsec flush
```

Parameters

None

Response

Command prompt.

ipsec list

Lists one or all of the IPSec security association (SA) entries.

Mgmt Class

Security (R)

Input Format

```
ipsec list [<saname>]
```

Parameters

<saname>[a]	Optional, name for a single IPSec SA to be listed.

[a] ASCII string

Response

Typical response:

```
-> ipsec list
IPSec security associations:
show_rx
    Gateway: 207.135.89.233
    Inbound
    Tunnel
    Both
    3DES
      key=111111112222222233333333444444445555555 5
    SHA1
      key=aaaaaaaabbbbbbbbccccccccdddddddd (20)
    No compression
    ID =424242
    seq=1, bitmap=ffffffff
show_tx
    Gateway: 207.135.89.233
    Outbound
    Tunnel
    Both
    3DES
      key=012344567890123456789012345678901234567890123456 7
    SHA1
      key=abcedfabcdefabcdefabcdefabcdefabcdefabcd (20)
    No compression
    ID =123456
    seq=6734
```

ipsec set authentication

Selects authentication for the IPSec SA using either SHA-1 (Secure Hashing Algorithm 1) or MD5 (Message Digest 5).

Mgmt Class

Security (R/W)

Input Format

```
ipsec set authentication <md5 | sha1> <saname>
```

Parameters

`md5`	Authentication using the Message Digest 5 algorithm.
`sha1`	Authentication using algorithm Secure Hash Algorithm-1.
`<saname>`[a]	Name of the IPSec SA to which the authentication parameter is added.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set authentication sha1 show_rx
```

Response

Command prompt.

ipsec set authkey

Specifies the authentication key for the IPSec SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set authkey <key> <saname>
```

Parameters

`<key>`	Hexadecimal authentication key.
`<saname>`[a]	Name of the IPSec SA to which the authentication key is added.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set authkey aaaaaaaabbbbbbbbccccccccdddddddd show_rx
```

Response

Command prompt.

ipsec set direction

Defines the direction of the IPSec SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set direction <inbound | outbound> <saname>
```

Parameters

Choose one of the following:

`inbound`	Inbound SA.
`outbound`	Outbound SA.
`<saname>`[a]	Name of the IPSec SA to which the direction parameter is added.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set direction inbound show_rx
```

Response

Command prompt.

ipsec set compression

Selects either LZ compression or no compression for the IPSec SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set compression <none | lzs> <saname>
```

Parameters

Choose one of the following:

`none`	No compression.
`lzs`	Compress using the LZS algorithm.
`<saname>`[a]	Name of the IPsec SA to which the compression parameter is added.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set compression none show_rx
```

Response

Command prompt.

ipsec set enckey

Specifies the encryption key for the IPSec SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set enckey <key> <saname>
```

Parameters

`<key>`[a]	Hexadecimal encryption key.
`<saname>`[b]	Name of the IPSec SA to which the authentication key is added.[c]

[a] 64-bits for DES, 192-bits for 3DES.
[b] ASCII string
[c] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set enckey 1111111122222222333333334444444455555555 show_rx
```

Response

Command prompt.

ipsec set encryption

Selects the method of encryption used for the IPSec SA: no encryption, DES (56-bit) encryption, or 3DES (168-bit) encryption.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set encryption <null | des-cbc | 3des> <saname>
```

Parameters

Choose one of the following:

`null`	No encryption.
`des-cbc`	Use DES encryption.
`3des`	Use 3DES encryption.
`<saname>`[a]	Name of the IPsec SA to which the encryption parameter is added.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set encryption null show_rx
```

Response

Command prompt.

ipsec set gateway

Defines the IP address of the IP gateway of the IPSec SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set gateway <ipaddress> <saname>
```

Parameters

`<ipaddress>`[a]	IP address of the IP gateway.
`<saname>`[b]	Name of the IPSec SA to which the gateway parameter is added.[c]

[a] Dotted-decimal notation.
[b] ASCII string
[c] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set gateway 207.135.89.233 show_rx
```

Response

Command prompt.

ipsec set ident

Specifies the identifier (SPID) for the IPSec tunnel. It must match the SPID at the other end of the tunnel, that is, the tx SPID on this end must match the rx SPID on the other end.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set ident <ident> <saname>
```

Parameters

`<ident>`[a]	SPID for the IPSec tunnel.
`<saname>`[a]	Name of the IPSec SA.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ipsec list command.

Example

```
-> ipsec set ident 424242 show_rx
```

Response

Command prompt.

ipsec set mode

Selects the encapsulation mode (tunnel or transport) for the SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set mode <tunnel | transport> <saname>
```

Parameters

`tunnel | transport`	Encapsulation method required for the connection. The default value is TUNNEL.
`<saname>`[a]	Name of the IPsec SA to which the encapsulation mode parameter is added.[a]

[a] To see the used IPSec SA names, use the ipsec list command.

Example

```
-> ipsec set mode transport rtr2rtr
```

Response

Command prompt.

ipsec set service

Selects the authentication and/or encryption services used for the IPSec SA.

Mgmt Class

Security (R/W)

Input Format

```
ipsec set service <esp | ah | both> <saname>
```

Parameters

Choose one of the following:

`esp`	ESP encryption.
`ah`	AH authentication.
`both`	Use Both ESP encryption and authentication.
`<saname>`[a]	Name of the IPsec SA to which the service parameter is added.[b]

[a] ASCII string
[b] To see the IPSec SA names in use, use the ike ipsec list command.

Example

```
-> ipsec set service both show_rx
```

Response

Command prompt.

CHAPTER 13

VOICE COMMANDS

The commands in this section are used to manage the voice functions of integrated access devices (IADs). The commands available on the command line will vary based on the voice gateway configuration. The voice commands found in this section include:

Table 13-1: Voice Command Listing

Command	Function
dsp ? / voice ?	Lists the top-level voice or dsp commands and keywords and a brief description of their function.
dsp ecode	Deletes the IP address of the entry in the Address Resolution Protocol (ARP) table.
dsp jitter	Lists ARP table entries.
dsp provision	Lists the root bridge, and indicates whether the mode is learning, listening, or forwarding.
dsp save	Lists the contents of the bridge table.
dsp vr	Displays the current voice rate and encoding type.
voice l2clear	Clears the L2 control channel statistics.
voice l2stats	Displays the L2 control channel statistics.
voice profile	Dials a remote router.
voice refreshcas	Displays or changes the current date on the router's clock.

dsp ? / voice ?

Two commands are used to list the voice related commands. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Voice (R)

Input Format

```
dsp | voice ?
```

Parameters

None

Response

Lists the supported DSP or Voice commands and keywords and a brief description of their function.

dsp ecode

Selects the voice encoding method for all voice ports.

Mgmt Class

Voice (R/W)

Input Format

```
dsp ecode <alaw | ulaw>
```

Parameters

`***`	When entered with no parameter, the current encoding method is displayed
`alaw`	Sets encoding method to alaw.
`ulaw`	Sets encoding method to ulaw.

Example

The following command example will set the voice encoding method to alaw.

```
-> dsp ecode alaw
```

Response

Typical response when entered with no parameters.

```
-> dsp ecode

Current Encoding Law: ALAW
```

dsp jitter

Adjusts the size of the jitter buffer for all voice ports.

CAUTION:
Setting the jitter buffer to a value less that the default (15 milliseconds) may cause degradation of voice quality.

NOTE:
Prior to changing the jitter buffer size, cease any active calls and close all data transfers.

Mgmt Class

Voice (R/W)

Input Format

```
dsp jitter <milliseconds>
```

Parameters

`***`	When entered with no parameter, the current jitter buffer value is displayed
`<milliseconds>`[a]	Optional, Length of jitter buffer in milliseconds.

[a] Integer, 0 - 60 (15)

Example

The following command example will change the jitter buffer size to 20 milliseconds.

```
-> dsp jitter 20
```

Response

Typical response when entered with no <milliseconds> parameter.

```
-> dsp jitter

Jitter Buffer: 15 ms
```

dsp provision

Sets the signalling the method in which phone lines (or trunks) are seized and released.

Mgmt Class

Voice (R/W)

Input Format

```
dsp provision <port> <loop | ground>
```

Parameters

`***`	When entered with no parameter, the current configuration is displayed
`<port>`[a]	Voice port to configure.[b]
`loop`	Sets voice signalling method to loop start
`ground`	Sets voice signalling method to ground start

[a] Integer, 1 - 4 (or 1 - 8 for 8-port IADs)
[b] When command is entered with <port> and no method <loop | ground>, the current port configuration is displayed.

Example

The following command example will configure voice port 4 for ground start.

```
-> dsp provision 4 ground
```

Response

Typical response when entered with no parameters:

```
-> dsp provision
[ 1]: Loop Start
[ 2]: Loop Start
[ 3]: Loop Start
[ 4]: Loop Start
```

Typical response when configuration has been changed:

```
-> dsp provision 4 ground

[ 4]: Ground Start
```

dsp save

Saves the current DSP configuration parameters to flash memory.

Mgmt Class

Voice (R/W)

Input Format

```
dsp save
```

Parameters

None

Response

Command prompt.

dsp vr

Displays the current voice rate and encoding type.

Mgmt Class

Voice (R)

Input Format

```
dsp vr <port>
```

Parameters

`***`	When entered with no parameter, the value for port 1 value is displayed.
`<port>`[a]	Voice port to configure.

[a] Integer, 1 - 4 (or 1 - 8 for 8-port IADs)

Response

```
-> dsp vr 4

Ingress: G711 uLaw  Egress: G711 uLaw
```

voice l2clear

Clears L2 control channel statistics. This command is only enabled when configured for operation with a Jetstream voice gateway.

Mgmt Class

Voice (R/W)

Input Format

```
voice profile <profile>
```

Parameters

None

Response

Command prompt.

voice l2stats

Displays L2 control channel statistics. This command is only enabled when configured for operation with a Jetstream voice gateway.

Mgmt Class

Voice (R)

Input Format

```
voice l2stats
```

Parameters

None

Response

```
-> voice l2stats
Stats for Sub ID 1:
    Rx Frames:          0
    Rx I Frames:        0
    Tx Frames:          0
    Tx I Frames:        0
    ReTx Frames:        0
```

voice profile

Defines the feature set and the voice packet payload size for voice connections as prescribed in ATMF Standards-based signalling profiles.

Mgmt Class

Voice (R/W)

Input Format

```
voice profile <profile>
```

Parameters

`***`	When entered with no parameter, the current voice profile setting is displayed
`<profile>`[a]	Defines the profile to be used.

[a] Integer, 7 - 12 (9)

Example

The following command example will change the voice profile to profile 7.

```
-> voice profile 7
```

Response

Example response confirming the configuration change.

```
-> voice profile 9

The active profile has been changed
Profile 9 active, pcm only, 44 byte packets
```

voice refreshcas

Defines the mode in which refresh CAS (channel associated signalling) cells will be sent to the voice gateway.

☞ **NOTE:**

A mode change is effective immediately. However you must perform a save command if the change is to be persistent across reboots.

