Administrator's Handbook

Motorola Netopia® Embedded Software Version 7.7.4

Qwest

MOTOROLA

Qwest.
Spirit of Service®

Copyright

Motorola reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola to provide notification of such revision or change. Motorola provides this guide without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Motorola may make improvements or changes in the product(s) described in this manual at any time. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me, and Windows NT are either trademarks or registered trademarks of Microsoft Corporation in the U.S and/or other countries. Macintosh is a registered trademark of Apple, Inc. Firefox is a registered trademark of the Mozilla Foundation. All other product or service names are the property of their respective owners.

Motorola, Inc.
6001 Shellmound Street
Emeryville, CA 94608
U.S.A.

Motorola, Inc. Part Number: 6161250-00-01

Table of Contents

Introduction

Intended Audience

This guide is targeted primarily to residential service subscribers.

Advanced sections may also be of use to the support staffs of broadband service providers and advanced residential service subscribers. See “Advanced Setup” on page 73.

About Motorola Netopia® Documentation

Motorola, Inc. provides a suite of technical information for its 2200 and 3300-series family of intelligent enterprise and consumer Gateways. It consists of:

- *Administrator’s Handbook*
- 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/*

NOTE:

This guide describes the wide variety of features and functionality of the Motorola Netopia® Gateway, when used in Router mode. The Motorola 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.

Organization

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

- **"Introduction"** — Describes the Motorola Netopia® document suite, the purpose of, the audience for, and structure of this guide. It gives a table of conventions.
- **Chapter 1, "Overview of Major Capabilities"** — Presents a product description summary.
- **Chapter 2, "Basic Mode Setup"** — Describes how to get up and running with your Motorola Netopia® Gateway, and the Basic Mode Web-based user interface.
- **Chapter 3, "Advanced Setup"** — Focuses on the Advanced Setup 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 Motorola Netopia® 2200 and 3300 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.

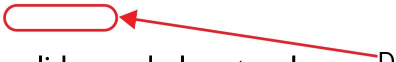
Documentation Conventions

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
light 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

CHAPTER 1 Overview of Major Capabilities

The Motorola Netopia® Gateway offers simplified setup and management features as well as advanced broadband Gateway capabilities. The following are some of the main features of the Motorola Netopia® Gateway:

- "Wide Area Network Termination" on page 12

  The Gateway combines an ADSL modem with an Internet Gateway. It translates protocols used on the Internet to protocols used by home personal computers and eliminates the need for special desktop software (i.e. PPPoE).

- "Simplified Local Area Network Setup" on page 14

  Built-in DHCP and DNS proxy features minimize or eliminate the need to program any network configuration into your home personal computer. UPnP™ feature allows ease of connection with many compatible networked devices.

- "Management" on page 16

  A Web server built into the Motorola Netopia® Operating System makes setup and maintenance easy using standard browsers. Diagnostic tools facilitate troubleshooting.

- "Security" on page 18

  Network Address Translation (NAT), password protection, Stateful Inspection firewall and other built-in security features prevent unauthorized remote access to your network. NAT Games and other services, default server, and other features permit access to computers on your home network that you can specify. VPN technology (standard VPN Passthrough and optional IPSec tunnelling) enables telecommuters, mobile workforce and branch offices to safely and affordably connect to a remote business network, for effective communication and collaboration.

Wide Area Network Termination

PPPoE/PPPoA (Point-to-Point Protocol over Ethernet/ATM)

The PPPoE specification, incorporating the PPP and Ethernet standards, allows your computer(s) to connect to your Service Provider's network through your Ethernet WAN connection. The 2200 and 3300-series Gateway supports PPPoE, eliminating the need to install PPPoE client software on any LAN computers.

Service Providers may require the use of PPP authentication protocols such as Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). CHAP and PAP use a username and password pair to authenticate users with a PPP server.

A CHAP authentication process works as follows:

1. **The password is used to scramble a challenge string.**
2. **The password is a shared secret, known by both peers.**
3. **The unit sends the scrambled challenge back to the peer.**

PAP, a less robust method of authentication, sends a username and password to a PPP server to be authenticated. PAP's username and password pair are not encrypted, and are therefore sent "unscrambled".

Instant-On PPP

You can configure your Gateway for one of two types of Internet connections:

- Always On
- Instant On

These selections provide either an uninterrupted Internet connection or an as-needed connection.

While an Always On connection is convenient, it does leave your network permanently connected to the Internet, and therefore potentially vulnerable to attacks.

Motorola Netopia®'s Instant On technology furnishes almost all the benefits of an Always-On connection while providing two 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.

When you configure Instant On access, you can also configure an idle time-out value. Your Gateway monitors traffic over the Internet link and when there has been no traffic for the configured number of seconds, it disconnects the link.

When new traffic that is destined for the Internet arrives at the Gateway, the Gateway will instantly re-establish the link.

Your service provider may be using a system that assigns the Internet address of your Gateway out of a pool of many possible Internet addresses. The address assigned varies with each connection attempt, which makes your network a moving target for any attacker.

Simplified Local Area Network Setup

DHCP (Dynamic Host Configuration Protocol) Server

DHCP Server functionality enables the Gateway to assign to your LAN computer(s) a “private” IP address and other parameters that allow network communication. The default DHCP Server configuration of the Gateway supports up to 253 LAN IP addresses.

This feature simplifies network administration because the Gateway maintains a list of IP address assignments. Additional computers can be added to your LAN without the hassle of configuring an IP address.

DNS Proxy

Domain Name System (DNS) provides end users with the ability to look for devices or web sites by typing their names, rather than IP addresses. For web surfers, this technology allows you to enter the URL (Universal Resource Locator) as text to surf to a desired website.

The Motorola Netopia® DNS Proxy feature allows the LAN-side IP address of the Gateway to be used for proxying DNS requests from hosts on the LAN to the DNS Servers configured in the gateway. This is accomplished by having the Gateway's LAN address handed out as the “DNS Server” to the DHCP clients on the LAN.

NOTE:

The Motorola Netopia® DNS Proxy only proxies UDP DNS queries, not TCP DNS queries.

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. 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 Motorola Netopia® Gateway, will not need application layer gateway support on the Motorola Netopia® Gateway to work through NAT. By default, UPnP is enabled on the Motorola Netopia® Gateway.

Management

Embedded Web Server

There is no specialized software to install on your PC to configure, manage, or maintain your Motorola Netopia® Gateway. Web pages embedded in the operating system provide access to the following Gateway operations:

- Setup
- System and security logs
- Diagnostics functions

Once you have removed your Motorola Netopia® Gateway from its packing container and powered the unit up, use any LAN attached PC or workstation running a common web browser application to configure and monitor the Gateway.

Diagnostics

In addition to the Gateway's visual LED indicator lights, you can run an extensive set of diagnostic tools from your Web browser.

Two of the facilities are:

- Automated "Multi-Layer" Test

  The ***Run Diagnostics*** link initiates a sequence of tests. They examine the entire functionality of the Gateway, from the physical connections to the data traffic.
- Network Test Tools

  Three test tools to determine network reachability are available:

  Ping - tests the "reachability" of a particular network destination by sending an ICMP echo request and waiting for a reply.

  NSLookup - 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 Gateway addresses of these hops.

The system log also provides diagnostic information.

NOTE:

Your Service Provider may request information that you acquire from these various diagnostic tools. Individual tests may be performed at the command line. (See “Command Line Interface” on page 163.).

Security

Remote Access Control

You can determine whether or not an administrator or other authorized person has access to configuring your Gateway. This access (either time-restricted or unlimited until the router is rebooted) can be turned on or off in the Web interface. Additionally, permanent remote access can be configured in the CLI.

Password Protection

Access to your Motorola Netopia® device can be controlled through two access control accounts, **Admin** or **User**.

- The **Admin**, or administrative user, performs all configuration, management or maintenance operations on the Gateway.
- The **User** account provides monitor capability **only**.
  A user may **NOT** change the configuration, perform upgrades or invoke maintenance functions.

Network Address Translation (NAT)

The Motorola Netopia® Gateway Network Address Translation (NAT) security feature lets you conceal the topology of a hard-wired Ethernet or wireless network connected to its LAN interface from Gateways on networks connected to its WAN interface. In other words, the end computer stations on your LAN are **invisible** from the Internet.

Only a **single WAN IP address** is required to provide this security support for your entire LAN.

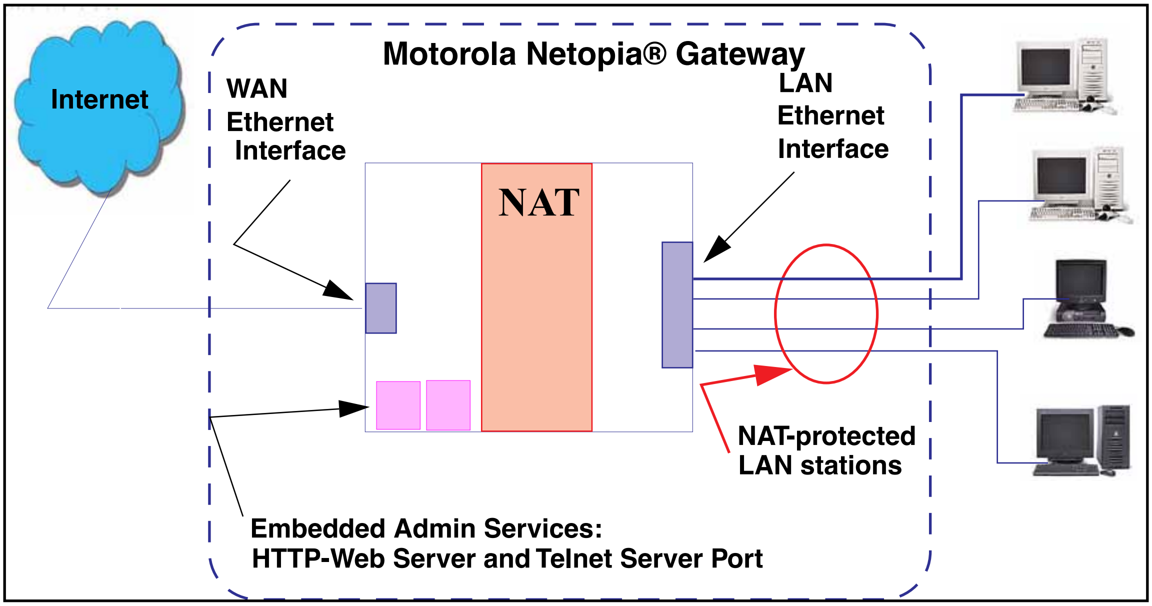
LAN sites that communicate through an Internet Service Provider typically enable NAT, since they usually purchase only one IP address from the ISP.

- When NAT is **ON**, the Motorola Netopia® Gateway “proxies” for the end computer stations on your network by pretending to be the originating host for network communications from non-originating networks. The WAN interface address is the only IP address exposed.

The Motorola Netopia® Gateway tracks which local hosts are communicating with which remote hosts. It routes packets received from remote networks to the correct computer on the LAN (Ethernet) interface.

- When NAT is **OFF**, a Motorola Netopia® Gateway acts as a traditional TCP/IP router, all LAN computers/devices are exposed to the Internet.

A diagram of a typical NAT-enabled LAN follows:


Internet
Motorola Netopia® Gateway
WAN Ethernet Interface
LAN Ethernet Interface
NAT
NAT-protected LAN stations
Embedded Admin Services:
HTTP-Web Server and Telnet Server Port

NOTE:

1. The default setting for NAT is **ON**.
2. Motorola uses Port Address Translation (PAT) to implement the NAT facility.
3. NAT Pinhole traffic (discussed below) is always initiated from the WAN side.

