Netopia® Software User Guide

Version 7.6

netopia®

BROADBAND WITHOUT BOUNDARIES®

Netopia® 2200 Series Gateways

July 2006

Copyright

V 7.6-BS-RBAN

Netopia, Inc. Part Number: 6161233-00-01

Table of Contents

CHAPTER 1 Introduction

About Netopia Documentation

NOTE:

This guide describes the wide variety of features and functionality of the Netopia Gateway, when used in Router mode. The Netopia Gateway may also be delivered in Bridge mode. In Bridge mode, the Gateway acts as a pass-through device and allows the workstations on your LAN to have public addresses directly on the Internet.

Netopia, Inc. provides a suite of technical information for its 2200-series family of intelligent enterprise and consumer Gateways. It consists of:

- *Software User Guide*
- Dedicated Quickstart guides
- Specific White Papers

The documents are available in electronic form as Portable Document Format (PDF) files. They are viewed (and printed) from Adobe Acrobat Reader, Exchange, or any other application that supports PDF files.

They are downloadable from Netopia's website:
http://www.netopia.com/

Intended Audience

This guide is targeted primarily to residential service subscribers.

Expert Mode sections may also be of use to the support staffs of broadband service providers and advanced residential service subscribers.

See “Expert Mode” on page 35.

Documentation Conventions

General

This manual uses the following conventions to present information:

Convention (Typeface)	Description
bold italic monospaced	Menu commands
bold italic sans serif	Web GUI page links and button names
`terminal`	Computer display text
`bold terminal`	User-entered text
Italic	Italic type indicates the complete titles of manuals.

Internal Web Interface

Convention (Graphics)	Description
blue rectangle or line	Denotes an “excerpt” from a Web page or the visual truncation of a Web page
solid rounded rectangle with an arrow	Denotes an area of emphasis on a Web page

Command Line Interface

Syntax conventions for the Netopia Gateway command line interface are as follows:

Convention	Description
straight ([ ]) brackets in cmd line	Optional command arguments
curly ({ }) brackets, with values separated with vertical bars (|).	Alternative values for an argument are presented in curly ({ }) brackets, with values separated with vertical bars (|).
bold terminal type face	User-entered text
italic terminal type face	Variables for which you supply your own values

Organization

This guide consists of eight chapters, including a glossary, and an index. It is organized as follows:

- **Chapter 1, "Introduction"** — Describes the Netopia document suite, the purpose of, the audience for, and structure of this guide. It gives a table of conventions.
- **Chapter 2, "Basic Mode Setup"** — Describes how to get up and running with your Netopia Gateway.
- **Chapter 3, "Expert Mode"** — Focuses on the "Expert Mode" Web-based user interface for advanced users. It is organized in the same way as the Web UI is organized. As you go through each section, functions and procedures are discussed in detail.
- **Chapter 4, "Basic Troubleshooting"** — Gives some simple suggestions for troubleshooting problems with your Gateway's initial configuration.
- **Chapter 5, "Command Line Interface"** — Describes all the current text-based commands for both the SHELL and CONFIG modes. A summary table and individual command examples for each mode is provided.
- **Chapter 6, "Glossary"**
- **Chapter 7, "Technical Specifications and Safety Information"**
- **Index**

A Word About Example Screens

This manual contains many example screen illustrations. Since Netopia 2200 Series Gateways offer a wide variety of features and functionality, the example screens shown may not appear exactly the same for your particular Gateway or setup as they appear in this manual. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.

CHAPTER 2 Basic Mode Setup

Most users will find that the basic Quickstart configuration is all that they ever need to use. This section may be all that you ever need to configure and use your Netopia Gateway. The following instructions cover installation in *Router Mode*.

This section covers:

Important Safety Instructions

POWER SUPPLY INSTALLATION

Connect the power supply cord to the power jack on the Netopia Gateway. Plug the power supply into an appropriate electrical outlet.

CAUTION:

Depending on the power supply provided with the product, either the direct plug-in power supply blades, power supply cord plug or the appliance coupler serves as the mains power disconnect. It is important that the direct plug-in power supply, socket-outlet or appliance coupler be located so it is readily accessible.
CAUTION (North America Only): For use only with a CSA Certified or UL Listed Limited Power Source or Class 2 power supply, rated 12Vdc.
(Sweden) Apparaten skall anslutas till jordat uttag när den ansluts till ett nätverk
(Norway) Apparatet må kun tilkoples jordet stikkontakt.
USB-powered models: For Use with Listed I.T.E. Only

TELECOMMUNICATION INSTALLATION

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

SAVE THESE INSTRUCTIONS

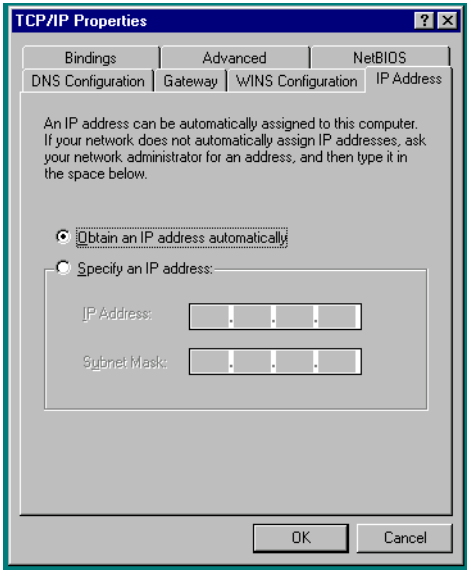
Set up the Netopia Gateway

Refer to your *Quickstart Guide* for instructions on how to connect your Netopia gateway to your power source, PC or local area network, and your Internet access point, whether it is a dedicated DSL outlet or a DSL or cable modem. Different Netopia Gateway models are supplied for any of these connections. Be sure to enable Dynamic Addressing on your PC. Perform the following:

Microsoft Windows:

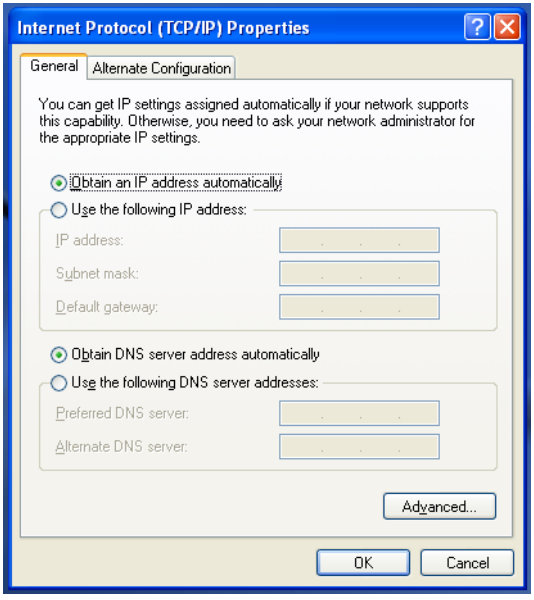
Step 1. Navigate to the TCP/IP Properties Control Panel.

a. Some Windows versions follow a path like this:	***Start*** menu -> ***Settings*** -> ***Control Panel*** -> ***Network*** (or ***Network and Dial-up Connections*** -> ***Local Area Connection*** -> ***Properties***) -> ***TCP/IP [your_network_card]*** or ***Internet Protocol [TCP/IP]*** -> ***Properties***



b. Some Windows versions follow a path like this:

Start menu -> ***Control Panel*** -> ***Network and Internet Connections*** -> ***Network Connections*** -> ***Local Area Connection*** -> ***Properties*** -> ***Internet Protocol [TCP/IP]*** -> ***Properties***



Then go to Step 2.

Step 2. Select *Obtain an IP address automatically.*

Step 3. Select *Obtain DNS server address automatically*, if available.

Step 4. Remove any previously configured Gateways, if available.

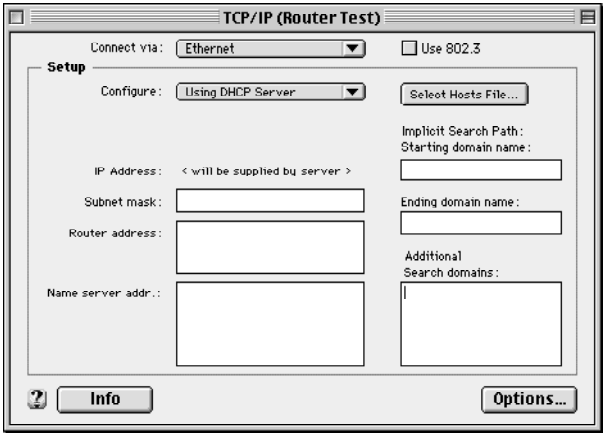
Step 5. OK the settings. Restart if prompted.

Macintosh MacOS 8 or higher or Mac OS X:

Step 1. Access the TCP/IP or Network control panel.

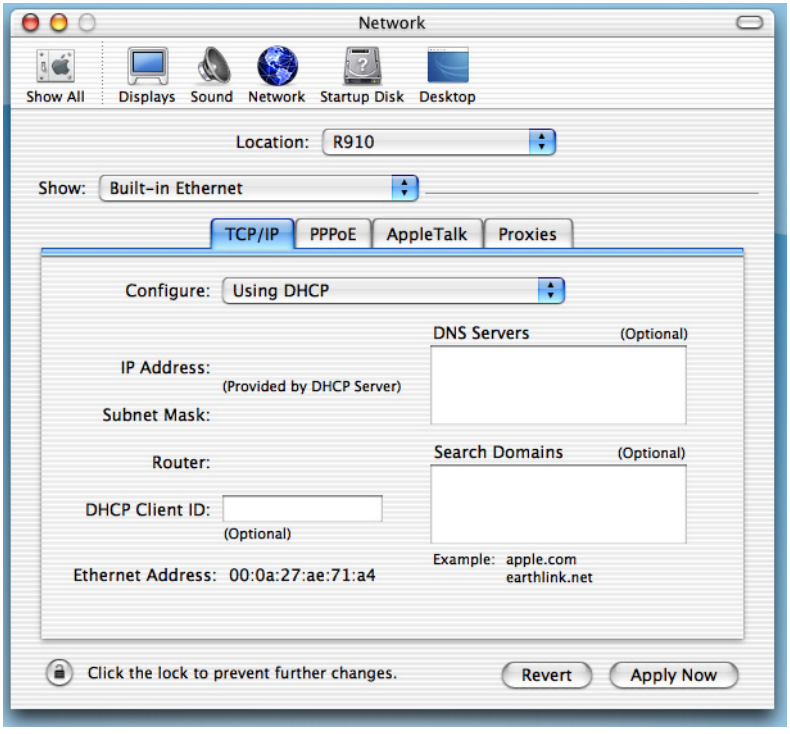
a. MacOS follows a path like this:

Apple Menu -> ***Control Panels*** -> ***TCP/IP*** Control Panel



b. Mac OS X follows a path like this:

Apple Menu -> ***System Preferences*** -> ***Network***



Then go to Step 2.

Step 2. Select *Built-in Ethernet*

Step 3. Select *Configure Using DHCP*

Step 4. Close and Save, if prompted.

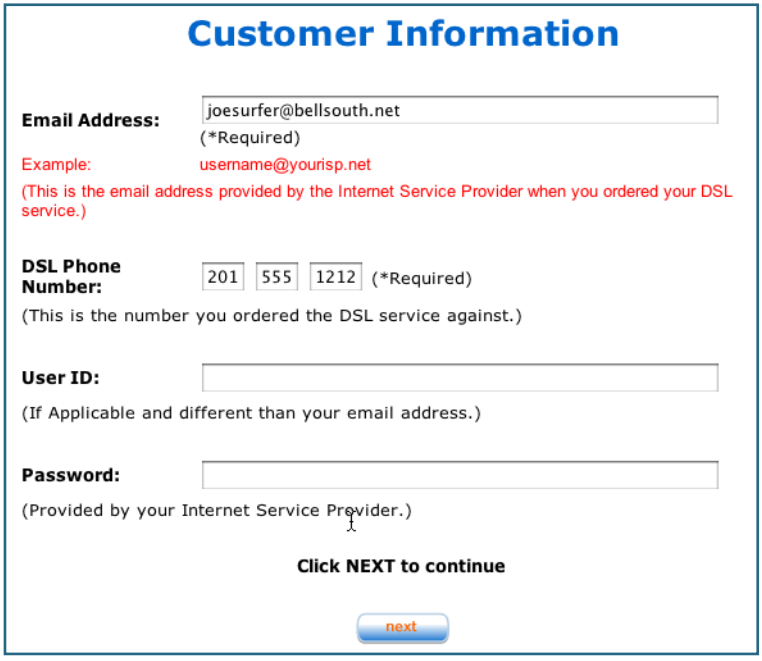
Proceed to "Quick Start" on page 17.

Quick Start

1. **Run your Web browser application, such as Firefox or Microsoft Internet Explorer, from the computer connected to the Netopia Gateway.**

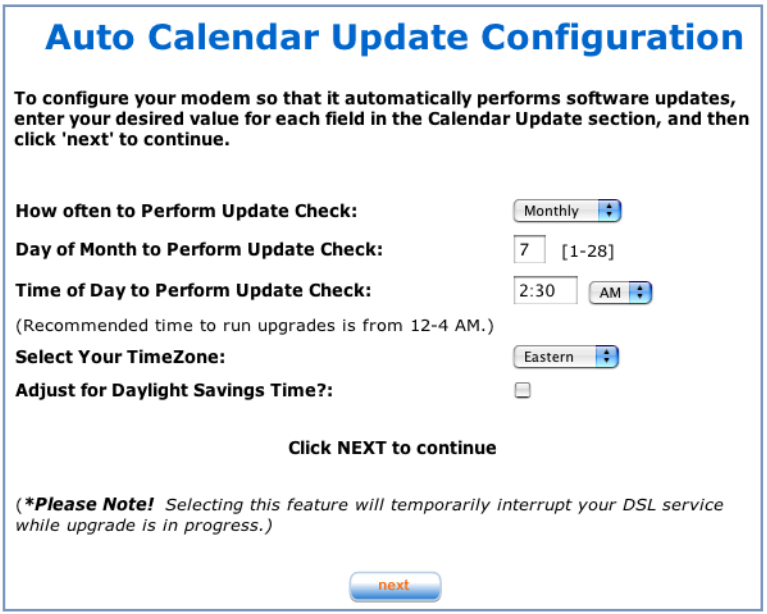
   Enter ***http://192.168.1.254*** in the Location text box.

   The **Customer Information** page appears.



2. **Enter the requested information and the User ID and Password supplied by your Internet Service Provider. Click the *next* button.**

The **Auto Calendar Update Configuration** page appears.



Your Netopia Gateway can automatically update itself. Choose a schedule when you would like it to perform updates. Click the ***next*** button.

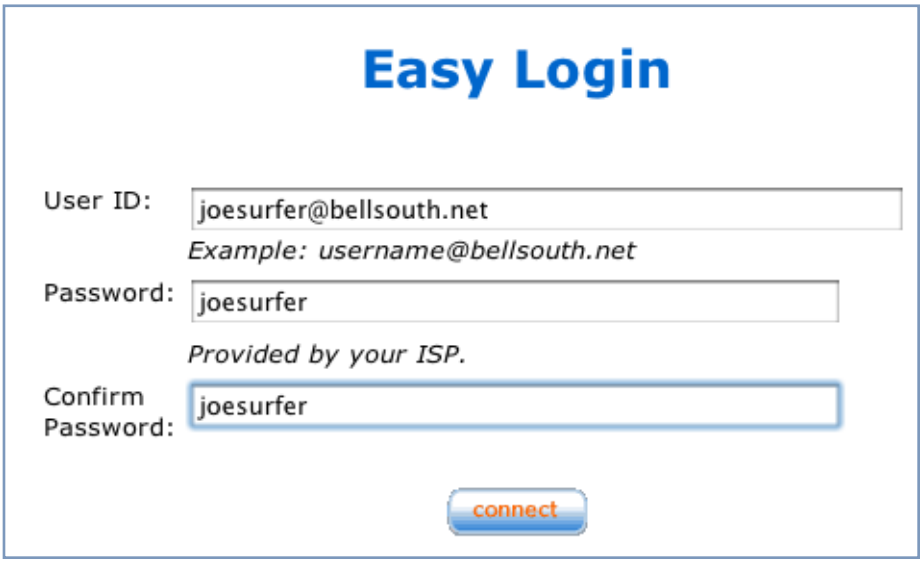
3. **Your browser will display a success message.**

Check to make sure the Internet LED is lit **GREEN** to verify that the connection to the Internet is active. At this point, you can close your browser window and re-open it.

NOTE:

If the device detects a problem with your connection or is unable to establish communication, it will display the **Diagnostics** page with some helpful information. You can also choose to ***run full diagnostics*** to help pinpoint the problem. This information is useful for communicating with the help desk.

The Easy Login page appears.



4. **Enter the User ID and Password supplied by your Internet Service Provider.**

   Once you enter your User ID and Password here, you will no longer need to enter them whenever you access the Internet. The Netopia Gateway stores this information and automatically connects you to the Internet.

5. **Click the *connect* button.**

   Your browser will display a success message.

You can now click the ***here*** link to go to the BellSouth home page.

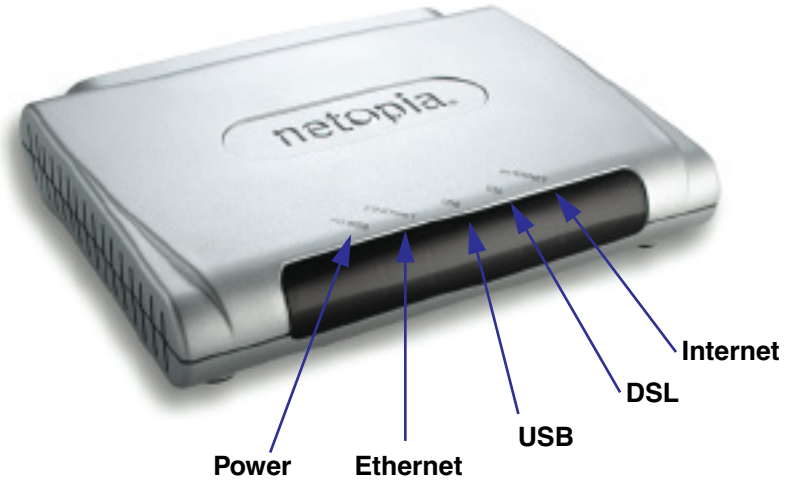
6. **Congratulations! Your installation is complete.**

   You can now surf to your favorite Web sites by typing an URL in your browser's location box or by selecting one of your favorite Internet bookmarks.

Netopia Gateway Status Indicator Lights

Colored LEDs on your Netopia Gateway indicate the status of various port activity.

Netopia Gateway 2241N status indicator lights



LED	Action
Power	**Green** when power is on.
Ethernet	Solid **green** when connected. Flash **green** when there is activity on the LAN.
USB	Flashes **green** when there is activity on the USB port.
DSL	Solid **green** when Internet connection is established.
Internet	Solid **green** when Broadband device is connected. Flashes **green** for activity on the WAN port.

home

(Basic mode)

After you have performed the basic Quickstart configuration, any time you log in to your Netopia Gateway you will access the Netopia Gateway Home Page.

You access the Home Page by typing ***http://192.168.1.254*** in your Web browser's location box.

The Basic Mode Home Page appears.

The Home Page displays the following information in the center section:

Item	Description
Serial Number	This is the unique serial number of your Gateway.
Software Release	This is the version number of the current embedded software in your Gateway.
Warranty Date	This is the date that your Gateway was installed and enabled.
Status of DSL	DSL connection (Internet) is either ***Up*** or ***Down***
Status of Connection	'Waiting for DSL' is displayed while the Gateway is training. This should change to 'Up' within two minutes. 'Up' is displayed when the ADSL line is synched and the PPPoE session is established. 'Down' indicates inability to establish a connection; possible line failure.
Local WAN IP Address	This is the negotiated address of the Gateway's WAN interface. This address is usually dynamically assigned.
Remote Gateway Address	This is the negotiated address of the remote router to which this Gateway is connected.
Primary DNS Secondary DNS	These are the negotiated DNS addresses.
ISP Username	This is your PPPoE username as assigned by your service provider.
Ethernet Status	(if so equipped) Local Area Network (Ethernet) is either ***Up*** or ***Down***
USB Status	If your Gateway is so equipped, Local Area Network (USB) is either ***Up*** or ***Down***
Date & Time	This is the current UTC time; blank if this is not available due to lack of a network connection.

button bar

The button bar is the blue bar at the left side of the page containing the major navigation buttons. These buttons are available from every page, allowing you to move freely about the site.

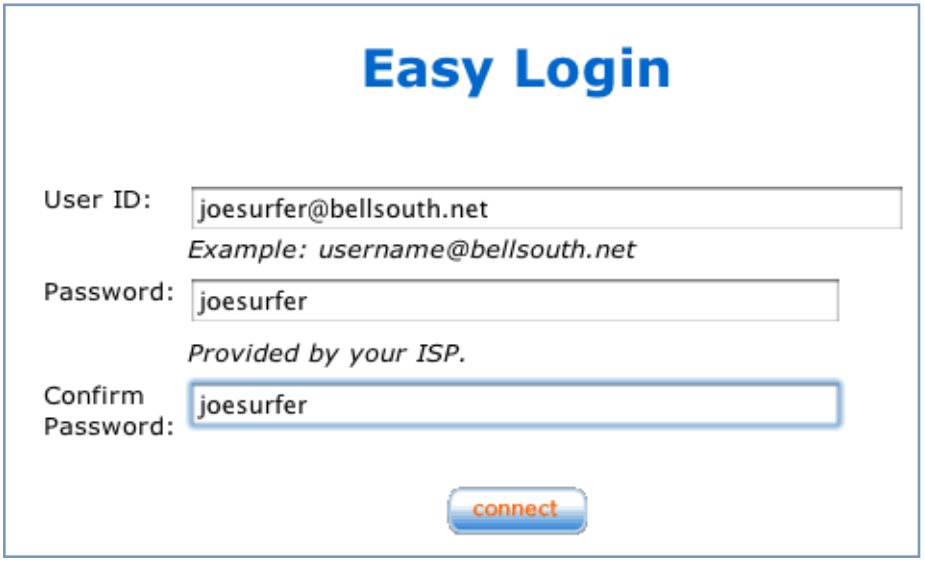
The buttons in the left-hand column on this page allow you to manage or configure several features of your Gateway. Each link is described in its own section.

Click the links below to be taken to each section.

- See “easy login” on page 26
- See “home” on page 23
- See “diagnostics” on page 27
- See “update device” on page 29
- See “reset device” on page 31
- See “self test” on page 32
- See “expert mode” on page 33

Button: easy login

When you click the ***easy login*** button the **Easy Login** page appears.

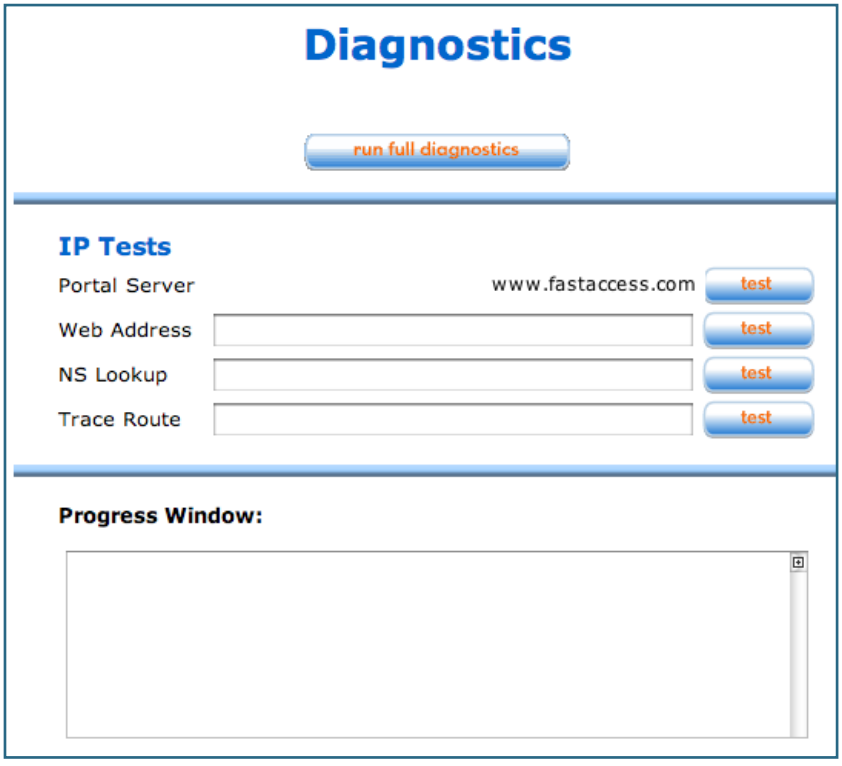


If you need to re-login to your Internet account, or if your User ID or Password changes, use this page to enter your authentication information.

Click the ***connect*** button.

Button: diagnostics

This automated multi-layer test examines the functionality of the Router from the physical connections to the data traffic being sent by users through the Router.



- **Portal Server** - tests the connection to a predefined server on the Internet.
- **Web Address** - tests the connection to a specified URL or IP address.
- **NS Lookup** - converts a domain name to its IP address and vice versa.
- **TraceRoute** - displays the path to a destination by showing the number of hops and the router addresses of these hops.

You enter a web address URL or an IP address in the respective field and click the ***test*** button.

Results will be displayed in the **Progress Window** as they are generated.