Mgmt Class

Voice (R/W)

Input Format

```
voice refreshcas active | always
```

Parameters

`***`	When entered with no parameter, the current mode is displayed
`active`	CAS refresh signals are sent only when voice is present. Default mode.
`always`	CAS refresh signals are sent both when voice is present and during an idle state.

Example

The following command example will change the refresh cas mode to always.

```
-> voice refreshcas always
```

The following command example entered with no parameters to display the current mode.

```
-> voice refreshcas
Refresh CAS signaling is currently "always".
```

Response

Command prompt.

This page intentionally left blank.

CHAPTER 14

RADIUS COMMANDS

This section contains Radius (RAD) command descriptions. Radius allows access control and user authentication to be managed from a remote server. For more information on Access Controland RADIUS, see “Radius” on page 5-10.

The Radius commands found in this section include:

Table 14-1: Radius Command Listing

Command	Function
rad ?	Lists the supported radius commands and key-words.
rad deleteserver	Deletes a configured radius server entry.
rad list secret	Displays the radius servers shared-secret authen-tication.
rad list server	Displays the IP address and port for the primary and secondary radius servers.
rad set retries	Sets the number of retires to a radius server before attempting the next radius server, if configured.
radius set secret	Sets the authentication secret for the specified radius server.
radius set server	Sets the IP address and port values for the primary and/or secondary radius server(s).
radius set timeout	Sets the number of seconds between retry at-tempts to the radius server.

rad ?

Lists the supported radius commands and keywords. To see the syntax for a command, enter the command followed by a ?.

Input Format

```
rad ?
```

Parameters

None

Response

A listing of the rad commands and keywords and a brief description of their function.

rad deleteserver

Deletes a configured radius server entry.

Mgmt Class

Security (R/W)

Input Format

```
rad deleteserver <integer>
```

Parameters

`<integer>`[a]	Radius server to delete (1 = primary, 2 = secondary).

[a] Integer, 1, 2 (1)

Response

A response confirming the server has been deleted shown displayed.

```
-> rad deleteserver 1
RADIUS Server 1 DELETED
```

rad list secret

Displays the radius servers shared-secret authentication.

☞ **NOTE:**

The local servers' shared-secret must match the remote server's shared-secret or authentication will not occur.

Mgmt Class

Security (R)

Input Format

```
rad list secret
```

Parameters

None

Response

A typical response is shown below.

```
-> rad list secret
RADIUS Secrets
----------------
  Server1: Set
  Server2: Set
```

rad list server

Displays the IP address and port for the primary and secondary radius servers.

Mgmt Class

Security (R)

Input Format

```
rad list server
```

Parameters

None

Response

A typical response is shown below.

```
-> rad list server

RADIUS Server 1
----------------
  IP Address: 192.168.12.251
  Port: 1812

RADIUS Server 2
----------------
  IP Address: 192.168.11.104
  Port: 150
```

rad set retries

Sets the number of retires to a radius server before attempting the next radius server, if configured.

Mgmt Class

Security (R/W)

Input Format

```
rad set retries <integer>
```

Parameters

`<integer>`[a]	Number of retry attempts.

[a] Integer, 0 - 5 (3)

Response

Command prompt.

radius set server

Sets the IP address and port values for the primary and/or secondary radius server(s).

Mgmt Class

Secret (R/W)

Input Format

```
radius set server <IPAddr> [port] [server]
```

Parameters

`<ipaddr>`[a]	Sets the IP address of the specified radius server.
`<port>`[b]	Sets the port number of the specified radius server.
`<server>`[c]	Specifies the radius server (1 = primary, 2 = secondary).

[a] dotted-decimal notation
[b] Integer, 1 - 65535 (1812)
[c] Integer, 1, 2 (1)

Response

Command prompt.

radius set secret

Sets the authentication secret for the specified (primary or secondary) radius server.

Mgmt Class

Secret (R/W)

Input Format

```
rad set secret <server> <secret>
```

Parameters

`<server>`[a]	Specifies the Radius server. (1 =primary, 2 = secondary).
`<secret>`[b]	Authentication secret for the specified radius server.

[a] Integer, 1 / 2 (1)
[b] ASCII string, maximum of 64 characters with no white-spaces.

Response

Command prompt.

radius set timeout

Sets the number of seconds between retry attempts to the radius server.

Mgmt Class

Security (R/W)

Input Format

```
rad set timeout <integer>
```

Parameters

`<integer>`[a]	Number of seconds between retry attempts.

[a] Integer, 0 - 5 (3)

Response

Command prompt.

CHAPTER 15

USER COMMANDS

This section contains User command descriptions. The user commands facilitate the following functions:

- Add or delete a user account
- Enable or disable a user account
- Grant read-only or read-write privileges for each management class for each user account
- Control user access methods
- Set a user password

For a complete discussion of access control, see Chapter 5, System Security in the Technical Reference Guide. The user commands found in this section include:

Table 15-1: User Command Listing

Command	Function
user ?	Lists the supported user commands and keywords.
user add access	Adds an access privilege to for the specified user.
user add class	Configures the managements class with read-only or read-write privileges for the specified user.
user add user	Creates a user account.
user delete access	Deletes an access path from the specified user account.
user delete class	Changes or deletes a user account management class privileges.
user delete user	Deletes a user account.
user disable	Disables an existing user account.

Table 15-1: User Command Listing (Cont.)

Command	Function
user enable	Enables or disables authentication of the remote router during tunnel establishment using the CHAP secret.
user list	Displays the contents of the user account database.
user list lookup	Lists the primary and secondary locations to access and validate user account.
user list template	Lists the characteristics of the pre-defined user templates.
user set lookup	Specifies the primary and secondary location for accessing and validating user account information.
user set password	Specifies the source IP address used when the tunnel is originated.

user ?

Lists the supported user commands and keywords. To see the additional sub-commands or the syntax for a command, enter the command followed by a ?.

Mgmt Class

Admin (R)

Input Format

```
user ?
```

Parameters

None

Response

Lists the supported user commands and keywords and a brief description of their function.

user add access

Adds an access privilege for the specified user. To view the current access methods for a user, use the command user list.

Mgmt Class

Admin (R/W)

Input Format

```
user add access <lan | wan | console> <username>
```

Parameters

`lan`	Adds user access through a LAN connection.
`wan`	Adds user access through the WAN connection.
`console`	Adds user access through the console (serial port).
`<username>`	User account to which access method will be added.

Example

The following example will add *console* access or the user *VoiceAdmin*:

```
-> user add access console VoiceAdmin
Added "CONSOLE" access for user "VoiceAdmin"
```

Response

See example above.

user add class

Configures the managements class with read-only or read-write privileges for the specified user. Multiple class and privilege pairs may be specified for a user. To view the current management class(es) for a user, use the command user list.

☞ **NOTE:**

If a user account currently has read-write privilege for a management class, adding the same user class with a read-only privilege will not revoke the read-write privilege. To revoke the read-write privilege, use the user delete class command, then re-establish the management class with read-only access.

Mgmt Class

Admin (R/W)

Input Format

```
user add class <class> read | write <user_name>
```

Parameters

`<class>`	Must be one of the following:	
	`admin`	Adds Admin management class for the specified user account.
	`voice`	Adds voice management class for the specified user account.
	`network`	Adds network management class for the specified user account.
	`system`	Adds system management class for the specified user account.
	`security`	Adds security management class to the specified user account.
	`debug`	Adds debug management class to the specified user account.
`read`	Class privileges are granted on a read-only access.	
`write`	Class privileges are granted for read and write access.	
`<user_name>`[a]	User account to which the management class is added.	

[a] ASCII string, 6 - 32 characters. User name is case sensitive.

Response

A typical response is shown below.

```
-> user add class security write Admin1

Added "SECURITY-WRITE" management class for user "Admin1"
```

user add user

Adds a user account. To add a user account a *user name* and *password* are required. The optional *template* parameter can be used to quickly and easily assign a user access privilege rights based on pre-defined templates. For additional information on adding a user account and templates, see “Templates” on page 5-4.

☞ **NOTE:**

The optional *template* and *enable/disable* parameters must be used concurrently; the command will fail if only one of the optional parameters is used.

Mgmt Class

Admin (R/W)

Input Format

```
user add user <user_name> <password> [<template> <enable|
disable>]
```

Parameters

`<user_name>`[a]	User name for the account.	
`<password>`[a]	Password for the user account.	
`<template>`	Must be one of the following:	
	`super`	Specifies the super-user template account privileges.
	`voice`	Specifies the voice template account privileges.
	`network`	Specifies the network template user account privileges.
	`security`	Specifies the security template account privileges.
	`viewer`	Specifies the viewer template account privileges.
`enable`	Enables the specified user upon account creation.	
`disable`	User account information is created, but user account has no access to the router.	

[a] ASCII string, 6 - 32 characters. User name and password are case-sensitive.

Examples

Example command adding the user *guiguy* with the access rights and privilege of the *network* template.

```
-> user add user guiguy htmlrus network enable
User "guiguy" added (enabled, with "network" template)
```

Example command adding a user account with no optional parameters.

```
-> user add user staff001 secret
User "staff001" added.
```

Response

See examples above.

user delete access

Deletes an access path from the specified user account. To view the current access methods for a user, use the command user list.

Mgmt Class

Admin (R/W)

Input Format

```
user delete access <lan | wan | console> <username>
```

Parameters

`lan`	Removes user access through a LAN connection.
`wan`	Removes user access through the WAN connection.
`console`	Removes user access through the console (serial port).
`<username>`	User account to which access method will be deleted.

Response

A typical response is shown below.

```
-> user delete access wan Admin1
Deleted "WAN" access for user "Admin1"
```

user delete class

Changes or deletes a user account management class privileges. To view the current management class(es) for a user, use the command user list.

☞ **NOTE:**

The system must contain at least one enabled user account with privilege read and write access. If only one Admin account exists, it cannot be deleted, disabled or have the privilege class changed to read-only or deleted.

☞ **NOTE:**

Deleting a read-only permission will remove the management class from a user account. Deleting a write permission from a user account will render the user account read-only for the management class.

Mgmt Class

Admin (R/W)

Input Format

```
user delete class <mgtclass> read | write <username>
```

Parameters

`<mgtclass>`	Must be one of the following:	
	`admin`	Specifies management class the that will changed or deleted.
	`voice`	
	`network`	
	`system`	
	`security`	
	`debug`	
`read`	Deletes read privilege management class from the specified user account.	
`write`	Deletes user write privilege for the specified management class (user enabled for read-only).	
`<username>`[a]	User account of which the management class is changed or deleted.	

[a] ASCII string. The user name is case-sensitive.

Examples

In the following example, the user (Admin1) has read-write permission for the privilege management class. The example below will delete the write permission and make the user account read only for the privilege management class.

```
-> user delete class admin write Admin1

Deleted "ADMIN-WRITE" management class for user "Admin1"
```

In the following example, read permission for the voice management class is removed, thus deleting the management class from the user account.

```
-> user delete class voice read Admin1

Deleted "VOICE-READ" management class for user "Admin1"
```

Response

See examples above.

user delete user

Deletes an existing user account from the management database. Deletion of multiple user accounts is supported. To view a user account listing, use the command user list.