Motorola Netopia® Advanced Features for NAT

Using the NAT facility provides effective LAN security. However, there are user applications that require methods to selectively by-pass this security function for certain types of Internet traffic.

Motorola Netopia® Gateways provide special gaming and other service configuration tools that enable you to establish NAT-protected LAN layouts that still provide flexible by-pass capabilities.

Some of these rules require coordination with the unit's embedded administration services: the internal Web (HTTP) Port (TCP 80) and the internal Telnet Server Port (TCP 23).

Internal Servers

The internal servers are the embedded Web and Telnet servers of the Gateway. You would change the internal server ports for Web and Telnet of the Gateway if you wanted to have these services on the LAN using pinholes or the Default server. Pinhole configuration rules provide an internal port forwarding facility that enables you to eliminate conflicts with embedded administrative ports 80 and 23.

Default Server

This feature allows you to:

- Direct your Gateway 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.

Combination NAT Bypass Configuration

Specific Games and services and Default Server settings, each directed to different LAN devices, can be used together.

WARNING:

NAT Bypass configuration allows inbound access to the specified LAN station. Contact your Network Administrator for LAN security questions.

IP-Passthrough

The Netopia Gateway now offers an IP passthrough feature. The IP passthrough feature allows a single PC on the LAN to have the Gateway'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.

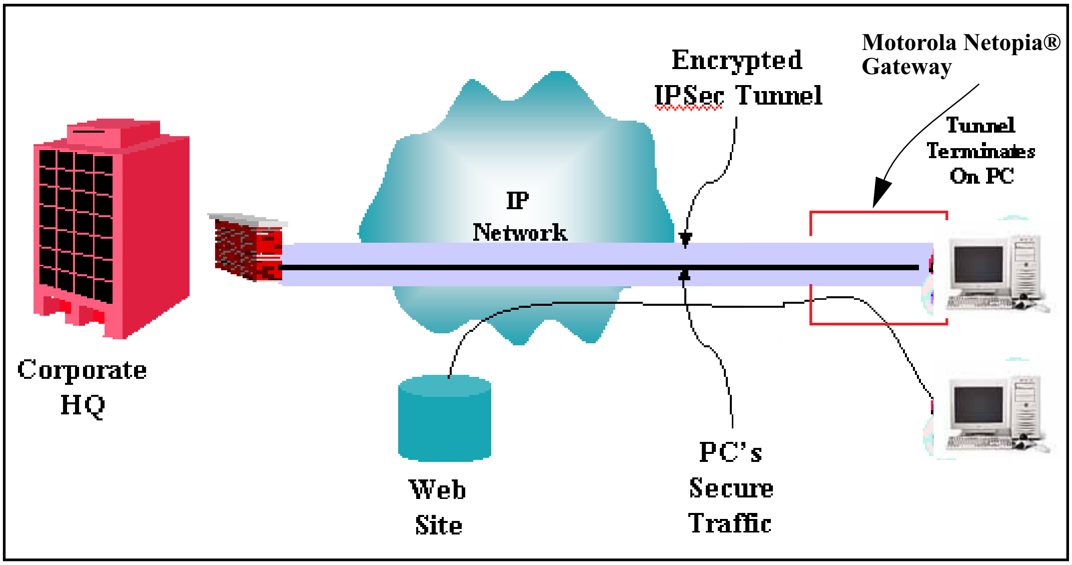
VPN IPSec Pass Through

This Motorola Netopia® service supports your independent VPN client software in a transparent manner. Motorola has implemented an Application Layer Gateway (ALG) to support multiple PCs running IP Security protocols.

This feature has three elements:

1. **On power up or reset, the address mapping function (NAT) of the Gateway's WAN configuration is turned on by default.**
2. **When you use your third-party VPN application, the Gateway recognizes the traffic from your client and your unit. It allows the packets to pass through the NAT "protection layer" via the encrypted IPSec tunnel.**
3. **The encrypted IPSec tunnel is established "through" the Gateway.**

A typical VPN IPSec Tunnel pass through is diagrammed below:



NOTE:

Typically, no special configuration is necessary to use the IPSec pass through feature.

In the diagram, VPN PC clients are shown behind the Motorola Netopia® Gateway and the secure server is at Corporate Headquarters across the WAN. You cannot have your secure server behind the Motorola Netopia® Gateway.

When multiple PCs are starting IPSec sessions, they must be started one at a time to allow the associations to be created and mapped.

VPN IPSec Tunnel Termination

This Motorola Netopia® service supports termination of VPN IPsec tunnels at the Gateway. This permits tunnelling from the Gateway without the use of third-party VPN client software on your client PCs. Currently one IPSec VPN tunnel is supported on Motorola Netopia® 2200 and 3300 Series Gateways. Unlike VPN Passthrough, IPsec VPN tunnel is a keyed feature that you can obtained from Motorola. See “Security Settings” on page 253.

Dynamic DNS

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. See “Dynamic DNS Settings” on page 210.

Stateful Inspection Firewall

Stateful inspection is a security feature that prevents unsolicited inbound access when NAT is disabled. You can configure UDP and TCP “no-activity” periods that will also apply to NAT time-outs if stateful inspection is enabled on the interface. Technical details are discussed in “Stateful Inspection” on page 262.

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 Motorola 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 Motorola 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 Motorola Netopia® Gateway

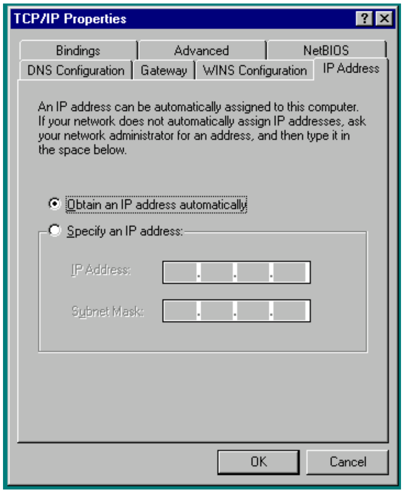
Refer to your *Quickstart Guide* for instructions on how to connect your Motorola Netopia® Gateway to your power source, PC or local area network, and your Internet access point, whether it is a dedicated DSL outlet or a DSL or cable modem. Different Motorola Netopia® Gateway models are supplied for 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. Windows 98, ME. and 2000 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***



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

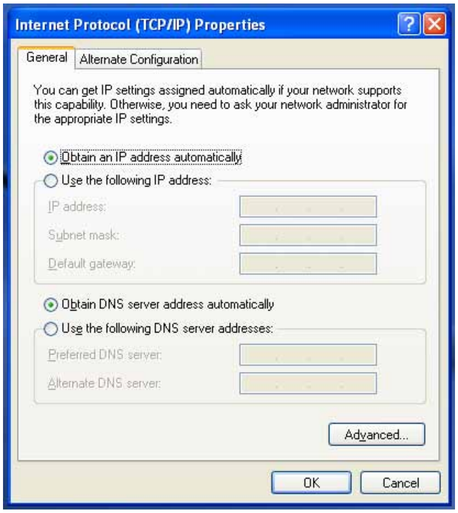
IP Address: . . .

Subnet Mask: . . .

b. Windows XP follows 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.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

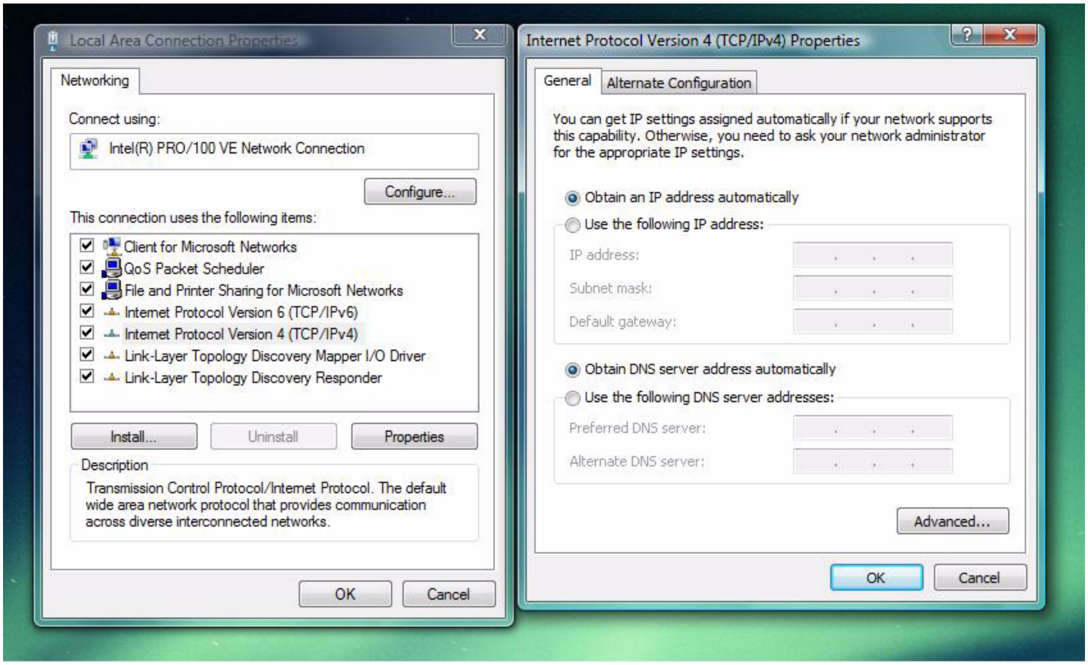
Step 3. Select *Obtain DNS server address automatically*, if available.

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

Step 5. OK the settings. Restart if prompted.

c. Windows Vista is set to obtain an IP address automatically by default. You may not need to configure it at all.

To check, open the **Networking** Control Panel and select **Internet Protocol Version 4 (TCP/IPv4)**. Click the **Properties** button.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address:
  - Subnet mask:
  - Default gateway:
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server:
  - Alternate DNS server:

The **Internet Protocol Version 4 (TCP/IPv4) Properties** window should appear as shown.

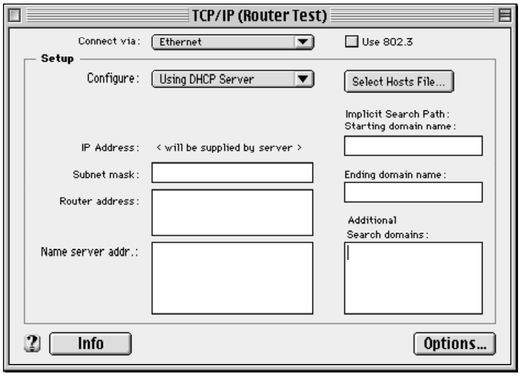
If not, select the radio buttons shown above, and click the **OK** button.

Macintosh MacOS 9 or higher or Mac OS X:

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

a. Mac OS 9 follows a path like this:

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



Connect via: Ethernet

□ Use 802.3

Configure: Using DHCP Server

IP Address: < will be supplied by server >

Subnet mask:

Router address:

Name server addr.:

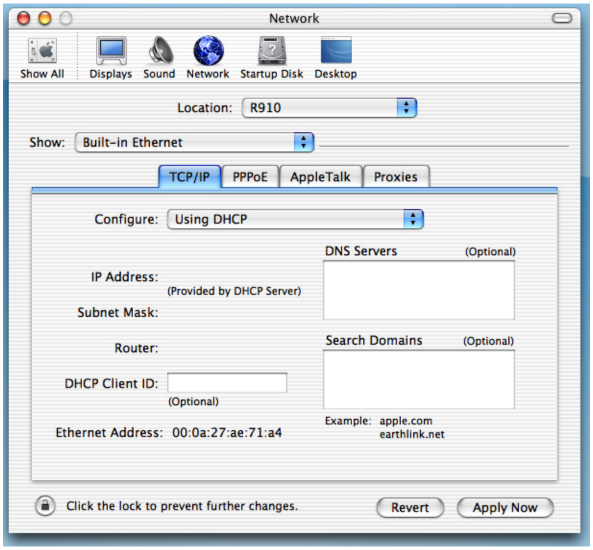
Implicit Search Path: Starting domain name:

Ending domain name:

Additional Search domains:

b. Mac OS X follows a path like this:

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



Location: R910

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: (Provided by DHCP Server)

Subnet Mask:

Router:

DHCP Client ID: (Optional)

DNS Servers (Optional)

Search Domains (Optional)

Example: apple.com
earthlink.net

Ethernet Address: 00:0a:27:ae:71:a4

Click the lock to prevent further changes.