This sequence of tests takes approximately one minute to generate results. Please wait for the test to run to completion.

Each test generates one of the following result codes:

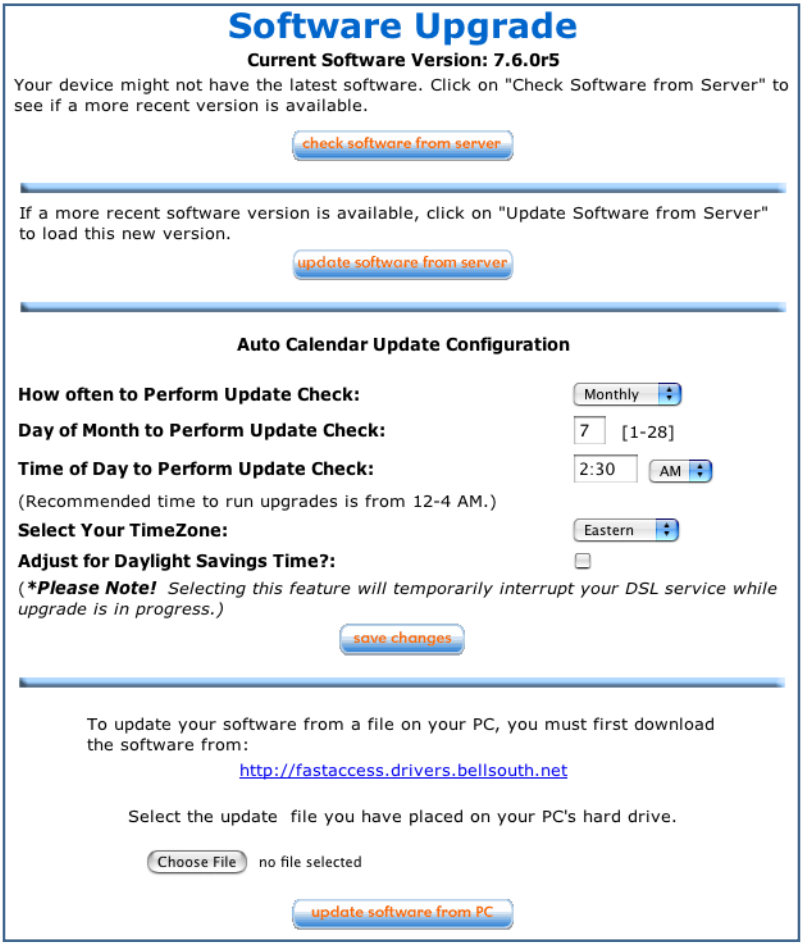
Result	Meaning
* PASS:	The test was successful.
* FAIL:	The test was unsuccessful.
* SKIPPED:	The test was skipped because a test on which it depended failed.
* PENDING:	The test timed out without producing a result. Try running Diagnostics again.
* WARNING:	The test was unsuccessful. The Service Provider equipment your Router connects to may not support this test.

You can run all the tests in order by clicking the ***run full diagnostics*** button.

Button: update device

Periodically, the embedded firmware in your Gateway may be updated to improve the operation or add new features. Your Gateway includes its own onboard installation capability. Your service provider may inform you when new firmware is available, or you can check for yourself.

Click the ***update device*** button. The Software Upgrade page appears.



Operating System Software is what makes your Router run and occasionally it needs to be updated. Your **Current Software Version** is displayed at the top of the page.

If you want to check for an updated version without installing it, click the ***check software from server*** button.

• Auto Calendar Update Configuration

You can schedule your Router to check for updates automatically, by setting the Auto Calendar schedule. Set your options and click the ***save changes*** button.

You can update your software in either of two ways:

• From a Server

- If an updated version exists, click the ***update software from server*** button, and a new version will automatically be downloaded to your Router.
- When the download and installation is complete, you will be prompted to restart the router.

• From your PC

To update your software from a file on your PC, you must first download the software from the website linked to the URL on this page. Once you have downloaded the software file to your PC:

1. **Browse your computer for the operating system file you downloaded.**
2. **Click the *update software from PC* button.**
3. **The install may take a few minutes; wait for it to complete.**
4. **Restart your Router and your new operating system will be running.**

Button: reset device

In some cases, you may need to clear all the configuration settings and start over again to program the Netopia Gateway. You can perform a factory reset to do this.

Click the ***reset device*** button to reset the Gateway back to its original factory default settings. You will be prompted to make sure you want to do this.

Click the ***yes, reset to factory settings*** button, if you want to proceed.

NOTE:

Exercise caution before performing a Factory Reset. This will erase any configuration changes that you may have made and allow you to reprogram your Gateway.

Button: self test

You can perform a self-test of your Router to be sure all systems are functioning.

When you click the ***self test*** button, the device tests itself and the Device Self Test page appears.

The device self test verifies the following device functionality:

- Memory.
- Ethernet connection.
- Configuration.
- DSL hardware (if supported).
- Wireless hardware (if supported).

If your device fails, contact your Service Provider.

Button: *expert mode*

Most users will find that the basic Quickstart configuration is all that they ever need to use. Some users, however, may want to do more advanced configuration. The Netopia Gateway has many advanced features that can be accessed and configured through the Expert Mode pages.

Click the ***expert mode*** button to display the Expert Mode Confirmation page.

You should carefully consider any configuration changes you want to make, and be sure that your service provider supports them.

Once you click the ***yes, enter expert mode*** button you will be taken to the Expert Mode Home Page.

The Expert Mode Home Page is the main access point for configuring and managing the advanced features of your Gateway. See “Expert Mode” on page 35 for information.

CHAPTER 3 Expert Mode

Using the Expert Mode Web-based user interface for the Netopia 2200-series Gateway you can configure, troubleshoot, and monitor the status of your Gateway.

Access the Expert Web Interface

Open the Web Connection

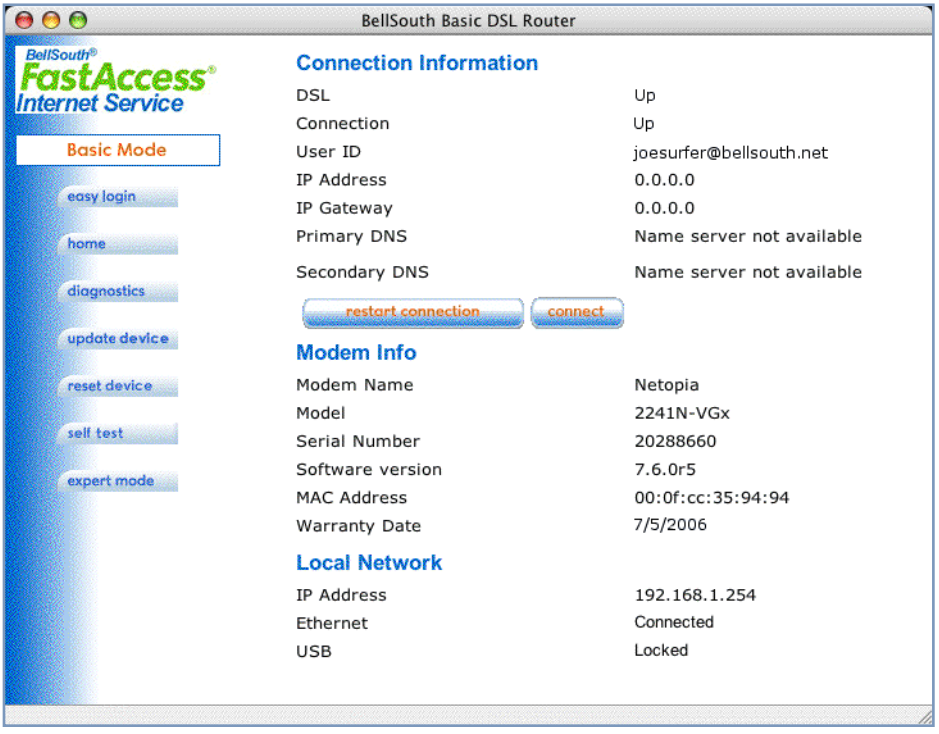
Once your Gateway is powered up, you can use any recent version of the best-known web browsers such as Netscape Navigator or Microsoft Internet Explorer from any LAN-attached PC or workstation. The procedure is:

1. **Enter the name or IP address of your Netopia Gateway in the Web browser's window and press Return.**

   For example, you would enter ***http://192.168.1.254***.

2. **If an administrator or user password has been assigned to the Netopia Gateway, enter *Admin* or *User* as the username and the appropriate password and click *OK*.**

The Basic Mode Home Page opens.



3. **Click the *expert mode* button in the left-hand column.**

You are challenged to confirm your choice.

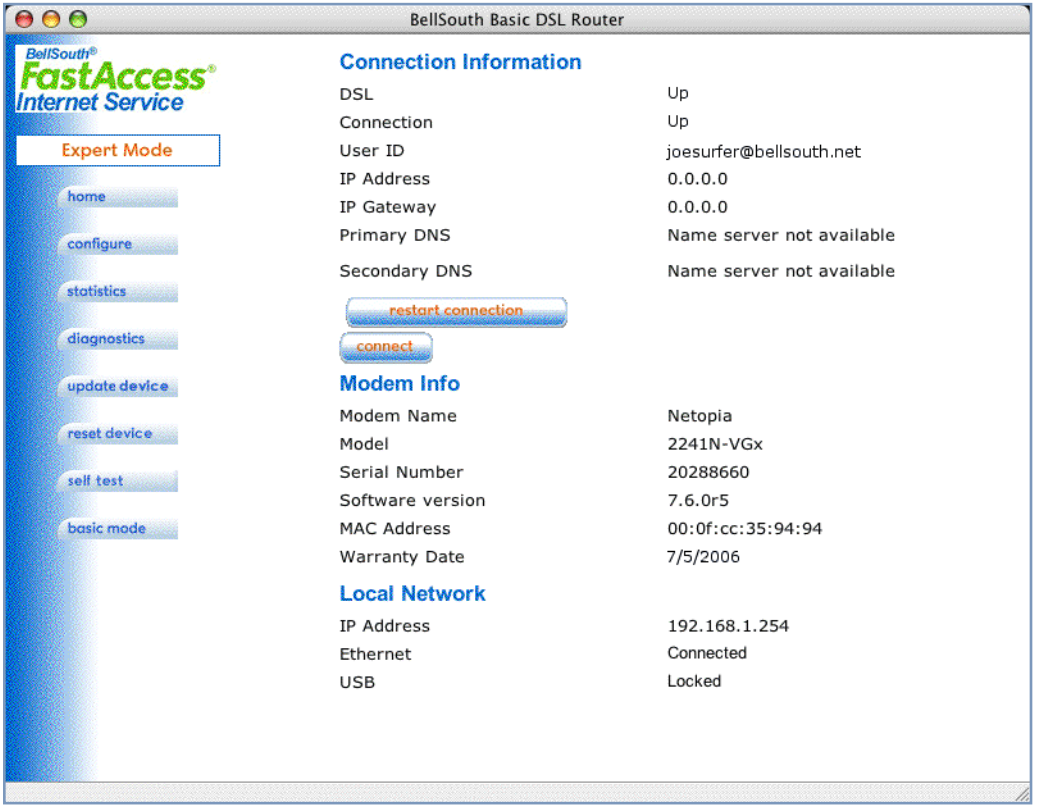
Click ***yes, enter expert mode***.

The Home Page opens in Expert Mode.

home

(Expert Mode)

The Home Page is the summary page for your Netopia Gateway. The toolbar at the left provides links to controlling, configuring, and monitoring pages. Critical configuration and operational status is displayed in the center section.



button bar

The buttons in the left-hand column on this page allow you to manage or configure several features of your Gateway. Each link is described in its own section.

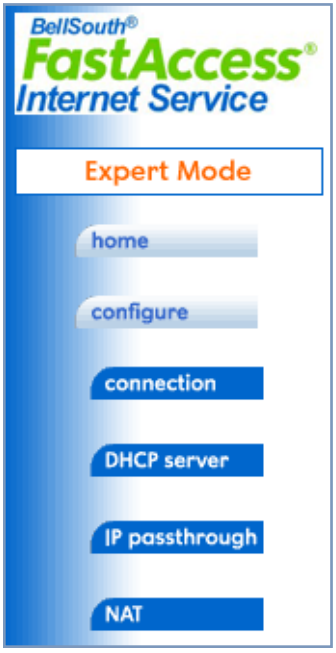
The button bar is the blue bar at the left side of the page containing the major navigation buttons. These buttons are available from every page, allowing you to move freely about the site.

Click the links below to be taken to each section.

- See “home” on page 38
- See “configure” on page 40
- See “statistics” on page 54
- See “diagnostics” on page 58
- See “update device” on page 60
- See “reset device” on page 62
- See “self test” on page 63
- See “basic mode” on page 64

Button: configure

When you click the ***configure*** button, the button bar expands.



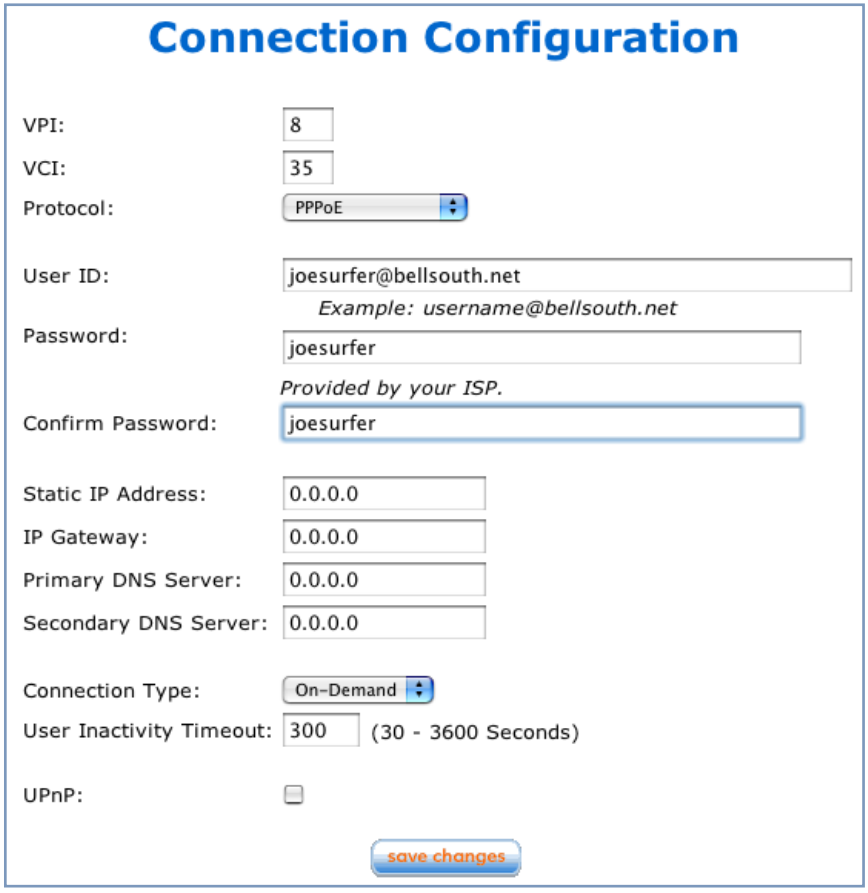
The Configuration options are presented in the order of likelihood you will need to use them. **Often, these settings should be changed only in accordance with information from your Service Provider.**

- See “connection” on page 41
- See “DHCP server” on page 44
- See “IP passthrough” on page 45
- See “NAT” on page 47

connection

When you click ***connection***, the Connection Configuration page appears. This screen's appearance will vary depending on your type of connection to the Internet.

Here is an example from a DSL model using PPPoE.



Here you can set up or change the way you connect to your ISP. You should only change these settings at your ISP's direction, or by agreement with your ISP.

- **VPI/VCI:** These values depend on the way your ISP's equipment is configured. 8/35 is the default virtual circuit pair, but others are also used. Check with your ISP.

- **Protocol:** The authentication and encapsulation protocol is determined by your ISP, often by the type of account that you have signed up for. Options here are:
  - PPPoE,
  - Bridged Ethernet,
  - PPPoA
- **Bridging:** Your Router can be turned into a simple bridge, if desired. However, it will no longer provide routing or security features in this mode.

  If you want the Gateway to do both bridging and routing, select **Routed Bridge** from the **Bridge Type** pull-down menu. When this mode is enabled, the Gateway will appear to be a router, but also bridge traffic from the LAN if it has a valid LAN-side address.
- **User ID** and **Password**: Provided by your ISP for PPP-based Protocols. Does not appear for RFC-1483-based Protocols.
- **Confirm Password:** Repeat your Password entry for confirmation
- **Static IP Address:** Your service provider may tell you that the WAN IP Address for your Router is static. In this case, enter the IP Address from your Service Provider in the appropriate field.
- **IP Gateway:** The IP Address of the default gateway, or peer address if using PPP. This is normally set to 0.0.0.0 for PPP connections.
- **Primary DNS Server:** The IP Address of the Primary Domain Name Server
- **Secondary DNS Server:** The IP Address of the backup Domain Name Server
- **Connection Type:** If using PPPoE, this is a choice to have either an uninterrupted connection or an as-needed connection. The type of service you have signed up for with your ISP. Options are On-Demand, Always ON, and Manual.

  Always ON: This setting provides convenience, but it leaves your network permanently connected to the Internet.

  On-Demand: Furnishes almost all the benefits of an Always On connection, but has additional security benefits:

  Your network cannot be attacked when it is not connected.

  Your network may change address with each connection, making it more difficult to attack.

  Manual: This setting disables automatic connection attempts. The user must bring the connection up and down via the Connect/Disconnect buttons.
- **User Inactivity Timeout**: (in seconds) If you chose either Manual or On Demand as your Connection Type, the User Inactivity Timeout setting can be used to control how long your connection will remain active before it disconnects automatically. You can set it for up to one hour (3600 seconds). After that period of time expires with no user activity, the connection must be reestablished.

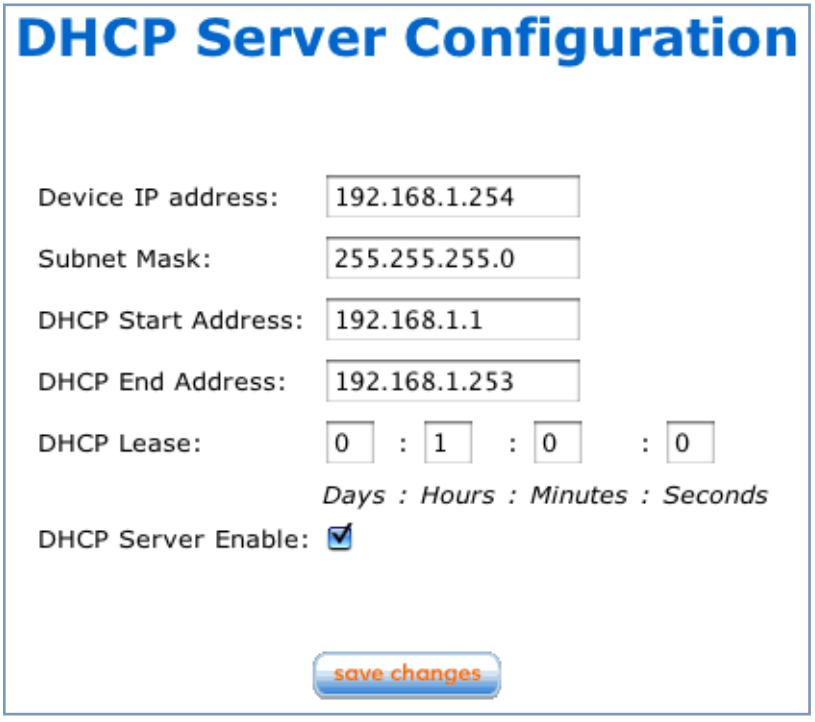
- **UPnP**: Universal Plug and Play (UPnP™) is a set of protocols that allows a PC to automatically discover other UPnP devices (anything from an internet gateway device to a light switch), retrieve an XML description of the device and its services, control the device, and subscribe to real-time event notification. By default, UPnP is enabled on the Netopia Router.

  For Windows XP users, the automatic discovery feature places an icon representing the Netopia Router automatically in the “My Network Places” folder. Double-clicking this icon opens the Router’s web UI.
  PCs using UPnP can retrieve the Router’s WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with a UPnP-enabled Netopia Router, will not need application layer gateway support on the Netopia Router to work through NAT.
  You can disable UPnP, if you are not using any UPnP devices or applications.

When all of your entries are made, click the ***save changes*** button.

DHCP server

When you click ***DHCP server***, the DHCP Server Configuration page appears.



The Server configuration determines the functionality of your DHCP Settings. This functionality enables the Router to assign your LAN computer(s) a “private” IP address and other parameters that allow network communication. This feature simplifies network administration because the Router maintains a list of IP address assignments. Additional computers can be added to your LAN without the hassle of configuring an IP address. This is the default mode for your Router.

- **Router IP Address:** Specifies the IP address of the Router itself.
- **Subnet Mask:** Specifies the common Class C subnet.
- **DHCP Start Address:** Specifies the first address in the DHCP address range. You can reserve a sequence of up to 253 IP addresses within a subnet, beginning with the specified address, for dynamic assignment.
- **DHCP End Address:** Specifies the last address in the DHCP address range.

- **DHCP Lease:** Specifies the default length for DHCP leases issued by the Router. Enter lease time in dd:hh:mm:ss (days/hours/minutes/seconds) format.
- **DHCP Server Enable:** Uncheck this setting if you already have a DHCP server on your LAN. This enables the DHCP server in this Router.

IP passthrough

When you click ***IP passthrough***, the IP Passthrough Configuration page appears.

The IP passthrough feature allows a single PC on the LAN to have the Router's public address assigned to it. It also provides PAT (NAPT) via the same public IP address for all other hosts on the private LAN subnet. Using IP passthrough:

- The public WAN IP is used to provide IP address translation for private LAN computers.
- The public WAN IP is assigned and reused on a LAN computer.
- DHCP address serving can automatically serve the WAN IP address to a LAN computer. When DHCP is used for addressing the designated passthrough PC, the acquired or configured WAN address is passed to DHCP, which will dynamically configure a single-servable-address subnet, and reserve the address for the configured PC's MAC address. This dynamic subnet configuration is based on the local and remote WAN address and subnet mask. If the WAN interface does not have a suitable subnet mask that is usable, for example when using PPP or PPPoE, the DHCP subnet configuration will default to a class C subnet mask.

1. **Select either User Configured PC or an IP address displayed in the selection window (these are the IP addresses currently being served to computers on your LAN.)**

   If you select “User Configured PC”, you must then configure a local PC to have the public WAN IP address.

2. **Click *enable*.**

   You will be reminded to restart the Router.

3. **Click the *restart modem* button and confirm the restart when prompted.**

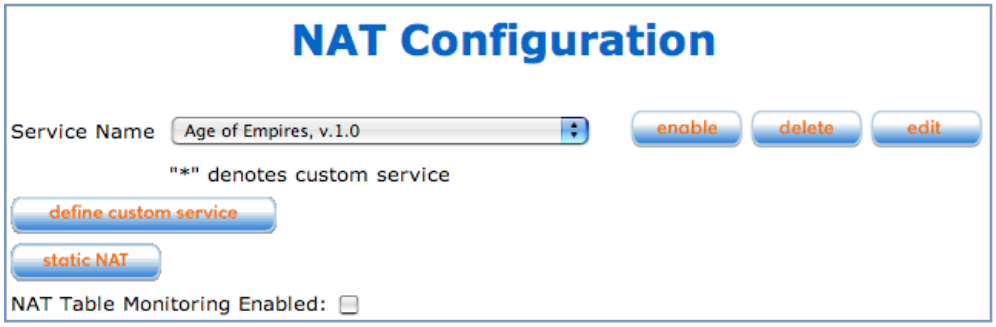
Once configured, the passthrough host's DHCP leases will be shortened to two minutes. This allows for timely updates of the host's IP address, which will be a private IP address *before* the WAN connection is established. *After* the WAN connection is established and has an address, the passthrough host can renew its DHCP address binding to acquire the WAN IP address.

A restriction

Since both the Router and the passthrough host will use the same IP address, new sessions that conflict with existing sessions will be rejected by the Router. For example, suppose you are a teleworker using an IPSec tunnel from the Router *and* from the passthrough host. Both tunnels go to the same remote endpoint, such as the VPN access concentrator at your employer’s office. In this case, the first one to start the IPSec traffic will be allowed; the second one – since, from the WAN, it's indistinguishable – will fail.

NAT

When you click ***NAT***, the NAT Configuration page appears.