☞ **NOTE:**
The system must contain at least one enabled user account with privilege read and write access. If only one admin acount exists, it cannot be deleted or disabled.

Mgmt Class

Admin (R/W))

Input Format

```
user delete user <username1> [<username2> <usernameN>]
```

Parameters

<username>[a]	User account to be deleted.

[a] ASCII string. The username is case-sensitive.

Response

A typical response confirms the user account has been deleted.

```
-> user delete user Admin1 staff001

User "Admin1" deleted
User "staff001" deleted
```

user disable

Disables an existing user account. The user account information is not changed, but the user acount cannot access the router. To view a user account listing, use the command user list.

☞ **NOTE:**
The system must contain at least one enabled user account with privilege read and write access. If only one privilege account exists, it cannot be deleted or disabled.

Mgmt Class

Admin (R/W))

Input Format

```
user disable <username>
```

Parameters

`<username>`[a] User account to be disabled.

[a] ASCII string. The username is case-sensitive.

Response

A typical response is shown when disabling the user account *VoiceAdmin*.

```
-> user disable VoiceAdmin

User "VoiceAdmin" disabled
```

user enable

Enables an existing user account. To add a new user account, use the user add user command. To view a user account listing, use the command user list.

Mgmt Class

Admin (R/W))

Input Format

```
user enable <username>
```

Parameters

<username>[a] User account to be enabled.

[a] ASCII string

Response

A typical response is shown when enabling the user account *Admin1*.

```
-> user enable Admin1
User "Admin1" enabled.
```

user list

Displays the contents of the user account database. The username, management class privileges, status, and access paths are listed for each configured user account.

☞ **NOTE:**
For security reasons, user passwords are not displayed; they are displayed as "**********".

Mgmt Class

Admin (R/W)

Input Format

```
user list
```

Parameters

None

Response

A typical response is shown below.

```
-> user list

Printing local user database (3 total valid users)...
Username: superuser
Password: ****************
Mgmt Class(read): NETWORK SYSTEM ADMIN VOICE SECURITY DEBUG
Mgmt Class(write): NETWORK SYSTEM ADMIN VOICE SECURITY DEBUG
Access: WAN LAN CONSOLE
Status: ENABLED

Username: Admin1
Password: ****************
Mgmt Class(read): NETWORK SYSTEM VOICE SECURITY DEBUG
Mgmt Class(write): NETWORK SYSTEM DEBUG
Access: WAN LAN CONSOLE
Status: ENABLED

Username: VoiceAdmin
Password: ****************
Mgmt Class(read): NETWORK SYSTEM VOICE
Mgmt Class(write): NETWORK SYSTEM VOICE
Access: WAN LAN CONSOLE
Status: DISABLED
```

user list lookup

Lists the primary and secondary locations to lookup and validate a user account. The primary and secondary locations are configured with the user set lookup command.

Mgmt Class

Admin (R/W)

Input Format

```
user list lookup
```

Parameters

None

Response

A typical response is shown below.

```
-> user list lookup
User Lookup Order - Primary: LOCAL Secondary: NONE
```

user list template

Displays the pre-defined user template information.

Mgmt Class

Admin (R)

Input Format

```
user list template
```

Parameters

None

Response

```
-> user list template
Template: 0
Username: SuperUser
Password: ****************
Mgmt Class(read): NETWORK SYSTEM ADMIN VOICE SECURITY DEBUG
Mgmt Class(write): NETWORK SYSTEM ADMIN VOICE SECURITY DEBUG
```

```
Access: WAN LAN CONSOLE
Status: ENABLED

Template: 1
Username: VoiceManager
Password: ****************
Mgmt Class(read): SYSTEM VOICE
Mgmt Class(write): SYSTEM VOICE
Access: WAN LAN CONSOLE
Status: ENABLED

Template: 2
Username: NetworkManager
Password: ****************
Mgmt Class(read): NETWORK SYSTEM
Mgmt Class(write): NETWORK SYSTEM
Access: WAN LAN CONSOLE
Status: ENABLED

Template: 3
Username: SecurityManager
Password: ****************
Mgmt Class(read): SYSTEM SECURITY
Mgmt Class(write): SYSTEM SECURITY
Access: WAN LAN CONSOLE
Status: ENABLED

Template: 4
Username: Viewer
Password: ****************
Mgmt Class(read): NETWORK SYSTEM VOICE SECURITY
Mgmt Class(write): NONE
Access: WAN LAN CONSOLE
Status: ENABLED
```

user set lookup

Sets the primary and secondary locations to lookup and validate user account information. To view the current lookup configuration, use the user list lookup command.

☞ **NOTE:**
The Radius client is a Key-Enabled feature and is not functional without entering a required key. For more information on Radius, see “Radius” on page 5-10.

Mgmt Class

Admin (R/W)

Input Format

```
user set lookup <primary|secondary> <local|radius|none>
[<primary|secondary> <local|radius|none>]
```

Parameters

☞ **NOTE:**
Atleast one location (primary or secondary) must be set to local.

Select the lookup order to configure.

`primary`	First location to be accessed for user database.
`secondary`	Second location to be accessed for user database.

Select the location of the user database to be accessed.

`local`	Local user database will be accessed.
`radius`	Radius server will be accessed.
`none`	No location is specified.

Response

A typical response is shown below.

```
-> user set lookup primary local secondary radius
User Lookup Order - Primary: LOCAL Secondary: RADIUS
```

user set password

Changes the password of an existing user account.

Mgmt Class

Admin (R/W)

Input Format

```
user setpassword <user_name> <new_password>
```

Parameters

<user_name>[a]	User account for the new password.
<new_password>[a]	New password for the user account.

[a] ASCII string, 6 - 32 characters. The user name and password are case-sensitive.

Response

A typical response is shown below.

```
-> user set password Admin1 secret
User "Admin1" password changed
```

This page intentionally left blank.

CHAPTER 16

KEY COMMANDS

This section contains KEY commands descriptions. Key-enabled features are optional router capabilitiesthat can be enabled by purchasing Activation keys. These optional capabilities include:

- 3DES Encryption
- DES Encryption
- Internal V.90 modem
- IP Stack
- IP Stack Check
- IP Security and IKE (Internet Key Exchange)
- L2TP Tunneling
- Quality of Service (QOS)
- Remote Authentication Service (RADIUS client)
- SSH Secure Shell (Server)
- Stateful Firewall
- VPN Accellerator

For a complete discussion of Key Enabled Features, see “Key Enabled Features” on page 4-29.

The KEY commands found in this section include:

Table 16-1: KEY Command Listing

Command	Function
key ?	Lists the supported key commands.
key add	Validates and adds a key to the key-enabled feature database.
key delete	Deletes a feature key from the key-enabled feature database.

Table 16-1: KEY Command Listing (Cont.)

Command	Function
key disable	Disables a key-enabled feature.
key enable	Enables a feature key that has been previously added to the key-enabled feature database.
key list	Displays the contents of the key-enabled features database and the status of each feature.
key revoke	Revokes a key-enabled feature key.
key unrevoke	Unrevokes a revoked feature key.
key update	Updates the expiration date of an expired feature key.

key ?

Lists the supported key commands. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Security (R)

Input Format

```
key ?
```

Parameters

None

Response

A listing of the supported key commands and a brief description of their function.

key add

Validates a the key that has been generated for the specific device. Once validated, adds key to key database. When adding a key enabled feature, the feature is enabled by default. To disable a feature, use the key disable command. A key cannot be entered if one of the following conditions exist:

- The key was generated for a different router.
- A non-revoked and non-expired key has already been added for the specified feature.
- The same key currently exists in a revoked condition.
- The key state is Manufacturing or Legacy

☞ **NOTE:**

The key will not be written to flash memory until a save command has been issued.

Mgmt Class

Security (R/W)

Input Format

```
key add <key_string>
```

Parameters

`<key_string>`[a] Key string. Example shown below.

`1H+zWqHlXa32Kir45Nqxean3a4kkvhSIH0H/cAHujbtRanrVpx9yxQZlLT6pCUnbuAZzHsLKin7=`

[a] The key string is case-sensitive and must be entered exactly as received and with no spaces.

Response

Example response when adding a key for *L2TP*.

```
-> key add 1H+zWqHlXa32Kir45Nqxean3a4kkvhSIH0H/cAHujbtRa=
10/03/2001-13:03:54:KEF: Load key for feature "l2tp" into DB SUCCEDEED
```

Example response when adding a key that already exists or has been revoked.

```
-> key add 1H+zWqHlXa32Kir45Nqxean3a4kkvhSIH0H/cAHujbtRa=
10/03/2001-13:50:31:KEF: Load key for feature "l2tp" into DB FAILED
```

key delete

Deletes the specified key from the key enabled feature database.

CAUTION:

Feature status (enabled /disabled) is disregarded when deleting the feature. Deleting an enabled feature may result in reduced security or quality of service, or may otherwise effect system operation.

NOTE:

Features with keys that have expired or have been revoked cannot be deleted, nor can Legacy or Manufacturing keys be deleted.

Mgmt Class

Security (R/W)

Input Format

```
key delete <feature_name>
```

Parameters

`<feature_name>`[a] Name of the feature to be deleted.[b]

[a] ASCII string
[b] To see the contents of the key enabled database, use the key list command.

Response

Example response when deleting the key for *Radius*.

```
-> key delete radius
10/03/2001-13:19:33:KEF: Delete key for feature "radius" SUCCEDEED
```

key disable

Disables the specified feature. Feature configuration is not changed, but feature is rendered non-operational. To view the current status of installed key features, use the key list command.

CAUTION:
Disabling a feature may result in reduced security or quality of service, or may otherwise effect system operation.

NOTE:
Disabling a feature does not change or extend the expiration date of the feature key.

NOTE:
Legacy or Manufacturing keys cannot be disabled.

Mgmt Class

Security (R/W)

Input Format

```
key disable <feature_name>
```

Parameters

`<feature_name>` Name of the feature to be disabled.[a]

[a] To see the contents of the key enabled database, use the key list command.

Response

A typical response is shown below.

```
-> key disable l2tp

10/03/2001-13:41:45:KEF: Disable key for feature "l2tp" SUCCEDEED
```

key enable

Enables a specified key-enabled feature. To enable a feature, the key must have been previously added with the key add command. To view the current status of installed key features, use the key list command.

☞ **NOTE:**
Features with a revoked or expired key cannot be enabled.

Mgmt Class

Security (R/W)

Input Format

```
key enable <featurename>
```

Parameters

`<featurename>`[a] Name of the feature to be enabled.[b]

[a] ASCII string
[b] To see the contents of the key enabled database, use the key list command.

Response

A typical response is shown below.

```
-> key enable l2tp

10/03/2001-14:00:47:KEF: Enable key for feature "l2tp" SUCCEDEED
```

key list

Lists the contents of the key-enabled feature database. Information provided includes the installation and expiration date, the feature status (enabled/disabled) and if the feature has expired or been revoked.