Then go to Step 2.

Step 2. Select *Built-in Ethernet*

Step 3. Select *Configure Using DHCP*

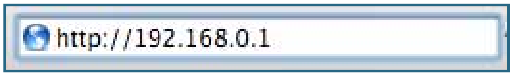
Step 4. Close and Save, if prompted.

Proceed to “Configure the Motorola Netopia® Gateway” on page 31.

Configure the Motorola Netopia® Gateway

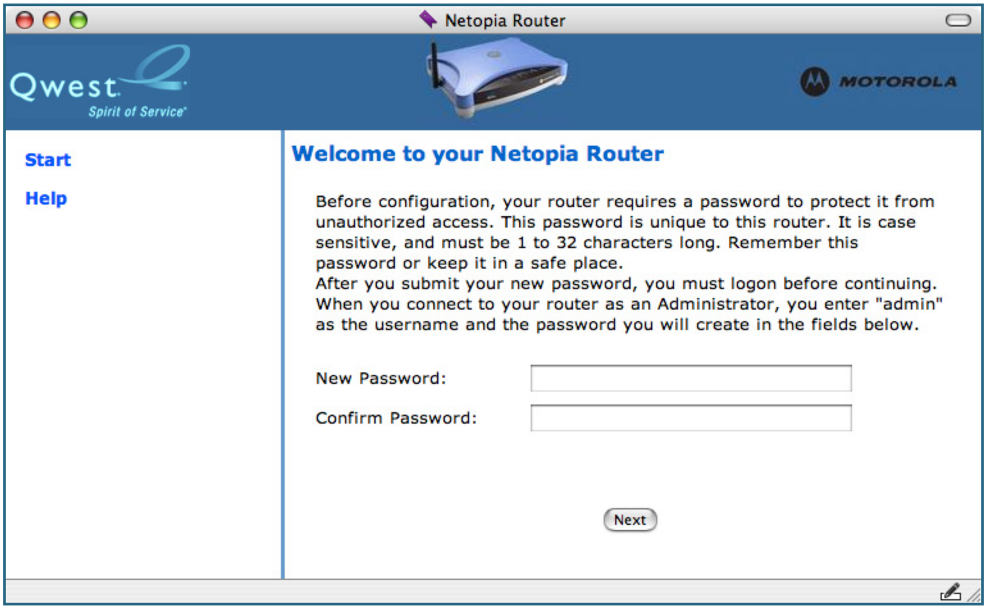
1. **Run your Web browser application, such as Firefox or Microsoft Internet Explorer, from the computer connected to the Motorola Netopia® Gateway.**

   Enter *http://192.168.0.1* in the URL Address text box. Press Enter or click Go.

   http://192.168.0.1

   The Admin Password page appears.

   Welcome to your Netopia Router

   Before configuration, your router requires a password to protect it from unauthorized access. This password is unique to this router. It is case sensitive, and must be 1 to 32 characters long. Remember this password or keep it in a safe place.
   After you submit your new password, you must logon before continuing. When you connect to your router as an Administrator, you enter "admin" as the username and the password you will create in the fields below.

   New Password:

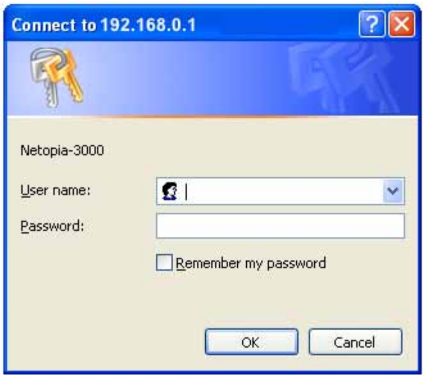
   Confirm Password:

   For security, you must create and enter an Administrative password for accessing the Motorola Netopia® Gateway.

   - The administrative User name is **admin.**
   - The initial Password can be whatever you choose, from one to 32 characters long.

   This user name and password are separate from the user name and password you will use to access the Internet. You may change them later. You will be challenged for this Admin username and password any time that you attempt to access the Motorola Netopia® Gateway's configuration pages.

When you connect to your Gateway as an Administrator, you enter “**admin**” as the User-Name and the Password you just created.



Connect to 192.168.0.1

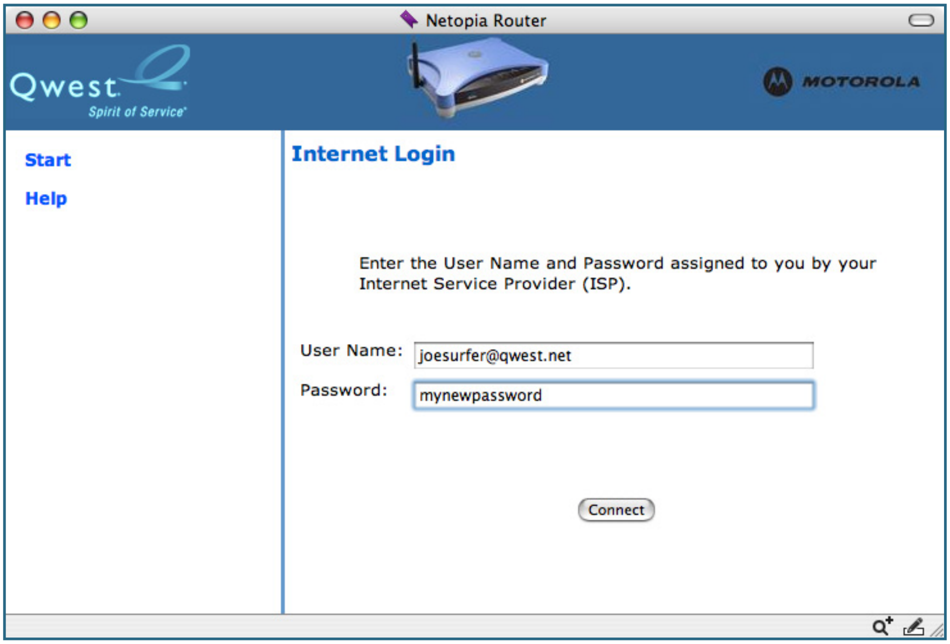
Netopia-3000

User name:

Password:

□ Remember my password

The browser displays the Internet Login page.



Internet Login

Enter the User Name and Password assigned to you by your Internet Service Provider (ISP).

User Name: joesurfer@qwest.net

Password: mynewpassword

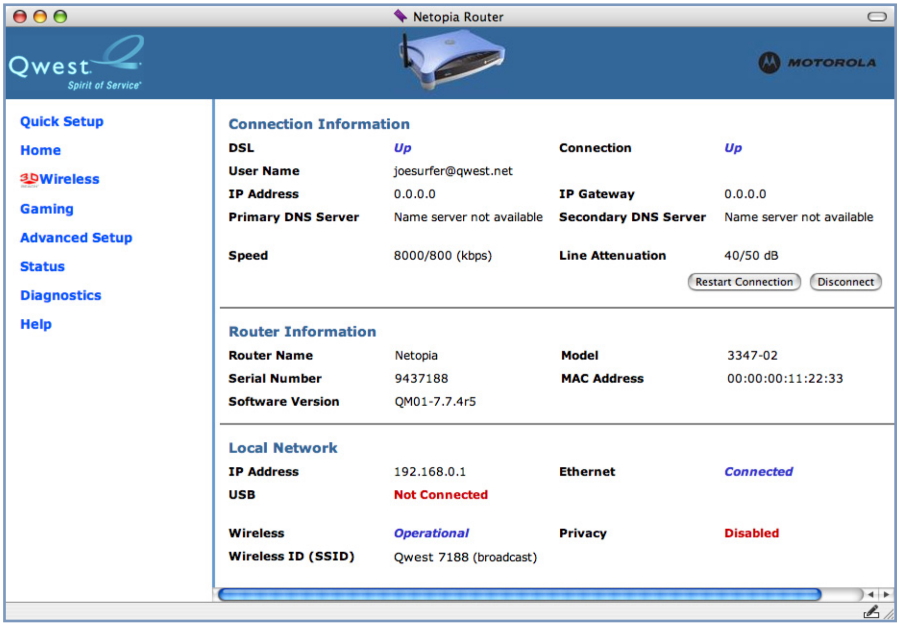
2. **Enter the User Name and Password supplied by your Internet Service Provider. Click the Connect button.**

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

3. **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.**

   You can access the Gateway's internal management pages at any time by entering *http://192.168.0.1* in your browser's address field.

   The Motorola Netopia® Gateway's home page appears.



Connection Information

DSL	Up	Connection	Up
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	IP Gateway	0.0.0.0
Primary DNS Server	Name server not available	Secondary DNS Server	Name server not available
Speed	8000/800 (kbps)	Line Attenuation	40/50 dB

Router Information

Router Name	Netopia	Model	3347-02
Serial Number	9437188	MAC Address	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

Local Network

IP Address	192.168.0.1	Ethernet	Connected
USB	Not Connected		
Wireless	Operational	Privacy	Disabled
Wireless ID (SSID)	Qwest 7188 (broadcast)		

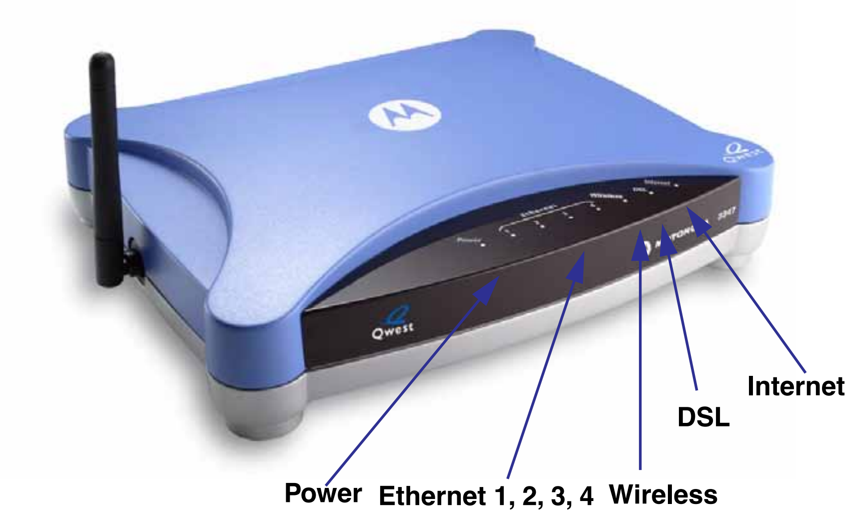
If you have any questions or encounter problems with your Motorola Netopia® Gateway, refer to the detailed documentation on the Motorola Netopia® CD, or contact your service provider's technical support helpdesk.

Answers to many frequently asked Motorola Netopia® modem questions are also available on-line at: http://www.netopia.com/support.

Motorola Netopia® Gateway Status Indicator Lights

Colored LEDs on your Motorola Netopia® Gateway indicate the status of various port activity. Also, see "Basic Troubleshooting" on page 157 for more information.