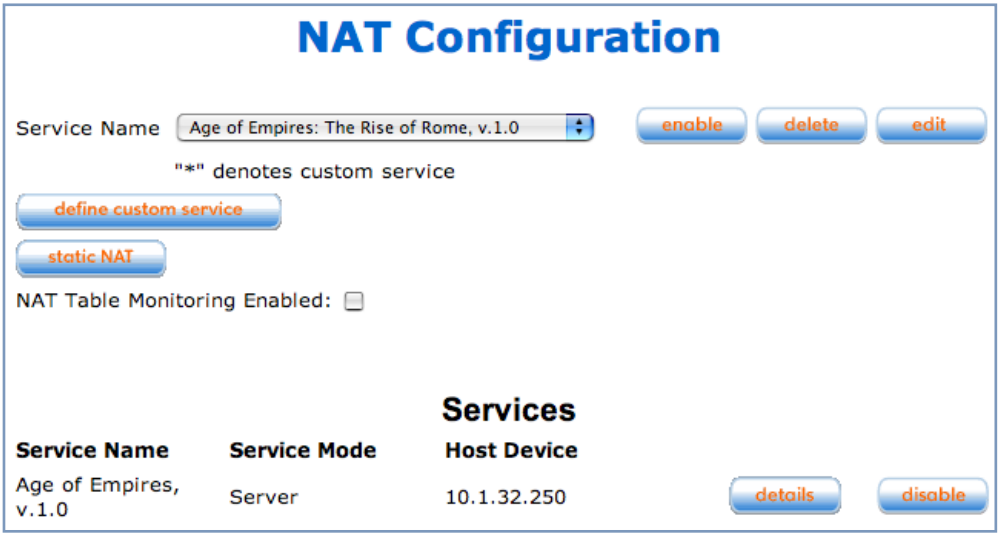
NAT Configuration allows you to host internet applications when NAT is enabled. You can host different games and software on different PCs.

From the **Service Name** pull-down menu, you can select any of a large number of pre-defined games and software. (See "List of Supported Games and Software" on page 48.)

1. **Once you choose a software service or game, click *enable*.**
   The Enable Service screen appears.

   Host Device specifies the machine on which the selected software is hosted.
2. **Select a PC to host the software from the Select Host Device pull-down menu and click *enable*.**

Each time you enable a software service or game your entry will be added to the list of **Service Names** displayed on the NAT Configuration page.



To remove a game or software from the hosted list, choose the game or software you want to remove and click the ***Disable*** button.

List of Supported Games and Software

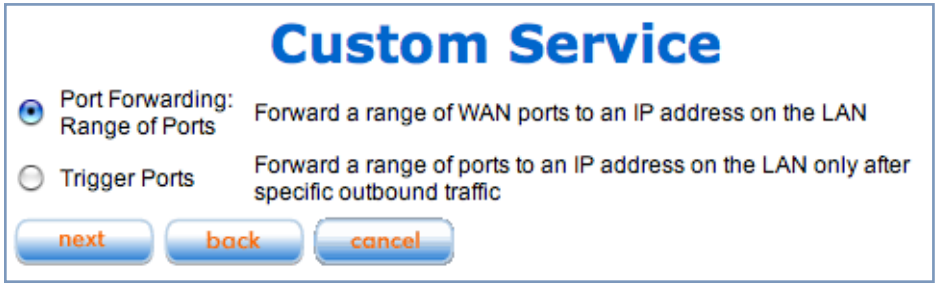
Age of Empires, v.1.0	Age of Empires: The Rise of Rome, v.1.0	Age of Wonders
Asheron's Call	Baldur's Gate	Battlefield Communicator
Buddy Phone	Calista IP Phone	CART Precision Racing, v 1.0
Citrix Metaframe/ICA Client	Close Combat for Windows 1.0	Close Combat: A Bridge Too Far, v 2.0
Close Combat III: The Russian Front, v 1.0	Combat Flight Sim: WWII Europe Series, v 1.0	Combat Flight Sim 2: WWII Pacific Thr, v 1.0
Dark Reign	Delta Force (Client and Server)	Delta Force 2
Diablo II Server	Dialpad	DNS Server
Dune 2000	eDonkey 2000	eMule

F-16, Mig 29	F-22, Lightning 3	Fighter Ace II
FTP	GNUtella	H.323 compliant (Netmeeting, CUSeeME)
Half Life	Hellbender for Windows, v 1.0	Heretic II
Hexen II	Hotline Server	HTTP
HTTPS	ICQ 2001b	ICQ Old
IMAP Client	IMAP Client v.3	Internet Phone
IPSec	IPSec IKE	Jedi Knight II: Jedi Outcast
Kali	KazaA	LimeWire
Links LS 2000	Mech Warrior 3	Mech Warrior 4: Vengeance
Medal of Honor Allied Assault	Microsoft Flight Simulator 98	Microsoft Flight Simulator 2000
Microsoft Golf 1998 Edition, v 1.0	Microsoft Golf 1999 Edition	Microsoft Golf 2001 Edition
Midtown Madness, v 1.0	Monster Truck Madness, v 1.0	Monster Truck Madness 2, v 2.0
Motocross Madness 2, v 2.0	Motocross Madness, v 1.0	MSN Game Zone
MSN Game Zone (DX7 an 8 Play)	Need for Speed 3, Hot Pursuit	Need for Speed, Porsche
Net2Phone	NNTP	Operation FlashPoint
Outlaws	pcAnywhere (incoming)	POP-3
PPTP	Quake II	Quake III
Rainbow Six	RealAudio	Return to Castle Wolfenstein
Roger Wilco	Rogue Spear	ShoutCast Server
SMTP	SNMP	SSH server
StarCraft	Starfleet Command	StarLancer, v 1.0
Telnet	TFTP	Tiberian Sun: Command and Conquer

Timbuktu	Total Annihilation	Ultima Online
Unreal Tournament Server	Urban Assault, v 1.0	VNC, Virtual Network Computing
Westwood Online, Command and Conquer	Win2000 Terminal Server	XBox Live Games
Yahoo Messenger Chat	Yahoo Messenger Phone	ZNES

Define Custom Service

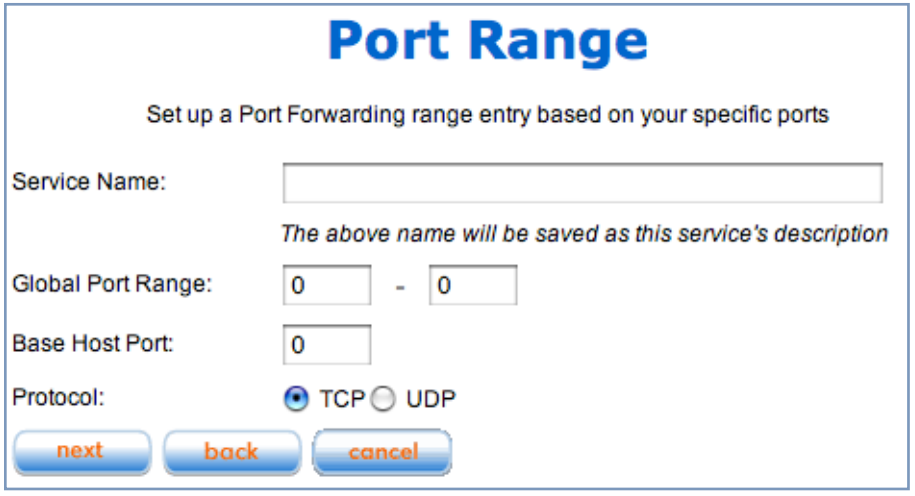
To configure a Custom Service, choose whether to use Port Forwarding or Trigger Ports.



- **Port Forwarding** forwards a range of WAN ports to an IP address on the LAN.
- **Trigger Ports** forwards a range of ports to an IP address on the LAN only after specific outbound traffic "triggers" the feature.

Click the ***next*** button.

If you chose Port Forwarding, the Port Range entry screen appears.

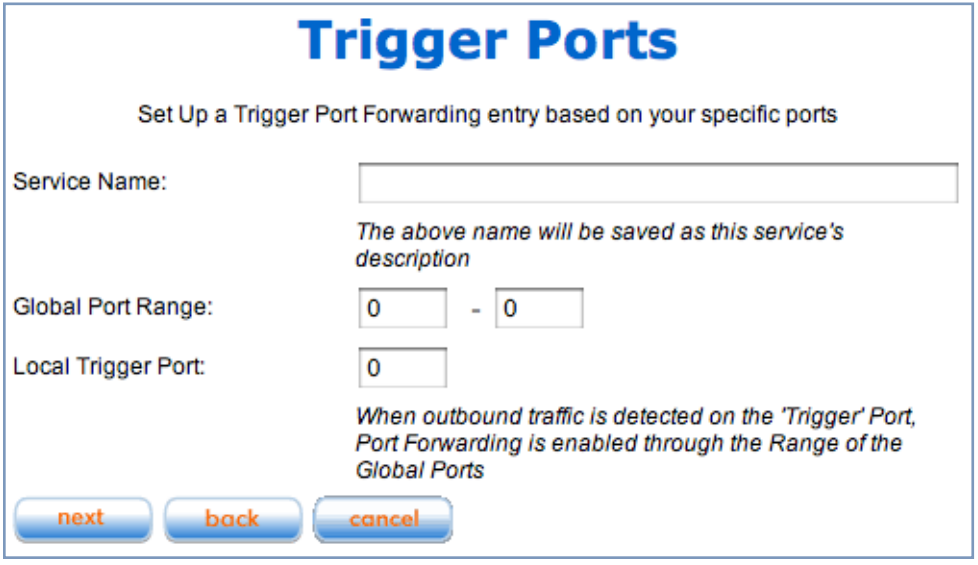


Port Forwarding forwards a range of WAN ports to an IP address on the LAN. Enter the following information:

- **Service Name:** A unique identifier for the Custom Service.
- **Global Port Range:** Range of ports on which incoming traffic will be received.
- **Base Host Port:** The port number at the start of the port range your Router should use when forwarding traffic of the specified type(s) to the internal IP address.
- **Protocol:** Protocol type of Internet traffic, TCP or UDP.

Click the ***next*** button.

If you chose Trigger Ports, the Trigger Ports entry screen appears.



Trigger Ports forwards a range of ports to an IP address on the LAN only after specific outbound traffic "triggers" the feature. Enter the following information:

- **Service Name:** A unique identifier for the Custom Service.
- **Global Port Range:** Range of ports on which incoming traffic will be received.
- **Local Trigger Port:** Port number of the type of outbound traffic that needs to happen (will be the trigger) to then allow the configured ports for inbound traffic.
  Example: Set the trigger port to 21 and configure a range of 25 – 110. You would need to do an outbound ftp before you were able to do an inbound smtp.

Click the ***next*** button.

Static NAT

This feature allows you to:

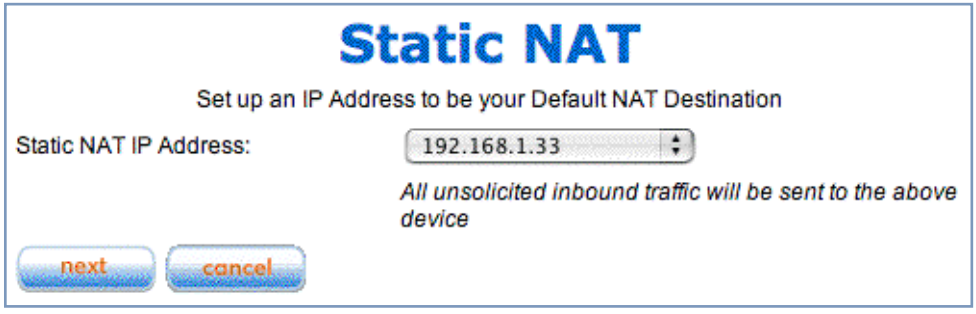
- Direct your Router to forward all externally initiated IP traffic (TCP and UDP protocols only) to a default host on the LAN.
- Enable it for certain situations:

  – Where you cannot anticipate what port number or packet protocol an in-bound application might use. For example, some network games select arbitrary port numbers when a connection is opened.

  – When you want all unsolicited traffic to go to a specific LAN host.

This feature allows you to direct unsolicited or non-specific traffic to a designated LAN station. With NAT "On" in the Router, these packets normally would be discarded.

For instance, this could be application traffic where you don't know (in advance) the port or protocol that will be used. Some game applications fit this profile.

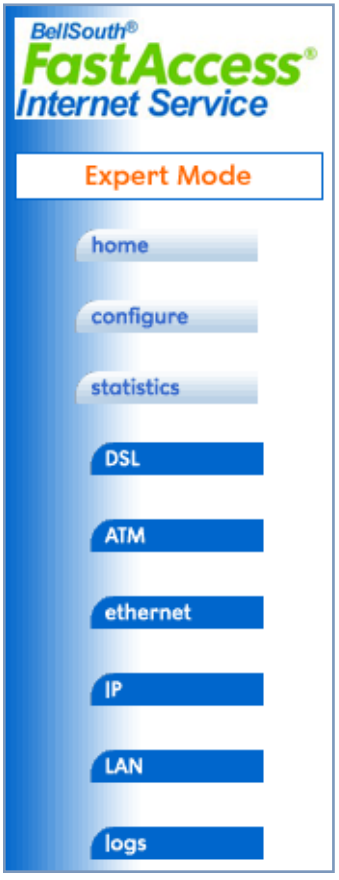


From the pull-down menu, select the address of the PC that you want to be your default NAT destination.

Click the ***next*** button, and your choice will be so designated.

Button: statistics

When you click the ***statistics*** button, the button bar expands.



- See “DSL” on page 55
- See “ATM” on page 55
- See “ethernet” on page 55
- See “IP” on page 56
- See “LAN” on page 56
- See “logs” on page 57

DSL

When you click ***DSL***, the DSL Statistics page appears.

The DSL Statistics page displays information about the Router's WAN connection to the Internet.

- **Line State:** May be Up (connected) or Down (disconnected).
- **Modulation:** Method of regulating the DSL signal. DMT (Discrete MultiTone) allows connections to work better when certain radio transmitters are present.
- **Data Path:** Type of path used by the device's processor.

Downstream and Upstream statistics

- **Max Allowed Speed (kbps):** Your maximum speeds for downloading (receiving) and uploading (sending) data on the DSL line, in kilobits per second.
- **SN Margin (db):** Signal to noise margin, in decibels. Reflects the amount of unwanted “noise” on the DSL line.
- **Line Attenuation:** Amount of reduction in signal strength on the DSL line, in decibels.
- **CRC Errors:** Number of times data packets have had to be resent due to errors in transmission or reception.

ATM

When you click ***ATM***, the ATM Statistics page appears.

The ATM Statistics page displays detailed statistics about the upstream and downstream data traffic handled by your Router. Displays the Virtual Circuit (VPI/VCI) settings as well as information about your PPPoE session if operating in PPPoE mode. This information is useful for troubleshooting and when seeking technical support.

ethernet

When you click ***ethernet***, the Ethernet Statistics page appears.

The Ethernet Statistics page:

- displays your Router's unique hardware (MAC) address.
- displays detailed statistics about your LAN data traffic, upstream and downstream.

IP

When you click ***IP***, the IP Statistics page appears. The IP Statistics page displays the IP interfaces and routing table information about your network.

General

- **IP WAN Address:** The public IP address of your Router, whether dynamically or statically assigned.
- **IP Gateway:** Your ISP's gateway router IP address
- **Primary DNS:** The IP address of the Primary Domain Name Server
- **Primary DNS name:** The name of the Primary Domain Name Server
- **Secondary DNS:** The IP address of the backup Domain Name Server (if any)
- **Secondary DNS name:** The name of the backup Domain Name Server

IP interfaces

- **Address:** Your Router's IP address as seen from your internal network (LAN), and from the public Internet (WAN)
- **Netmask:** The subnet mask for the respective IP interfaces (LAN and WAN)
- **Name:** The name of each IP interface (example:Eth0, WAN2)

Network Routing Table and Host Routing Table

The Routing tables display all of the IP routes currently known to your Router

LAN

When you click ***LAN***, the LAN Statistics page appears.

The LAN Statistics page displays detailed information about your LAN IP configuration and names and IP addresses of devices on your LAN.

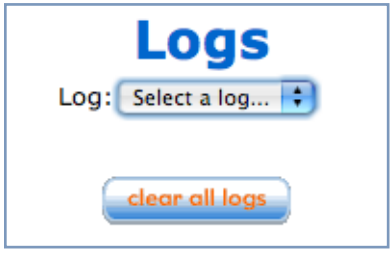
- **Router IP Address:** The IP address of your Router as seen from the LAN
- **DHCP Netmask:** Subnet mask of your LAN
- **DHCP Start Address:** First IP address in the range being served to your LAN by the Router's DHCP server
- **DHCP End Address:** Last IP address in the range being served to your LAN by the Router's DHCP server
- **DHCP Server Status:** May be On or Off
- **DNS Server:** The IP address of the default DNS server

Devices on LAN

Displays the IP Address, MAC (hardware) Address, and network Name for each device on your LAN connected to the Router.

logs

When you click ***Logs***, the Logs page appears.



Select a log from the pull-down menu:

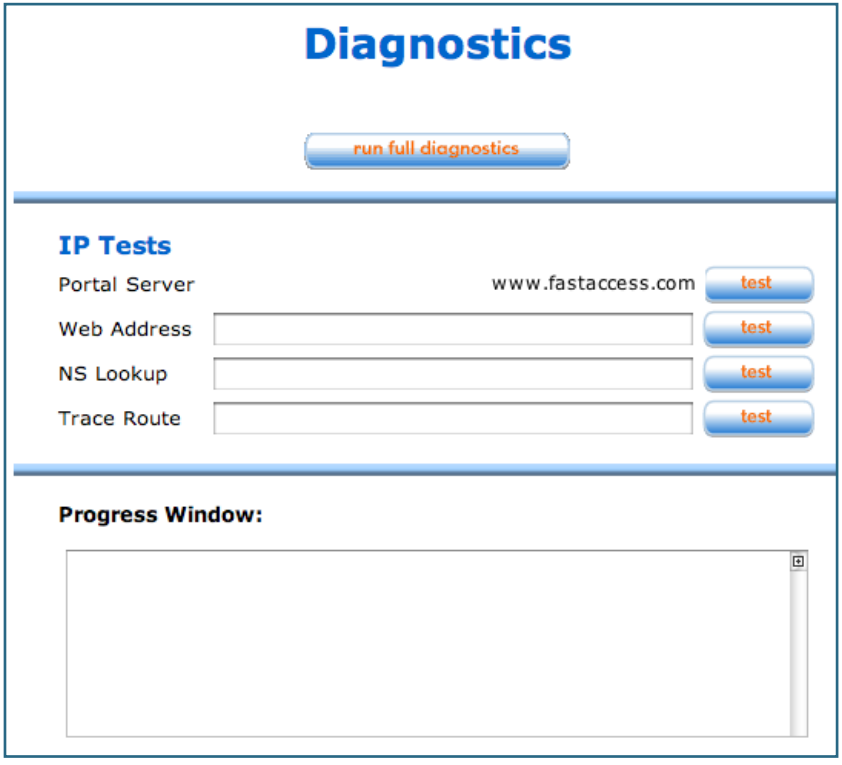
- **All**: Displays the entire system log.
- **Connection:** Displays events logged for the WAN connection.
- **System:** Displays events logged for the Router system configuration.

The current status of the Router is displayed for all logs.

You can clear all log entries by clicking the ***clear all logs*** button.

Button: diagnostics

This automated multi-layer test examines the functionality of the Router from the physical connections to the data traffic being sent by users through the Router.



- **Portal Server** - tests the connection to a predefined server on the Internet.
- **Web Address** - tests the connection to a specified URL or IP address.
- **NS Lookup** - converts a domain name to its IP address and vice versa.
- **TraceRoute** - displays the path to a destination by showing the number of hops and the router addresses of these hops.

You enter a web address URL or an IP address in the respective field and click the ***Test*** button.

Results will be displayed in the **Progress Window** as they are generated.

This sequence of tests takes approximately one minute to generate results. Please wait for the test to run to completion.

Each test generates one of the following result codes:

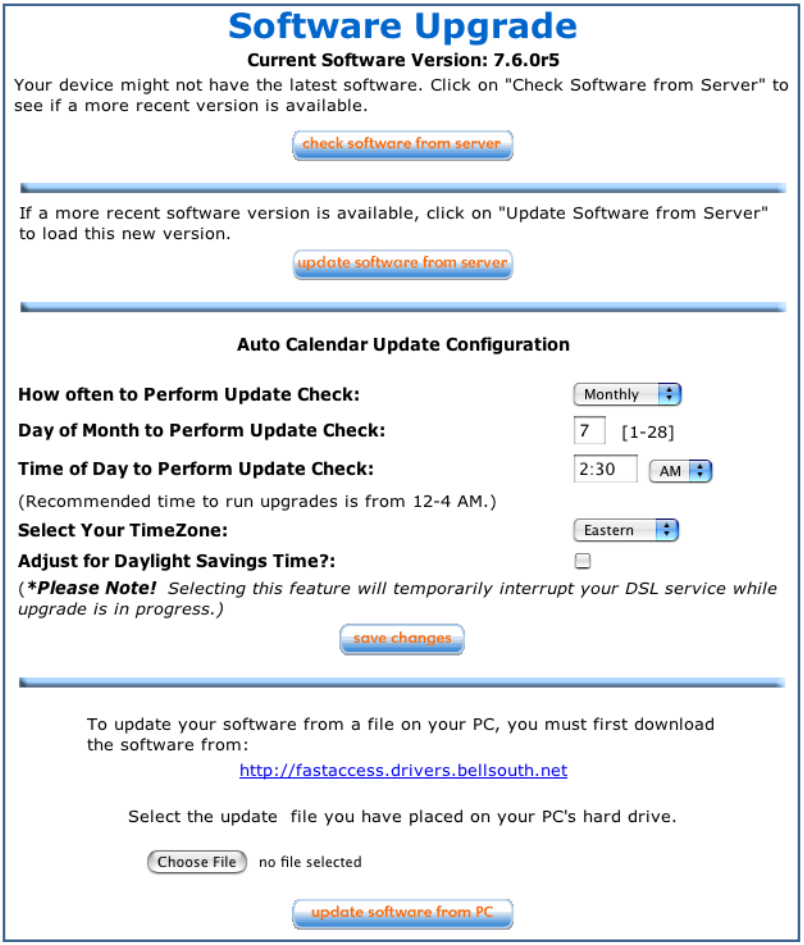
Result	Meaning
* PASS:	The test was successful.
* FAIL:	The test was unsuccessful.
* SKIPPED:	The test was skipped because a test on which it depended failed.
* PENDING:	The test timed out without producing a result. Try running Diagnostics again.
* WARNING:	The test was unsuccessful. The Service Provider equipment your Router connects to may not support this test.

You can run all the tests in order by clicking the ***run full diagnostics*** button.

Button: update device

Periodically, the embedded firmware in your Gateway may be updated to improve the operation or add new features. Your Gateway includes its own onboard installation capability. Your service provider may inform you when new firmware is available, or you can check for yourself.

Click the ***update device*** button. The Software Upgrade page appears.



Operating System Software is what makes your Router run and occasionally it needs to be updated. Your **Current Software Version** is displayed at the top of the page.

If you want to check for an updated version without installing it, click the ***check software from server*** button.

• Auto Calendar Update Configuration

You can schedule your Router to check for updates automatically, by setting the Auto Calendar schedule. Set your options and click the ***save changes*** button.

You can update your software in either of two ways:

• From a Server

- If an updated version exists, click the ***update software from server*** button, and a new version will automatically be downloaded to your Router.
- When the download and installation is complete, you will be prompted to restart the router.

• From your PC

To update your software from a file on your PC, you must first download the software from the website linked to the URL on this page. Once you have downloaded the software file to your PC:

1. **Browse your computer for the operating system file you downloaded.**
2. **Click the *update software from PC* button.**
3. **The install may take a few minutes; wait for it to complete.**
4. **Restart your Router and your new operating system will be running.**

Button: reset device

In some cases, you may need to clear all the configuration settings and start over again to program the Netopia Gateway. You can perform a factory reset to do this.

Click the ***reset device*** button to reset the Gateway back to its original factory default settings. You will be prompted to make sure you want to do this.

Click the ***yes, reset to factory settings*** button, if you want to proceed.

NOTE:

Exercise caution before performing a Factory Reset. This will erase any configuration changes that you may have made and allow you to reprogram your Gateway.

Button: self test

You can perform a self-test of your Router to be sure all systems are functioning.

When you click the ***self test*** button, the Router tests itself and the Device Self Test page appears.

The device self test verifies the following device functionality:

- Memory.
- Ethernet connection.
- Configuration.
- DSL hardware (if supported).
- Wireless hardware (if supported).

If your device fails, contact your Service Provider.

Button: basic mode

When you click the ***basic mode*** button. you are returned to the basic mode home page.

It is a good practice to return to basic mode after doing any advanced configuration, to avoid any inadvertent misconfiguration.

CHAPTER 4 Basic Troubleshooting

This section gives some simple suggestions for troubleshooting problems with your Gateway's initial configuration.

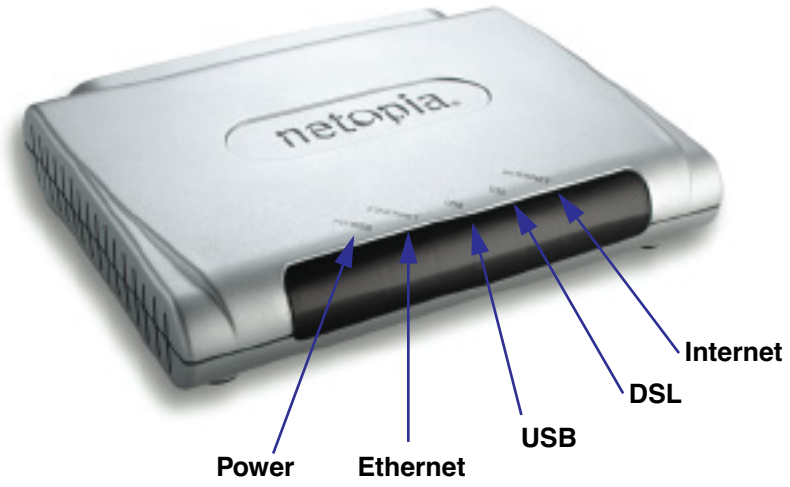
Before troubleshooting, make sure you have

- read the *Quickstart Guide*;
- plugged in all the necessary cables; and
- set your PC's TCP/IP controls to obtain an IP address automatically.