Mgmt Class

Security (R)

Input Format

```
key list [-l]
```

Parameters

`-l` This optional parameter will include the key strings for each feature installed.

Response

A typical response is shown below.

```
Feature name  Description        En Rv Ex Installed  Expires
3des          3DES Encryption    1  0  0  08/29/2001 12/31/2001
VPNaccell     VPN Accellerator   1  0  0  08/28/2001 12/31/2001
Intmodem      Internal Modem     1  -  -  --/--/---- --/--/---- Not Inst'd
QoS           Quality of Service -  -  -  --/--/---- --/--/---- Not Inst'd
des           DES Encryption     1  0  0  08/28/2001 12/31/2001
firewall      Stateful Firewall  -  -  -  --/--/---- --/--/---- Not Inst'd
ipcheck       IP stack check     1  -  -  --/--/---- --/--/---- MFG
ipfilter      IP Filter          1- -  -  --/--/---- --/--/---- MFG
                                 -
ipsec         IP Security        -  -  -  --/--/---- --/--/---- Not Inst'd
ipstack       IP Stack           1  -  -  --/--/---- --/--/---- MFG
l2tp          L2TP Tunneling     -  -  -  --/--/---- --/--/---- Not Inst'd
radius        RADIUS Client      -  -  -  --/--/---- --/--/---- Not Inst'd
sshd          SSH Server         -  -  -  --/--/---- --/--/---- Not Inst'd
```

A typical response with the *-l* parameter is shown below.

```
Feature name  Description      En Rv Ex Installed  Expires
3des          3DES Encryption  1  0  0  08/29/2001 12/31/2001
1H+zWqHlXa32Kir45Nqxean3a4kkvhSTFS0H/cAHujbtRanrVpx9yxQZlLT6pCUnbuAZzHsLKin7=
VPNaccell     VPN Accellerator 1  0  0  08/28/2001 12/31/2001
1H+zWqHlXa32Kir45Nqxean3a4kkvhSTFS0H/cAHujbtRanrVpx9yxQZlLT6pCUnbuAZzHsLKin7=
Intmodem      Internal Modem   1  -  -  --/--/---- --/--/---- Not Inst'd
QoS           QoS              -  -  -  --/--/---- --/--/---- Not Inst'd
des           DES Encryption   1  0  0  08/28/2001 12/31/2001
3H+zWqHlXa32Kir45Nqxwen3a4qkvhSIH0H/cAHujbtRanrPpx9yxQZlLT6pCUnbuAZzHsLwin7=
firewall      Stateful Firewall- -  -  --/--/---- --/--/---- Not Inst'd
ipcheck       IP stack check   1  -  -  --/--/---- --/--/---- MFG
firewall      Stateful Firewall1  -  -  --/--/---- --/--/---- MFG
ipsec         IP Security      -  -  -  --/--/---- --/--/---- Not Inst'd
ipstack       IP Stack         1  -  -  --/--/---- --/--/---- MFG
l2tp          L2TP Tunneling   -  -  -  --/--/---- --/--/---- Not Inst'd
radius        RADIUS Client    -  -  -  --/--/---- --/--/---- Not Inst'd
sshd          SSH Server       -  -  -  --/--/---- --/--/---- Not Inst'd
```

key revoke

Revokes a key-enabled feature.

☞ **NOTE:**

Once a feature has been revoked, it may not be enabled, updated or deleted. To re-enable a feature that has been revoked, a new key must be generated and added.

☞ **NOTE:**

Manufacturing or Legacy keys cannot be revoked.

Mgmt Class

Security (R/W)

Input Format

```
key revoke <feature>
```

Parameters

`<feature_name>`[a] Name of the feature key to be revoked.

[a] ASCII string

Response

A typical response is shown below.

```
-> key revoke qos
10/03/2001-14:19:04:KEF: Revoke key for feature "QoS" SUCCEDEED
```

key unrevoke

Unrevokes a previously revoked key for the specified feature.

☞ **NOTE:**

The unrevoke key string is a different key than was used initially with the key add command.

Mgmt Class

Security (R/W)

Input Format

```
key unrevoke <key_string>
```

Parameters

`<key_string>`[a] Unrevoke keystring.

[a] The key string is case-sensitive and must be entered exactly as received and with no spaces.

Response

A typical response is shown below.

```
-> key unrevoke XtdHVZCPNSJWGJykx9jw2WMDzaZW4/atl0viRvnNX+Mv2wdX=

10/03/2001-14:22:20:KEF: Unrevoke key for feature "ipfilter" SUCCEDEED
```

key update

Updates the expiration date for the specified feature key.

☞ **NOTE:**
A key update cannot be used for a key that has been revoked or Manufacturing and Legacy keys.

Mgmt Class

Admin (R/W), System (R/W)

Input Format

```
key update <key_string>
```

Parameters

`<key_string>`[a] Key string for the feature.

[a] The key string is case-sensitive and must be entered exactly as received and with no spaces.

Response

A typical response is shown below.

```
-> key update XtdHVZCPNSJWGJykx9jw2WMDzaZW4/atl0viRvnNX+Mv2wdX=

10/03/2001-14:31:17:KEF: Update key for feature "QoS" SUCCEDEED
```

This page intentionally left blank.

CHAPTER 17

SNMP COMMANDS

This section contains SNMP command descriptions. For a complete discussion of SNMP, see “SNMP” on page 7-2.

The SNMP commands found in this section include:

Table 17-1: SNMP Command Listing

Command	Function
snmp ?	Lists the supported SNMP keywords and commands.
snmp addsnmpfilter	Validates SNMP clients by defining a range of IP addresses that are allowed to access the router via SNMP. Same function as system addsnmpfilter.
snmp addtrapdest	Adds an SNMP Trap manager by IP address.
snmp community	Sets the SNMP community to which the router belongs.
snmp delsnmpfilter	Deletes the specified SNMP client range. Same function as system delsnmpfilter.
snmp deltrapdest	Deletes a SNMP Trap manager by IP address.
snmp disablesnmpif	Disables SNMP access from the specified interface.
snmp enablesnmpif	Enables SNMP access from the specified interface.
snmp settrapenable	Enables or disables transmission of unsolicited trap event messages to trap destinations.
snmp snmppasswd	Sets an authentication password for an SNMP Manager.
snmp snmpport	Manages SNMP port access. Same function as system snmpport.

snmp ?

Lists the supported SNMP commands and keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
snmp ?
```

Parameters

None

Response

Lists the supported SNMP commands and keywords and a brief description of their function.

snmp addsnmpfilter

Validates SNMP clients by defining a range of IP addresses that are allowed to access the router via SNMP. This validation feature is *off* by default.

☞ **NOTE:**
This command is functionally equivalent to system addsnmpfilter.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

☞ **NOTE:**
To list the range of allowed clients, use the command system list when you are logged in with read and write permission (be sure to log in with password). To delete addresses from the SNMP filter, use the command snmp delsnmpfilter or system delsnmpfilter.

For more information on SNMP, see.

Mgmt Class

Security (R/W)

Input Format

```
snmp addsnmpfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the client range.
`<last ipaddr>`[a]	Last IP address of the client range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

snmp addtrapdest

Adds the IP address for a SNMP Trap manager. To view the existing trap addresses, use the command snmp list. For additional information on SNMP, see “SNMP” on page 7-2.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Network (R/W)

Input Format

```
snmp addstrapdest <ip addr>
```

Parameters

`<ipaddr>`[a]	IP address of the trap manager.

[a] Dotted-decimal notation

Response

Command prompt.

snmp community

Sets the SNMP community to which the router belongs; the default community is "*public*". For additional information on SNMP, see “SNMP” on page 7-2.

☞ **NOTE:**
This command requires a save to be persistent across reboots.

Mgmt Class

Network (R/W)

Input Format

```
snmp community <snmp community name>
```

Parameters

`***`	When entered with no parameters, the current SNMP community name is displayed.
`<name>`[a]	SNMP community name.

[a] ASCII string, 1 - 40 characters with no white-spaces (public)

Example

The following example sets the SNMP community name to iads:

```
-> snmp community iads
```

Response

Example response when the command is entered with no community name parameter:

```
-> snmp community

SNMP Community name: iads
```

snmp delsnmpfilter

Deletes the client range previously defined by the commands snmp addsnmpfilter or system addsnmpfilter.

NOTE:
This command is functionally equivalent to system delsnmpfilter.

NOTE:
This command does not require a reboot and is effective immediately.

NOTE:
To list the range of allowed clients, use the command system list.

For more information on SNMP, see.

Mgmt Class

Network (R/W)

Input Format

```
snmp delsnmpfilter <first ip addr> [<last ip addr>] | lan
```

Parameters

`<first ipaddr>`[a]	First IP address of the client range.
`<last ipaddr>`[a]	Last IP address of the client range.[b]
`lan`	Local Ethernet LAN.

[a] Dotted-decimal notation
[b] May be omitted if the range contains only one IP address.

Response

Command prompt.

snmp deltrapdest

Deletes the IP address of a current SNMP Trap manager. To view the existing trap addresses, use the command snmp list. For additional information, see “SNMP” on page 7-2.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Network (R/W)

Input Format

```
snmp deltrapdest <ip addr>
```

Parameters

`<ipaddr>`[a] IP address of the trap manager that will be deleted.

[a] Dotted-decimal notation

Response

Command prompt.

snmp disablesnmpif

Disables SNMP access from the specified interface. To see the current interface(s) enabled, use the command snmp list.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Network (R/W)

Input Format

```
snmp disablesnmpif <wan|lan>
```

Parameters

`wan	lan`	Interface from which SNMP access will be disabled.

Response

Command prompt.

snmp enablesnmpif

Enables SNMP access from the specified interface. To see the current interface(s) enabled, use the command snmp list.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Network (R/W)

Input Format

```
snmp enablesnmpif <wan|lan>
```

Parameters

`wan	lan`	Interface from which SNMP access will be enabled.

Response

Command prompt.

snmp list

Displays current SNMP configuration information.

☞ **NOTE:**
If changes to the SNMP configuration have been made since the last reboot, the changes will be displayed, but may not be in effect until after a save and reboot.

Mgmt Class

Network (R)

Input Format

```
snmp list
```

Parameters

None

Response

Typical response:

```
-> snmp list
SNMP CONFIGURATION INFORMATION
    Community name..................... iads
    Port............................... default (161)
    IF Enabled......................... LAN only
    Clients............................ all
    Global Trap Enable................. on
    Configured Trap Destinations......... none
```

snmp settrapenable

Enables or disables transmission of unsolicited trap event messages to trap destinations. To see the current Global Trap Enable setting, use the command snmp list.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Network (R/W)

Input Format

```
snmp settrapenable on | off
```

Parameters

`on`	Enables trap event message transmission.
`off`	Disables trap event message transmission.

Response

Command prompt.

snmp snmppasswd

Sets an authentication password for an SNMP Manager. Once authenticated, SNMP set requests will be honored allowing changes to the system configuration.

☞ **NOTE:**
This command does not require a reboot and is effective immediately.