Motorola Netopia® Gateway 3347-02 status indicator lights

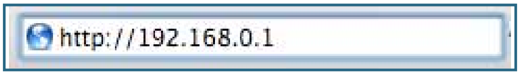


LED	Action
Power	**Green** when power is on. **Red** when updating embedded software, or for system failure.
Ethernet 1, 2, 3, 4	Solid **green** when connected. Flash **green** when there is activity on the LAN. **Red** when bad userid and password are entered.
Wireless	Flashes **green** when there is activity on the wireless LAN.
DSL	Solid **green** when Internet connection is established.
Internet	Solid **green** when router is connected. Flashes **green** when transmitting or receiving data.

Accessing the Web User Interface

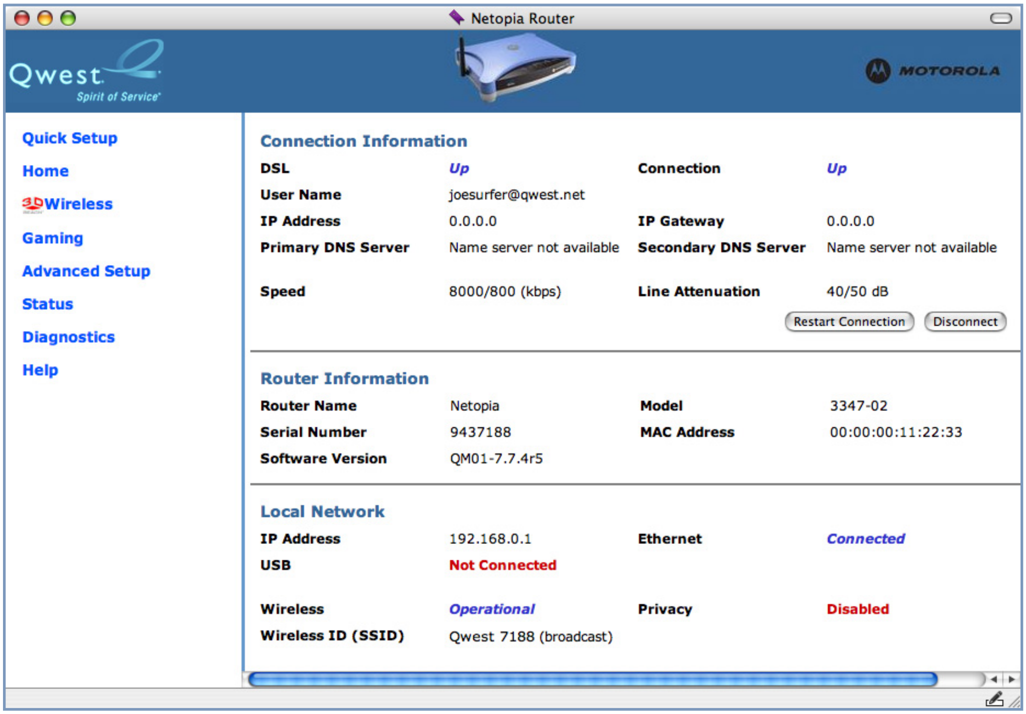
After you have performed the basic Quickstart configuration, any time you log in to your Motorola Netopia® Gateway you will access the Motorola Netopia® Gateway Home page.

You access the Home Page by typing http://192.168.0.1 in your Web browser's location box.



http://192.168.0.1

The Basic Mode Home Page appears.



Connection Information

DSL	*Up*	Connection	*Up*
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	IP Gateway	0.0.0.0
Primary DNS Server	Name server not available	Secondary DNS Server	Name server not available
Speed	8000/800 (kbps)	Line Attenuation	40/50 dB

Router Information

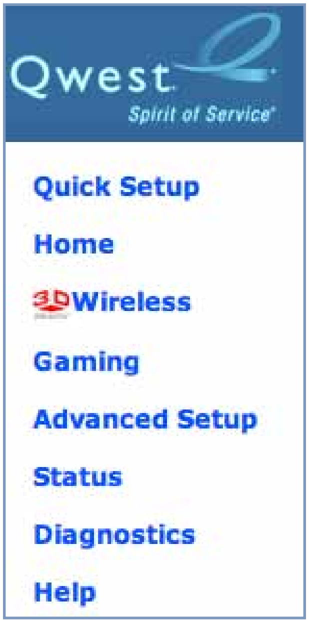
Router Name	Netopia	Model	3347-02
Serial Number	9437188	MAC Address	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

Local Network

IP Address	192.168.0.1	Ethernet	*Connected*
USB	Not Connected		
Wireless	*Operational*	Privacy	Disabled
Wireless ID (SSID)	Qwest 7188 (broadcast)		

The links 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.

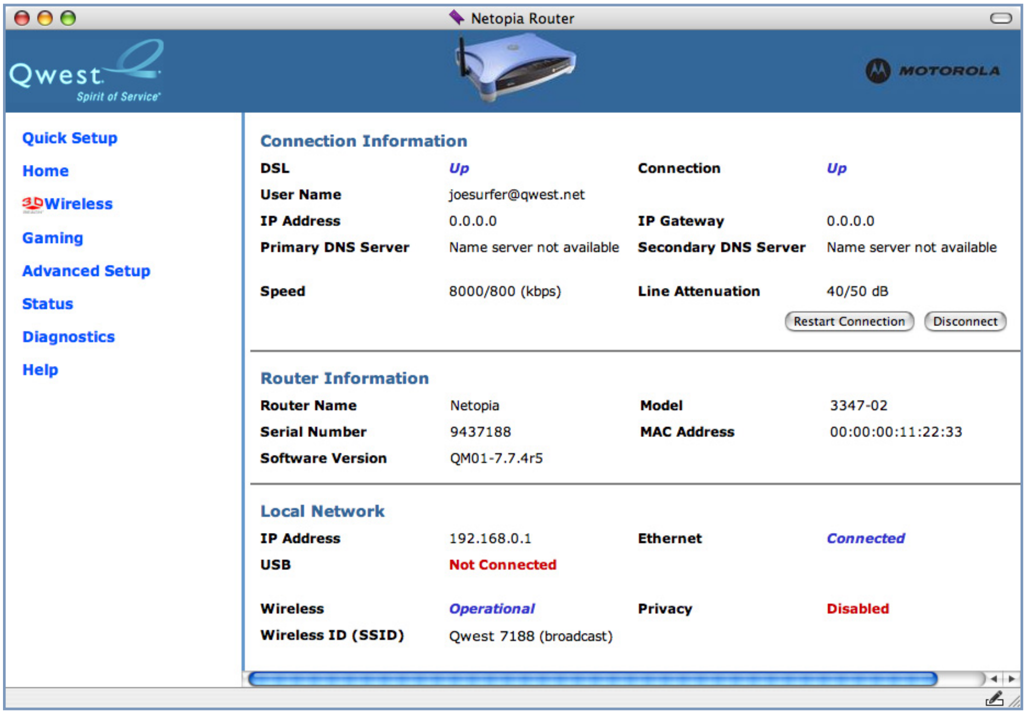
Links Bar



The Links Bar is the frame at the left-hand side of the page containing the major navigation links. These links are available from almost every page, allowing you to move freely about the site. The headings in the following table are hyperlinks. You can click on any heading to read about that feature.

"Home" on page 37
"Wireless" on page 39
"Gaming" on page 58
"Advanced Setup" on page 65
"Status" on page 66
"Diagnostics" on page 71
"Help" on page 72

Home



Connection Information

DSL	Up	Connection	Up
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	IP Gateway	0.0.0.0
Primary DNS Server	Name server not available	Secondary DNS Server	Name server not available
Speed	8000/800 (kbps)	Line Attenuation	40/50 dB

Router Information

Router Name	Netopia	Model	3347-02
Serial Number	9437188	MAC Address	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

Local Network

IP Address	192.168.0.1	Ethernet	Connected
USB	Not Connected		
Wireless	Operational	Privacy	Disabled
Wireless ID (SSID)	Qwest 7188 (broadcast)		

Home Page Information

The Home page displays information about the following categories:

- Connection Information
- Router Information
- Local Network

Click the Help link in the left-hand column of links to display a page of explanatory information. Help is available for every page in the Web interface.

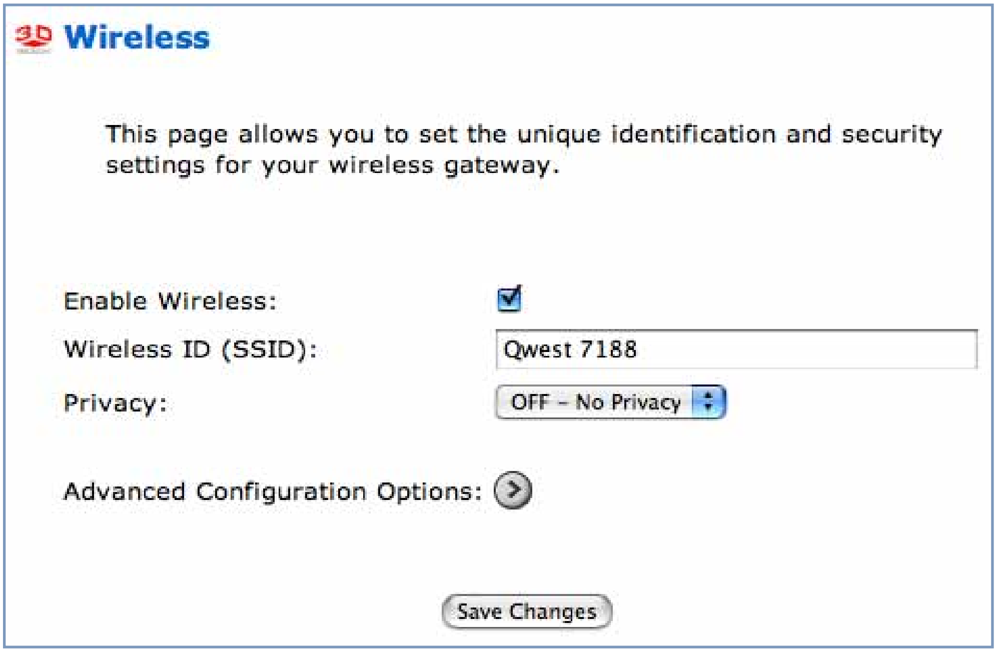
Home Page Links

The links in the left-hand column of the Home page access a series of pages to allow you to monitor, diagnose, and update your router. The following sections give descriptions of these pages.

Link: Wireless

(supported models only)

When you click **Wireless**, the 3-D Reach **Wireless** configuration page appears.



Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless: ☑

Wireless ID (SSID): Qwest 7188

Privacy: OFF - No Privacy

Enable Wireless

The wireless function is not automatically enabled by default. If you check the **Enable Wireless** checkbox, the Wireless Options are enabled, and the Gateway will provide or broadcast its wireless LAN services.

Wireless ID (SSID)

The Wireless ID is preset to a number unique to your unit. You can either leave it as is, or change it by entering a freeform name of up to 32 characters, for example “Hercule’s Wireless LAN”. On client PCs’ software, this might also be called the *Network Name*. The Wireless ID is used to identify this particular wireless LAN. Depending on their operating system or client wireless card, users must either:

- select from a list of available wireless LANs that appear in a scanned list on their client

- or enter this name on their clients in order to join this wireless LAN.