Status Indicator Lights

The first step in troubleshooting is to check the status indicator lights (LEDs) in the order outlined below.

Netopia Gateway 2241N status indicator lights



LED	Action
Power	**Green** when power is on.
Ethernet	Solid **green** when connected. Flash **green** when there is activity on the LAN.
USB	Solid **green** when connected. Flashes **green** when there is activity on the USB port.
DSL	Solid **green** when Internet connection is established.
Internet	Solid **green** when Broadband device is connected. Flashes **green** for activity on the WAN port.

LED Function Summary Matrix

	Power	USB Active	DSL Sync	DSL Traffic	Ethernet Traffic	Ethernet Link
Unlit	No power	No signal	No signal	No signal	No signal	No signal
Solid Green	Power on	USB port connected to PC	DSL line synched with the DSLAM	N/A	N/A	Synched with Ethernet card
Flashing Green	N/A	Activity on the USB cable	Attempting to train with DSLAM	Activity on the DSL cable	Activity on the Ethernet cable	N/A

If a status indicator light does not look correct, look for these possible problems:

LED	State	Possible problems
Power	**Unlit**	1. Make sure the power switch is in the ON position. 2. Make sure the power adapter is plugged into the 2200-series DSL Gateway properly. 3. Try a known good wall outlet. 4. Replace the power supply and/or unit.
DSL Sync	**Unlit**	1. Make sure the you are using the correct cable. The DSL cable is the thinner standard telephone cable. 2. Make sure the DSL cable is plugged into the correct wall jack. 3. Make sure the DSL cable is plugged into the DSL port on the 2200-series DSL Gateway. 4. Make sure the DSL line has been activated at the central office DSLAM. 5. Make sure the 2200-series DSL Gateway is not plugged into a micro filter.

EN Link	**Unlit**	**Note:** EN Link light is inactive if only using USB. 1. Make sure the you are using the Ethernet cable, not the DSL cable. The Ethernet cable is thicker than the standard telephone cable. 2. Make sure the Ethernet cable is securely plugged into the Ethernet jack on the PC. 3. If plugging a 2200-series DSL Gateway into a hub the you may need to plug into an uplink port on the hub, or use an Ethernet cross over cable. 4. Make sure the Ethernet cable is securely plugged into the Ethernet port on the 2200-series DSL Gateway. 5. Try another Ethernet cable if you have one available.
EN Traffic	**Unlit**	1. Make sure you have Ethernet drivers installed on the PC. 2. Make sure the PC's TCP/IP Properties for the Ethernet Network Control Panel is set to obtain an IP address via DHCP. 3. Make sure the PC has obtained an address in the 192.168.1.x range. (You may have changed the subnet addressing.) 4. Make sure the PC is configured to access the Internet over a LAN. 5. Disable any installed network devices (Ethernet, Home-PNA, wireless) that are not being used to connect to the 2200-series DSL Gateway.

USB Active	**Unlit**	**Note:** USB Active light is inactive if only using Ethernet. 1. Make sure you have USB drivers installed on the PC. 2. Make sure the PC's TCP/IP Properties for the USB Network Control Panel is set to obtain an IP address via DHCP. 3. Make sure the PC has obtained an address in the 192.168.1.x range. (You may have changed the subnet addressing.) 4. Make sure the PC is configured to access the Internet over a LAN. 5. Disable any installed network devices (Ethernet, HomePNA, wireless) that are not being used to connect to the 2200-series DSL Gateway.
DSL Traffic	**Unlit**	Launch a browser and try to browse the Internet. If the DSL Active light still does not flash, then proceed to Advanced Troubleshooting below.

Factory Reset Switch

Lose your password? This section shows how to reset the Netopia Gateway so that you can access the configuration screens once again.

NOTE: Keep in mind that all of your settings will need to be reconfigured.

If you don't have a password, the only way to access the Netopia Gateway is the following:

1. **Referring to the diagram below, find the round Reset Switch opening.**

Factory Reset Switch: Push to clear all settings

2. **Carefully insert the point of a pen or an unwound paperclip into the opening.**

- If you press the factory default button for less than 1/2 a second, the unit will continue to run as normal.
- If you press the factory default button for more than 3 seconds, when you release it, the Gateway will perform a factory reset, clear all settings and configurations, and reboot.

CHAPTER 5 Command Line Interface

The Netopia Gateway operating software includes a command line interface (CLI) that lets you access your Netopia Gateway over a telnet connection. You can use the command line interface to enter and update the unit's configuration settings, monitor its performance, and restart it.

This chapter covers the following topics:

Overview

The CLI has two major command modes: **SHELL** and **CONFIG**. **Summary tables** that list the commands are provided below. Details of the entire command set follow in this section.

SHELL Commands

Command	Status and/or Description
arp	to send ARP request
atmping	to send ATM OAM loopback
clear	to erase all stored configuration information
clear_certificate	to remove an SSL certificate that has been installed
clear_log	to erase all stored log info in flash memory
configure	to configure unit's options
diagnose	to run self-test
download	to download config file
exit	to quit this shell
help	to get more: “help all” or “help help”
install	to download and program an image into flash
license	to enter an upgrade key to add a feature
log	to add a message to the diagnostic log
loglevel	to report or change diagnostic log level
netstat	to show IP information
nslookup	to send DNS query for host
ping	to send ICMP Echo request
quit	to quit this shell
reset	to reset subsystems
restart	to restart unit
show	to show system information
start	to start subsystem
status	to show basic status of unit
telnet	to telnet to a remote host
traceroute	to send traceroute probes
upload	to upload config file
who	to show who is using the shell

CONFIG Commands	
Command Verbs	**Status and/or Description**
delete	Delete configuration list data
help	Help command option
save	Save configuration data
script	Print configuration data
set	Set configuration data
validate	Validate configuration settings
view	View configuration data
Keywords	
atm	ATM options (DSL only)
bridge	Bridge options
dhcp	Dynamic Host Configuration Protocol options
dmt	DMT ADSL options
diffserv	Differentiated Services options
dns	Domain Name System options
dslf-cpewan	TR-069 CPE WAN management
dslf-lanmgnt	TR-064 LAN management
dynamic-dns	Dynamic DNS options
ethernet	Ethernet options
igmp	IGMP configuration options
ip	TCP/IP protocol options
ip-maps	IPmaps options
nat-default	Network Address Translation default options
pinhole	Pinhole options
ppp	Peer-to-Peer Protocol options
pppoe	PPP over Ethernet options
preferences	Shell environment settings
radius	RADIUS Server options
security	Security options
servers	Internal Server options
snmp	SNMP management options
system	Gateway's system options
upnp	UPnP options
vlan	VLAN options

Command Utilities	
top	Go to top level of configuration mode
quit	Exit from configuration mode; return to shell mode
exit	Exit from configuration mode; return to shell mode

Starting and Ending a CLI Session

Open a telnet connection from a workstation on your network.

You initiate a telnet connection by issuing the following command from an IP host that supports telnet, for example, a personal computer running a telnet application such as NCSA Telnet.

```
telnet <ip_address>
```

You must know the IP address of the Netopia Gateway before you can make a telnet connection to it. By default, your Netopia Gateway uses 192.168.1.254 as the IP address for its LAN interface. You can use a Web browser to configure the Netopia Gateway IP address.

Logging In

The command line interface log-in process emulates the log-in process for a UNIX host. To logon, enter the username (either admin or user), and your password.

- Entering the administrator password lets you display and update all Netopia Gateway settings.
- Entering a user password lets you display (but not update) Netopia Gateway settings.

When you have logged in successfully, the command line interface lists the username and the security level associated with the password you entered in the diagnostic log.

Ending a CLI Session

You end a command line interface session by typing **`quit`** from the SHELL node of the command line interface hierarchy.

Saving Settings

In CONFIG mode, the **save** command saves the working copy of the settings to the Gateway. The Gateway automatically validates its settings when you save and displays a warning message if the configuration is not correct.

Using the CLI Help Facility

The **help** command lets you display on-line help for SHELL and CONFIG commands. To display a list of the commands available to you from your current location within the command line interface hierarchy, enter **`help`**.

To obtain help for a specific CLI command, type **`help <command>`**. You can truncate the ***help*** command to ***h*** or a question mark when you request help for a CLI command.

About SHELL Commands

You begin in SHELL mode when you start a CLI session. SHELL mode lets you perform the following tasks with your Netopia Gateway:

- Monitor its performance
- Display and reset Gateway statistics
- Issue administrative commands to restart Netopia Gateway functions

SHELL Prompt

When you are in SHELL mode, the CLI prompt is the name of the Netopia Gateway followed by a right angle bracket (>). For example, if you open a CLI connection to the Netopia Gateway named “Coconut,” you would see ***Coconut>*** as your CLI prompt.

SHELL Command Shortcuts

You can **truncate** most commands in the CLI to their shortest unique string. For example, you can use the truncated command ***q*** in place of the full ***quit*** command to exit the CLI. However, you would need to enter ***rese*** for the ***reset*** command, since the first characters of ***reset*** are common to the ***restart*** command.

The only commands you cannot truncate are ***restart*** and ***clear***. To prevent accidental interruption of communications, you must enter the ***restart*** and ***clear*** commands in their entirety.

You can use the Up and Down arrow keys to scroll backward and forward through recent commands you have entered. Alternatively, you can use the ***!!*** command to repeat the last command you entered.

SHELL Commands

Common Commands

arp *nnn.nnn.nnn.nnn*

Sends an Address Resolution Protocol (ARP) request to match the *nnn.nnn.nnn.nnn* IP address to an Ethernet hardware address.

clear [yes]

Clears the configuration settings in a Netopia Gateway. If you do not use the optional **yes** qualifier, you are prompted to confirm the **clear** command.

clear_certificate

Removes an SSL certificate that has been installed.

clear_log

Erases the log information stored in flash if persistent logging is enabled.

configure

Puts the command line interface into Configure mode, which lets you configure your Netopia Gateway with Config commands. Config commands are described starting on page 73.

diagnose

Runs a diagnostic utility to conduct a series of internal checks and loopback tests to verify network connectivity over each interface on your Netopia Gateway. The console displays the results of each test as the diagnostic utility runs. If one test is dependent on another, the diagnostic utility indents its entry in the console window. For example, the diagnostic utility indents the Check IP connect to Ethernet (LAN) entry, since that test will not run if the Check Ethernet LAN Connect test fails.

Each test generates one of the following result codes:

CODE	Description
PASS	The test was successful.
FAIL	The test was unsuccessful.
SKIPPED	The test was skipped because a test on which it depended failed, or because the test did not apply to your particular setup or model.
PENDING	The test timed out without producing a result. Try running the test again.

download [*server_address*] [*filename*] [confirm]

This command installs a file of configuration parameters into the Netopia Gateway from a TFTP (Trivial File Transfer Protocol) server. The TFTP server must be accessible on your Ethernet network.

You can include one or more of the following arguments with the download command. If you omit arguments, the console prompts you for this information.

- The *server_address* argument identifies the IP address of the TFTP server from which you want to copy the Netopia Gateway configuration file.
- The *filename* argument identifies the path and name of the configuration file on the TFTP server.
- If you include the optional **confirm** keyword, the download begins as soon as all information is entered.

Beginning with Firmware Version 7.5.1, you can also download an SSL certificate file from a trusted Certification Authority (CA), on platforms that support SSL, as follows:

download [-cert] [*server_address*] [*filename*] [confirm]

install [*server_address*] [*filename*] [confirm]

Downloads a new version of the Netopia Gateway operating software from a TFTP (Trivial File Transfer Protocol) server, validates the software image, and programs the image into the Netopia Gateway memory. After you install new operating software, you must restart the Netopia Gateway.

The *server_address* argument identifies the IP address of the TFTP server on which your Netopia Gateway operating software is stored. The *filename* argument identifies the path and name of the operating software file on the TFTP server.

If you include the optional keyword *confirm*, you will not be prompted to confirm whether or not you want to perform the operation.

license [key]

This command installs a software upgrade key. An upgrade key is a purchased item, based on the serial number of the gateway.

log *message_string*

Adds the message in the *message_string* argument to the Netopia Gateway diagnostic log.

loglevel [*level*]

Displays or modifies the types of log messages you want the Netopia Gateway to record. If you enter the **loglevel** command without the optional *level* argument, the command line interface displays the current log level setting.

You can enter the **loglevel** command with the *level* argument to specify the types of diagnostic messages you want to record. All messages with a level number equal to or greater than the level you specify are recorded. For example, if you specify loglevel 3, the diagnostic log will retain high-level informational messages (level 3), warnings (level 4), and failure messages (level 5).

Use the following values for the *level* argument:

- **1** or **low** – Low-level informational messages or greater; includes trivial status messages.

- **2** or **medium** – Medium-level informational messages or greater; includes status messages that can help monitor network traffic.
- **3** or **high** – High-level informational messages or greater; includes status messages that may be significant but do not constitute errors.
- **4** or **warning** – Warnings or greater; includes recoverable error conditions and useful operator information.
- **5** or **failure** — Failures; includes messages describing error conditions that may not be recoverable.

netstat -i

Displays the IP interfaces for your Netopia Gateway.

netstat -r

Displays the IP routes stored in your Netopia Gateway.

nslookup { *hostname* | *ip_address* }

Performs a domain name system lookup for a specified host.

- The *hostname* argument is the name of the host for which you want DNS information; for example, ***nslookup klaatu***.
- The *ip_address* argument is the IP address, in dotted decimal notation, of the device for which you want DNS information.

ping [-s *size*] [-c *count*]{ *hostname* | *ip_address* }

Causes the Netopia Gateway to issue a series of ICMP Echo requests for the device with the specified name or IP address.

- The *hostname* argument is the name of the device you want to ping; for example, ***ping ftp.netopia.com***.
- The *ip_address* argument is the IP address, in dotted decimal notation, of the device you want to locate. If a host using the specified name or IP address is active, it returns one or more ICMP Echo replies, confirming that it is accessible from your network.
- The ***-s*** *size* argument lets you specify the size of the ICMP packet.
- The ***-c*** *count* argument lets you specify the number of ICMP packets generated for the ping request. Values greater than 250 are truncated to 250.

You can use the **ping** command to determine whether a hostname or IP address is already in use on your network. You cannot use the **ping** command to ping the Netopia Gateway's own IP address.

quit

Exits the Netopia Gateway command line interface.

reset arp

Clears the Address Resolution Protocol (ARP) cache on your unit.

reset atm

Resets the Asynchronous Transfer Mode (ATM) statistics.

reset crash

Clears crash-dump information, which identifies the contents of the Netopia Gateway registers at the point of system malfunction.

reset dhcp server

Clears the DHCP lease table in the Netopia Gateway.

reset diffserv

Resets the Differentiated Services (diffserv) statistics.

reset enet

Resets Ethernet statistics to zero

reset heartbeat

Restarts the heartbeat sequence.

reset ipmap

Clears the IPMap table (NAT).

reset log

Rewinds the diagnostic log display to the top of the existing Netopia Gateway diagnostic log. The **`reset`** log command does not clear the diagnostic log. The next **`show log`** command will display information from the beginning of the log file.

reset security-log

Clears the security monitoring log to make room to capture new entries.

reset wan-users [all | *ip-address*]

This function disconnects the specified WAN User to allow for other users to access the WAN. This function is only available if the number of WAN Users is restricted and NAT is on. Use the **all** parameter to disconnect all users. If you logon as Admin you can disconnect any or all users. If you logon as User, you can only disconnect yourself.

restart [*seconds*]

Restarts your Netopia Gateway. If you include the optional *`seconds`* argument, your Netopia Gateway will restart when the specified number of seconds have elapsed. You must enter the complete **`restart`** command to initiate a restart.

show all-info

Displays all settings currently configured in the Netopia Gateway.

show dhcp agent

Displays DHCP relay-agent leases.

show diffserv

Displays the Differentiated Services and QoS values configured in the Netopia Gateway.

show features

Displays standard and keyed features installed in the Netopia Gateway.

show enet

Displays Ethernet interfaces maintained by the Netopia Gateway.

show bridge interfaces

Displays bridge interfaces maintained by the Netopia Gateway.

show bridge table

Displays the bridging table maintained by the Netopia Gateway.

show crash

Displays the most recent crash information, if any, for your Netopia Gateway.

show dhcp server leases

Displays the DHCP leases stored in RAM by your Netopia Gateway.

show ip arp

Displays the Ethernet address resolution table stored in your Netopia Gateway.

show ip igmp

Displays the contents of the IGMP Group Address table and the IGMP Report table maintained by your Netopia Gateway.

show ip interfaces

Displays the IP interfaces for your Netopia Gateway.

show ip ipsec

Displays IPSec Tunnel statistics.

show ip firewall

Displays firewall statistics.

show ip lan-discovery

Displays the LAN Host Discovery Table of hosts on the wired or wireless LAN, and whether or not they are currently online.

show ip routes

Displays the IP routes stored in your Netopia Gateway.

show ip state-insp

Displays whether stateful inspection is enabled on an interface or not, exposed addresses and blocked packet statistics because of stateful inspection.

show log

Displays blocks of information from the Netopia Gateway diagnostic log. To see the entire log, you can repeat the **`show log`** command or you can enter **`show log all.`**

show memory [all]

Displays memory usage information for your Netopia Gateway. If you include the optional ***all*** argument, your Netopia Gateway will display a more detailed set of memory statistics.

show pppoe

Displays status information for each PPP socket, such as the socket state, service names, and host ID values.

show status

Displays the current status of a Netopia Gateway, the device's hardware and software revision levels, a summary of errors encountered, and the length of time the Netopia Gateway has been running since it was last restarted. Identical to the **`status`** command.

show summary

Displays a summary of WAN, LAN, and Gateway information.

show wireless [all]

Shows wireless status and statistics.

show wireless clients [*MAC_address*]

Displays details on connected clients, or more details on a particular client if the MAC address is added as an argument.

telnet { *hostname* | *ip_address* } [*port*]

Lets you open a telnet connection to the specified host through your Netopia Gateway.

- The *`hostname`* argument is the name of the device to which you want to connect; for example, ***telnet ftp.netopia.com***.
- The *`ip_address`* argument is the IP address, in dotted decimal notation, of the device to which you want to connect.
- The *`port`* argument is the number of t he port over which you want to open a telnet session.

traceroute (*ip_address* | *hostname*)

Traces the routing path to an IP destination.

upload [*server_address*] [*filename*] [confirm]

Copies the current configuration settings of the Netopia Gateway to a TFTP (Trivial File Transfer Protocol) server. The TFTP server must be accessible on your Ethernet network. The *`server_address`* argument identifies the IP address of the TFTP server on which you

want to store the Netopia Gateway settings. The *filename* argument identifies the path and name of the configuration file on the TFTP server. If you include the optional **confirm** keyword, you will not be prompted to confirm whether or not you want to perform the operation.

who

Displays the names of the current shell and PPP users.

WAN Commands

atmping vccn [*segment* | *end-to-end*]

Lets you check the ATM connection reachability and network connectivity. This command sends five Operations, Administration, and Maintenance (OAM) loopback calls to the specified vpi/vci destination. There is a five second total timeout interval.

Use the **segment** argument to ping a neighbor switch.
Use the **end-to-end** argument to ping a remote end node.

reset dhcp client release [*vcc-id*]

Releases the DHCP lease the Netopia Gateway is currently using to acquire the IP settings for the specified DSL port. The ***vcc-id*** identifier is a letter in the range B-I. Enter the **reset dhcp client release** without the variable to see the letter assigned to each virtual circuit.

reset dhcp client renew [*vcc-id*]

Releases the DHCP lease the Netopia Gateway is currently using to acquire the IP settings for the specified DSL port. The ***vcc-id*** identifier is a letter in the range B-I. Enter the **reset dhcp client release** without the variable to see the letter assigned to each virtual circuit.

reset dsl

Resets any open DSL connection.

reset ppp *vccn*

Resets the point-to-point connection over the specified virtual circuit. This command only applies to virtual circuits that use PPP framing.

show atm [all]

Displays ATM statistics for the Netopia Gateway. The optional **`all`** argument displays a more detailed set of ATM statistics.

show config

Dumps the Netopia Gateway's configuration script just as the **`script`** command does in config mode.

show dsl

Displays DSL port statistics, such as upstream and downstream connection rates and noise levels.

show ppp [{ stats | lcp | ipcp }]

Displays information about open PPP links. You can display a subset of the PPP statistics by including an optional **`stats`**, **`lcp`**, or **`ipcp`** argument for the **`show ppp`** command.

start ppp vccn

Opens a PPP link on the specified virtual circuit.

view config

Dumps the Netopia Gateway's configuration just as the **`view`** command does in config mode.

About CONFIG Commands

You reach the configuration mode of the command line interface by typing ***configure*** (or any truncation of ***configure***, such as ***con*** or ***config***) at the CLI SHELL prompt.

CONFIG Mode Prompt

When you are in CONFIG mode, the CLI prompt consists of the name of the Netopia Gateway followed by your current **node** in the hierarchy and two right angle brackets (>>). For example, when you enter CONFIG mode (by typing ***config*** at the SHELL prompt), the **`Coconut (top)>>`** prompt reminds you that you are at the top of the CONFIG hierarchy. If you move to the **`ip`** node in the CONFIG hierarchy (by typing **`ip`** at the CONFIG prompt), the prompt changes to **`Coconut (ip)>>`** to identify your current location.

Some CLI commands are not available until certain conditions are met. For example, you must enable IP for an interface before you can enter IP settings for that interface.

Navigating the CONFIG Hierarchy

- **Moving from CONFIG to SHELL** — You can navigate from anywhere in the CONFIG hierarchy back to the SHELL level by entering **`quit`** at the CONFIG prompt and pressing RETURN.

```
Dogzilla (top)>> quit
Dogzilla >
```

- **Moving from *top* to a subnode** — You can navigate from the top node to a subnode by entering the node name (or the significant letters of the node name) at the CONFIG prompt and pressing RETURN. For example, you move to the IP subnode by entering **`ip`** and pressing RETURN.

```
Dogzilla (top)>> ip
Dogzilla (ip)>>
```

As a shortcut, you can enter the significant letters of the node name in place of the full node name at the CONFIG prompt. The significant characters of a node name are the letters that uniquely identify the node. For example, since no other CONFIG node starts with I, you could enter one letter ("**`i`**") to move to the IP node.

- **Jumping down several nodes at once** — You can jump down several levels in the CONFIG hierarchy by entering the complete path to a node.
- **Moving up one node** — You can move up through the CONFIG hierarchy one node at a time by entering the **`up`** command.

- **Jumping to the top node** — You can jump to the top level from anywhere in the CONFIG hierarchy by entering the **`top`** command.
- **Moving from one subnode to another** — You can move from one subnode to another by entering a partial path that identifies how far back to climb.
- **Moving from any subnode to any other subnode** — You can move from any subnode to any other subnode by entering a partial path that starts with a top-level CONFIG command.
- **Scrolling backward and forward through recent commands** — You can use the Up and Down arrow keys to scroll backward and forward through recent commands you have entered. When the command you want appears, press Enter to execute it.

Entering Commands in CONFIG Mode

CONFIG commands consist of keywords and arguments. Keywords in a CONFIG command specify the action you want to take or the entity on which you want to act. Arguments in a CONFIG command specify the values appropriate to your site. For example, the CONFIG command

set ip ethernet A *ip_address*

consists of two keywords (***ip***, and ***ethernet A***) and one argument (*ip_address*). When you use the command to configure your Gateway, you would replace the argument with a value appropriate to your site.

For example:

set ip ethernet A 192.31.222.57

Guidelines: CONFIG Commands

The following table provides guidelines for entering and formatting CONFIG commands.

Command component	Rules for entering CONFIG commands
Command verbs	CONFIG commands must start with a command verb (set, view, delete). You can truncate CONFIG verbs to three characters (set, vie, del). CONFIG verbs are case-insensitive. You can enter "SET," "Set," or "set."
Keywords	Keywords are case-insensitive. You can enter "Ethernet," "ETHERNET," or "ethernet" as a keyword without changing its meaning. Keywords can be abbreviated to the length that they are differentiated from other keywords.
Argument Text	Text strings can be as many as 64 characters long, unless otherwise specified. In some cases they may be as long as 255 bytes. Special characters are represented using backslash notation. Text strings may be enclosed in double (") or single (') quote marks. If the text string includes an embedded space, it must be enclosed in quotes. Special characters are represented using backslash notation.
Numbers	Enter numbers as integers, or in hexadecimal, where so noted.
IP addresses	Enter IP addresses in dotted decimal notation (0 to 255).

If a command is ambiguous or miskeyed, the CLI prompts you to enter additional information. For example, you must specify which virtual circuit you are configuring when you are setting up a Netopia Gateway.

Displaying Current Gateway Settings

You can use the ***view*** command to display the current CONFIG settings for your Netopia Gateway. If you enter the ***view*** command at the top level of the CONFIG hierarchy, the CLI displays the settings for all enabled functions. If you enter the ***view*** command at an intermediate node, you see settings for that node and its subnodes.

Step Mode: A CLI Configuration Technique

The Netopia Gateway command line interface includes a step mode to automate the process of entering configuration settings. When you use the CONFIG step mode, the command line interface prompts you for all required and optional information. You can then enter the configuration values appropriate for your site without having to enter complete CLI commands.