Mgmt Class

Network (R/W)

Input Format

```
snmp snmppasswd <passwd>
```

Parameters

`***`	Entering command with no password parameter will display the current password.
`<passwd>`[a]	SNMP Manager authentication password.

[a] ASCII string

Response

Example response when a password parameter is entered:

```
-> snmp snmppasswd admin

New snmp password is set to: admin
```

snmp snmpport

This command manages SNMP port access. It can:

- Disable SNMP for this router (sets the SNMP port to 0).
- Request the default SNMP port (161). This re-enables SNMP after it is disabled.
- Redefines the SNMP port.

☞ **NOTE:**
This command is the functional equivalent of system snmpport.

☞ **NOTE:**
This command requires a save and reboot to take effect.

To see the current setting, use the command snmp list. For more information on SNMP, see.

Mgmt Class

Network (R/W)

Input Format

```
snmp snmpport  default | disabled | <port>
```

Parameters

`default`	Restores the port value to the default value 161 and re-enables the port.
`disable`	Disables the existing SNMP port.
`<port>`[a]	Defines a new SNMP port number. Use this option to restrict remote access.

[a] Integer, 1 - 65535 (161)

Response

Command prompt.

CHAPTER 18

STATEFUL FIREWALL COMMANDS

This section contains command descriptions for the key-enabled Stateful Firewall feature. For an overview of firewalls and more detailed information on Stateful Firewall, see “Stateful Firewall” on page 4-34. For Internet firewall filtering commands, see eth ip firewall, in Chapter 5, Ethernet Interface Commands.

The firewall commands found in this section include:

Table 18-1: Firewall Command Listing

Command	Function
firewall ?	Lists the supported stateful firewall keywords.
firewall allow	Creates a firewall rule for inclusion in the allow rules list.
firewall clearcounter	Clears the counter for a specified rule.
firewall clearcounter all	Clears counters for all stateful firewall rules.
firewall delete	Deletes a single firewall rule or range of firewall rules based on firewall rule numbers.
firewall delete all	Deletes all entries from the allow rules or deny rules list or both.
firewall deny	Creates a firewall rule for inclusion in the deny rules list.
firewall list	Displays the current stateful firewall settings and configured rules.
firewall modify	Allows modification of an existing firewall rule.
firewall set	Enables or disables the stateful firewall function.
firewall setdroppkt-threshold	Sets the threshold of packets dropped per second (due to firewall rules) that when exceeded, will log a message to the console.

Table 18-1: Firewall Command Listing (Cont.)

Command	Function
firewall seticmpflood-threshold	Sets the threshold value for the number of ICMP packets per second, which when exceeded, will cause the firewall to block any subsequent ICMP packets until the ICMP traffic drops below the threshold value.
firewall setsynflood-threshold	Sets the threshold value for the number of SYN packets per second, which when exceeded, will cause the firewall to block any subsequent SYN packets until the SYN traffic drops below the threshold value.
firewall setudpflood-threshold	Sets the threshold value for the number of UDP packets per second, which when exceeded, will cause the firewall to block any subsequent UDP packets until the UDP traffic drops below the threshold value.
firewall viewdroppkts	Displays a listing of up to 200 of the most recent dropped packets.
firewall watch	Enables and disables the console watch for firewall messages.

firewall ?

Lists the supported firewall keywords. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Security (R)

Input Format

```
firewall ?
```

Parameters

None

Response

A listing of all the supported firewall commands and keywords with a brief description of their function.

firewall allow

Creates a firewall rule that will be added to the firewall allow rules list. To view the current allow firewall rules, use the firewall list command.

☞ **NOTE:**

If NAT is enabled on the router, then the outgoing firewall rules should be specified in terms of the private addresses. However, for inbound rules, the rules would need to use the router's WAN address.

Mgmt Class

Security (R/W)

Input Format

```
firewall allow <protocol | application> [<parameters>]
```

Parameters

The following parameters specify the <protocol> (-p) or <application> (-a) characteristics that a packet must have in order to match the firewall rule:

`-p tcp | udp | icmp | <protocol number>`[a]

The packet must have the specified protocol.

`-a imap | telnet | bootp | nntp | rpc | tftp | smtp | dns | ftp | rexec | rsh | rlogin | syslog | winframe | rdp | http | https | ntp | smb | ras | realaudio | netmeeting | aolim| quicktime | cuseeme | netshow | pptp | nfs | nis | traceroute | sqlnet | ipsec`

Packets must match the assigned application characteristics.

[a] Integer, numerical protocol ID.

The following <parameters> specify additional characteristics that an IP packet must have in order to match the firewall rule.

`-sp <ICMP type> | <first source port>[:<last source port>]`

If the protocol is ICMP, the packet must match the specified ICMP type. If the packet is TCP or UDP, if only one source port is specified, the packet must have the specified port, or if a range is defined, a source port that is within the specified port range. If no source port is specified, the firewall rule matches any source port in the range 0 - 65535.

`-dp <ICMP code> | <first dest port>[:<last dest port>]`

If the protocol is ICMP, the packet must match the specified ICMP code. If the packet is TCP or UDP, if only one port is specified, the packet must have the specified destination port, or if a range is defined, a port that is within the specified destination port range. If no destination port is specified, the firewall rule matches any destination port in the range 0 - 65535.

`-da <first dest ip addr>[:<last dest ip addr>]`

The packet must have a destination IP address within the specified address range. If only one address is specified, the packet must have that destination IP address. If no destination IP address is specified, the firewall rule matches any valid IPV4 address.

`-sa <first source ip addr>[:<last source ip addr>]`

The packet must have a source IP address within the specified address range. If only one address is specified, the packet must have that source IP address. If no source IP address is specified, the firewall rule matches any valid IPV4 address.

`-sm <source ip mask>`

The firewall rule uses the specified mask when comparing the <first source ip addr>...<last source ip addr> with the source IP address in the IP packet. If no source mask is specified, the mask used is 255.255.255.255.

`-dm <dest ip mask>`

The firewall rule uses the specified mask when comparing the <first dest ip addr>...<last dest ip addr> with the destination IP address in the IP packet. If no destination mask is specified, the mask used is 255.255.255.255.

Specify one of these options to determine when watch messages are displayed for this firewall rule. The messages are sent to the console serial port and a Syslog server, if configured.

`- q | -v`

If `-q` (quiet) is specified, no messages are displayed for this firewall rule, even if the rule causes a packet to be dropped. This is the default setting for firewall *allow* rules.

If `-v` (verbose) is specified, a message is displayed every time this firewall rule matches a packet, regardless of the rule action.

Specify one of these options to specify the direction of the packet to which the firewall rule is applied. If no direction parameter is specified, the direction is defaulted to *both*.

`in | out`

Examples

The following examples assume that the LAN nodes behind the router are on the subnet 192.168.1.0 with a subnet mask of 255.255.255.0. The router has a WAN address of 12.10.1.1.

The following example will allow the machines behind the router to FTP to any machine on the internet.

```
-> firewall allow -a FTP -sa 192.168.1.0 -sm 255.255.255.0 -d out
```

The following example will allow the machines behind the router to FTP to any one particular machine (64.12.11.1) on the internet.

```
-> firewall allow -a FTP -sa 192.168.1.0 -sm 255.255.255.0 -da
64.12.11.1 -d out
```

The following example will allow only one machine (192.168.1.34) in the subnet to be able to FTP to the internet.

```
-> firewall allow -a FTP -sa 192.168.1.34 -d out
```

The following example will enable ports for one machine (192.168.1.34) in the subnet to use the application 'netmeeting'.

```
-> firewall -a netmeeting -sa 192.168.1.23 -d out
```

Response

Command prompt.

firewall clearcounter

Clears the counters for a firewall rule or a range of firewall rules.

Mgmt Class

Security (R/W)

Input Format

```
firewall clearcounter <firstrulenumber> [<lastrulenumber>]
allow | deny
```

Parameters

`<firstrulenumber>`[a]	Specifies a filter rule number. If a value is entered for the optional *last rule number* parameter, this parameter specifies the first rule in a range of filter rules (inclusive).
`<lastrulenumber>`[a]	Optional, specifies the last rule number in a range of rule numbers.
`allow`	Indicates the specified rule is in the allow rules list.
`deny`	Indicates the specified rule is in the deny rules list.

[a] Integer

Examples

The following example will clear the counter value for firewall rule 13 of the allow rules list.

```
-> firewall clearcounter 13 allow
```

The following example will clear the counter values for firewall rules 4 thorugh 10 of the .deny rules list.

```
-> firewall clearcounter 4 10 deny
```

Response

Command prompt.

firewall clearcounter all

Clears the counters for all firewall rules in both the allow and deny rule lists.

Mgmt Class

Security (R/W)

Input Format

```
firewall clearcounter all
```

Parameters

None

Response

Command prompt.

firewall delete

Deletes a single firewall rule or range of firewall rules based on firewall rule numbers.

☞ **NOTE:**
If deleting a rule or rules from the firewall allow rules list, the change will only be effective for subsequent sessions; current sessions remain unchanged.

☞ **NOTE:**
When defining a range of firewall rules to be deleted, the start and end rule numbers are inclusive and will be deleted.

☞ **NOTE:**
Firewall rules are numbered sequentially, deleting a rule (or range of rules) will decrement remaining rules with higher numbers.

Mgmt Class

Security (R/W)

Input Format

```
firewall delete <start rule number> [<end rule number>] <allow
| deny>
```

Parameters

`<start rule number>`[a]	Specifies the firewall rule, or first rule in the specified range of rules, to be deleted.
`<end rule number>`[a]	Optional, last rule in range of rules to delete.
`allow`	
`deny`	Rule list from which the firewall rule will be deleted.

[a] Integer

Example

Example command deletes rule 3 from the deny rules list.

```
-> firewall delete 3 deny
```

Response

Command prompt.

firewall delete all

Deletes all entries from the allow or deny rules list or both.

☞ **NOTE:**
If the firewall contains allow rules, once the rules are deleted, a reboot must be performed for the changes to become effective.

Mgmt Class

Security (R/W)

Input Format

```
firewall delete all [<allow | deny>]
```

Parameters

`***`	Entering command with no parameter will delete all configured stateful firewall rules.
`allow`	Will delete all rules from the allow rules list
`deny`	Will delete all rules from the deny rules list.

Example

Example command deletes all firewall rules from the allow rules list.

```
-> firewall delete all allow
```

Response

Command prompt.

firewall deny

Creates a firewall rule that will be added to the firewall deny rules list. To view the current deny firewall rules, use the firewall list command.

☞ **NOTE:**
If NAT is enabled on the router, then the outgoing firewall rules should be specified in terms of the private addresses. However, for inbound rules, the rules would need to use the router's WAN address.

Mgmt Class

Security (R/W)

Input Format

```
firewall deny <protocol | application> [<parameters>]
```

Parameters

The following parameters specify the <protocol> (-p) or <application> (-a) characteristics that a packet must have in order to match the firewall rule:

`-p | tcp | udp | icmp | <protocol number>`[a]
The packet must have the specified protocol.