Privacy

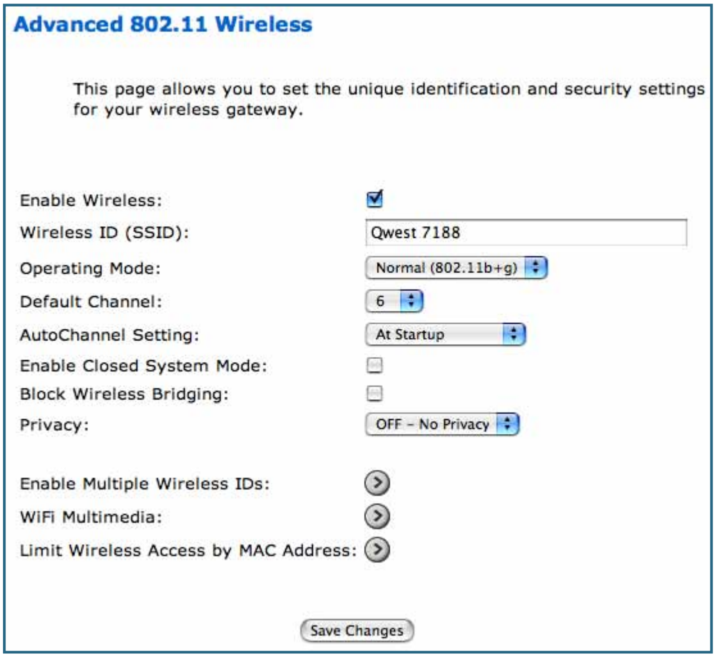
The pull-down menu for enabling **Privacy** offers four settings: **WPA-802.1x, WPA-PSK**, **WEP-Manual**, and **Off - No Privacy.**

IT IS STRONGLY RECOMMENDED THAT YOU ENABLE SOME FORM OF PRIVACY FOR THE SECURITY OF YOUR WIRELESS NETWORK.

See “Privacy” on page 44 for more information.

Advanced Configuration Options (optional)

When you click the Advanced Configuration Options button, the **Advanced 802.11 Wireless** screen appears. This screen varies its options depending on which form of wireless Privacy you have selected.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	□
Block Wireless Bridging:	□
Privacy:	OFF – No Privacy
Enable Multiple Wireless IDs:	⊙
WiFi Multimedia:	⊙
Limit Wireless Access by MAC Address:	⊙

Operating Mode

The pull-down menu allows you to select and lock the Gateway into the wireless transmission mode you want. For compatibility with clients using 802.11**b** (up to 11 Mbps transmission) and 802.11**g** (up to 20+ Mbps), select **Normal (802.11b + g)**. To limit your wireless LAN to one mode or the other, select **802.11b Only**, or **802.11g Only**.

NOTE:

If you choose to limit the operating mode to 802.11b or 802.11g only, clients using the mode you excluded will not be able to connect.

Default Channel

(1 through 11, for North America) on which the network will broadcast. This is a frequency range within the 2.4Ghz band. Channel selection depends on government regulated radio frequencies that vary from region to region. The widest range available is from 1 to 14. Europe, France, Spain and Japan differ. Channel selection can have a significant impact on performance, depending on other wireless activity close to this Router. Channel selection is not necessary at the client computers; the clients will scan the available channels seeking access points using the same SSID as the client.

AutoChannel Setting

For 802.11G models, AutoChannel is a feature that allows the Motorola Netopia® Gateway to determine the best channel to broadcast automatically.

Three settings are available from the pull-down menu: **Off-Use default**, **At Startup**, and **Continuous**.

- **Off-Use default**: the Motorola Netopia® Gateway will use the configured default channel selected from the previous pull-down menu.
- **At Startup** – the default setting – causes the Motorola Netopia® Gateway at startup to briefly initialize on the default channel, then perform a full two- to three-second scan, and switch to the best channel it can find, remaining on that channel until the next reboot.
- **Continuous** performs the at-startup scan, and will continuously monitor the current channel for any other Access Point beacons. If an Access Point beacon is detected on the same channel, the Motorola Netopia® Gateway will initiate a three- to four-minute scan of the channels, locate a better one, and switch. Once it has switched, it will remain on this channel for at least 30 minutes before switching again if another Access Point is detected.

Enable Closed System Mode

If enabled, Closed System Mode hides the wireless network from the scanning features of wireless client computers. Unless both the wireless clients and the Router share the same Wireless ID in Closed System mode, the Router’s wireless LAN will not appear as an available network when scanned for by wireless-enabled computers. Members of the Closed System WLAN must log onto the Router’s wireless network with the identical SSID as that configured in the router.

Closed System mode is an ideal way to increase wireless security and to prevent casual detection by unwanted neighbors, office users, or malicious users such as hackers.

If you do not enable Closed System Mode, it is more convenient, but potentially less secure, for clients to access your WLAN by scanning available access points. You must decide based on your own network requirements.

About Closed System Mode and Wireless Encryption

Enabling Closed System Mode on your wireless Router provides another level of security, since your wireless LAN will no longer appear as an available access point to client PCs that are casually scanning for one.

Your own wireless network clients, however, must log into the wireless LAN by using the exact SSID of the Motorola Netopia® Router.

In addition, if you have enabled WEP or WPA encryption on the Motorola Netopia® Router, your network clients must also have WEP or WPA encryption enabled, and must have the same WEP or WPA encryption key as the Motorola Netopia® Router.

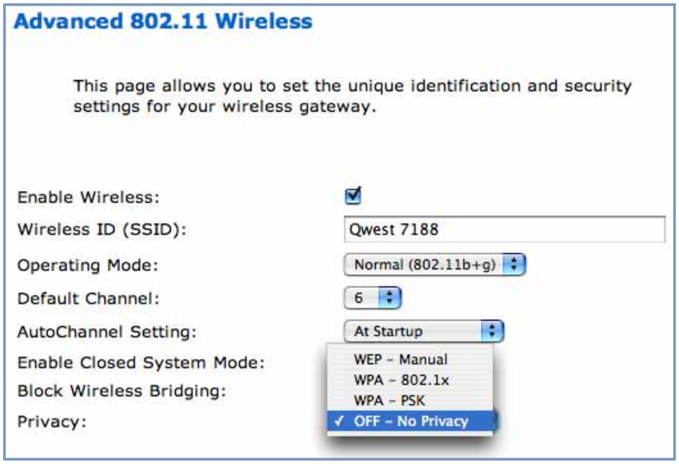
Once the Motorola Netopia® Gateway is located by a client computer, by setting the client to a matching SSID, the client can connect immediately if WEP or WPA is not enabled. If WEP or WPA is enabled then the client must also have WEP or WPA enabled and a matching WEP or WPA key.

Wireless client cards from different manufacturers and different operating systems accomplish connecting to a wireless LAN and enabling WEP or WPA in a variety of ways. Consult the documentation for your particular wireless card and/or operating system.

Block Wireless Bridging

Check the checkbox to block wireless clients from communicating with other wireless clients on the LAN side of the Gateway.

Privacy



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless: ☑

Wireless ID (SSID): Qwest 7188

Operating Mode: Normal (802.11b+g)

Default Channel: 6

AutoChannel Setting: At Startup

Enable Closed System Mode:

Block Wireless Bridging:

Privacy: ✓ OFF – No Privacy

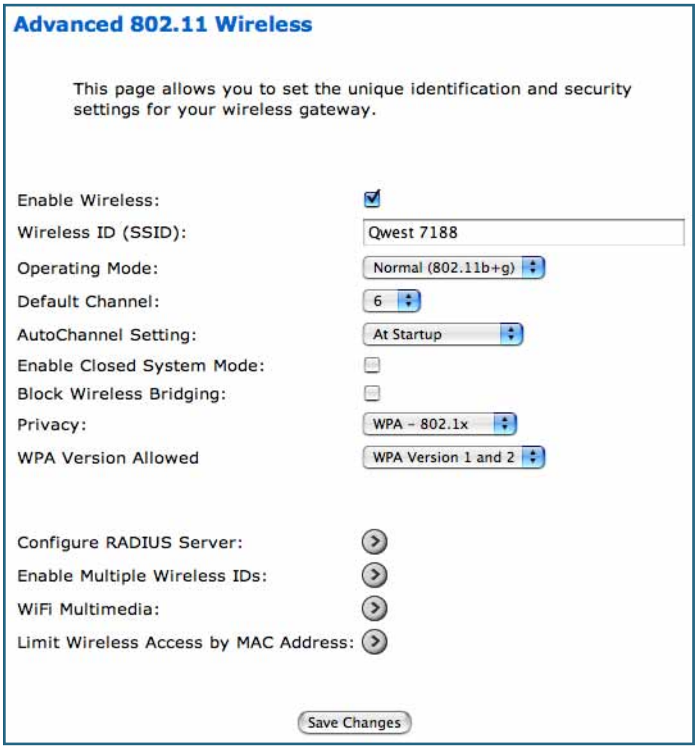
- **OFF - No Privacy:** This mode disables privacy on your network, allowing any wireless users to connect to your wireless LAN. Use this option if you are using alternative security measures such as VPN tunnels, or if your network is for public use.
- **WEP - Manual:** WEP Security is a Privacy option that is based on encryption between the Router and any PCs (“clients”) you have with wireless cards. If you are not using WPA-PSK Privacy, you can use WEP Encryption instead. For this encryption to work, both your Router and each client must share the same Wireless ID, and both must be using the same encryption keys.
- **WPA-802.1x** provides RADIUS server authentication support. See RADIUS Server authentication below.
- **WPA-PSK** provides Wireless Protected Access, the most secure option for your wireless network. See “WPA-PSK” on page 47. This mechanism provides the best data protection and access control.

  Be sure that your Wi-Fi client adapter supports this option. Not all Wi-Fi clients support WPA-PSK.

RADIUS Server authentication

RADIUS servers allow external authentication of users by means of a remote authentication database. The remote authentication database is maintained by a Remote Authentication Dial-In User Service (RADIUS) server. In conjunction with Wireless User Authentication, you can use a RADIUS server database to authenticate users seeking access to the wireless services, as well as the authorized user list maintained locally within the Gateway.

If you select **WPA-802.1x**, the screen expands.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	☐
Block Wireless Bridging:	☐
Privacy:	WPA - 802.1x
WPA Version Allowed	WPA Version 1 and 2

Configure RADIUS Server:

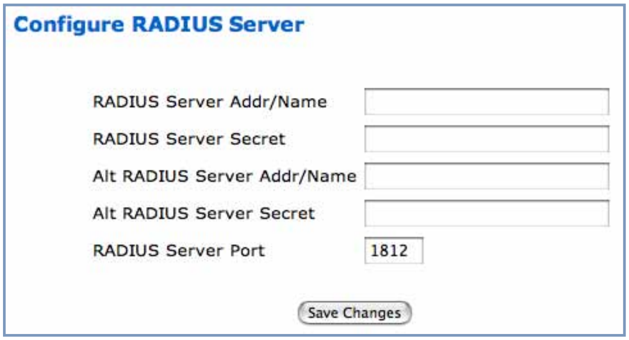
Enable Multiple Wireless IDs:

WiFi Multimedia:

Limit Wireless Access by MAC Address:

Click the **Configure RADIUS Server** button.

The Configure RADIUS Server screen appears.