When you are in step mode, the command line interface prompts you to enter required and optional settings. If a setting has a default value or a current setting, the command line interface displays the default value for the command in parentheses. If a command has a limited number of acceptable values, those values are presented in brackets, with each value separated by a vertical line. For example, the following CLI step command indicates that the default value is **`off`** and that valid entries are limited to **`on`** and **`off`**.

```
option (off) [ on | off] : on
```

You can accept the default value for a field by pressing the Return key. To use a different value, enter it and press Return.

You can enter the CONFIG step mode by entering ***set*** from the top node of the CONFIG hierarchy. You can enter step mode for a particular service by entering ***set*** *`service_name`*`.` In stepping set mode (press Control-X <Return/Enter> to exit. For example:

```
Dogzilla (top)>> set system
...
system
   name (“Dogzilla”): Mycroft
   Diagnostic Level (High): medium
Stepping mode ended.
```

Validating Your Configuration

You can use the **`validate`** CONFIG command to make sure that your configuration settings have been entered correctly. If you use the **`validate`** command, the Netopia Gateway verifies that all required settings for all services are present and that settings are consistent.

```
Dogzilla (top)>> validate
Error: Subnet mask is incorrect
Global Validation did not pass
inspection!
```

You can use the **validate** command to verify your configuration settings at any time. Your Netopia Gateway automatically validates your configuration any time you save a modified configuration.

CONFIG Commands

This section describes the keywords and arguments for the various CONFIG commands.

DSL Commands

ATM Settings. You can use the CLI to set up each ATM virtual circuit.

set atm option {on | off }

Enables the WAN interface of the Netopia Gateway to be configured using the Asynchronous Transfer Mode (ATM) protocol.

set atm [vcc *n*] option {on | off }

Selects the virtual circuit for which further parameters are set. Up to eight VCCs are supported; the maximum number is dependent on your Netopia Operating System tier and the capabilities that your Service Provider offers.

set atm [vcc *n*] qos service-class { cbr | ubr | vbr }

Sets the Quality of Service class for the specified virtual circuit – Constant (**cbr**), Unspecified (**ubr**), or Variable (**vbr**) Bit Rate.

- **ubr**: No configuration is needed for UBR VCs. Leave the default value 0 (maximum line rate).

- **cbr**: One parameter is required for CBR VCs. Enter the **Peak Cell Rate** that applies to the VC. This value should be between 1 and the line rate. You set this value according to specifications defined by your service provider.
- **vbr**: Three parameters are required for VBR VCs. Enter the **Peak Cell Rate**, the **Sustained Cell Rate**, and the **Maximum Burst Size** that apply to the VC. You set these values according to specifications defined by your service provider.

set atm [vcc *n*] qos peak-cell-rate { 1 ...*n* }

If QoS class is set to **cbr** or **vbr** then specify the **peak-cell-rate** that should apply to the specified virtual circuit. This value should be between 1 and the line rate.

The Peak Cell Rate (PCR) should be set to the maximum rate a PVC can oversubscribe its Sustained Cell Rate (SCR). The Peak Cell Rate (see below) must be less than, or equal to the raw WAN (DSL) bit rate. The Maximum Burst Size (MBS) is the number of cells that can be sent at the PCR rate, after which the PVC must fall back to the SCR rate.

set atm [vcc *n*] qos sustained-cell-rate { 1 ...*n* }

If QoS class is set to **vbr**, then specify the **sustained-cell-rate** that should apply to the specified virtual circuit. This value should be less than, or equal to the Peak Cell Rate, which should be less than, or equal to the line rate.

set atm [vcc *n*] qos max-burst-size { 1 ...*n* }

If QoS class is set to **vbr** then specify the **max-burst-size** that should apply to the specified virtual circuit. This value is the maximum number of cells that can be transmitted at the Peak Cell Rate after which the ATM VC transmission rate must drop to the Sustained Cell Rate.

set atm [vcc *n*] vpi { 0 ... 255 }

Select the virtual path identifier (vpi) for VCC n.

Your Service Provider will indicate the required vpi number.

set atm [vcc *n*] vci { 0 ... 65535 }

Select the virtual channel identifier (vci) for VCC n. Your Service Provider will indicate the required vci number.

set atm [vccn] encap { ppp-vcmux | ppp-llc | ether-llc | ip-llc | ppoe-vcmux | pppoe-llc }

Select the encapsulation mode for VCC n. The options are:

ppp-vcmux	PPP over ATM, VC-muxed
ppp-llc	PPP over ATM, LLC-SNAP
ether-llc	RFC-1483, bridged Ethernet, LLC-SNAP
ip-llc	RFC-1483, routed IP, LLC-SNAP
pppoe-vcmux	PPP over Ethernet, VC-muxed
pppoe-llc	PPP over Ethernet, LLC-SNAP

Your Service Provider will indicate the required encapsulation mode.

set atm [vccn] pppoe-sessions { 1 ... 8 }

Select the number of PPPoE sessions to be configured for VCC 1, up to a total of eight. The total number of **pppoe-sessions** and PPPoE VCCs configured must be less than or equal to eight.

Bridging Settings

Bridging lets the Netopia Gateway use MAC (Ethernet hardware) addresses to forward non-TCP/IP traffic from one network to another. When bridging is enabled, the Netopia Gateway maintains a table of up to 512 MAC addresses. Entries that are not used within 30 seconds are dropped. If the bridging table fills up, the oldest table entries are dropped to make room for new entries.

Virtual circuits that use IP framing cannot be bridged.

NOTE:

For bridging in the 2241 (or any model with a USB port), you cannot set the **bridge option off**, or **bridge ethernet option off**; these are on by default because of the USB port.

Common Commands

set bridge sys-bridge {on l off }

Enables or disables bridging services in the Netopia Gateway. You must enable bridging services within the Netopia Gateway before you can enable bridging for a specific interface.

set bridge concurrent-bridging-routing {on l off }

Enables or disables Concurrent Bridging/Routing.

set bridge ethernet option { on l off }

Enables or disables bridging services for the specified virtual circuit using Ethernet framing.

set bridge dsl vcc*n* option { on l off }

Enables or disables bridging services for the specified interface. Specified interface must be part of a VLAN if bridge is turned **on**. Only RFC-1483 Bridged encapsulation is supported currently.

- **show log** command will show that WAN Bridge is enabled when at least one WAN interface is bridged.
- **show ip interfaces** and **show bridge interfaces** commands will show the interfaces that are not in bridged mode and that are in bridged modes, respectively.

set bridge table-timeout [30 ... 6000]

Sets the timeout value for bridging table timeout. Default = 30 secs; range = 30 secs – 6000 secs (1–100 mins).

DHCP Settings

As a Dynamic Host Control Protocol (DHCP) server, your Netopia Gateway can assign IP addresses and provide configuration information to other devices on your network dynamically. A device that acquires its IP address and other TCP/IP configuration settings from the Netopia Gateway can use the information for a fixed period of time (called the DHCP lease).

Common Commands

set dhcp option { off | server | relay-agent }

Enables or disables DHCP services in the Netopia Gateway. You must enable DHCP services before you can enter other DHCP settings for the Netopia Gateway.

If you turn off DHCP services and save the new configuration, the Netopia Gateway clears its DHCP settings.

set dhcp start-address *ip_address*

If you selected **`server`**, specifies the first address in the DHCP address range. The Netopia Gateway can reserve a sequence of up to 253 IP addresses within a subnet, beginning with the specified address for dynamic assignment.

set dhcp end-address *ip_address*

If you selected **`server`**, specifies the last address in the DHCP address range.

set dhcp lease-time *lease-time*

If you selected **`server`**, specifies the default length for DHCP leases issued by the Netopia Gateway. Enter lease time in **`dd:hh:mm:ss`** (day/hour/minute/second) format.

set dhcp server-address *ip_address*

If you selected **`relay-agent`**, specifies the IP address of the relay agent server.

DMT Settings

DSL Commands

set dmt type [lite | dmt | ansi | multi]

Selects the type of Discrete Multitone (DMT) asynchronous digital subscriber line (ADSL) protocol to use for the WAN interface.

NOTE:

dmt type is not supported for Annex B (335x) platforms.

set dmt autoConfig [off | on]

Enables support for automatic VPI/VCI detection and configuration. When set to **on** (the default), a pre-defined list of VPI/VCI pairs are searched to find a valid configuration for your ADSL line. Entering a value for the VPI or VCI setting will disable this feature.

set dmt wiringMode [auto | tip_ring | A_A1]

(not supported on all models) This command configures the wiring mode setting for your ADSL line. Selecting **auto** (the default) causes the Gateway to detect which pair of wires (inner or outer pair) are in use on your phone line. Specifying **tip_ring** forces the inner pair to be used; and **A_A1** the outer pair.

Domain Name System Settings

Domain Name System (DNS) is an information service for TCP/IP networks that uses a hierarchical naming system to identify network domains and the hosts associated with them. You can identify a primary DNS server and one secondary server.

Common Commands

set dns domain-name *domain-name*

Specifies the default domain name for your network. When an application needs to resolve a host name, it appends the default domain name to the host name and asks the DNS server if it has an address for the “fully qualified host name.”

set dns primary-address *ip_address*

Specifies the IP address of the primary DNS name server.

set dns proxy-enable

This allows you to disable the default behavior of acting as a DNS proxy. The default is **on**.

set dns secondary-address *ip_address*

Specifies the IP address of the secondary DNS name server. Enter ***0.0.0.0*** if your network does not have a secondary DNS name server.

Dynamic DNS Settings

These commands are supported beginning with Firmware Version 7.4.2.

Dynamic DNS support allows you to use the free services of *www.dyndns.org*. Dynamic DNS automatically directs any public Internet request for your computer's name to your current dynamically-assigned IP address. This allows you to get to the IP address assigned to your Gateway, even though your actual IP address may change as a result of a PPPoE connection to the Internet.

set dynamic-dns option [off | dyndns.org]
set dynamic-dns ddns-host-name *myhostname*.dyndns.org
set dynamic-dns ddns-user-name *myusername*
set dynamic-dns ddns-user-password *myuserpassword*

Enables or disables dynamic DNS services. The default is **off**. If you specify **dyndns.org**, you must supply your hostname, username for the service, and password.

Because different dynamic DNS vendors use different proprietary protocols, currently only www.dyndns.org is supported.

IGMP Settings

These commands are supported beginning with Firmware Version 7.5.1.

set igmp snooping [off | on]

Enables IGMP Snooping. Enables the Netopia Gateway to “listen in” to IGMP traffic. The Gateway discovers multicast group membership for the purpose of restricting multicast transmissions to only those ports which have requested them. This helps to reduce overall network traffic from streaming media and other bandwidth-intensive IP multicast applications.

set igmp robustness *value*

Sets IGMP robustness range: from 2 – 255. The default is 2. Robustness is a way of indicating how sensitive to lost packets the network is. IGMP can recover from robustness minus 1 lost IGMP packet. The default value is 2.

set igmp query-intvl *value*

Sets the query-interval range: from 10 seconds – 600 seconds, The default is 125 seconds.

set igmp query-response-intvl *value*

Sets the query-response interval range: from 5 deci-seconds (tenths of a second) – 255 deci-seconds. The default is 100 deci-seconds.

show group-mgmt

Displays the IGMP Snooping Table.

IP Settings

You can use the command line interface to specify whether TCP/IP is enabled, identify a default Gateway, and to enter TCP/IP settings for the Netopia Gateway LAN and WAN ports.

NOTE:

For the DSL platform you must identify the virtual PPP interface [**vccn**], a number from 1 to 8.

Common Settings

set ip option { on | off }

Enables or disables TCP/IP services in the Netopia Gateway. You must enable TCP/IP services before you can enter other TCP/IP settings for the Netopia Gateway. If you turn off

TCP/IP services and save the new configuration, the Netopia Gateway clears its TCP/IP settings.

ARP Timeout Settings

set ip arp-timeout [60 ... 6000]

Sets the timeout value for ARP timeout. Default = 600 secs (10 mins); range = 60 secs - 6000 secs (1–100 mins).

DSL Settings

set ip dsl vccn address *ip_address*

Assigns an IP address to the virtual circuit. Enter 0.0.0.0 if you want the virtual circuit to obtain its IP address from a remote DHCP server.

set ip dsl vccn broadcast *broadcast_address*

Specifies the broadcast address for the TCP/IP network connected to the virtual circuit. IP hosts use the broadcast address to send messages to every host on your network simultaneously.

The broadcast address for most networks is the network number followed by 255. For example, the broadcast address for the 192.168.1.0 network would be 192.168.1.255.

set ip dsl vccn netmask *netmask*

Specifies the subnet mask for the TCP/IP network connected to the virtual circuit. The subnet mask specifies which bits of the 32-bit binary IP address represents network information. The default subnet mask for most networks is 255.255.255.0 (Class C subnet mask).

set ip dsl *vccn* restriction { admin-disabled l none }

Specifies restrictions on the types of traffic the Netopia Gateway accepts over the DSL virtual circuit. The **`admin-disabled`** argument means that access to the device via telnet, web, and SNMP is disabled. RIP and ICMP traffic is still accepted. The **`none`** argument means that all traffic is accepted.

set ip dsl vccn addr-mapping { on | off }

Specifies whether you want the Netopia Gateway to use network address translation (NAT) when communicating with remote routers. Address mapping lets you conceal details of your network from remote routers. It also permits all LAN devices to share a single IP address. By default, address mapping is turned “On”.

set ip dsl vccn rip-send { off | v1 | v2 | v1-compat | v2-MD5 }

Specifies whether the Netopia Gateway should use Routing Information Protocol (RIP) broadcasts to advertise its routing tables to other routers. RIP Version 2 (RIP-2) is an extension of the original Routing Information Protocol (RIP-1) that expands the amount of useful information in the RIP packets. While RIP-1 and RIP-2 share the same basic algorithms, RIP-2 supports several additional features, including inclusion of subnet masks in RIP packets and implementation of multicasting instead of broadcasting (which reduces the load on hosts which do not support routing protocols. RIP-2 with MD5 authentication is an extension of RIP-2 that increases security by requiring an authentication key when routes are advertised.

Depending on your network needs, you can configure your Netopia Gateway to support RIP-1, RIP-2, or RIP-2MD5.

If you specify **v2-MD5**, you must also specify a **rip-send-key**. Keys are ASCII strings with a maximum of 31 characters, and must match the other router(s) keys for proper operation of MD5 support.

set ip dsl vccn rip-receive { off | v1 | v2 | v1-compat | v2-MD5 }

Specifies whether the Netopia Gateway should use Routing Information Protocol (RIP) broadcasts to update its routing tables with information received from other routers.

If you specify **v2-MD5**, you must also specify a **rip-receive-key**. Keys are ASCII strings with a maximum of 31 characters, and must match the other router(s) keys for proper operation of MD5 support.

Ethernet LAN Settings

set ip ethernet option { on | off }

Enables or disables communications through the designated Ethernet port in the Gateway. You must enable TCP/IP functions for an Ethernet port before you can configure its network settings.

set ip ethernet A address *ip_address*

Assigns an IP address to the Netopia Gateway on the local area network. The IP address you assign to the local Ethernet interface must be unique on your network. By default, the Netopia Gateway uses 192.168.1.254 as its LAN IP address.

set ip ethernet A broadcast *broadcast_address*

Specifies the broadcast address for the local Ethernet interface. IP hosts use the broadcast address to send messages to every host on your network simultaneously.

The broadcast address for most networks is the network number followed by 255. For example, the broadcast address for the 192.168.1.0 network would be 192.168.1.255.

set ip ethernet A netmask *netmask*

Specifies the subnet mask for the local Ethernet interface. The subnet mask specifies which bits of the 32-bit binary IP address represent network information. The default subnet mask for most networks is 255.255.255.0 (Class C subnet mask).

set ip ethernet [A | B] restrictions { none | admin-disabled }

Specifies whether an administrator can open a telnet connection to a Netopia Gateway over an Ethernet interface (**A** = the LAN; **B** = the WAN, in the case of Ethernet WAN models) to monitor and configure the unit.

The **admin-disabled** argument prevents access to the device via telnet, web, and SNMP.

By default, administrative restrictions are **none** on the LAN, but **admin-disabled** is set on the WAN. This means that, by default, an administrator can open, for example, a telnet connection from the LAN, but not the WAN.

set ip ethernet A rip-send { off | v1 | v2 | v1-compat | v2-MD5 }

Specifies whether the Netopia Gateway should use Routing Information Protocol (RIP) broadcasts to advertise its routing tables to other routers on your network. RIP Version 2 (RIP-2) is an extension of the original Routing Information Protocol (RIP-1) that expands the amount of useful information in the RIP packets. While RIP-1 and RIP-2 share the same basic algorithms, RIP-2 supports several additional features, including inclusion of subnet masks in RIP packets and implementation of multicasting instead of broadcasting (which reduces the load on hosts which do not support routing protocols. RIP-2 with MD5 authentication is an extension of RIP-2 that increases security by requiring an authentication key when routes are advertised.

If you specify **v2-MD5**, you must also specify a **rip-send-key**. Keys are ASCII strings with a maximum of 31 characters, and must match the other router(s) keys for proper operation of MD5 support.

Depending on your network needs, you can configure your Netopia Gateway to support RIP-1, RIP-2, or RIP-2MD5.

set ip ethernet A rip-receive { off | v1 | v2 | v1-compat | v2-MD5 }

Specifies whether the Netopia Gateway should use Routing Information Protocol (RIP) broadcasts to update its routing tables with information received from other routers on your network.

If you specify **v2-MD5**, you must also specify a **rip-receive-key**. Keys are ASCII strings with a maximum of 31 characters, and must match the other router(s) keys for proper operation of MD5 support.

Default IP Gateway Settings

set ip gateway option { on | off }

Specifies whether the Netopia Gateway should send packets to a default Gateway if it does not know how to reach the destination host.

set ip gateway interface { ip-address | ppp-vccn }

Specifies how the Netopia Gateway should route information to the default Gateway. If you select **ip-address**, you must enter the IP address of a host on a local or remote network. If you specify **ppp**, the Netopia unit uses the default gateway being used by the remote PPP peer.

IP-over-PPP Settings. Use the following commands to configure settings for routing IP over a virtual PPP interface.

NOTE:

For a DSL platform you must identify the virtual PPP interface [**vccn**], a number from 1 to 8.

set ip ip-ppp [*vccn*] option { on l off }

Enables or disables IP routing through the virtual PPP interface. By default, IP routing is turned on. If you turn off IP routing and save the new configuration, the Netopia Gateway clears IP routing settings

set ip ip-ppp [*vccn*] address *ip_address*

Assigns an IP address to the virtual PPP interface. If you specify an IP address other than 0.0.0.0, your Netopia Gateway will not negotiate its IP address with the remote peer. If the remote peer does not accept the IP address specified in the *ip_address* argument as valid, the link will not come up.

The default value for the *ip_address* argument is 0.0.0.0, which indicates that the virtual PPP interface will use the IP address assigned to it by the remote peer. Note that the remote peer must be configured to supply an IP address to your Netopia Gateway if you enter 0.0.0.0 for the *ip_address* argument.

set ip ip-ppp [*vccn*] peer-address *ip_address*

Specifies the IP address of the peer on the other end of the PPP link. If you specify an IP address other than 0.0.0.0, your Netopia Gateway will not negotiate the remote peer's IP

address. If the remote peer does not accept the address in the *ip_address* argument as its IP address (typically because it has been configured with another IP address), the link will not come up.

The default value for the *ip_address* argument is 0.0.0.0, which indicates that the virtual PPP interface will accept the IP address returned by the remote peer. If you enter 0.0.0.0, the peer system must be configured to supply this address.

set ip ip-ppp [*vccn*] restriction { admin-disabled | none }

Specifies restrictions on the types of traffic the Netopia Gateway accepts over the PPP virtual circuit. The **admin-disabled** argument means that access to the device, via telnet, web and SNMP is disabled. The **none** argument means that all traffic is accepted.

set ip ip-ppp [*vccn*] addr-mapping { on | off }

Specifies whether you want the Netopia Gateway to use network address translation (NAT) when communicating with remote routers. Network address translation lets you conceal details of your network from remote routers. By default, address mapping is turned on.

set ip ip-ppp [*vccn*] rip-send { off | v1 | v2 | v1-compat | v2-MD5 }

Specifies whether the Netopia Gateway unit should use Routing Information Protocol (RIP) broadcasts to advertise its routing tables to routers on the other side of the PPP link. An extension of the original Routing Information Protocol (RIP-1), RIP Version 2 (RIP-2) expands the amount of useful information in the packets. While RIP-1 and RIP-2 share the same basic algorithms, RIP-2 supports several new features. For example, inclusion of subnet masks in RIP packets and implementation of multicasting instead of broadcasting. This last feature reduces the load on hosts which do not support routing protocols. RIP-2 with MD5 authentication is an extension of RIP-2 that increases security by requiring an authentication key when routes are advertised.

This command is only available when address mapping for the specified virtual circuit is turned “off”.

If you specify **v2-MD5**, you must also specify a **rip-send-key**. Keys are ASCII strings with a maximum of 31 characters, and must match the other router(s) keys for proper operation of MD5 support.

set ip ip-ppp [*vccn*] rip-receive { off | v1 | v2 | v1-compat | v2-MD5 }

Specifies whether the Netopia Gateway should use Routing Information Protocol (RIP) broadcasts to update its routing tables with information received from other routers on the other side of the PPP link.

If you specify **v2-MD5**, you must also specify a **rip-receive-key**. Keys are ASCII strings with a maximum of 31 characters, and must match the other router(s) keys for proper operation of MD5 support.

Static ARP Settings

Your Netopia Gateway maintains a dynamic Address Resolution Protocol (ARP) table to map IP addresses to Ethernet (MAC) addresses. Your Netopia Gateway populates this ARP table dynamically, by retrieving IP address/MAC address pairs only when it needs them. Optionally, you can define static ARP entries to map IP addresses to their corresponding Ethernet MAC addresses. Unlike dynamic ARP table entries, static ARP table entries do not time out.

You can configure as many as 16 static ARP table entries for a Netopia Gateway. Use the following commands to add static ARP entries to the Netopia Gateway static ARP table:

set ip static-arp `ip-address` *ip_address*

Specifies the IP address for the static ARP entry. Enter an IP address in the *`ip_address`* argument in dotted decimal format. The *`ip_address`* argument cannot be 0.0.0.0.

set ip static-arp `ip-address` *ip_address* `hardware-address` *MAC_address*

Specifies the Ethernet hardware address for the static ARP entry. Enter an Ethernet hardware address in the *`MAC_address`* argument in ***nn.nn.nn.nn.nn.nn*** (hexadecimal) format.

IGMP Forwarding

set ip igmp-forwarding [off | on]

Turns IP IGMP forwarding off or on. The default is off.

IPsec Passthrough

set ip ipsec-passthrough [off | on]

Turns IPsec client passthrough off or on. The default is on.

IP Prioritization

set ip prioritize [off l on]

Allows you to support traffic that has the TOS bit set. This defaults to **off**.

Differentiated Services (DiffServ)

The commands in this section are supported beginning with Firmware Version 7.4.2.

set diffserv option [off l on]

Turns the DiffServ option **off** (default) or **on**. **on** enables the service and IP TOS bits are used, even if no flows are defined. Consequently, if the end-point nodes provide TOS settings from an application that can be interpreted as one of the supported states, the Gateway will handle it as if it actively marked the TOS field itself.

NOTE:

The Gateway itself will not override TOS bit settings made by the endpoints. Support for source-provided IP TOS priorities within the Gateway is achieved simply by turning the DiffServe option “on” and by setting the lohi-asymmetry to adjust the behavior of the Gateway’s internal queues.

set diffserv lohi-ratio [60 - 100 percent]

Sets a percentage between 60 and 100 used to regulate the level of packets allowed to be pending in the low priority queue. The default is 92. It can be used in some degree to adjust the relative throughput bandwidth for low- versus high-priority traffic.

set diffserv custom-flows name *name*
protocol [TCP | UDP | ICMP | other]
direction [outbound | inbound | both]
start-port [0 - 49151]
end-port [0 - 49151]
inside-ip *inside-ip-addr*
outside-ip *outside-ip-addr*
qos [off | assure | expedite]

Defines or edits a custom flow. Select a ***name*** for the custom-flow from the **set** command. The CLI will step into the newly-named or previously-defined flow for editing.

- **protocol** – Allows you to choose the IP protocol for the stream: **TCP**, **UDP**, **ICMP**, or **other**.

  other is appropriate for setting up flows on protocols with non-standard port definitions, for example, IPSEC or PPTP. If you select **other**, an additional field, **numbered-protocol** will appear with a range of 0–255. Choose the protocol number from this field.
- **direction** – Allows you to choose whether to apply the marking and gateway queue behavior for inbound packets, outbound packets, or to both. If the Gateway is used as an "edge" gateway, its more important function is to mark the packets for high-priority streams in the outbound direction.
- **start-port**/**end-port** – Allows you to specify a range of ports to check for a particular flow, if the protocol selection is TCP or UDP.
- **inside-ip** – If you want packets originating from a certain LAN IP address to be marked, enter the IP address here. If you leave the address equal to zero, this check is ignored for outbound packets. The check is always ignored for inbound packets. The DiffServe queuing function must be applied ahead of NAT; and, before NAT re-maps the inbound packets, all inbound packets are destined for the Gateway's WAN IP address.
- **outside-ip** – If you want packets destined for and originating from a certain WAN IP address to be marked, enter this address here. If you leave the address equal to zero, the outside address check is ignored. For outbound flows, the outside address is the destination IP address for the packets. For inbound packets, the outside address is the source IP address for the packets.
- **qos** – Allows you to specify the Quality of Service for the flow: **off**, **assure**, or **expedite**. These are used both to mark the IP TOS byte and to distribute packets into the queues as if they were marked by the source.