`-a imap | telnet | bootp | nntp | rpc | tftp | smtp | dns | ftp | rexec | rsh | rlogin | syslog | winframe | rdp | http | htps | ntp | smb | ras | realaudio | netmeeting | aolim| quicktime | cuseme | netshow | pptp | nfs | nis | traceroute | sqlnet | ipsec`
Packets must match the assigned application characteristics.

[a] Integer, numerical protocol ID.

The following <parameters> specify additional characteristics that an IP packet must have in order to match the firewall rule.

`-sp <ICMP type> | <first source port>[:<last source port>]`

If the protocol is ICMP, the packet must match the specified ICMP type. If the packet is TCP or UDP, if only one source port is specified, the packet must have the specified port, or if a range is defined, a port that is within the specified source port range. If no source port is specified, the firewall rule matches any source port in the range 0 - 65535.

`-dp <ICMP code> | <first dest port>[:<last dest port>]`

If the protocol is ICMP, the packet must match the specified ICMP code. If the packet is TCP or UDP, if only one port is specified, the packet must have the specified destination port, or if a range is defined, a port that is within the specified destination port range. If no destination port is specified, the firewall rule matches any destination port in the range 0 - 65535.

`-da <first dest ip addr>[:<last dest ip addr>]`

The packet must have a destination IP address within the specified address range. If only one address is specified, the packet must have that destination IP address. If no destination IP address is specified, the firewall rule matches any valid IPV4 address.

`-sa <first source ip addr>[:<last source ip addr>]`

The packet must have a source IP address within the specified address range. If only one address is specified, the packet must have that source IP address. If no source IP address is specified, the firewall rule matches any valid IPV4 address.

`-sm <source ip mask>`

The firewall rule uses the specified mask when comparing the <first source ip addr>...<last source ip addr> with the source IP address in the IP packet. If no source mask is specified, the mask used is 255.255.255.255.

`-dm <dest ip mask>`

The firewall rule uses the specified mask when comparing the <first dest ip addr>...<last dest ip addr> with the destination IP address in the IP packet. If no destination mask is specified, the mask used is 255.255.255.255.

Specify one of these options to determine when watch messages are sent for this firewall rule. The messages are sent to the console serial port and, if configured, a Syslog server.

`- q | -v`

If `-q` (quiet) is specified, no messages are displayed for this firewall rule, even if the rule causes a packet to be dropped.

If `-v` (verbose) is specified, a message is displayed every time this firewall matches a packet, regardless of the rule action. This is the default setting for firewall *deny* rules.

Specify one of these options to specify the direction of the packet of the packet to which the firewall rule is applied. If no direction parameter is specified, the direction is defaulted to *both*.

`in | out`

Response

Command prompt.

firewall list

Displays the current stateful firewall settings and configured rules. Optional parameters will display only the specified allow or deny rules listing.

Mgmt Class

Security (R/W)

Input Format

```
firewall list [<allow | deny>]
```

Parameters

`allow`	Optional parameter will display only allow rules list.
`deny`	Optional parameter will display only deny rules list.

Examples

Command entered with no parameters.

```
-> firewall list
INFORMATION FOR FIREWALL
   Status.............................. off
   Watch............................... on
   SYNFloodThreshold................... 200
   ICMPFloodThreshold.................. 1000
   UDPFloodThreshold................... 1000
   DropPktThreshold.................... 200

# Begin rules for firewall deny list
   no deny rule available

# End rules for firewall deny list

# Begin rules for firewall allow list
   1. firewall allow -a NNTP -sa 10.0.0.1 -c 0 -q -d in
   2. firewall allow -p TCP -sp 20:21 -c 0 -q -d in
   3. firewall allow -p TCP -sp 23 -c 0 -q -d in
   4. firewall allow -a SMTP -sa 192.168.113.254 -c 0 -q -d in

# End rules for firewall allow list
```

Command entered with the optional *allow* parameter.

```
-> firewall list allow

# Begin rules for firewall allow list
   1. firewall allow -a NNTP -sa 10.0.0.1 -c 0 -q -d in
   2. firewall allow -p TCP -sp 20:21 -c 0 -q -d in
   3. firewall allow -p TCP -sp 23 -c 0 -q -d in
   4. firewall allow -a SMTP -sa 192.168.113.254 -c 0 -q -d in

# End rules for firewall allow list
```

Response

See examples above.

firewall modify

Allows modification of an existing firewall rule.

☞ **NOTE:**
If a firewall rule is modified to deny something that was previously allowed by a firewall allow rule, the change will only apply to subsequent sessions; current sessions will not be effected. When modifying a rule to allow what was previously denied, the changes will be in effect for current sessions.

Mgmt Class

Security (R/W)

Input Format

```
firewall modify <allow | deny> <number> <parameter>
```

Parameters

The following identifies the firewall rule to be modified.

`allow | deny`
Identifies the rules list of which the rule to be modified belongs.

`<number>`[a]
Rule number (of the specified rules list) to be modified.

[a] Integer

The following paragraphs identify the <parameter>s for modification:

`-ac allow | deny`
Changes the action taken on the packet when the rule is matched. Rule will move from one allow | deny rules list to the other list.

`-p <protocol> | tcp | udp | icmp | <protocol number>`[a]
Specifies the protocol a packet must have.

`-a <application> imap | telnet | bootp | nntp | rpc | tftp | smtp | dns | ftp | rexec | rsh | rlogin | syslog | winframe | rdp | http | https | ntp | smb | ras | realaudio | netmeeting | aolim| quicktime | cuseeme | netshow | pptp | nfs | nis | traceroute | sqlnet | ipsec`
Modifies the firewall rule type.

`-sp <ICMP type> | <first source port>[:<last source port>]`
Modifies the source port, specified port range, or ICMP type.

`-dp <ICMP type> | <first dest port>[:<last dest port>]`
Modifies the destination port, specified port range, or ICMP code.

`-sa <first source ip addr>[:<last source ip addr>]`
Modifies the source IP address or specified address range.

`-da <first dest ip addr>[:<last dest ip addr>]`
Modifies the destination IP address or specified address range.

`-sm <source ip mask>`
Modifies the specified source ip mask.

`-dm <dest ip mask>`
Modifies the specified destination ip mask.

`- q | -v`
Modifies the message logging characteristic for the firewall rule.

`-d in | out`
Modifies the specified direction of the rule.

[a] Integer, numerical protocol ID.

Example

Example command changes the allow rule number 7 to a deny rule with no changes to the existing parameters

```
-> firewall modify allow 7 -ac deny
```

Response

Command prompt.

firewall set

Enables or disables the stateful firewall configuration. To view the current firewall status, use the firewall list command.

☞ **NOTE:**
Firewall rules can be added, deleted, or modified regardless of the firewall status.

Mgmt Class

Security (R/W)

Input Format

```
firewall set on | off
```

Parameters

`on`	Enables the firewall as currently configured.
`off`	Disables the firewall.

Response

Command prompt.

firewall setdroppktthreshold

Specifies a threshold value for the number of dropped packets per second (due to a firewall rule). When the threshold value is exceeded, a message will be logged to the console. To view the current threshold value, use the firewall list command.

Mgmt Class

Security (R/W)

Input Format

```
firewall setdroppktthreshold <number>
```

Parameters

<number>[a] Specifies the threshold value in dropped packets per second.

[a] Integer (200)

Example

Example command that sets the threshold to 150 dropped packets per second.

```
-> firewall setdroppkthreshold 150
```

Response

Command prompt.

firewall seticmpfloodthreshold

As a method to prevent a flooding of the system with ICMP requests, use this command set the threshold value for the number of ICMP packets per second. When the specified threshold is exceeded, the firewall will block any subsequent ICMP packets until the ICMP traffic drops below the threshold value. For more information on ICMP flood attacks, see “Stateful Firewall” on page 4-34.

Mgmt Class

Security (R/W)

Input Format

```
firewall seticmpfloodthreshold <number>
```

Parameters

<number>[a] Threshold value in packets per seconds.

[a] Integer (1000)

Response

Command prompt.

firewall setsynfloodthreshold

As a method to prevent a flooding of the system with SYN requests, use this command set the threshold value for the number of SYN packets per second. When the specified threshold is exceeded, the firewall will block any subsequent SYN packets until the SYN traffic drops below the threshold value. For more information on SYN attacks, see “Stateful Firewall” on page 4-34.

Mgmt Class

Security (R/W)

Input Format

```
firewall setsynfloodthreshold <number>
```

Parameters

`<number>`[a] Threshold value in packets per seconds.

[a] Integer (200)

Response

Command prompt.

firewall setudpfloodthreshold

As a method to prevent a flooding of the system with User Datagram Protocol (UDP) packets, use this command set the threshold value for the number of UDP packets per second. When the specified threshold is exceeded, the firewall will block any subsequent UDP packets until the UDP traffic drops below the threshold value. For more information on UDP attacks, see “Stateful Firewall” on page 4-34.

Mgmt Class

Security (R/W)

Input Format

```
firewall setudpfloodthreshold <number>
```

Parameters

`<number>`[a] Threshold value in packets per seconds.

[a] Integer (1000)

Response

Command prompt.

firewall viewdroppkts

Displays a listing of up to 200 of the most recent dropped packets.

Mgmt Class

Security (R/W)

Input Format

```
firewall viewdroppkts <number>
```

Parameters

`<number>`[a] Specifies the number of dropped packets to display.

[a] Integer 1 - 200 (200)

Response

Typical response using the optional <number> parameter.

```
-> firewall viewdroppkts 6

1.  10/17/2001 at 19:01:33:000  (Packet matched a Deny Rule)
Protocol: ICMP  Src Addr: 192.168.1.2 Dest Addr: 1.1.1.1
                ICMP type: 8  ICMP code: 0
2.   10/17/2001 at 19:01:32:000  (Packet matched a Deny Rule)
Protocol: ICMP  Src Addr: 192.168.1.2 Dest Addr: 1.1.1.1
                ICMP type: 8  ICMP code: 0
3.  10/17/2001 at 19:01:31:000  (Packet matched a Deny Rule)
Protocol: ICMP  Src Addr: 192.168.1.2 Dest Addr: 1.1.1.1
                ICMP type: 8  ICMP code: 0
4.  10/17/2001 at 19:00:58:000  (Packet did not match an Allow Rule)
Protocol: TCP  Src Addr: 192.168.1.2 Dest Addr: 1.1.1.1
                Src Port: 1194  Dest Port: 389
5.  10/17/2001 at 19:00:45:000  (Packet did not match an Allow Rule)
Protocol: TCP  Src Addr: 192.168.1.2 Dest Addr: 1.1.1.1
                Src Port: 1194  Dest Port: 389
6.  10/17/2001 at 19:00:39:000  (Packet did not match an Allow Rule)
Protocol: TCP  Src Addr: 192.168.1.2 Dest Addr: 1.1.1.1
                Src Port: 1194  Dest Port: 389
```

firewall watch

Enables or disables the console watch for firewall messages. If the watch is on, a message is printed to the console serial port (and any Syslog Servers) when a packet is dropped or accepted or as specified in the message logging parameter within the firewall rule.