Configure RADIUS Server

RADIUS Server Addr/Name

RADIUS Server Secret

Alt RADIUS Server Addr/Name

Alt RADIUS Server Secret

RADIUS Server Port 1812

Enter your RADIUS Server information in the appropriate fields:

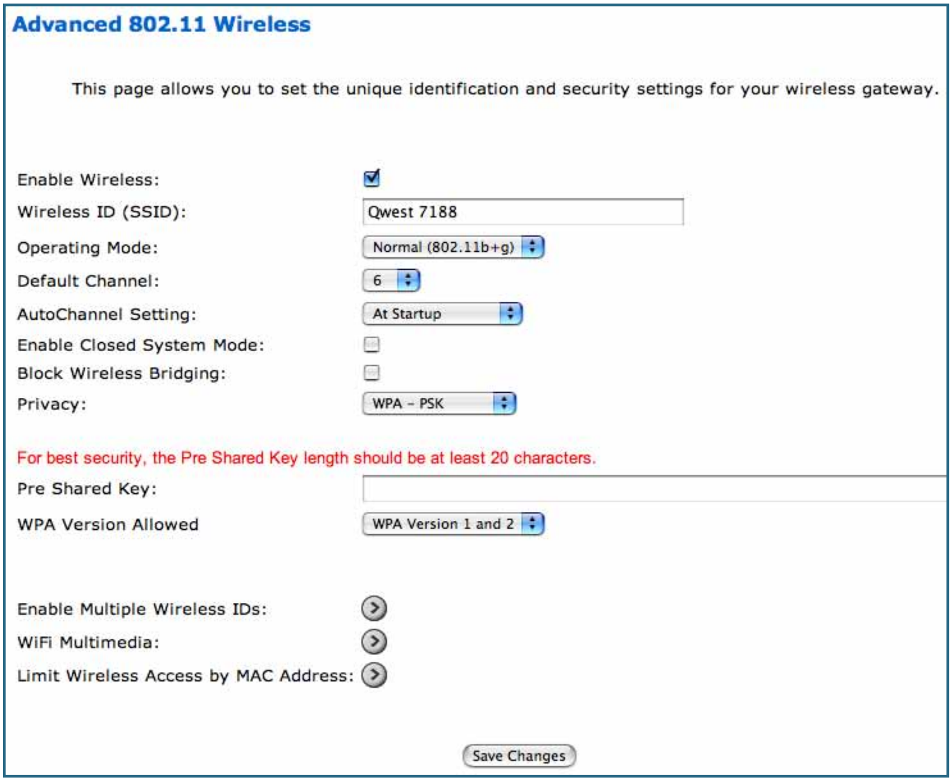
- **RADIUS Server Addr/Name:** The default RADIUS server name or IP address that you want to use.
- **RADIUS Server Secret:** The RADIUS secret key used by this server. The shared secret should have the same characteristics as a normal password.
- **Alt RADIUS Server Addr/Name:** An alternate RADIUS server name or IP address, if available.
- **Alt RADIUS Server Secret:** The RADIUS secret key used by this alternate server. The shared secret should have the same characteristics as a normal password.
- **RADIUS Server Port:** The port on which the RADIUS server is listening, typically, the default 1812.

Click the **Save Changes** button.

WPA-PSK

One of the easiest ways to enable Privacy on your Wireless network is by selecting **WPA-PSK** (Wi-Fi Protected Access) from the pull-down menu.

The screen expands to allow you to enter a **Pre Shared Key**. The key can be between 8 and 63 characters, but for best security it should be at least 20 characters. When you have entered your key, click the **Save Changes** button.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

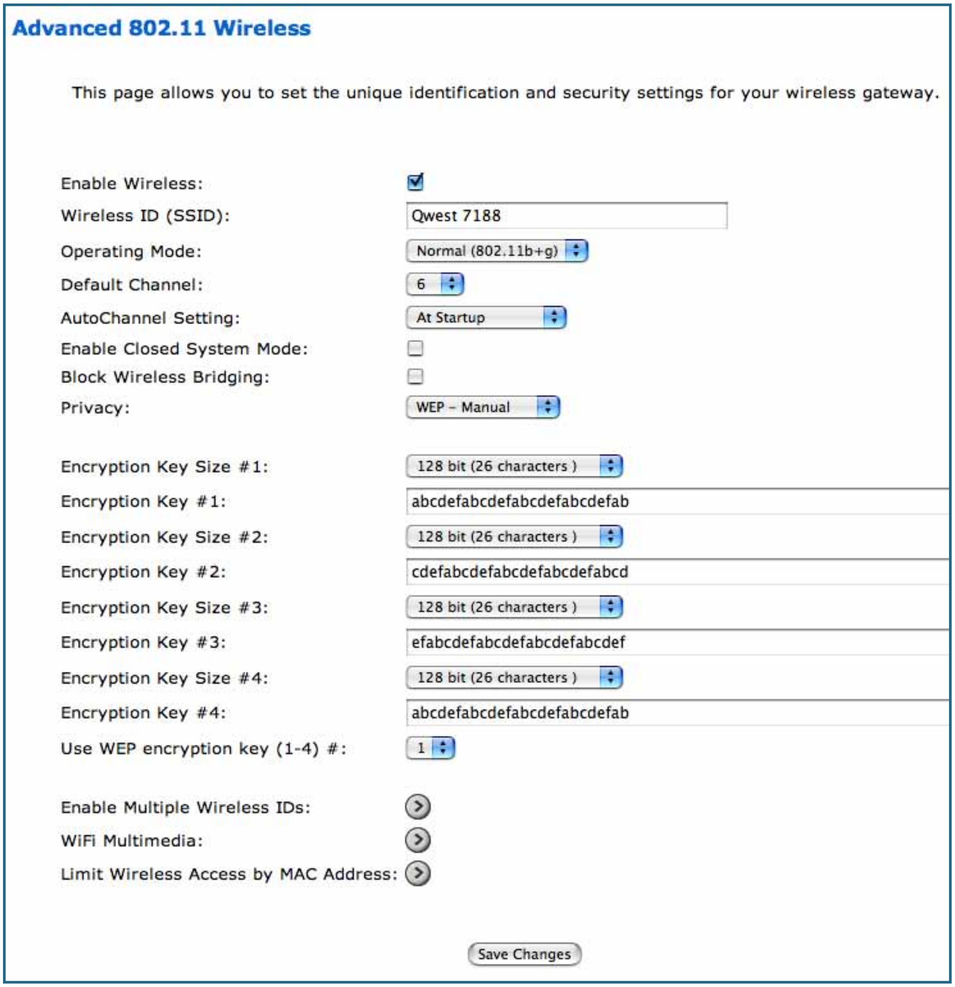
Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	□
Block Wireless Bridging:	□
Privacy:	WPA - PSK

For best security, the Pre Shared Key length should be at least 20 characters.

Pre Shared Key:	
WPA Version Allowed	WPA Version 1 and 2
Enable Multiple Wireless IDs:	>
WiFi Multimedia:	>
Limit Wireless Access by MAC Address:	>

WEP-Manual

Alternatively, you can enable WEP (Wired Equivalent Privacy) encryption by selecting **WEP-Manual** from the Privacy pull-down menu.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	□
Block Wireless Bridging:	□
Privacy:	WEP – Manual
Encryption Key Size #1:	128 bit (26 characters)
Encryption Key #1:	abcdefabcdefabcdefabcdefab
Encryption Key Size #2:	128 bit (26 characters)
Encryption Key #2:	cdefabcdefabcdefabcdefabcd
Encryption Key Size #3:	128 bit (26 characters)
Encryption Key #3:	efabcdefabcdefabcdefabcdef
Encryption Key Size #4:	128 bit (26 characters)
Encryption Key #4:	abcdefabcdefabcdefabcdefab
Use WEP encryption key (1-4) #:	1
Enable Multiple Wireless IDs:	›
WiFi Multimedia:	›
Limit Wireless Access by MAC Address:	›

You can provide a level of data security by enabling WEP (Wired Equivalent Privacy) for encryption of network data. You can enable 40-, 128-, or 256-bit WEP Encryption (depending on the capability of your client wireless card) for IP traffic on your LAN.

WEP - Manual allows you to enter your own encryption keys manually. This is a difficult process, but only needs to be done once. Avoid the temptation to enter all the same characters.

Encryption Key Size #1 – #4: Selects the length of each encryption key. The longer the key, the stronger the encryption and the more difficult it is to break the encryption.

Encryption Key #1 – #4: The encryption keys. You enter keys using hexadecimal digits. For 40/64bit encryption, you need ten digits; 26 digits for 128bit, and 58 digits for 256bit WEP. Hexadecimal characters are 0 – 9, and a – f.

Examples:

- 40bit: 02468ACE02
- 128bit: 0123456789ABCDEF0123456789
- 256bit: 592CA140F0A238B0C61AE162F592CA140F0A238B0C61AE162F21A09C

Use WEP encryption key (1 – 4) #: Specifies which key the Gateway will use to encrypt transmitted traffic. The default is key #1.

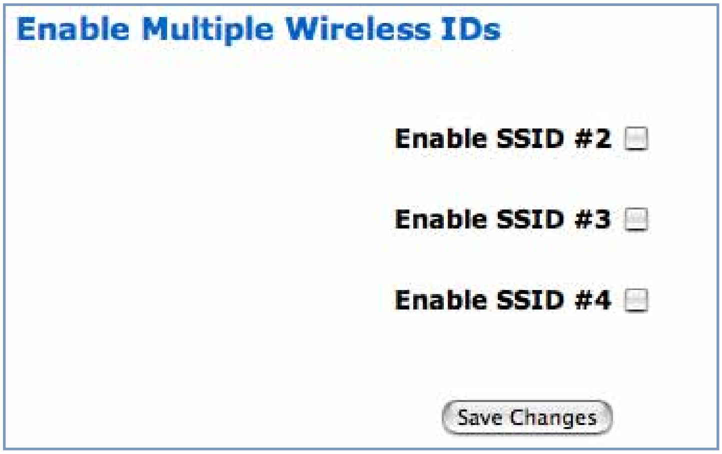
Click the click **Save Changes** button.

Any WEP-enabled client must have an identical key of the same length as the Router, in order to successfully receive and decrypt the traffic. Similarly, the client also has a ‘default’ key that it uses to encrypt its transmissions. In order for the Router to receive the client’s data, it must likewise have the identical key of the same length.

Enable Multiple Wireless IDs

This feature allows you to add additional network identifiers (SSIDs or *Network Names*) for your wireless network. To enable Multiple Wireless IDs, click the button.

The **Enable Multiple Wireless IDs** screen appears to allow you to add up to three additional Wireless IDs.



Enable Multiple Wireless IDs

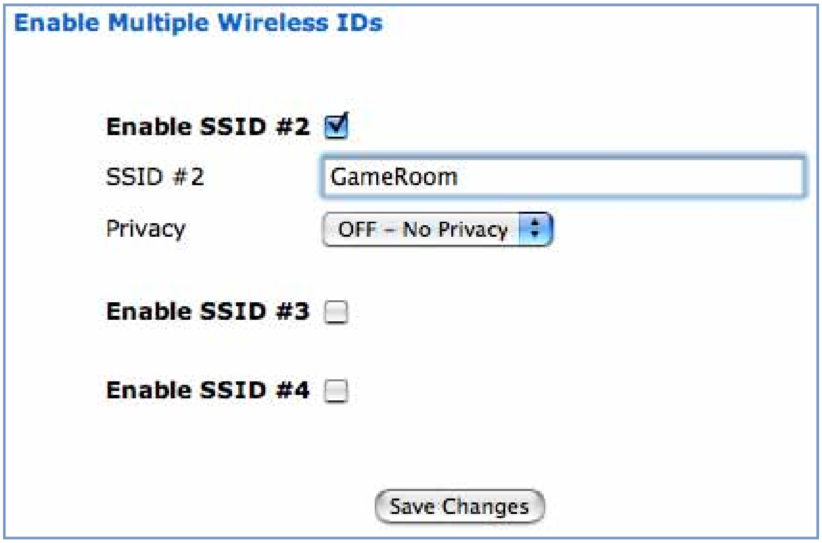
Enable SSID #2 □

Enable SSID #3 □

Enable SSID #4 □

When the Multiple Wireless SSIDs screen appears, check the **Enable SSID** checkbox for each SSID you want to enable.

The screen expands to allow you to name each additional Wireless ID, and specify a Privacy mode for each one.