SIP Passthrough

set ip sip-passthrough [on | off]

Turns Session Initiation Protocol application layer gateway client passthrough on or off. The default is **on**.

Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging.

Static Route Settings

A static route identifies a manually configured pathway to a remote network. Unlike dynamic routes, which are acquired and confirmed periodically from other routers, static routes do not time out. Consequently, static routes are useful when working with PPP, since an intermittent PPP link may make maintenance of dynamic routes problematic.

You can configure as many as 32 static IP routes for a Netopia Gateway. Use the following commands to maintain static routes to the Netopia Gateway routing table:

set ip static-routes `destination-network` *net_address*

Specifies the network address for the static route. Enter a network address in the *`net_address`* argument in dotted decimal format. The *`net_address`* argument cannot be 0.0.0.0.

set ip static-routes `destination-network` *net_address* netmask *netmask*

Specifies the subnet mask for the IP network at the other end of the static route. Enter the *`netmask`* argument in dotted decimal format. The subnet mask associated with the destination network must represent the same network class (A, B, or C) or a lower class (such as a class C subnet mask for class B network number) to be valid.

set ip static-routes destination-network *net_address* interface { ip-address | ppp-vccn }

Specifies the interface through which the static route is accessible.

set ip static-routes destination-network *net_address* gateway-address *gate_address*

Specifies the IP address of the Gateway for the static route. The default Gateway must be located on a network connected to the Netopia Gateway configured interface.

set ip static-routes destination-network *net_address* metric *integer*

Specifies the metric (hop count) for the static route. The default metric is 1. Enter a number from 1 to 15 for the integer argument to indicate the number of routers (actual or best guess) a packet must traverse to reach the remote network.

You can enter a metric of 1 to indicate either:

- The remote network is one router away and the static route is the best way to reach it;
- The remote network is more than one router away but the static route should not be replaced by a dynamic route, even if the dynamic route is more efficient.

set ip static-routes destination-network *net_address* rip-advertise [SplitHorizon | Always | Never]

Specifies whether the gateway should use Routing Information Protocol (RIP) broadcasts to advertise to other routers on your network and which mode to use. The default is **SplitHorizon.**

delete ip static-routes destination-network *net_address*

Deletes a static route. Deleting a static route removes all information associated with that route.

IPMaps Settings

set ip-maps name <*name*> internal-ip <*ip address*>

Specifies the name and static ip address of the LAN device to be mapped.

set ip-maps name <*name*> external-ip <*ip address*>

Specifies the name and static ip address of the WAN device to be mapped.

Up to 8 mapped static IP addresses are supported.

Network Address Translation (NAT) Default Settings

NAT default settings let you specify whether you want your Netopia Gateway to forward NAT traffic to a default server when it doesn't know what else to do with it. The NAT default host function is useful in situations where you cannot create a specific NAT pinhole for a traffic stream because you cannot anticipate what port number an application might use. For example, some network games select arbitrary port numbers when a connection is being opened. By identifying your computer (or another host on your network) as a NAT default server, you can specify that NAT traffic that would otherwise be discarded by the Netopia Gateway should be directed to a specific hosts.

set nat-default mode [off | default-server | ip-passthrough]

Specifies whether you want your Netopia Gateway to forward unsolicited traffic from the WAN to a default server or an IP passthrough host when it doesn't know what else to do with it.

set nat-default dhcp-enable [on | off]

Allows the IP passthrough host to acquire its IP address via DHCP, if **ip-passthrough** is enabled.

set nat-default { address *ip_address* | host-hardware-address *MAC_address* }

Specifies the IP address of the NAT default server or the hardware (MAC) address of the IP passthrough host.

Network Address Translation (NAT) Pinhole Settings

NAT pinholes let you pass specific types of network traffic through the NAT interfaces on the Netopia Gateway. NAT pinholes allow you to route selected types of network traffic, such as FTP requests or HTTP (Web) connections, to a specific host behind the Netopia Gateway transparently.

To set up NAT pinholes, you identify the type(s) of traffic you want to redirect by port number, and you specify the internal host to which each specified type of traffic should be directed.

The following list identifies protocol type and port number for common TCP/IP protocols:

- FTP (TCP 21)
- telnet (TCP 23)
- SMTP (TCP 25),
- TFTP (UDP 69)
- SNMP (TCP 161, UDP 161)

set pinhole name *name*

Specifies the identifier for the entry in the router's pinhole table. You can name pinhole table entries sequentially (1, 2, 3), by port number (21, 80, 23), by protocol, or by some other naming scheme.

set pinhole name *name* protocol-select { tcp | udp }

Specifies the type of protocol being redirected.

set pinhole name *name* external-port-start [0 - 49151]

Specifies the first port number in the range being translated.

set pinhole name *name* external-port-end [0 - 49151]

Specifies the last port number in the range being translated.

set pinhole name *name* internal-ip *internal-ip*

Specifies the IP address of the internal host to which traffic of the specified type should be transferred.

set pinhole name *name* internal-port *internal-port*

Specifies the port number your Netopia Gateway should use when forwarding traffic of the specified type. Under most circumstances, you would use the same number for the external and internal port.

PPPoE /PPPoA Settings

You can use the following commands to configure basic settings, port authentication settings, and peer authentication settings for PPP interfaces on your Netopia Gateway.

Configuring Basic PPP Settings.

NOTE:

For the DSL platform you must identify the virtual PPP interface [**vccn**], a number from 1 to 8.

set ppp module [vccn] option { on | off }

Enables or disables PPP on the Netopia Gateway.

set ppp module [vccn] auto-connect { on | off }

Supports manual mode required for some vendors. The default **on** is not normally changed. If auto-connect is disabled (**off**), you must manually start/stop a ppp connection.

set ppp module [vccn] mru *integer*

Specifies the Maximum Receive Unit (MRU) for the PPP interface. The *integer* argument can be any number between 128 and 1492 for PPPoE; 1500 otherwise.

set ppp module [vccn] magic-number { on | off }

Enables or disables LCP magic number negotiation.

set ppp module [vccn] protocol-compression { on | off }

Specifies whether you want the Netopia Gateway to compress the PPP Protocol field when it transmits datagrams over the PPP link.

set ppp module [vccn] lcp-echo-requests { on | off }

Specifies whether you want your Netopia Gateway to send LCP echo requests. You should turn off LCP echoing if you do not want the Netopia Gateway to drop a PPP link to a nonresponsive peer.

set ppp module [vccn] echo-period *integer*

Specifies the number of seconds the Netopia Gateway should wait before sending another echo from an LCP echo request. The integer argument can be any number from between 5 and 300 (seconds).

set ppp module [vccn] lost-echoes-max *integer*

Specifies the maximum number of lost echoes the Netopia Gateway should tolerate before bringing down the PPP connection. The integer argument can be any number from between 1 and 20.

set ppp module [vccn] failures-max *integer*

Specifies the maximum number of Configure-NAK messages the PPP module can send without having sent a Configure-ACK message. The integer argument can be any number between 1 and 20.

set ppp module [vccn] configure-max *integer*

Specifies the maximum number of unacknowledged configuration requests that your Netopia Gateway will send. The integer argument can be any number between 1 and 10.

set ppp module [vccn] terminate-max *integer*

Specifies the maximum number of unacknowledged termination requests that your Netopia Gateway will send before terminating the PPP link. The integer argument can be any number between 1 and 10.

set ppp module [vccn] restart-timer *integer*

Specifies the number of seconds the Netopia Gateway should wait before retransmitting a configuration or termination request. The integer argument can be any number between 1 and 30.

set ppp module [vccn] connection-type { instant-on | always-on }

Specifies whether a PPP connection is maintained by the Netopia Gateway when it is unused for extended periods. If you specify **`always-on`**, the Netopia Gateway never shuts down the PPP link. If you specify **`instant-on`**, the Netopia Gateway shuts down the PPP link after the number of seconds specified in the **`time-out`** setting (below) if no traffic is moving over the circuit.

set ppp module [vccn] time-out *integer*

If you specified a connection type of **`instant-on`**, specifies the number of seconds, in the range 30 - 3600, with a default value of 300, the Netopia Gateway should wait for communication activity before terminating the PPP link.

Configuring Port Authentication. You can use the following command to specify how your Netopia Gateway should respond when it receives an authentication request from a remote peer.

The settings for port authentication on the local Netopia Gateway must match the authentication that is expected by the remote peer. For example, if the remote peer requires CHAP authentication and has a name and CHAP secret for the Netopia Gateway, you must enable CHAP and specify the same name and secret on the Netopia Gateway before the link can be established.

set ppp module [vccn] port-authentication

option [off | on | pap-only | chap-only]

Specifying **on** turns both PAP and CHAP on, or you can select PAP or CHAP. Specify the **username** and **password** when port authentication is turned on (both CHAP and PAP, CHAP or PAP.) Authentication must be enabled before you can enter other information.

set ppp module [vccn] port-authentication username *username*

The **username** argument is 1- 255 alphanumeric characters. The information you enter must match the username configured in the PPP peer's authentication database.

set ppp module [vccn] port-authentication password *password*

The **password** argument is 1-32 alphanumeric characters. The information you enter must match the password used by the PPP peer.

Ethernet Port Settings

set ethernet ethernet A mode { auto | 100M-full | 100M-full-fixed | 100M-half-fixed | 10M-full-fixed | 10M-half-fixed | 100M-half | 10M-full | 10M-half }

Allows mode setting for the ethernet port. Only supported on units without a LAN switch, or dual ethernet products (338x). In the dual ethernet case, “ethernet B” would be specified for the WAN port. The default is **auto**.

Command Line Interface Preference Settings

You can set command line interface preferences to customize your environment.

set preference verbose { on | off }

Specifies whether you want command help and prompting information displayed. By default, the command line interface verbose preference is turned off. If you turn it on, the command line interface displays help for a node when you navigate to that node.

set preference more *lines*

Specifies how many lines of information you want the command line interface to display at one time. The lines argument specifies the number of lines you want to see at one time. The range is 1-65535. By default, the command line interface shows you 22 lines of text before displaying the prompt: **More ...[yln] ?**.

If you enter 100 for the ***lines*** argument, the command line interface displays information as an uninterrupted stream (which is useful for capturing information to a text file).

Port Renumbering Settings

If you use NAT pinholes to forward HTTP or telnet traffic through your Netopia Gateway to an internal host, you must change the port numbers the Netopia Gateway uses for its own configuration traffic. For example, if you set up a NAT pinhole to forward network traffic on Port 80 (HTTP) to another host, you would have to tell the Netopia Gateway to listen for configuration connection requests on a port number other than 80, such as 6080.

After you have changed the port numbers the Netopia Gateway uses for its configuration traffic, you must use those port numbers instead of the standard numbers when configuring the Netopia Gateway. For example, if you move the router's Web service to port "6080" on a box with a system (DNS) name of "superbox", you would enter the URL ***http://superbox:6080*** in a Web browser to open the Netopia Gateway graphical user interface. Similarly, you would have to configure your telnet application to use the appropriate port when opening a configuration connection to your Netopia Gateway.

set servers web-http [1 - 65534]

Specifies the port number for HTTP (web) communication with the Netopia Gateway. Because port numbers in the range 0-1024 are used by other protocols, you should use numbers in the range 1025-65534 when assigning new port numbers to the Netopia Gateway web configuration interface. A setting of **0** (zero) will turn the server off.

set servers telnet-tcp [1 - 65534]

Specifies the port number for telnet (CLI) communication with the Netopia Gateway. Because port numbers in the range 0-1024 are used by other protocols, you should use numbers in the range 1025-65534 when assigning new port numbers to the Netopia Gateway telnet configuration interface. A setting of **0** (zero) will turn the server off.

NOTE:

You cannot specify a port setting of **0** (zero) for both the web and telnet ports at the same time. This would prevent you from accessing the Gateway.

Security Settings

Security settings include the Firewall and IPSec parameters. All of the security functionality is keyed.

Firewall Settings (for BreakWater Firewall)

set security firewall option [ClearSailing | SilentRunning | LANdLocked]

SafeHarbour IPSec Settings

SafeHarbour VPN is a tunnel between the local network and another geographically dispersed network that is interconnected over the Internet. This VPN tunnel provides a secure, cost-effective alternative to dedicated leased lines. Internet Protocol Security (IPsec) is a series of services including encryption, authentication, integrity, and replay protection. Internet Key Exchange (IKE) is the key management protocol of IPsec that establishes keys for encryption and decryption. Because this VPN software implementation is built to these standards, the other side of the tunnel can be either another Netopia unit or another IPsec/IKE based security product. For VPN you can choose to have traffic authenticated, encrypted, or both.

When connecting the Netopia unit in a telecommuting scenario, the corporate VPN settings will dictate the settings to be used in the Netopia unit. If a parameter has not been specified from the other end of the tunnel, choose the default unless you fully understand the ramifications of your parameter choice.

Parameter Descriptions

The following tables describe SafeHarbour's parameters that are used for an IPSec VPN tunnel configuration:

Table 1: IPSec Configuration page parameters

Field	Description
Name	The Name parameter refers to the name of the configured tunnel. This is mainly used as an identifier for the administrator. The Name parameter is an ASCII value and is limited to 31characters. The tunnel name is the only IPSec parameter that does not need to match the peer gateway.
Peer External IP Address	The Peer External IP Address is the public, or routable IP address of the remote gateway or VPN server you are establishing the tunnel with.
Encryption Protocol	Encryption protocol for the tunnel session. Parameter values supported include NONE or ESP.
Authentication Protocol	Authentication Protocol for IP packet header. The three parameter values are None, Encapsulating Security Payload (ESP) and Authentication Header (AH)
Key Management	The Key Management algorithm manages the exchange of security keys in the IPSec protocol architecture. SafeHarbour supports the standard Internet Key Exchange (IKE)

Table 2: IPSec Tunnel Details page parameters

Field	Description
Name	The Name parameter refers to the name of the configured tunnel. This is mainly used as an identifier for the administrator. The Name parameter is an ASCII value and is limited to 31characters. The tunnel name is the only IPSec parameter that does not need to match the peer gateway.
Peer Internal Network	The Peer Internal IP Network is the private, or Local Area Network (LAN) address of the remote gateway or VPN Server you are communicating with.
Peer Internal Netmask	The Peer Internal IP Netmask is the subnet mask of the Peer Internal IP Network.
NAT enable	Turns NAT on or off for this tunnel.

Table 2: IPSec Tunnel Details page parameters

PAT Address	If NAT is enabled, this field appears. You can specify a Port Address Translation (PAT) address or leave the default all-zeroes (if Xauth is enabled). If you leave the default. the address will be requested from the remote router and dynamically applied to the Gateway.
Negotiation Method	This parameter refers to the method used during the Phase I key exchange, or IKE process. SafeHarbour supports Main or Aggressive Mode. Main mode requires 3 two-way message exchanges while Aggressive mode only requires 3 total message exchanges.
Local ID type	If Aggressive mode is selected as the Negotiation Method, this option appears. Selection options are: IP Address, Subnet, Hostname, ASCII
Local ID Address/ Value	If Aggressive mode is selected as the Negotiation Method, this field appears. This is the local (Gateway-side) IP address (or Name Value, if Subnet or Hostname are selected as the Local ID Type).
Local ID Mask	If Aggressive mode is selected as the Negotiation Method, and Subnet as the Local ID Type, this field appears. This is the local (Gateway-side) subnet mask.
Remote ID Type	If Aggressive mode is selected as the Negotiation Method, this option appears. Selection options are: IP Address, Subnet, Hostname, ASCII.
Remote ID Address/Value	If Aggressive mode is selected as the Negotiation Method, this field appears. This is the remote (central-office-side) IP address (or Name Value, if Subnet or Hostname are selected as the Local ID Type).
Remote ID Mask	If Aggressive mode is selected as the Negotiation Method, and Subnet as the Remote ID Type, this field appears. This is the remote (central-office-side) subnet mask.
Pre-Shared Key Type	The Pre-Shared Key Type classifies the Pre-Shared Key. SafeHarbour supports ASCII or HEX types
Pre-Shared Key	The Pre-Shared Key is a parameter used for authenticating each side. The value can be ASCII or Hex and a maximum of 64 characters. ASCII is case-sensitive.
DH Group	Diffie-Hellman is a public key algorithm used between two systems to determine and deliver secret keys used for encryption. Groups 1, 2 and 5 are supported.
PFS Enable	Perfect Forward Secrecy (PFS) is used during SA renegotiation. When PFS is selected, a Diffie-Hellman key exchange is required. If enabled, the PFS DH group follows the IKE phase 1 DH group.
SA Encrypt Type	SA Encryption Type refers to the symmetric encryption type. This encryption algorithm will be used to encrypt each data packet. SA Encryption Type values supported include DES and 3DES.

Table 2: IPSec Tunnel Details page parameters

SA Hash Type	SA Hash Type refers to the Authentication Hash algorithm used during SA negotiation. Values supported include MD5 and SHA1. N/A will display if NONE is chosen for Auth Protocol.
Invalid SPI Recovery	Enabling this allows the Gateway to re-establish the tunnel if either the Netopia Gateway or the peer gateway is rebooted.
Soft MBytes	Setting the Soft MBytes parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Soft MByte value. The value can be configured between 1 and 1,000,000 MB and refers to data traffic passed. If this value is not achieved, the Hard MBytes parameter is enforced.
Soft Seconds	Setting the Soft Seconds parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Soft Seconds value. The value can be configured between 60 and 1,000,000 seconds.
Hard MBytes	Setting the Hard MBytes parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Hard MByte value. The value can be configured between 1 and 1,000,000 MB and refers to data traffic passed.
Hard Seconds	Setting the Hard Seconds parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Hard Seconds value. The value can be configured between 60 and 1,000,000 seconds
IPSec MTU	Some ISPs require a setting of e.g. 1492 (or other value). The default 1500 is the most common and you usually don't need to change this unless otherwise instructed. Accepted values are from 100 – 1500. This is the starting value that is used for the MTU when the IPSec tunnel is installed. It specifies the maximum IP packet length for the encapsulated AH or ESP packets sent by the router. The MTU used on the IPSec connection will be automatically adjusted based on the MTU value in any received ICMP *can't fragment* error messages that correspond to IPSec traffic initiated from the router. Normally the MTU only requires manual configuration if the ICMP error messages are blocked or otherwise not received by the router.

Table 2: IPSec Tunnel Details page parameters

Xauth Enable	Extended Authentication (XAuth), an extension to the Internet Key Exchange (IKE) protocol. The Xauth extension provides dual authentication for a remote user's Netopia Gateway to establish a VPN, authorizing network access to the user's central office. IKE establishes the tunnel, and Xauth authenticates the specific remote user's Gateway. Since NAT is supported over the tunnel, the remote user network can have multiple PCs behind the client Gateway accessing the VPN. By using XAuth, network VPN managers can centrally control remote user authentication.
Xauth Username/ Password	Xauth authentication credentials.

set security ipsec option (off) {on | off}

Turns on the SafeHarbour IPsec tunnel capability. Default is off.

set security ipsec tunnels name "123"

The name of the tunnel can be quoted to allow special characters and embedded spaces.

set security ipsec tunnels name "123" tun-enable (on) {on | off}

This enables this particular tunnel. Currently, one tunnel is supported.

set security ipsec tunnels name "123" dest-ext-address *ip-address*

Specifies the IP address of the destination gateway.

set security ipsec tunnels name "123" dest-int-network *ip-address*

Specifies the IP address of the destination computer or internal network.

set security ipsec tunnels name "123" dest-int-netmask *netmask*

Specifies the subnet mask of the destination computer or internal network. The subnet mask specifies which bits of the 32-bit IP address represents network information. The default subnet mask for most networks is 255.255.255.0 (class C subnet mask).

set security ipsec tunnels name "123" encrypt-protocol (ESP) { ESP | none }

set security ipsec tunnels name "123" auth-protocol (ESP) {AH | ESP | none}

set security ipsec tunnels name "123" IKE-mode pre-shared-key-type (hex) {ascii | hex}

set security ipsec tunnels name "123" IKE-mode pre-shared-key ("") {hex string}

Example: **0x1234**

set security ipsec tunnels name "123" IKE-mode neg-method {main | aggressive}

Note: *Aggressive Mode* is a little faster, but it does not provide identity protection for negotiations nodes.

set security ipsec tunnels name "123" IKE-mode DH-group (1) { 1 | 2 | 5}

set security ipsec tunnels name "123" IKE-mode isakmp-SA-encrypt (DES) { DES | 3DES }

set security ipsec tunnels name "123" IKE-mode ipsec-mtu *mtu_value*

This command is supported beginning with Version 7.4

The **M**aximum **T**ransmission **U**nit is a link layer restriction on the maximum number of bytes of data in a single transmission. The maximum allowable value (also the default) is 1500, and the minimum is 100.

set security ipsec tunnels name "123" IKE-mode isakmp-SA-hash (MD5) {MD5 | SHA1}

set security ipsec tunnels name "123" IKE-mode PFS-enable { off | on }

set security ipsec tunnels name "123" IKE-mode invalid-spi-recovery { off | on }

Enables the Gateway to re-establish the tunnel if either the Netopia Gateway or the peer gateway is rebooted.

set security ipsec tunnels name "123" xauth enable {off | on }

Enables or disables Xauth extensions to IPsec, when **IKE-mode neg-method** is set to **aggressive**. Default is **off**.

set security ipsec tunnels name "123" xauth username *username*

Sets the Xauth username, if Xauth is enabled.

set security ipsec tunnels name "123" xauth password *password*

Sets the Xauth password, if Xauth is enabled.

set security ipsec tunnels name "123" nat-enable { on | off }

Enables or disables NAT on the specified IPsec tunnel. The default is **off**.

set security ipsec tunnels name "123" nat-pat-address *ip-address*

Specifies the NAT port address translation IP address for the specified IPsec tunnel.

set security ipsec tunnels name "123" local-id-type { IP-address | Subnet | Hostname | ASCII }

Specifies the NAT local ID type for the specified IPsec tunnel.

set security ipsec tunnels name "123" local-id *id_value*

Specifies the NAT local ID value as specified in the **local-id-type** for the specified IPsec tunnel.

Note: If **subnet** is selected, the following two values are used instead:

set security ipsec tunnels name "123" local-id-addr *ip-address*

set security ipsec tunnels name "123" local-id-mask *ip-mask*

set security ipsec tunnels name "123" remote-id-type
{ IP-address | Subnet | Hostname | ASCII }

Specifies the NAT remote ID type for the specified IPsec tunnel.

set security ipsec tunnels name "123" remote-id *id_value*

Specifies the NAT remote ID value as specified in the **remote-id-type** for the specified IPsec tunnel.

Note: If **subnet** is selected, the following two values are used instead:

set security ipsec tunnels name "123" remote-id-addr *ip-address*
set security ipsec tunnels name "123" remote-id-mask *ip-mask*

Internet Key Exchange (IKE) Settings

The following four IPsec parameters configure the rekeying event.

set security ipsec tunnels name "123" IKE-mode ipsec-soft-mbytes (1000) {1-1000000}

set security ipsec tunnels name "123" IKE-mode ipsec-soft-seconds (82800) {60-1000000}

set security ipsec tunnels name "123" IKE-mode ipsec-hard-mbytes (1200) {1-1000000}

set security ipsec tunnels name "123" IKE-mode ipsec-hard-seconds (86400) {60-1000000}

- The **soft** parameters designate when the system negotiates a new key. For example, after 82800 seconds (23 hours) or 1 Gbyte has been transferred (whichever comes first) the key will be renegotiated.
- The **hard** parameters indicate that the renegotiation must be complete or the tunnel will be disabled. For example, 86400 seconds (24 hours) means that the renegotiation must be complete within one day.

Both ends of the tunnel set parameters, and typically they will be the same. If they are not the same, the rekey event will happen when the longest time period expires or when the largest amount of data has been sent.

Stateful Inspection

Stateful inspection options are accessed by the **security state-insp** tag.

set security state-insp [ip-ppp | dsl] vcc*n* option [off | on]
set security state-insp ethernet [A | B] option [off | on]

Sets the stateful inspection option **off** or **on** on the specified interface. This option is disabled by default. Stateful inspection prevents unsolicited inbound access when NAT is disabled.

set security state-insp [ip-ppp | dsl] vcc*n*
default-mapping [off | on]
set security state-insp ethernet [A | B]
default-mapping [off | on]

Sets stateful inspection default mapping to router option **off** or **on** on the specified interface.

set security state-insp [ip-ppp | dsl] vcc*n* tcp-seq-diff
[0 - 65535]
set security state-insp ethernet [A | B] tcp-seq-diff
[0 - 65535]

Sets the acceptable TCP sequence difference on the specified interface. The TCP sequence number difference maximum allowed value is 65535. If the value of **tcp-seq-diff** is 0, it means that this check is disabled.

set security state-insp [ip-ppp | dsl] vcc*n*
deny-fragments [off | on]
set security state-insp ethernet [A | B]
deny-fragments [off | on]

Sets whether fragmented packets are allowed to be received or not on the specified interface.

set security state-insp tcp-timeout [30 - 65535]

Sets the stateful inspection TCP timeout interval, in seconds.

set security state-insp udp-timeout [30 - 65535]

Sets the stateful inspection UDP timeout interval, in seconds.

set security state-insp xposed-addr exposed-address# "*n*"

Allows you to add an entry to the specified list, or, if the list does not exist, creates the list for the stateful inspection feature. **xposed-addr** settings only apply if NAT is off.