Mgmt Class

Security (R/W)

Input Format

```
firewall watch on | off
```

Parameters

`on`	Messages will be printed to the console and Syslog server (if configured).
`off`	No messages are printed to the console or Syslog server.

Response

Command prompt.

This page intentionally left blank.

CHAPTER 19

SSH COMMANDS

The commands in this section are used to Secure Shell (SSH) connections. For additional information Secure Shell, see SSH in Chapter 5, System Security.

The commands found in this section include:

Table 19-1: SSH Command Listing

Command	Function
ssh ?	List the supported SSH sub-commands.
ssh keygen	Generates the Private-Public key-pair for the local server.
ssh list	Displays the current SSH configuration with the exception of the list of public-private key pairs and the configured SSH port.
ssh load privatekey	Loads a precomputed private-key, from the specified TFTP server.
ssh load publickey	Loads a precomputed public-key, from the specified TFTP server.
ssh set encryption	Sets the type of encryption the SSH connections will use.
ssh set idletimeout	Sets the idle timeout period for SSH connections.
ssh set keepalive	Enables and disables keepalive messages transmission.
ssh set mac	Sets the type of message authentication code use for SSH connections.
ssh set rekey	Sets the interval between key re-exchange.
ssh set status	Enables and disables SSH connections.
system sshport	Manages system SSH port access.

ssh ?

Lists the supported SSH commands. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Security (R)

Input Format

```
ssh ?
```

Parameters

None

Response

Lists the supported SSH commands and a brief description of their functions.

ssh keygen

Generates the Private-Public key-pair for the local server.

Mgmt Class

Security (R/W)

Input Format

```
ssh keygen
```

Parameters

None

Response

A typical response is shown below.

```
-> ssh keygen

SSH KEYGEN has been started...
This runs in the background and can take up to 60 minutes.
There is no progress indication, and you may logoff if desired.
Use "ps" commands to see if SSH_KEYGEN task is still running.
```

ssh list

Displays the current SSH configuration with the exception of the list of host public keys.

Mgmt Class

Security (R)

Input Format

```
ssh list
```

Parameters

None

Response

A typical response is shown below.

```
-> ssh list

   SSH List
-----------------------
   Supported SSH versions: ssh2
   Encryption Set: 3des-cbc
   MAC Set: hmac-md5
   Idle Timeout: 600 seconds.
   D-H Rekey Interval: 60 minutes (0=never rekey)
   KEEPALIVE msg to detect broken connection: ENABLED
   SSH STATUS: ENABLED
```

ssh load privatekey

Loads a precomputed private-key, from the given TFTP server.

☞ **NOTE:**
This command should be use in conjunction with the ssh load publickey command.

Mgmt Class

Security (R/W)

Input Format

```
ssh load publickey tftp@<server-addr>:<priv-key-file>
```

Parameters

`<server-addr>`[a]	IP address of the TFTP server.
`<priv-key-file>`[b]	Key file to load.

[a] Dotted-decimal notation.
[b] ASCII string

Response

A typical response is shown below.

```
-> ssh load privatekey tftp@192.168.13.174:mykey

copying...
copied 882 bytes
```

ssh load publickey

Loads a precomputed public-key, from the given TFTP server.

☞ **NOTE:**
This command should be use in conjunction with the ssh load privatekey command.

Mgmt Class

Security (R/W)

Input Format

```
ssh load publickey TFTP@<server-addr>:<pub-key-file>
```

Parameters

`<server-addr>`[a]	IP address of the TFTP server.
`<pub-key-file>`[b]	Key file to load.

[a] Dotted-decimal notation.
[b] ASCII string

Response

A typical response is shown below.

```
-> ssh load publickey tftp@192.168.13.174:mykey

copying...
copied 751 bytes
```

ssh set encryption

Sets the type(s) of encryption the SSH connections will use.

Mgmt Class

Security (R/W)

Input Format

```
ssh set encryption <type>
```

☞ **NOTE:**
Multiple <types> are allowed on the command line.

Parameters

Select from the following encryption <types>

`des`	DES (56-bit) encryption.
`3des`[a]	3DES (168-bit) encryption
`arc4`	ARC4 encryption
`twofish`	Twofish (128-bit) encryption
`blowfish`	Blowfish encryption

[a] Default value

Response

A typical response is shown below.

```
-> ssh set encryption 3des

SSH Encryption List set to: 3des-cbc
```

ssh set idletimeout

Sets the idle timeout period (time an SSH connection can remain idle) before the SSH session is disconnected.

Mgmt Class

Security (R/W)

Input Format

```
ssh set idletimeout <seconds>
```

Parameters

`seconds`[a] Idle timeout period (in seconds).

[a] Integer, 30 - 1200 (600)

Response

A typical response is shown below.

```
-> ssh set idletimeout 600
SSH Idle Timeout set to 600 seconds
```

ssh set keepalive

Enables and disables keepalive messages transmission. Keepalive messages are sent to detect when the SSH connection has been severed.

Mgmt Class

Security (R/W)

Input Format

```
ssh set keepalive enable | disable
```

Parameters

`enable`[a]	Keepalive messages are sent.
`disable`	Keepalive messages are not sent.

[a] Default value

Response

A typical response is shown below.

```
-> ssh set keepalive enable
SSH Keepalive messages enabled.
```

ssh set mac

Sets the type(s) of message authentication code use for SSH connections.

Mgmt Class

Security (R/W)

Input Format

```
ssh set mac <md5 | sha1>
```

☞ **NOTE:**
Multiple <types> are allowed on the command line .

Parameters

`md5`[a]	Authentication using the Message Digest 5 algorithm.
`sha1`	Authentication using algorithm Secure Hash Algorithm-1.

[a] Default value

Response

A typical response is shown below.

```
-> ssh set mac md5
SSH MAC List set to: hmac-md5
```

ssh set rekey

Specifies the interval at which additional key exchanges will be performed.

Mgmt Class

Security (R/W)

Input Format

```
ssh set rekeyinterval <interval>
```

Parameters

`<interval>`[a]	Interval in minutes. Entering a zero "*0*" for this value will disable re-key requests.

[a] Integer, 0 - 600 (60).

Response

A typical response is shown below.

```
-> ssh set rekey interval 50

SSH Rekey Interval set to 50 minutes
```

ssh set status

Enables and disables SSH server connections.

Mgmt Class

Security (R/W)

Input Format

```
ssh set status <enable | disable>
```

Parameters

`enable`[a]	Allows SSH connections.
`disable`	Disallows SSH connections.

[a] Default value

Response

A typical response is shown below.

```
-> ssh set status enable

SSH Enabled. Connections now permitted.
```

system sshport

Specifies the port that the SSH server listens on.

Mgmt Class

Security (R/W)

Input Format

```
system sshport <port>
```

Parameters

`default`	Restores the SSH port value to the default value 22 and re-enables the port.
`disable`	Disables the existing SSH port.
`<port>`[a]	Defines a new SNMP port number. Use this option to restrict remote access.

[a] Integer, 1 - 65525 (22)

Examples

This command sets the SSH port to the default value (22)

```
-> system sshport default
```

This command disables the existing SNMP port.

```
-> system sshport disabled
```

This command remaps the SSH port to port 1320.

```
-> system sshport 1320
```

This page intentionally left blank.

CHAPTER 20

QOS COMMANDS

The commands in this section are used to manage the Quality of Service (QoS); a key-enabled feature. For additional information on QoS, see the Technical Reference Manual.

The commands found in this section include:

Table 20-1: QoS Command Listing

Command	Function
qos ?	List the supported QoS commands and a brief description of their functions.
qos append	Creates a new QoS policy name and appends it to the end QoS policies list.
qos del	Deletes a single or all existing QoS policies.
qos diffserv	Enables and disables marking of the differentiated services field.
qos disable	Deletes an existing IPSec policy.
qos enable	Disables an IPSec policy.
qos insert	Creates a new QoS policy name and inserts it into a specified location in the QoS policies list.
qos list	Displays QoS queue parameters and all user-configured QoS policies.
qos move	Moves an existing QoS policy to a specified location in the QoS policies list.
qos movetoend	Moves an existing QoS policy to the end of the policies list.
qos off	Disables the QoS feature.
qos on	Enables the QoS feature.

Table 20-1: QoS Command Listing (Cont.)

Command	Function
qos save	Saves the current QoS configuration and QoS policies.
qos set	Defines the pfs filtering parameter value for the policy.
qos setweight	Defines a proposal filtering parameter value for the policy.

qos ?

Provides a list of the supported QoS commands. To see the syntax for a command, enter the command followed by a ?.

Mgmt Class

Network (R)

Input Format

```
qos ?
```

Parameters

None

Response

Lists the supported QoS commands and a brief description of their functions.

qos append

Creates a new QoS policy name and appends it to the end QoS policies list. To view the existing QoS policy names, use the qos list command.

☞ **NOTE:**

QOS policies are numbered sequentially with the initial policy number of 1. Additional policies numbers are created incrementing the last policy number by one.

Mgmt Class

Network (R/W)

Input Format

```
qos append <policy name>
```

Parameters

`<policy name>`[a]	Specifies the QoS policy name to be added.

[a] ASCII string, policy name is case-sensitive.

Example

Example command will add new policy *mypolicy1* to the end of the QoS policies list.

```
-> qos append mypolicy1
```

Response

Command prompt.

qos del

Deletes a single or all existing QoS policies. To view the existing QoS policy numbers, use the qos list command.

☞ **NOTE:**
A QoS policy that is currently enabled cannot be deleted until it is disabled with the qos disable command.

Mgmt Class

Network (R/W)

Input Format

```
qos del <policy name> | all
```

Parameters

`<policy name>`[a]	Specifies the QoS policy to be deleted.
`all`	Specifies that all (disabled) QoS policies will be deleted.

[a] ASCII string, policy name is case-sensitive.

Example

Example command that deletes all disabled QoS policies.

```
-> qos del all
```

Response

Command prompt.

qos diffserv

Enables and disables marking of the Differentiated Services (DiffServ) field of the IP header.

Mgmt Class

Network (R/W)

Input Format

```
qos diffserv <on | off>
```

Parameters

`on`	QOS will mark Diffserv field in IP header.
`off`	No QOS Diffserv marking will be performed.

Response

Command prompt.

qos disable

Disables an existing QoS policy. To view the existing QoS policies, use the qos list command.

☞ **NOTE:**
A QoS policy must be disabled before it can be modified or deleted.

Mgmt Class

network (R/W)

Input Format

```
qos disable <policy name>
```

Parameters

`<policy name>`[a] Specifies the QoS policy to be disabled.

[a] ASCII string, policy name is case-sensitive.

Response

Command prompt.

qos enable

Enables an existing QoS policy. To view the existing QoS policies and their status, use the qos list command.

Mgmt Class

Network (R/W)

Input Format

```
qos enable <policy name>
```

Parameters

`<policy name>`[a] Specifies the QoS policy to be enabled.

[a] ASCII string, policy name is case-sensitive.