Enable Multiple Wireless IDs

Enable SSID #2 ☑

SSID #2: GameRoom

Privacy: OFF – No Privacy

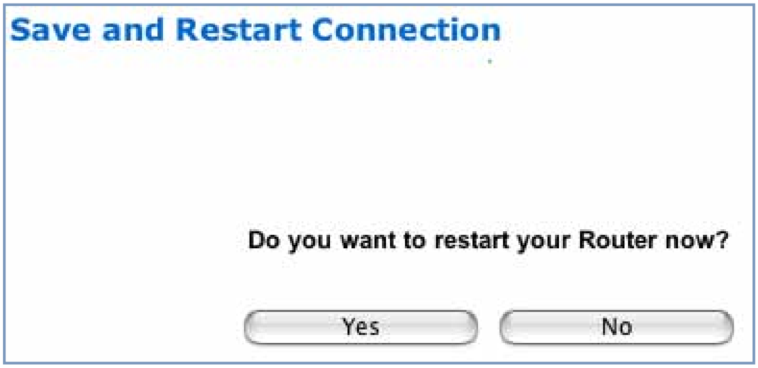
Enable SSID #3 □

Enable SSID #4 □

Privacy modes available from the pull-down menu for the multiple SSIDs are: **WPA-PSK**, **WPA-802.1x**, or **Off-No Privacy**.

These additional Wireless IDs are “Closed System Mode” Wireless IDs (see below) that will not be shown by a client scan, and therefore must be manually configured at the client. In addition, wireless bridging between clients is disabled for all members of these additional network IDs.

Click the **Save Changes** button. The Gateway will prompt you to restart it.



Save and Restart Connection

Do you want to restart your Router now?

Click the **Yes** button, and the Gateway will restart with your new settings.

NOTES:

The Gateway supports up to 4 different SSIDs:

- One SSID is broadcast by default and has wireless bridging enabled by default.
- Three additional SSIDs are in “Closed System Mode” and have wireless bridging disabled.
- These network IDs cannot be configured separately in terms of MAC Address filtering.
- You can configure privacy on one SSID and disable it on another SSID.

WiFi Multimedia

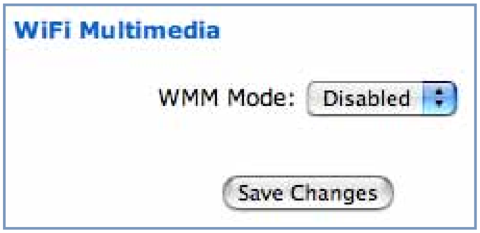
WiFi Multimedia is an advanced feature that allows you to prioritize various types of data travelling over the wireless network. Certain types of data that are sensitive to delays, such as voice or video, must be prioritized ahead of other, less delay-sensitive types, such as email.

WiFi Multimedia currently implements wireless Quality of Service (QoS) by transmitting data depending on Diffserv priority settings. These priorities are mapped into four Access Categories (AC), in increasing order of priority:

- Background (BK),
- Best Effort (BE),
- Video (VI), and
- Voice (VO).

It requires WiFi Multimedia (WMM)-capable clients, usually a separate feature enabled at the client network settings, and client PC software that makes use of Differentiated Services (Diffserv). Refer to your operating system instructions for enabling Diffserv QoS.

When you click the **WiFi Multimedia** button the **WiFi Multimedia** page appears.

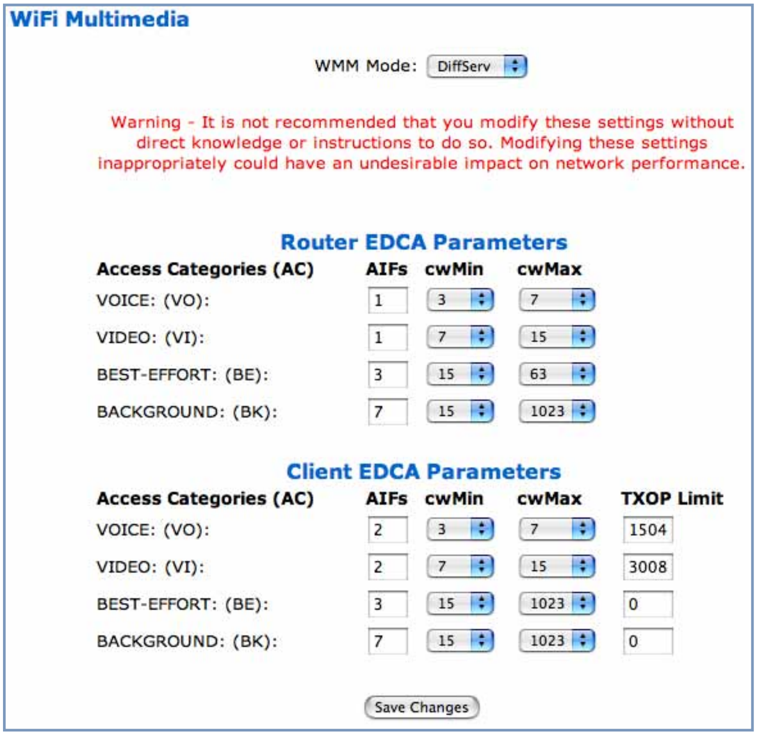


WiFi Multimedia

WMM Mode: Disabled

To enable the WiFi Multimedia custom settings, select **Diffserv** from the pull-down menu.

The screen expands.



WiFi Multimedia

WMM Mode: DiffServ

Warning - It is not recommended that you modify these settings without direct knowledge or instructions to do so. Modifying these settings inappropriately could have an undesirable impact on network performance.

Router EDCA Parameters

Access Categories (AC)	AIFs	cwMin	cwMax
VOICE: (VO):	1	3	7
VIDEO: (VI):	1	7	15
BEST-EFFORT: (BE):	3	15	63
BACKGROUND: (BK):	7	15	1023

Client EDCA Parameters

Access Categories (AC)	AIFs	cwMin	cwMax	TXOP Limit
VOICE: (VO):	2	3	7	1504
VIDEO: (VI):	2	7	15	3008
BEST-EFFORT: (BE):	3	15	1023	0
BACKGROUND: (BK):	7	15	1023	0

Router EDCA Parameters (Enhanced Distributed Channel Access) govern wireless data from your Gateway to the client; **Client EDCA Parameters** govern wireless data from the client to your Gateway.

NOTE:

It is not recommended that you modify these settings without direct knowledge or instructions to do so. Modifying these settings inappropriately could seriously degrade network performance.

- **AIFs**: (Arbitration Interframe Spacing) the wait time in milliseconds for data frames.
- **cwMin**: (Minimum Contention Window) upper limit in milliseconds of the range for determining initial random backoff. The value you choose must be lower than cwMax.

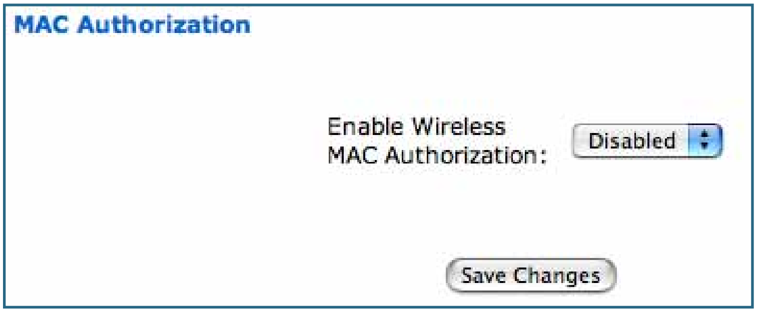
- **cwMax**: (Maximum Contention Window) upper limit in milliseconds of the range of determining final random backoff. The value you choose must be higher than cwMin.
- **TXOP Limit**: Time interval in microseconds that clients may initiate transmissions.

  (When **Operating Mode** is **B-only**, default values are used and this field is not configurable.)

Click the **Save Changes** button.

Wireless MAC Authorization (optional)

MAC Authorization allows you to specify which client PCs are allowed to join the wireless LAN by unique hardware (MAC) address. To enable this feature, click the **Limit Wireless Access by MAC Address** button. The MAC Authorization screen appears.

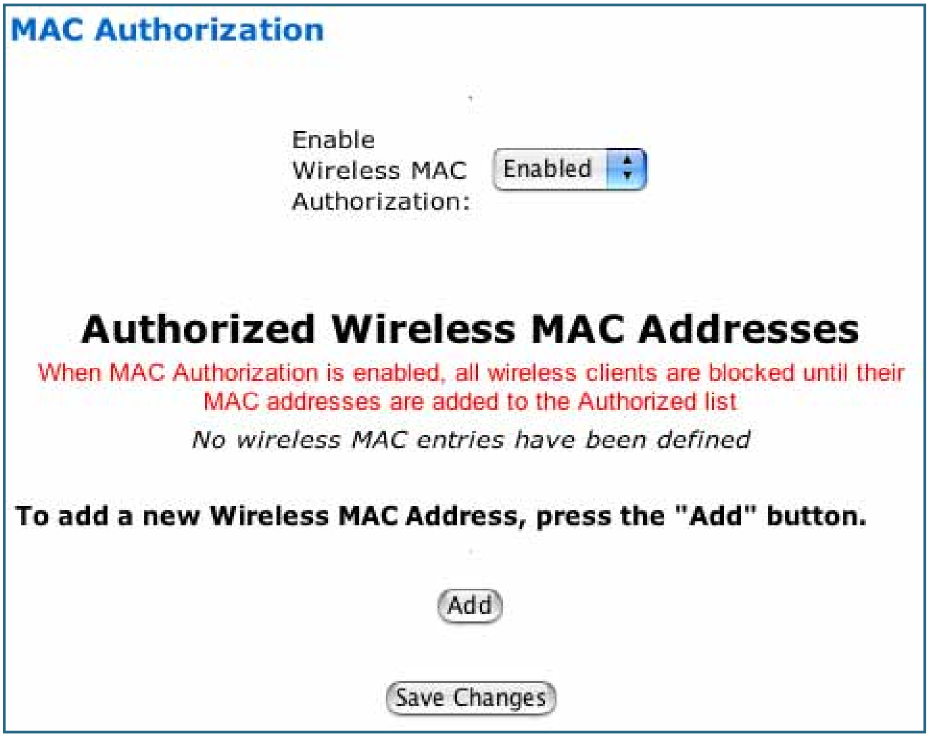


MAC Authorization

Enable Wireless MAC Authorization: Disabled

Select **Enabled** from the pull-down menu.

The screen expands to permit you to add MAC addresses.



MAC Authorization

Enable Wireless MAC Authorization: Enabled

Authorized Wireless MAC Addresses

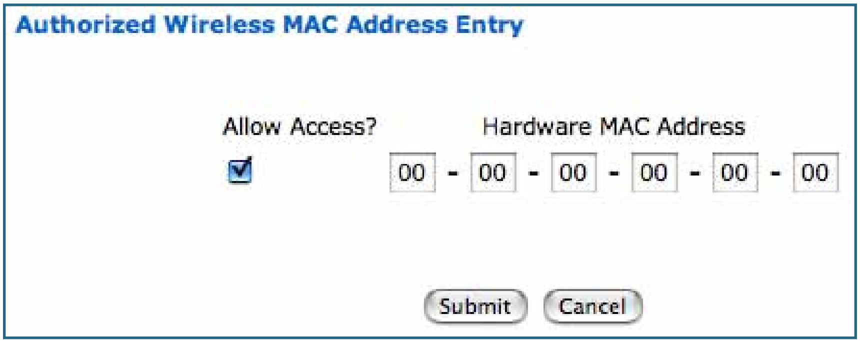
When MAC Authorization is enabled, all wireless clients are blocked until their MAC addresses are added to the Authorized list

No wireless MAC entries have been defined

To add a new Wireless MAC Address, press the "Add" button.

Click the **Add** button.