Example:

```
set security state-insp xposed-addr exposed-address#
(?): 32
```

32 has been added to the **xposed-addr** list.

Sets the exposed list address number.

set security state-insp xposed-addr exposed-address# "*n*" start-ip *ip_address*

Sets the exposed list range starting IP address, in dotted quad format.

set security state-insp xposed-addr exposed-address# "*n*" end-ip *ip_address*

Sets the exposed list range ending IP address, in dotted quad format.

32 exposed addresses can be created. The range for exposed address numbers are from 1 through 32.

set security state-insp xposed-addr exposed-address# "*n*" protocol [tcp | udp | both | any]

Sets the protocol for the stateful inspection feature for the exposed address list. Accepted values for **protocol** are **tcp**, **udp**, **both**, or **any**.

If **protocol** is not **any**, you can set port ranges:

set security state-insp xposed-addr exposed-address# "*n*" start-port [1 - 65535]

set security state-insp xposed-addr exposed-address# "*n*" end-port [1 - 65535]

Packet Filtering Settings

Packet Filtering settings are supported beginning with Firmware Version 7.4.

Packet Filtering has two parts:

- Create/Edit/Delete Filter Sets, create/edit/delete rules to a Filter Set.
- Associate a created Filter Set with an WAN or LAN interface

set security pkt-filter filterset *filterset-name* in *index* forward [on | off]

Creates or edits a filter rule, specifying whether packets will be forwarded or not.

NOTE:

If this is the first rule, it will create the filter-set called *filterset-name*, otherwise it will edit the filterset.
If the index is not consecutive, the system will select the next consecutive index. If the index does not exist, a rule will be created. If a rule exists, the rule will be edited.

set security pkt-filter filterset *filterset-name* in *index* idle-reset [on | off]

Turns idle reset on or off for the specified filter rule. A match on this rule resets idle-timeout status and keeps the WAN connection alive. The default is **off**.

set security pkt-filter filterset *filterset-name* in *index* frc-rte [on | off]

Turns forced routing on or off for the specified filter rule. A match on this rule will force a route for packets. The default is **off**.

set security pkt-filter filterset *filterset-name* in *index* gateway *ip_addr*

Specifies the gateway IP address for forced routed packets, if forced routing is enabled.

set security pkt-filter filterset *filterset-name* in *index* src-ip *ip_addr*

Specifies the source IP address to match packets (where the packet was sent from).

set security pkt-filter filterset *filterset-name* in *index* src-mask *mask*

Specifies the source IP mask to match packets (where the packet was sent from).

set security pkt-filter filterset *filterset-name* in *index* dest-ip *ip_addr*

Specifies the destination IP address to match packets (where the packet is going).

set security pkt-filter filterset *filterset-name* in *index* dest-mask *mask*

Specifies the destination IP mask to match packets (where the packet is going).

set security pkt-filter filterset *filterset-name* in *index* tos *value*

Specifies the TOS (Type Of Service) value to match packets. The value for **tos** can be from 0 – 255.

set security pkt-filter filterset *filterset-name* in *index* tos-mask *value*

Specifies the TOS (Type Of Service) mask to match packets. The value for **tos-mask** can be from 0 – 255.

set security pkt-filter filterset *filterset-name* in *index* protocol *value*

Specifies the protocol value to match packets, the type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP. The value for **protocol** can be from 0 – 255.

set security pkt-filter filterset *filterset-name* in *index*

src-compare [nc | ne | lt | le | eq | gt | ge]

Sets the source compare operator action for the specified filter rule.

Operator	Action
nc	No compare
ne	Not equal to
lt	Less than
le	Less than or equal to
eq	Equal to
ge	Greater than or equal to
gt	Greater than

set security pkt-filter filterset *filterset-name* in *index* dst-compare [nc | ne | lt | le | eq | gt | ge]

Sets the destination compare operator action for the specified filter rule.

Operator	Action
nc	No compare
ne	Not equal to
lt	Less than
le	Less than or equal to
eq	Equal to
ge	Greater than or equal to
gt	Greater than

set security pkt-filter filterset *filterset-name* in *index* src-port *value*

Specifies the source IP port to match packets (the port on the sending host that originated the packet, if the underlying protocol is TCP or UDP).

set security pkt-filter filterset *filterset-name* in *index* dst-port *value*

Specifies the destination IP port to match packets (the port on the receiving host that the packet is destined for, if the underlying protocol is TCP or UDP).

SNMP Settings

The Simple Network Management Protocol (SNMP) lets a network administrator monitor problems on a network by retrieving settings on remote network devices. The network administrator typically runs an SNMP management station program on a local host to obtain information from an SNMP agent such as the Netopia Gateway.

set snmp community read *name*

Adds the specified name to the list of communities associated with the Netopia Gateway. By default, the Netopia Gateway is associated with the public community.

set snmp community write *name*

Adds the specified name to the list of communities associated with the Netopia Gateway.

set snmp community trap *name*

Adds the specified name to the list of communities associated with the Netopia Gateway.

set snmp trap ip-traps *ip-address*

Identifies the destination for SNMP trap messages. The *`ip-address`* argument is the IP address of the host acting as an SNMP console.

set snmp sysgroup contact *contact_info*

Identifies the system contact, such as the name, phone number, beeper number, or email address of the person responsible for the Netopia Gateway. You can enter up to 255 characters for the *`contact_info`* argument. You must put the *`contact_info`* argument in double-quotes if it contains embedded spaces.

set snmp sysgroup location *location_info*

Identifies the location, such as the building, floor, or room number, of the Netopia Gateway. You can enter up to 255 characters for the *location_info* argument. You must put the *location_info* argument in double-quotes if it contains embedded spaces.

SNMP Notify Type Settings

SNMP Notify Type is supported beginning with Firmware Version 7.4.2.

set snmp notify type [v1-trap | v2-trap | inform]

Sets the type of SNMP notifications that the system will generate:

- **v1-trap** – This selection will generate notifications containing an SNMPv1 Trap *Protocol Data Unit* (PDU)
- **v2-trap** – This selection will generate notifications containing an SNMPv2 Trap PDU
- **inform** – This selection will generate notifications containing an SNMPv2 InformRequest PDU.

System Settings

You can configure system settings to assign a name to your Netopia Gateway and to specify what types of messages you want the diagnostic log to record.

set system name *name*

Specifies the name of your Netopia Gateway. Each Netopia Gateway is assigned a name as part of its factory initialization. The default name for a Netopia Gateway consists of the word “Netopia-3000/XXX” where “XXX” is the serial number of the device; for example, Netopia-3000/9437188. A system name can be 1 – 255 characters long. Once you have assigned a name to your Netopia Gateway, you can enter that name in the ***Address*** text field of your browser to open a connection to your Netopia Gateway.

NOTE:

Some broadband cable-oriented Service Providers use the **System Name** as an important identification and support parameter. If your Gateway is part of

this type of network, do **NOT** alter the System Name unless specifically instructed by your Service Provider.

set system diagnostic-level { off | low | medium | high | alerts | failures }

Specifies the types of log messages you want the Netopia Gateway to record. All messages with a level equal to or greater than the level you specify are recorded. For example, if you specify set system diagnostic-level **medium**, the diagnostic log will retain medium-level informational messages, alerts, and failure messages. Specifying **off** turns off logging.

Use the following guidelines:

- **low** - Low-level informational messages or greater; includes trivial status messages.
- **medium** - Medium-level informational messages or greater; includes status messages that can help monitor network traffic.
- **high** - High-level informational messages or greater; includes status messages that may be significant but do not constitute errors. The default.
- **alerts** - Warnings or greater; includes recoverable error conditions and useful operator information.
- **failures** - Failures; includes messages describing error conditions that may not be recoverable.

set system log-size [10240... 65536]

Specifies a size for the system log. The most recent entries are posted to the beginning of the log. When the log becomes full, the oldest entries are dropped. The default is 30000.

set system persistent-log [off | on]

When set to **on**, causes the log information to be kept in flash memory.

set system idle-timeout { telnet [1...120] | http [1... 120] }

Specifies a timeout period of inactivity for telnet or HTTP access to the Gateway, after which a user must re-login to the Gateway. Defaults are 5 minutes for HTTP and 15 minutes for telnet.

set system username { administrator *name* | user *name* }

Specifies the usernames for the administrative user – the default is **admin**; and a non-administrative user – the default is **user**.

set system password { admin | user }

Specifies the administrator or user password for a Netopia Gateway. When you enter the **`set system password`** command, you are prompted to enter the old password (if any) and new password. You are prompted to repeat the new password to verify that you entered it correctly the first time. To prevent anyone from observing the password you enter, characters in the old and new passwords are not displayed as you type them. For security, you cannot use the "step" method to set the system password.

A password can be as many as 8 characters. Passwords are case-sensitive.

Passwords go into effect immediately. You do not have to restart the Netopia Gateway for the password to take effect. Assigning an administrator or user password to a Netopia Gateway does not affect communications through the device.

set system heartbeat option { on | off }
protocol [udp | tcp]
port-client [1 - 65535]
ip-server *ip_address*
port-server [1 - 65535]
url-server ("*server_name*")
number [1 – 1073741823]
interval (00:00:00:20)
sleep (00:00:30:00)
contact-email ("*string@domain_name*")
location ("*string*"):

The heartbeat setting is used in conjunction with the configuration server to broadcast contact and location information about your Gateway. You can specify the **protocol**, **port**, **IP**-, **port**-, and **URL-server**.

- The **interval** setting specifies the broadcast update frequency. Part of sequence control. The interval is the spacing between heartbeats, in d:h:m:s.

- The **contact-email** setting is a quote-enclosed text string giving an email address for the Gateway's administrator.
- The **location** setting is a text string allowing you to specify your geographical or other location, such as "Secaucus, NJ."
- The **number** setting is part of the sequence control. This is the number of heartbeats to send, at each "interval", before sleeping. For example, if this is 20, in the above layout, each heartbeat sequence will send out a total 20 heartbeats, spaced at 30 second intervals, and then sleep for 30 minutes. So to have the Gateway send out packets "forever", this number can be set very high. If it is 1440 and the interval is 1 minute, say, the heartbeat will go out every minute for 1440 minutes, or one day, before sleeping.
- The **sleep** setting is part of sequence control. This is the time to sleep before starting another heartbeat sequence, in d:h:m:s.

set system ntp
option [off | on]:
server-address (204.152.184.72)
alt-server-address (18.72.0.3):
time-zone [-12 - 12]
update-period (60) [1 - 65535]:
daylight-savings [off | on]

Specifies the NTP server address, time zone, and how often the Gateway should check the time from the NTP server. NTP time-zone of 0 is GMT time; options are -12 through 12 (+/- 1 hour increments from GMT time). **update-period** specifies how often, in minutes, the Gateway should update the clock. **daylight-savings** specifies whether daylight savings time is in effect; it defaults to **off**.

set system zerotouch option [on | off]

Enables or disables the Zero Touch option.

Zero Touch refers to automatic configuration of your Netopia Gateway. The Netopia Gateway has default settings such that initial connection to the Internet will succeed. If the **zerotouch** option is set to **on**, HTTP requests to any destination IP address except the IP address(es) of the configured redirection URL(s) will access a redirection server. DNS traffic will not be blocked. Other traffic from the LAN to all destinations will be dropped.

set system zerotouch redirect-url *redirection-URL*

Specifies the URL(s) of the desired redirection server(s) when the **zerotouch** option is set to **on**. URLs may be a maximum of 192 characters long, and may be in any of the following forms:

```
http://<domain-name OR IP address>/optionalPath:port

http://<domain-name OR IP address>/optionalPath

https://<domain-name OR IP address>/optionalPath:port

https://<domain-name OR IP address>/optionalPath

<domain-name OR IP address>/optionalPath:port

<domain-name OR IP address>/optionalPath
```

If the port number is omitted, port 80 will be assumed. Save and Restart are required to enforce these commands.

Syslog

set system syslog option [off | on]

Enables or disables system syslog feature. If syslog option is **on**, the following commands are available:

set system syslog host-nameip [*ip_address* | *hostname*]

Specifies the syslog server's address either in dotted decimal format or as a DNS name up to 64 characters.

set system syslog log-facility [local0 ... local7]

Sets the UNIX syslog Facility. Acceptable values are **local0** through **local7**.

set system syslog log-violations [off | on]

Specifies whether violations are logged or ignored.

set system syslog log-accepted [off | on]

Specifies whether acceptances are logged or ignored.

set system syslog log-attempts [off | on]

Specifies whether connection attempts are logged or ignored.

Default *syslog* installation procedure

1. **Access the router via telnet from the private LAN.**
   DHCP server is enabled on the LAN by default.
2. **The product's stateful inspection feature must be enabled in order to examine TCP, UDP and ICMP packets destined for the router or the private hosts.**
   This can be done by entering the **CONFIG** interface.
   - Type **`config`**
   - Type the command to enable stateful inspection

set security state-insp eth B option on

- Type the command to enable the router to drop fragmented packets

set security state-insp eth B deny-fragments on

3. **Enabling syslog:**
   - Type **config**
   - Type the command to enable syslog

     set system syslog option on
   - Set the IP Address of the syslog host

     set system syslog host-nameip <ip-addr>

     (example: **set system syslog host-nameip 10.3.1.1**)
   - Enable/change the options you require

     set system syslog log-facility local1

     set system syslog log-violations on

     set system syslog log-accepted on

     set system syslog log-attempts on
4. **Set NTP parameters**
   - Type **config**
   - Set the time-zone – Default is 0 or GMT

     set system ntp time-zone <zone>

     (example: **set system ntp time-zone –8**)
   - Set NTP server-address if necessary (default is 204.152.184.72)

     set system ntp server-address <ip-addr>

     (example:

     set system ntp server-address 204.152.184.73)
   - Set alternate server address

     set system ntp alt-server-address <ip-addr>
5. **Type the command to save the configuration**
   - Type **save**
   - Exit the configuration interface by typing

     exit
   - Restart the router by typing

     restart

The router will reboot with the new configuration in effect.

Wireless Settings (supported models)

set wireless option (on | off)

Administratively enables or disables the wireless interface.

set wireless network-id ssid { *network_name* }

Specifies the wireless network id for the Gateway. A unique *ssid* is generated for each Gateway. You must set your wireless clients to connect to this exact id, which can be changed to any 32-character string.

set wireless auto-channel mode { off | at-startup | continuous }

Specifies the wireless AutoChannel Setting for 802.11G models. AutoChannel is a feature that allows the Netopia Gateway to determine the best channel to broadcast automatically.

set wireless default-channel { 1...14 }

Specifies the wireless 2.4GHz sub channel on which the wireless Gateway will operate. For US operation, this is limited to channels 1–11. Other countries vary; for example, Japan is channel 14 only. The default channel in the US is 6. Channel selection can have a significant impact on performance, depending on other wireless activity in proximity to this AP. Channel selection is not necessary at the clients; clients will scan the available channels and look for APs using the same ssid as the client.

set wireless network-id closed-system { on | off }

When this setting is enabled, a client must know the ssid in order to connect or even see the wireless access point. When disabled, a client may scan for available wireless access points and will see this one. Enable this setting for greater security. The default is **on**.

set wireless mode { both-b-and-g | b-only | g-only }

Beginning with Netopia Firmware Version 7.5.1. specifies the wireless operating mode for connecting wireless clients: **both-b-and-g**, **b-only**, or **g-only**, and locks the Gateway in that mode.

NOTE:

If you choose to limit the operating mode to B or G only, clients using the mode you excluded will not be able to connect.

set wireless multi-ssid option { on | off }

Beginning with Netopia Firmware Version 7.5.1. enables or disables the **multi-ssid** feature which allows you to add additional network identifiers (SSIDs or *Network Names*) for your wireless network. When enabled, you can specify up to three additional SSIDs with separate privacy settings for each. See below.

set wireless multi-ssid {second-ssid | third-ssid | fourth-ssid } *name*

Specifies a descriptive name for each SSID. when **multi-ssid option** is set to **on.**

set wireless multi-ssid {second-ssid-privacy | third-ssid-privacy | fourth-ssid-privacy } { off | WPA-PSK | WPA-8021.x }

Specifies a privacy setting for each SSID. when **multi-ssid option** is set to **on.** Options are **off**, **WPA-PSK**, or **WPA-802.1x**.

set wireless no-bridging [off | on]

When set to **on**, this will block wireless clients from communicating with other wireless clients on the LAN side of the Gateway.

set wireless tx-power [full | medium | fair | low | minimal]

Sets the wireless transmit power, scaling down the router's wireless transmit coverage by lowering its radio power output. Default is **full** power. Transmit power settings are useful in

large venues with multiple wireless routers where you want to reuse channels. Since there are only three non-overlapping channels in the 802.11b spectrum, it helps to size the router's cell to match the location. This allows you to install a router to cover a small “hole” without conflicting with other routers nearby.

set wireless network-id privacy option { off | WEP | WPA-PSK | WPA-802.1x }

Specifies the type of privacy enabled on the wireless LAN. off = no privacy; WEP = WEP encryption; WPA-PSK = Wireless Protected Access/Pre-Shared Key; WPA-802.1x = Wireless Protected Access/802.1x authentication.

WPA provides Wireless Protected Access, the most secure option for your wireless network. This mechanism provides the best data protection and access control. PSK requires a Pre-Shared Key; 802.1x requires a RADIUS server for authentication.

WEP is Wired Equivalent Privacy, a method of encrypting data between the wireless Gateway and its clients. It is strongly recommended to turn this **on** as it is the primary way to protect your network and data from intruders. Note that 40bit is the same as 64bit and will work with either type of wireless client. The default is **off**.

A single key is selected (see **default-key**) for encryption of outbound/transmitted packets. The WEP-enabled client must have the identical key, of the same length, in the identical slot (1..4) as the wireless Gateway, in order to successfully receive and decrypt the packet. Similarly, the client also has a ‘default’ key that it uses to encrypt its transmissions. In order for the wireless Gateway to receive the client’s data, it must likewise have the identical key, of the same length, in the same slot. For simplicity, a wireless Gateway and its clients need only enter, share, and use the first key.

set wireless network-id privacy pre-shared-key *string*

The Pre Shared Key is a passphrase shared between the Router and the clients and is used to generate dynamically changing keys, when **WPA-PSK** is selected or enabled. The passphrase can be 8 – 63 characters. It is recommended to use at least 20 characters for best security.

set wireless network-id privacy default-keyid { 1...4 }

Specifies which WEP encryption key (of 4) the wireless Gateway will use to transmit data. The client *must* have an identical matching key, in the same numeric slot, in order to suc-

cessfully decode. Note that a client allows you to choose which of its keys it will use to transmit. Therefore, you must have an identical key in the same numeric slot on the Gateway.

For simplicity, it is easiest to have both the Gateway and the client transmit with the same key. The default is **1**.

set wireless network-id privacy encryption-key1-length {40/64bit, 128bit, 256bit}
set wireless network-id privacy encryption-key2-length {40/64bit, 128bit, 256bit}
set wireless network-id privacy encryption-key3-length {40/64bit, 128bit, 256bit}
set wireless network-id privacy encryption-key4-length {40/64bit, 128bit, 256bit}

Selects the length of each encryption key. **40bit** encryption is equivalent to **64bit** encryption. The longer the key, the stronger the encryption and the more difficult it is to break the encryption.

set wireless network-id privacy encryption-key1 { *hexadecimal digits* }
set wireless network-id privacy encryption-key2 { *hexadecimal digits* }
set wireless network-id privacy encryption-key3 { *hexadecimal digits* }
set wireless network-id privacy encryption-key4 { *hexadecimal digits* }

The encryption keys. Enter keys using hexadecimal digits. For 40/64bit encryption, you need 10 digits; 26 digits for 128bit, and 58 digits for 256bit WEP. Valid hexadecimal characters are 0 – 9, a – f.

Example 40bit key: 02468ACE02.

Example 128bit key: 0123456789ABCDEF0123456789.

Example 256bit key:
592CA140F0A238B0C61AE162F592CA140F0A238B0C61AE162F21A09C.

You must set at least one of these keys, indicated by the default-keyid.

Wireless MAC Address Authorization Settings

set wireless mac-auth option { on | off }

Enabling this feature limits the MAC addresses that are allowed to access the LAN as well as the WAN to specified MAC (hardware) addresses.

set wireless mac-auth wrlss-MAC-list mac-address *MAC-address_string*

Enters a new MAC address into the MAC address authorization table. The format for an Ethernet MAC address is six hexadecimal values between 00 and FF inclusive separated by colons or dashes (e.g., 00:00:C5:70:00:04).

set wireless mac-auth wrlss-MAC-list mac-address "*MAC-address_string*" allow-access { on | off }

Designates whether the MAC address is enabled or not for wireless network access. Disabled MAC addresses cannot be used for access until enabled.

RADIUS Server Settings

set radius radius-name "*server_name_string*"

Specifies the default RADIUS server name or IP address.

set radius radius-secret "*shared_secret*"

Specifies the RADIUS secret key used by this server. The shared secret should have the same characteristics as a normal password.

set radius alt-radius-name "*server_name_string*"

Specifies an alternate RADIUS server name or IP address to be used if the primary server is unreachable.

set radius alt-radius-secret "*shared_secret*"

Specifies the secret key used by the alternate RADIUS server.

set radius radius-port *port_number*

Specifies the port on which the RADIUS server is listening. The default value is 1812.

VLAN Settings

These settings are supported beginning with Firmware Version 7.4.2.

You can create up to 32 VLANs, and you can also restrict any VLAN, and the computers on it, from administering the Gateway.

set vlan name *string*

Sets the descriptive name for the VLAN. If no name is specified, displays a selection list of node names to select for editing.

Once a new VLAN name is specified, presents the list of VLAN characteristics to define:

- **id** – numerical range of possible IDs is 1 - 4096
- **type** [**by-port**] – currently the only selection is **by-port**
- **admin-restricted** [**off** | **on**] – default is **off**. If you select **on**, administrative access to the Gateway is blocked from this VLAN.
- **port** – VLAN's physical port or wireless SSID.

You must save the changes, exit out of configuration mode, and restart the Gateway for the changes to take effect.

Example:

- Navigate to the VLAN item:

```
Netopia-3000/9459252 (top)>> vlan
Netopia-3000/9459252 (vlan)>> set
  vlan
    name

(name) node list ...
Select (name) node to modify from list,
or enter new (name) to create.
    name (?): vlan1
(vlan1) has been added to the (name) list
      "vlan1"
```

```
        id (1) [ 1 - 4096 ]: 52
        type (by-port) [ by-port ]:
        admin-restricted (off) [ off | on ]: off
        port

(port) node list ...
Select (port) node to modify from list,
or enter new (port) to create.
```

- At this point you have created a VLAN. It is called **vlan1**, with **vlan-id 52**, without any admin restrictions.
- Next, add the port **ethernet0** port to this VLAN:

```
        port (?): 1
(1) has been added to the (port) list
          1
            interface ()
              [ lan-uplink | ethernet0 | vcc1 ]: ethernet0
Netopia-3000/9459252 (vlan)>>
```

- To make the VLAN vlan1 routable add the port **lan-uplink**:

```
Netopia-3000/9459252 (vlan)>> name vlan1
Netopia-3000/9459252 (vlan name "vlan1")>> set
      "vlan1"
        id (52) [ 1 - 4096 ]:
        type (by-port) [ by-port ]:
        admin-restricted (off) [ off | on ]:
        port

(port) node list ...
            1
Select (port) node to modify from list,
or enter new (port) to create.
        port (?): 2
(2) has been added to the (port) list
          2
            interface ()
              [ lan-uplink | ethernet0 | vcc1 ]: lan-uplink
Netopia-3000/9459252 (vlan name "vlan1")>>
```

Note:

To make a set of VLANs non-routable, the lan-uplink port must be included in at least one VLAN and must be excluded from any VLANs that are non-routable.

UPnP settings

set upnp option [on | off]

PCs using UPnP can retrieve the Gateway's WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with a UPnP-enabled Netopia Gateway, will not need application layer gateway support on the Netopia Gateway to work through NAT. The default is **on**.

You can disable UPnP, if you are not using any UPnP devices or applications.

DSL Forum settings

TR-064 is a LAN-side DSL CPE configuration specification and TR-069 is a WAN-side DSL CPE Management specification.

TR-064. DSL Forum LAN Side CPE Configuration (TR-064) is an extension of UPnP. It defines more services to locally manage the Netopia Gateway. While UPnP allows open access to configure the Gateway's features, TR-064 requires a password to execute any command that changes the Gateway's configuration.

set dslf-lanmgmt option [off | on]

Turns TR-064 LAN side management services on or off. The default is **on**.

TR-069. DSL Forum CPE WAN Management Protocol (TR-069) provides services similar to UPnP and TR-064. The communication between the Netopia Gateway and management agent in UPnP and TR-064 is strictly over the LAN, whereas the communication in TR-069 is over the WAN link for some features and over the LAN for others. TR-069 allows a remote Auto-Config Server (ACS) to provision and manage the Netopia Gateway. TR-069 protects sensitive data on the Gateway by not advertising its presence, and by password protection.

set dslf-cpewan option [off | on]

set dslf-cpewan acs-url "*acs_url:port_number*"

set dslf-cpewan acs-user-name "*acs_username*"

set dslf-cpewan acs-user-password "*acs_password*"

set dslf-cpewan acs-filter1-ip *filter1-ip_addr*

set dslf-cpewan acs-filter1-mask *filter1-mask*

set dslf-cpewan acs-filter2-ip *filter2-ip_addr*

set dslf-cpewan acs-filter2-mask *filter2-mask*

set dslf-cpewan acs-filter3-ip *filter3-ip_addr*

set dslf-cpewan acs-filter3-mask *filter3-mask*

Turns TR-069 WAN side management services on or off. The default is **off**. If TR-069 WAN side management services are enabled, specifies the auto-config server URL and port number. A username and password must also be supplied, if TR-069 is enabled.