Response

Command prompt.

qos insert

Creates a new QoS policy name and inserts it into a specified location in the QoS policies list. To view the existing QoS policy list, use the qos list command.

Mgmt Class

Security (R/W)

Input Format

```
qos del <policy name> <insert before this policy>
```

Parameters

`<policy name>`[a]	Specifies the QoS policy to be deleted.
`<insert before this policy>`[a]	Specifies the new QoS policy location.The policy being inserted will immediately proceed the specified policy in the QoS policy list.

[a] ASCII string, policy name is case-sensitive.

Example

Example command adds the QoS policy *mypolicya* in the policies list immediately before *mypolicy2*.

```
-> qos insert mypolicya mypolicy2
```

Response

Command prompt.

qos list

Displays QoS queue parameters and all user-configured QoS policies. For more information on QoS, see the Technical Reference Manual.

Mgmt Class

Network (R)

Input Format

```
qos list [<policy name>]
```

Parameters

<policy name>[a]	Optional parameter that will display only the specified policy name.

[a] ASCII string, policy name is case-sensitive

Example

Example command using the optional <policy name> parameter to display only *mypolicy3* configuration information.

```
-> qos list mypolicy3

QoS: On
   DiffServ: On
   Queue     Priority     Code-Point     Weight
      0       HIGH             0x4       10
      1       MEDIUM           0x3       10
      2       NORMAL           0x2       10
      3       LOW              0x1       10
Number of policies : 5
QOS INFORMATION FOR <mypolicy3>
   Status.............................Enabled Active
   Policy number .....................4
   Policy hit count ..................0
   Source IP .........................Not Specified
   Destination IP ....................Not Specified
   Source Port........................181
   Destination Port...................181
   Bi-Directional.....................ON
   Incoming CodePoint.................2
   Protocol...........................TCP
   Outgoing CodePoint.................1
   Queue Priority.....................LOW
   Scheduling.........................Always on
```

Response

See example above.

qos move

Moves an existing QoS policy within the policies list. To view the existing QoS policy order, use the qos list command.

Mgmt Class

Network (R/W)

Input Format

```
qos move <policy name> <move to before this policy>
```

Parameters

`<policy name>`[a]	Specifies the QoS policy to be moved.
`<move to before this policy>`[a]	Specifies the QoS policy location. The policy being moved will immediately proceed the specified policy in the QoS policy list.

[a] ASCII string

Example

Example command moves the QoS policy *mypolicy3* to the location immediately before *mypolicy4* in the QoS policies list.

```
-> qos insert mypolicy3 mypolicy4
```

Response

Command prompt.

qos movetoend

Moves an existing QoS policy to the end of the policies list. To display the current QoS policies, use the qos list command.

Mgmt Class

Network (R/W)

Input Format

```
qos movetoend <policy name>
```

Parameters

`<policy name>`[a]	Specifies the policy to be moved to the end of the QoS policies list.

[a] ASCII string, policy name is case-sensitive.

Response

Command prompt.

qos off

Disables the QOS feature. To view the current QoS status, use the qos list command.

Mgmt Class

Network (R/W)

Input Format

```
qos off
```

Parameters

None

Response

Command prompt.

qos on

Enables the QOS feature as currently configured. To view the current QoS status, use the qos list command.

☞ **NOTE:**

QoS policies that are currently *disabled* will not be active.

Mgmt Class

Network (R/W)

Input Format

```
qos on
```

Parameters

None

Response

Command prompt.

qos save

Saves the current QoS feature and policy configurations.

Mgmt Class

Network (R/W)

Input Format

```
qos save
```

Parameters

None

Response

Command prompt.

qos set

Defines one or more parameters of a QoS policy. To view the current configuration of a policy, use the qos list <policy name> command.

☞ **NOTE:**

The QoS policy must exist (created with the qos append or qos insert commands) and be *disabled* prior to configuration.

Mgmt Class

Network (R/W)

Input Format

```
qos set [<parameter>] <policy name>
```

Parameters

Multiple parameters can be entered in the same command for a single QoS policy; the sequence of parameters in not essential. The parameters are listed below.

`-sa <source address>`[a] `off | <start address>[:end address>]`

Specifies the source address or range of addresses. *Off* will disable source-address checking.

`-da <destination address>`[a] `off | <start address>[:<end address>]`

Specifies the destination address or range of addresses. *Off* will disable destination-address checking.

`-p <protocol> off | <protocol number>`[b] `tcp | udp`

Specifies the protocol by protocol number or explicitly *TCP* or *UDP*. Entering *off* will disable the protocol check.

`-sp <source port>`[c] `off | <start port number>[:<end port number>]`

Specifies the source port or range of ports by number or specific application. *Off* disables the port check.

```
-dp <destination port> off | <start port number>[:<end port number>]
off | ftp | telnet | smtp | http | snmp |tftp | dns | login | rsh |
h323 | t120
```

Specifies the destination port or range of ports by number or specific application. *Off* disables the port check.

`-pr <priority> high | medium | normal | low`

Specifies the priority, with *normal* the default value.

`-ic <incoming code point> off | <code point>`

Specifies the incoming code point.

`-oc <outgoing code point>`[d] `off | <code point>`

Specifies the outgoing code point.

`-b <bi-directional> on | off`

`-st <start time> <hh:mm>`[e]

Specifies the time of day when the specified policy becomes active.

`-du <duration> <hh:mm>`[e]

Specifies the active time period for the policy.

`-r <repetition> off | <once<mm/dd/yy>> | <everyday | mon | tue | wed | thu | fri | sat | sun>`

Specifies the policy as a one-time, repeating, or always-on policy. Default value is *off*.

`<policy name>`[f]

Specifies the policy to which the configuration changes will be applied.

[a] Dotted-decimal notation
[b] Integer, 1 - 255
[c] Integer, 1 - 65535
[d] Hex or decimal notation
[e] Integer, 0 - 60 (requires entering of 2 characters per hh:mm)
[f] ASCII string, policy name is case-sensitive.

Response

Command prompt.

qos setweight

Configures the weighted fair queue that manages bandwidth based on traffic priority. For more information on bandwidth management, see the Technical Reference Manual.

Mgmt Class

Network (R/W)

Input Format

```
qos setweight <high|meduim|normal|low> <weight>
```

Parameters

Select one of the following:
`high`
`medium`
`normal`
`low`
	Specifies the priority level queue to configure.

`<weight>`[a]	Sets the desired minimum bandwidth allocated to the selected queue.

[a] Integer

Response

Command prompt.

This page intentionally left blank.

CHAPTER 21

SWITCH COMMANDS

This section contains Switch command descriptions. These commands are used for Ethernet switch management and include:

Table 21-1: Switch Command Listing

Command	Function
switch ?	Lists the supported Switch sub-commands.
switch agetime	Specifies the aging time of the switch.
switch block	Disables the specified Ethernet port.
switch mirror	Configures port traffic mirroring.
switch status	Displays the current port states for the Ethernet switch.
switch unblock	Enables a blocked Ethernet port.

switch ?

Lists the supported Switch commands and keywords. To see the syntax for a command, enter the command followed by a *?* or *help*.

Mgmt Class

Network (R)

Input Format

```
switch ? | help
```

Parameters

None

Response

Lists the supported Switch commands and a brief description of their function.

switch agetime

Specifies the aging time of the switch. When age time expires the port-MAC address entry will be removed from the table containing this information.

Mgmt Class

Network (R/W)

Input Format

```
switch agetime <seconds>
```

Parameters

`***`	When the command is entered with no parameter, the current age time value displayed. If no age time has been specified, the valid range is displayed.
`<seconds>`[1]	Specifies the switch aging time. Aging time can be disabled by entering a value of *'0'*.

[1] Integer, 10-1,000,000 (300)

Response

Command prompt.

switch block

Disables the specified Ethernet Port. The port can be re-enabled with the switch unblock command.

Mgmt Class

Network (R/W)

Input Format

```
switch block <port>
```

Parameters

<port>[1]	Ethernet port to be disabled.

[1] Integer

Response

```
-> switch block 7
Port 7 is disabled
```

switch mirror

Configures port traffic mirroring. Switch mirroring allows traffic from an Ethernet port(s) to be mirrored to another Ethernet port. Switch mirroring is disabled by default.

☞ **NOTE:**
Port 9 is the uplink of the switch to the WAN/router.

Mgmt Class

Network (R/W)

Input Format

```
switch mirror [on | off | capture <port> | map <port>| unmap
<port>]
```

Parameters

`***`	When entered with no parameters, the current port mirroring state information is displayed; see Response below.
`on`	Enables port mirroring function. If no additional parameters are supplied, the current mirroring configuration is used.
`off`	Disables port mirroring function. Mirror settings are not changed.
`capture <port>`[1]	Specifies the port that will capture traffic from the mirrored port.[2]
`map <port>`[1]	Specifies the port that will to be mirrored. Multiple ports can be mapped to the capture port.
`unmap <port>`[1]	Un-maps the specified port.

[1] Integer
[2] When a capture <port> parameter is specified on the command line, port mirroring is auto-enabled.

Example

The following example will enable port mirroring; traffic from ports 3 and 4 will be mirrored to the capture port 6:

```
-> switch mirror capture 6
-> switch mirror map 3
-> switch mirror map 4
```

Response

When the command is entered with parameters, a command prompt is returned.

```
-> switch mirror capture 3
->
```

Response when the command is entered with no parameters and port mirroring is currently disabled:

```
-> switch mirror
Port mirroring is disabled
```

Typical response when entered with no parameters and port mirroring is currently enabled:

```
-> switch mirror
Port mirroring is enabled:
Port 1: Mirrored Port
Port 2: Capture Port
Port 3: Not Mirrored
Port 4: Not Mirrored
Port 5: Not Mirrored
Port 6: Not Mirrored
Port 7: Not Mirrored
Port 8: Not Mirrored
Port 9: Not Mirrored
```

switch status

Displays the current port states for the Ethernet switch.

Mgmt Class

Network (R)

Input Format

```
switch status
```

Parameters

None

Response

Typical response:

```
-> switch status
Port 1 status: No Connection, 10Mb/s , Half Duplex, Enabled
Port 2 status: No Connection, 10Mb/s , Half Duplex, Enabled
Port 3 status: No Connection, 10Mb/s , Half Duplex, Disabled
Port 4 status: Connected    , 100Mb/s, Full Duplex, Enabled
Port 5 status: Connected    , 10Mb/s,  Half Duplex, Enabled
Port 6 status: Connected    , 100Mb/s, Full Duplex, Enabled
Port 7 status: Connected    , 100Mb/s, Full Duplex, Enabled
Port 8 status: Connected    , 100Mb/s, Full Duplex, Disabled
Port 9 status: Connected    , 100Mb/s, Full Duplex, Enabled
```

switch unblock

Re-enables a disabled Ethernet Port. Ethernet ports are disabled with the switch block command.

Mgmt Class

Network (R/W)

Input Format

```
switch unblock <port>
```

Parameters

<port>[1]	Ethernet port to be enabled.

[1] Integer

Response

```
-> switch unblock 3
Port 3 is enabled
```