The auto-config server is specified by URL and port number. The format for the ACS URL is as follows:

`http://some_url.com:port_number`

or

`http://123.45.678.910:port_number`

On units that support SSL, the format for the ACS URL can also be:

```
https://some_url.com:port_number
```

or

```
https://123.45.678.910:port_number
```

CHAPTER 6 Glossary

10Base-T. IEEE 802.3 specification for Ethernet that uses unshielded twisted pair (UTP) wiring with RJ-45 eight-conductor plugs at each end. Runs at 10 Mbps.

100Base-T. IEEE 802.3 specification for Ethernet that uses unshielded twisted pair (UTP) wiring with RJ-45 eight-conductor plugs at each end. Runs at 100 Mbps.

-----A-----

ACK. Acknowledgment. Message sent from one network device to another to indicate that some event has occurred. See NAK.

access rate. Transmission speed, in bits per second, of the circuit between the end user and the network.

adapter. Board installed in a computer system to provide network communication capability to and from that computer system.

address mask. See subnet mask.

ADSL. Asymmetric Digital Subscriber Line. Modems attached to twisted pair copper wiring that transmit 1.5-9 Mbps downstream (to the subscriber) and 16 -640 kbps upstream, depending on line distance. (Downstream rates are usually lower that 1.5Mbps in practice.)

AH. The **A**uthentication **H**eader provides data origin authentication, connectionless integrity, and anti-replay protection services. It protects all data in a datagram from tampering, including the fields in the header that do not change in transit. Does not provide confidentiality.

ANSI. American National Standards Institute.

ASCII. American Standard Code for Information Interchange (pronounced ASK-ee). Code in which numbers from 0 to 255 represent individual characters, such as letters, numbers, and punctuation marks; used in text representation and communication protocols.

asynchronous communication. Network system that allows data to be sent at irregular intervals by preceding each octet with a start bit and following it with a stop bit. Compare synchronous communication.

Auth Protocol. Authentication Protocol for IP packet header. The three parameter values are None, Encapsulating Security Payload (ESP) and Authentication Header (AH).

-----B-----

backbone. The segment of the network used as the primary path for transporting traffic between network segments.

baud rate. Unit of signaling speed equal to the number of number of times per second a signal in a communications channel varies between states. Baud is synonymous with bits per second (bps) if each signal represents one bit.

binary. Numbering system that uses only zeros and ones.

bps. Bits per second. A measure of data transmission speed.

BRI. Basic Rate Interface. ISDN standard for provision of low-speed ISDN services (two B channels (64 kbps each) and one D channel (16 kbps)) over a single wire pair.

bridge. Device that passes packets between two network segments according to the packets' destination address.

broadcast. Message sent to all nodes on a network.

broadcast address. Special IP address reserved for simultaneous broadcast to all network nodes.

buffer. Storage area used to hold data until it can be forwarded.

-----C-----

carrier. Signal suitable for transmission of information.

CCITT. Comité Consultatif International Télégraphique et Téléphonique or Consultative Committee for International Telegraph and Telephone. An international organization responsible for developing telecommunication standards.

CD. Carrier Detect.

CHAP. Challenge-Handshake Authentication Protocol. Security protocol in PPP that prevents unauthorized access to network services. See RFC 1334 for PAP specifications Compare PAP.

client. Network node that requests services from a server.

CPE. Customer Premises Equipment. Terminating equipment such as terminals, telephones and modems that connects a customer site to the telephone company network.

CO. Central Office. Typically a local telephone company facility responsible for connecting all lines in an area.

compression. Operation performed on a data set that reduces its size to improve storage or transmission rate.

crossover cable. Cable that lets you connect a port on one Ethernet hub to a port on another Ethernet hub. You can order an Ethernet crossover cable from Netopia, if needed.

CSU/DSU. Channel Service Unit/Data Service Unit. Device responsible for connecting a digital circuit, such as a T1 link, with a terminal or data communications device.

-----D-----

data bits. Number of bits used to make up a character.

datagram. Logical grouping of information sent as a network-layer unit. Compare frame, packet.

DCE. Digital Communication Equipment. Device that connects the communication circuit to the network end node (DTE). A modem and a CSU/DSU are examples of a DCE.

dedicated line. Communication circuit that is used exclusively to connect two network devices. Compare dial on demand.

DES. Data **E**ncryption **S**tandard is a 56-bit encryption algorithm developed by the U.S. National Bureau of Standards (now the National Institute of Standards and Technology).

3DES. Triple DES, with a 168 bit encryption key, is the most accepted variant of DES.

DH Group. Diffie-Hellman is a public key algorithm used between two systems to determine and deliver secret keys used for encryption. Groups 1, 2 and 5 are supported. Also, see Diffie-Hellman listing.

DHCP. Dynamic Host Configuration Protocol. A network configuration protocol that lets a router or other device assign IP addresses and supply other network configuration information to computers on your network.

dial on demand. Communication circuit opened over standard telephone lines when a network connection is needed.

Diffie-Hellman. A group of key-agreement algorithms that let two computers compute a key independently without exchanging the actual key. It can generate an unbiased secret key over an insecure medium.

diffserv. Differentiated Services. A method for controlling Quality of Service (QoS) queue priority settings. It allows a Gateway to make Quality of Service (QoS) decisions about what path Internet traffic, such as Voice over IP (VoIP), should travel across your network.

domain name. Name identifying an organization on the Internet. Domain names consists of sets of characters separated by periods (dots). The last set of characters identifies the type of organization (.GOV, .COM, .EDU) or geographical location (.US, .SE).

domain name server. Network computer that matches host names to IP addresses in response to Domain Name System (DNS) requests.

Domain Name System (DNS). Standard method of identifying computers by name rather than by numeric IP address.

DSL. Digital Subscriber Line. Modems on either end of a single twisted pair wire that delivers ISDN Basic Rate Access.

DTE. Data Terminal Equipment. Network node that passes information to a DCE (modem) for transmission. A computer or router communicating through a modem is an example of a DTE device.

DTR. Data Terminal Ready. Circuit activated to indicate to a modem (or other DCE) that the computer (or other DTE) is ready to send and receive data.

dynamic DNS. Allows you to use the free services of *www.dyndns.org*. Dynamic DNS automatically directs any public Internet request for your computer's name to your current dynamically-assigned IP address.

-----E-----

echo interval. Frequency with which the router sends out echo requests.

Enable. This toggle button is used to enable/disable the configured tunnel.

encapsulation. Technique used to enclose information formatted for one protocol, such as AppleTalk, within a packet formatted for a different protocol, such as TCP/IP.

Encrypt Protocol. Encryption protocol for the tunnel session.

Parameter values supported include NONE or ESP.

encryption. The application of a specific algorithm to a data set so that anyone without the encryption key cannot understand the information.

ESP. Encapsulation Security Payload (ESP) header provides confidentiality, data origin authentication, connectionless integrity, anti-replay protection, and limited traffic flow confidentiality. It encrypts the contents of the datagram as specified by the Security Association. The ESP transformations encrypt and decrypt portions of datagrams, wrapping or unwrapping the datagram within another IP datagram. Optionally, ESP transformations may perform data integrity validation and compute an Integrity Check Value for the datagram being sent. The complete IP datagram is enclosed within the ESP payload.

Ethernet crossover cable. See crossover cable.

-----F-----

FCS. Frame Check Sequence. Data included in frames for error control.

flow control. Technique using hardware circuits or control characters to regulate the transmission of data between a computer (or other DTE) and a modem (or other DCE). Typically, the modem has buffers to hold data; if the buffers approach capacity, the modem signals the computer to stop while it catches up on processing the data in the buffer. See CTS, RTS, xon/xoff.

fragmentation. Process of breaking a packet into smaller units so that they can be sent over a network medium that cannot transmit the complete packet as a unit.

frame. Logical grouping of information sent as a link-layer unit. Compare datagram, packet.

FTP. File Transfer Protocol. Application protocol that lets one IP node transfer files to and from another node.

FTP server. Host on network from which clients can transfer files.

-----H-----

Hard MBytes. Setting the Hard MBytes parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Hard MByte value.

The value can be configured between 1 and 1,000,000 MB and refers to data traffic passed.

Hard Seconds. Setting the Hard Seconds parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Hard Seconds value. The value can be configured between 60 and 1,000,000 seconds.

A tunnel will start the process of renegotiation at the soft threshold and renegotiation *must* happen by the hard limit or traffic over the tunnel is terminated.

hardware handshake. Method of flow control using two control lines, usually Request to Send (RTS) and Clear to Send (CTS).

header. The portion of a packet, preceding the actual data, containing source and destination addresses and error-checking fields.

HMAC. Hash-based **M**essage **A**uthentication **C**ode

hop. A unit for measuring the number of routers a packet has passed through when traveling from one network to another.

hop count. Distance, measured in the number of routers to be traversed, from a local router to a remote network. See metric.

hub. Another name for a repeater. The hub is a critical network element that connects everything to one centralized point. A hub is simply a box with multiple ports for network connections. Each device on the network is attached to the hub via an Ethernet cable.

-----|-----

IGMP. Internet **G**roup **M**anagement **P**rotocol allows a router to determine which host groups have members on a given network segment.

IKE. Internet **K**ey **E**xchange protocol provides automated key management and is a preferred alternative to manual key management as it provides better security. Manual key management is practical in a small, static environment of two or three sites. Exchanging the key is done through manual means. Because IKE provides automated key exchange, it is good for larger, more dynamic environments.

INSPECTION. The best option for Internet communications security is to have an SMLI firewall constantly inspecting the flow of traffic: determining direction, limiting or eliminating inbound access, and verifying down to the packet level that the network traffic is only what the customer chooses. The Netopia Gateway works like a network super traffic cop, inspecting and filtering out undesired traffic based on your security policy and resulting configuration.

interface. A connection between two devices or networks.

internet address. IP address. A 32-bit address used to route packets on a TCP/IP network. In dotted decimal notation, each eight bits of the 32-bit number are presented as a decimal number, with the four octets separated by periods.

IPCP. Internet Protocol Control Protocol. A network control protocol in PPP specifying how IP communications will be configured and operated over a PPP link.

IPSEC. A protocol suite defined by the Internet Engineering Task Force to protect IP traffic at packet level. It can be used for protecting the data transmitted by any service or application that is based on IP, but is commonly used for VPNs.

ISAKMP. Internet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol is a framework for creating connection specific parameters. It is a protocol for establishing, negotiating, modifying, and deleting SAs and provides a framework for authentication and key exchange. ISAKMP is a part of the IKE protocol.

-----K-----

Key Management . The Key Management algorithm manages the exchange of security keys in the IPSec protocol architecture. SafeHarbour supports the standard *Internet Key Exchange (IKE)*

-----L-----

LCP. Link Control Protocol. Protocol responsible for negotiating connection configuration parameters, authenticating peers on the link, determining whether a link is functioning properly, and terminating the link. Documented in RFC 1331.

LQM Link Quality Monitoring. Optional facility that lets PPP make policy decisions based on the observed quality of the link between peers. Documented in RFC 1333.

loopback test. Diagnostic procedure in which data is sent from a devices's output channel and directed back to its input channel so that what was sent can be compared to what was received.

-----M-----

magic number. Random number generated by a router and included in packets it sends to other routers. If the router receives a packet with the same magic number it is using, the router sends and receives packets with new random numbers to determine if it is talking to itself.

MD5. A 128-bit, **m**essage-**d**igest, authentication algorithm used to create digital signatures. It computes a secure, irreversible, cryptographically strong hash value for a document. Less secure than variant SHA-1.

metric. Distance, measured in the number of routers a packet must traverse, that a packet must travel to go from a router to a remote network. A route with a low metric is considered more efficient, and therefore preferable, to a route with a high metric. See hop count.

modem. Modulator/demodulator. Device used to convert a digital signal to an analog signal for transmission over standard telephone lines. A modem

at the other end of the connection converts the analog signal back to a digital signal.

MRU. Maximum Receive Unit. The maximum packet size, in bytes, that a network interface will accept.

MSSID. Multiple **S**ervice **S**et **ID**entifier. Unique identifiers of data sent over a wireless connection that act as passwords when wireless devices try to join wireless networks. An SSID differentiates one wireless network from another, so all access points and all devices attempting to connect to a specific network must use the same SSID. Netopia Gateways support up to four SSIDs.

SSIDs are also sometimes referred to as *Network Names* because they are names that identify wireless networks.

MTU. Maximum Transmission Unit. The maximum packet size, in bytes, that can be sent over a network interface.

MULTI-LAYER. The Open System Interconnection (OSI) model divides network traffic into seven distinct levels, from the Physical (hardware) layer to the Application (software) layer. Those in between are the Presentation, Session, Transport, Network, and Data Link layers. Simple first and second generation firewall technologies inspect between 1 and 3 layers of the 7 layer model, while our SMLI engine inspects layers 2 through 7.

-----N-----

NAK. Negative acknowledgment. See ACK.

Name. The Name parameter refers to the name of the configured tunnel. This is mainly used as an identifier for the administrator. The Name parameter is an ASCII and is limited to 31 characters. The tunnel name is the only IPSec parameter that does not need to match the peer gateway.

NCP. Network Control Protocol.

Negotiation Method. This parameter refers to the method used during the Phase I key exchange, or IKE process. SafeHarbour supports Main or

Aggressive Mode. Main mode requires 3 two-way message exchanges while Aggressive mode only requires 3 total message exchanges.

null modem. Cable or connection device used to connect two computing devices directly rather than over a network.

-----P-----

packet. Logical grouping of information that includes a header and data. Compare frame, datagram.

PAP. Password Authentication Protocol. Security protocol within the PPP protocol suite that prevents unauthorized access to network services. See RFC 1334 for PAP specifications. Compare CHAP.

parity. Method of checking the integrity of each character received over a communication channel.

Peer External IP Address. The Peer External IP Address is the public, or routable IP address of the remote gateway or VPN server you are establishing the tunnel with.

Peer Internal IP Network. The Peer Internal IP Network is the private, or Local Area Network (LAN) address of the remote gateway or VPN Server you are communicating with.

Peer Internal IP Netmask. The Peer Internal IP Netmask is the subnet mask of the Peer Internal IP Network.

PFS Enable. Enable **P**erfect **F**orward **S**ecrecy. PFS forces a DH negotiation during Phase II of IKE-IPSec SA exchange. You can disable this or select a DH group 1, 2, or 5. PFS is a security principle that ensures that any single key being compromised will permit access to only data protected by that single key. In PFS, the key used to protect transmission of data must not be used to derive any additional keys. If the key was derived from some other keying material, that material must not be used to derive any more keys.

PING. Packet INternet Groper. Utility program that uses an ICMP echo message and its reply to verify that one network node can reach another. Often used to verify that two hosts can communicate over a network.

PPP. Point-to-Point Protocol. Provides a method for transmitting datagrams over serial router-to-router or host-to-network connections using synchronous or asynchronous circuits.

Pre-Shared Key. The Pre-Shared Key is a parameter used for authenticating each side. The value can be an ASCII or Hex and a maximum of 64 characters.

Pre-Shared Key Type. The Pre-Shared Key Type classifies the Pre-Shared Key. SafeHarbour supports *ASCII* or *HEX* types

protocol. Formal set of rules and conventions that specify how information can be exchanged over a network.

PSTN. Public Switched Telephone Network.

-----R-----

repeater. Device that regenerates and propagates electrical signals between two network segments. Also known as a hub.

RFC. Request for Comment. Set of documents that specify the conventions and standards for TCP/IP networking.

RIP. Routing Information Protocol. Protocol responsible for distributing information about available routes and networks from one router to another.

RJ-11. Four-pin connector used for telephones.

RJ-45. Eight-pin connector used for 10BaseT (twisted pair Ethernet) networks.

route. Path through a network from one node to another. A large internetwork can have several alternate routes from a source to a destination.

routing table. Table stored in a router or other networking device that records available routes and distances for remote network destinations.

-----S-----

SA Encrypt Type. SA Encryption Type refers to the symmetric encryption type. This encryption algorithm will be used to encrypt each data packet. SA Encryption Type values supported include *DES* and *3DES*.

SA Hash Type. SA Hash Type refers to the Authentication Hash algorithm used during SA negotiation. Values supported include *MD5 SHA1*. N/A will display if NONE is chose for Auth Protocol.

Security Association. From the IPSEC point of view, an SA is a data structure that describes which transformation is to be applied to a datagram and how. The SA specifies:

- The authentication algorithm for AH and ESP
- The encryption algorithm for ESP
- The encryption and authentication keys
- Lifetime of encryption keys
- The lifetime of the SA
- Replay prevention sequence number and the replay bit table

An arbitrary 32-bit number called a Security Parameters Index (SPI), as well as the destination host's address and the IPSEC protocol identifier, identify each SA. An SPI is assigned to an SA when the SA is negotiated. The SA can be referred to by using an SPI in AH and ESP transformations. SA is unidirectional. SAs are commonly setup as bundles, because typically two SAs are required for communications. SA management is always done on bundles (setup, delete, relay).

serial communication. Method of data transmission in which data bits are transmitted sequentially over a communication channel

SHA-1. An implementation of the U.S. Government **S**ecure **H**ash **A**lgorithm; a 160-bit authentication algorithm.

Soft MBytes. Setting the Soft MBytes parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Soft MByte value. The value can be configured between *1 and 1,000,000 MB* and refers to data traffic passed. If this value is not achieved, the Hard MBytes parameter is enforced.

Soft Seconds. Setting the Soft Seconds parameter forces the renegotiation of the IPSec Security Associations (SAs) at the configured Soft Seconds value. The value can be configured between 60 and 1,000,000 seconds.

SPI . The **S**ecurity **P**arameter **I**ndex is an identifier for the encryption and authentication algorithm and key. The SPI indicates to the remote firewall the algorithm and key being used to encrypt and authenticate a packet. It should be a unique number greater than 255.

SSL. Secure **S**ockets **L**ayer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message.

STATEFUL. The Netopia Gateway monitors and maintains the state of any network transaction. In terms of network request-and-reply, state consists of the source IP address, destination IP address, communication ports, and data sequence. The Netopia Gateway processes the stream of a network conversation, rather than just individual packets. It verifies that packets are sent from and received by the proper IP addresses along the proper communication ports in the correct order and that no imposter packets interrupt the packet flow. Packet filtering monitors only the ports involved, while the Netopia Gateway analyzes the continuous conversation stream, preventing session hijacking and denial of service attacks.

static route. Route entered manually in a routing table.

subnet mask. A 32-bit address mask that identifies which bits of an IP address represent network address information and which bits represent node identifier information.

synchronous communication. Method of data communication requiring the transmission of timing signals to keep peers synchronized in sending and receiving blocks of data.

-----T-----

telnet. IP protocol that lets a user on one host establish and use a virtual terminal connection to a remote host.

TR-064. TR-064 is a LAN-side DSL Gateway configuration specification; an extension of UPnP. It defines more services to locally manage a Gateway.

TR-069. TR-069 is a WAN-side DSL Gateway Management specification; provides services similar to UPnP and TR-064. The communication between a Gateway and management agent in UPnP and TR-064 is strictly over the LAN, whereas the communication in TR-069 is over the WAN link for some features and over the LAN for others. TR-069 allows a remote Auto-Config Server to provision and manage a Gateway.

twisted pair. Cable consisting of two copper strands twisted around each other. The twisting provides protection against electromagnetic interference.

-----U-----

UTP. Unshielded twisted pair cable.

-----V-----

VJ. Van Jacobson. Abbreviation for a compression standard documented in RFC 1144.

VLAN. Virtual Local Area Network. A network of computers that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN. VLANs are configured in software rather than hardware.

-----W-----

WAN. Wide Area Network. Private network facilities, usually offered by public telephone companies but increasingly available from alternative access providers (sometimes called Competitive Access Providers, or CAPs), that link business network nodes.

WWW. World Wide Web.

-----X-----

XAuth. Extended Authentication. An extension to the Internet Key Exchange (IKE) protocol, for IPSec tunnelling. Requires SafeHarbour IPsec tunneling feature key.

CHAPTER 7 Technical Specifications and Safety Information

Description

Dimensions:

Smart Modems: 13.5 cm (w) x 13.5 cm (d) x 3.5 cm (h); 5.25” (w) x 5.25” (d) x 1.375” (h)
Wireless Models: 19.5 cm (w) x 17.0 cm (d) x 4.0 cm (h); 7.6” (w) x 6.75” (d) x 1.5” (h)
3342/3352: 8.5 cm (w) x 4.5 cm (d) x 2 cm (h); 3.375” (w) x 1.75” (d) x .875” (h)

Communications interfaces: The Netopia Gateways have an RJ-11 jack for DSL line connections or an RJ-45 jack for cable/DSL modem connections and 1 or 4–port 10/100Base-T Ethernet switch for your LAN connections. Some models have a USB port that can be used to connect to your PC; in some cases, the USB port also serves as the power source. Some models contain an 802.11b wireless LAN transmitter.

Power requirements

- 12 VDC input

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% noncondensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via TFTP or web upload. (does not apply to 3342/3352)

Routing: TCP/IP Internet Protocol Suite, RIP

WAN support: PPPoA, PPPoE, DHCP, static IP address

Security: PAP, CHAP, UI password security, IPsec

Management/configuration methods: HTTP (Web server), Telnet, SNMP

Diagnostics: Ping, event logging, routing table displays, statistics counters, web-based management, traceroute, nslookup, and diagnostic commands.

Agency approvals

North America

Safety Approvals:

- United States – UL 60950, Third Edition
- Canada – CSA: CAN/CSA-C22.2 No. 60950-00

EMC:

- United States – FCC Part 15 Class B
- Canada – ICES-003

Telecom:

- United States – 47 CFR Part 68
- Canada – CS-03

International

Safety Approvals:

- Low Voltage (European directive) 73/23
- EN60950 (Europe)

EMI Compatibility:

- 89/336/EEC (European directive)
- EN55022:1994 CISPR22 Class B
- EN300 386 V1.2.1 (non-wireless products)
- EN 301-489 (wireless products)

Regulatory notices

European Community. This Netopia product conforms to the European Community CE Mark standard for the design and manufacturing of information technology equipment. This standard covers a broad area of product design, including RF emissions and immunity from electrical disturbances.

The Netopia Firmware Version 7.6 complies with the following EU directives:

- Low Voltage, 73/23/EEC
- EMC Compatibility, 89/336/EEC, conforming to EN 55 022

Manufacturer's Declaration of Conformance

Warnings:

This is a Class B product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.
Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

United States. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

Service requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or our of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 6001 Shellmound Street, Emeryville, California, 94608. Telephone: 510-597-5400.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This Class B digital apparatus meets all requirements of the Canadian Interference - Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

Declaration for Canadian users

NOTICE: The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Important Safety Instructions

Australian Safety Information

The following safety information is provided in conformance with Australian safety requirements:

Caution

DO NOT USE BEFORE READING THE INSTRUCTIONS: Do not connect the Ethernet ports to a carrier or carriage service provider's telecommunications network or facility unless: a) you have the written consent of the network or facility manager, or b) the connection is in accordance with a connection permit or connection rules.

Connection of the Ethernet ports may cause a hazard or damage to the telecommunication network or facility, or persons, with consequential liability for substantial compensation.

Caution

- The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply near the product for easy access.
- For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.0A.

Telecommunication installation cautions

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

47 CFR Part 68 Information

FCC Requirements

1. The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.
2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.
3. The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.
4. If the telephone company requests information on what equipment is connected to their lines, inform them of:

   a. The telephone number to which this unit is connected.

   b. The ringer equivalence number. [0.XB]

   c. The USOC jack required. [RJ11C]

   d. The FCC Registration Number. [XXXUSA-XXXXX-XX-E]

   Items (b) and (d) are indicated on the label. The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN's of all devices on any one line should not exceed five (5.0). If too many devices are attached, they may not ring properly.

FCC Statements

a) This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

b) List all applicable certification jack Universal Service Order Codes (“USOC”) for the equipment: RJ11.

c) A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

d) The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2002, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

e) If this equipment, the Netopia 2200/3300 Series router, causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

f) The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

g) If trouble is experienced with this equipment, the Netopia 2200/3300 Series router, for repair or warranty information, please contact:

Netopia Technical Support
510-597-5400
www.netopia.com.

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

h) This equipment not intended to be repaired by the end user. In case of any problems, please refer to the troubleshooting section of the Product User Manual before calling Netopia Technical Support.

i) Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

j) If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this Netopia 2200/3300 Series router does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or qualified installer.

RF Exposure Statement:

NOTE: Installation of the wireless models must maintain at least 20 cm between the wireless router and any body part of the user to be in compliance with FCC RF exposure guidelines.

Electrical Safety Advisory

Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources. This has been identified as a major nationwide problem. Therefore it is advised that this equipment be connected to AC power through the use of a surge arrestor or similar protection device.

Index

Q

R

S

T

U

V

Z

Netopia 2200/3300 Series by Netopia

Netopia, Inc.
6001 Shellmound Street
Emeryville, CA 94608

July 10, 2006