Once it is enabled, only entered MAC addresses that have been set to ***Allow*** will be accepted onto the wireless LAN. All unlisted addresses will be blocked, in addition to the listed addresses with *Allow* disabled.

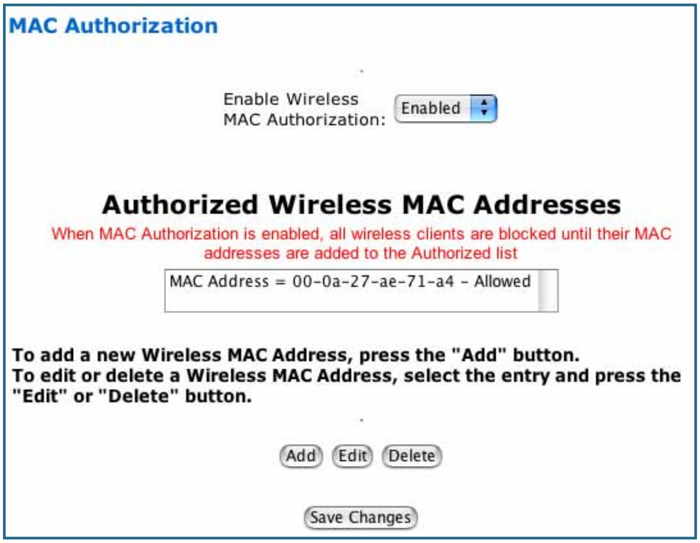


Authorized Wireless MAC Address Entry

Allow Access? ☑

Hardware MAC Address: 00 - 00 - 00 - 00 - 00 - 00

Click the **Submit** button.



MAC Authorization

Enable Wireless MAC Authorization: Enabled

Authorized Wireless MAC Addresses

When MAC Authorization is enabled, all wireless clients are blocked until their MAC addresses are added to the Authorized list

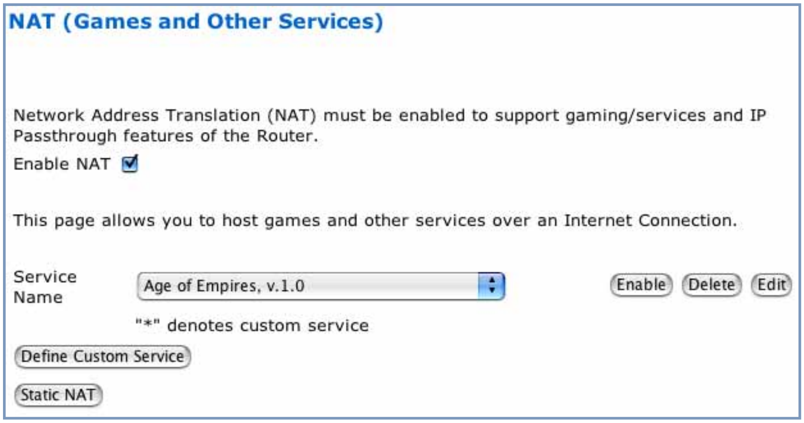
MAC Address = 00-0a-27-ae-71-a4 - Allowed

To add a new Wireless MAC Address, press the "Add" button.
To edit or delete a Wireless MAC Address, select the entry and press the "Edit" or "Delete" button.

When you are finished adding MAC addresses click the **Save Changes** button. You will be returned to the 802.11 Wireless page. You can **Add**, **Edit**, or **Delete** any of your entries later by returning to this page.

Link: Gaming

When you click Gaming, the **NAT (Games and Other Services)** page appears.



NAT (Games and Other Services)

Network Address Translation (NAT) must be enabled to support gaming/services and IP Passthrough features of the Router.

Enable NAT ☑

This page allows you to host games and other services over an Internet Connection.

Service Name: Age of Empires, v.1.0

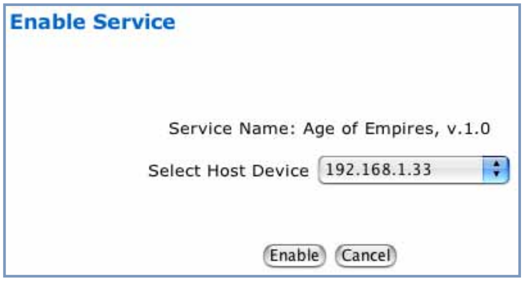
"*" denotes custom service

NAT (Games and Other Services) allows you to host internet applications when NAT is enabled. You can host different games and software on different PCs. If you uncheck the **Enable NAT** checkbox, the rest of the information on the page is hidden.

From the **Service Name** pull-down menu, you can select any of a large number of pre-defined games and software. (See "Supported Games and Software" on page 59.)

1. **Once you choose a software service or game, click Enable.**

   The Enable Service screen appears.

   Enable Service

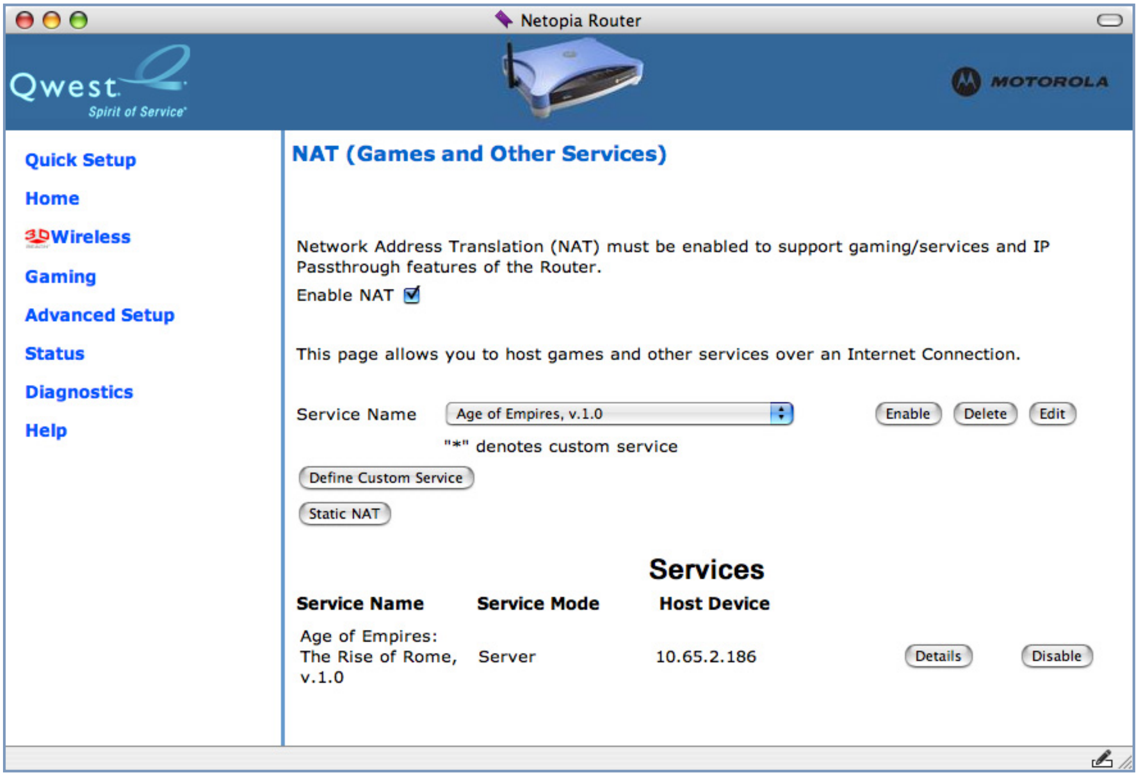
   Service Name: Age of Empires, v.1.0

   Select Host Device: 192.168.1.33

   Select 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.



NAT (Games and Other Services)

Network Address Translation (NAT) must be enabled to support gaming/services and IP Passthrough features of the Router.

Enable NAT ☑

This page allows you to host games and other services over an Internet Connection.

Service Name: Age of Empires, v.1.0

"*" denotes custom service

Services

Service Name	Service Mode	Host Device
Age of Empires: The Rise of Rome, v.1.0	Server	10.65.2.186

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

Supported Games and Software

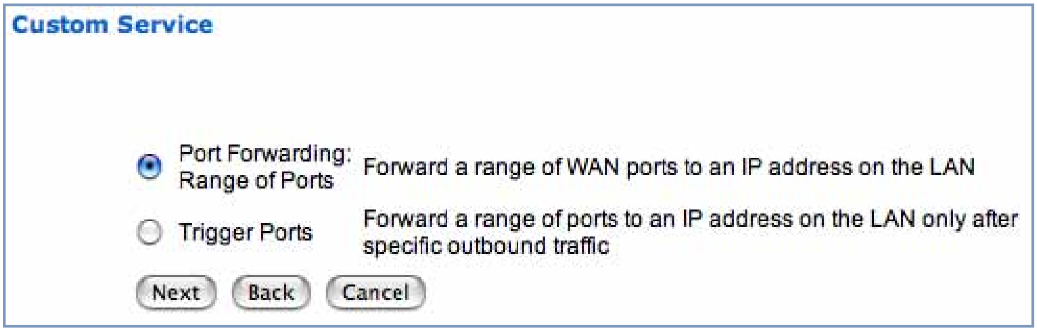
Age of Empires, v.1.0	Age of Empires: The Rise of Rome, v.1.0	Age of Wonders
Asheron's Call	Baldur's Gate	Battlefield Communicator
Buddy Phone	Calista IP Phone	CART Precision Racing, v 1.0
Citrix Metaframe/ICA Client	Close Combat for Windows 1.0	Close Combat: A Bridge Too Far, v 2.0

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.



Custom Service

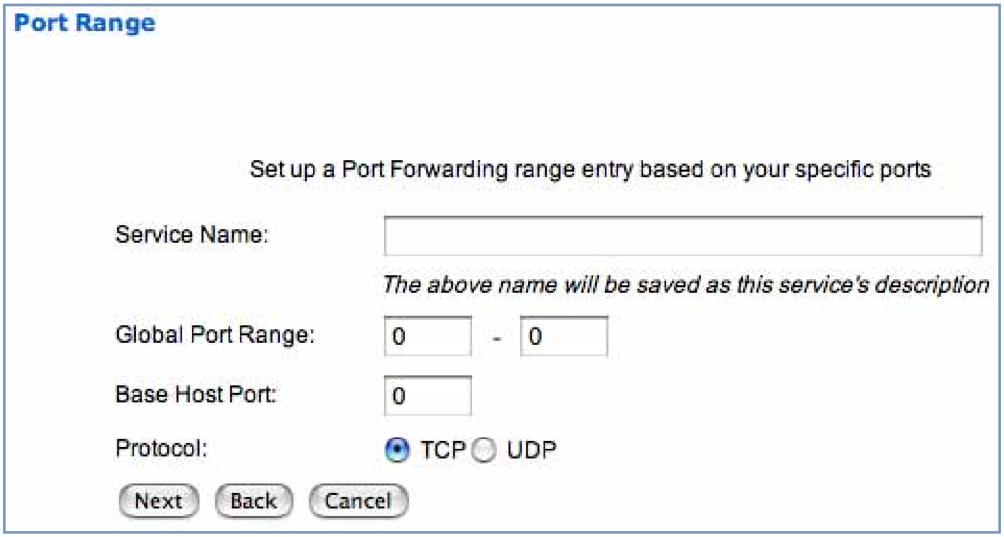
● Port Forwarding: Range of Ports — Forward a range of WAN ports to an IP address on the LAN

○ Trigger Ports — Forward a range of ports to an IP address on the LAN only after specific outbound traffic

- **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 Range

Set up a Port Forwarding range entry based on your specific ports

Service Name:

The above name will be saved as this service's description

Global Port Range: 0 - 0

Base Host Port: 0

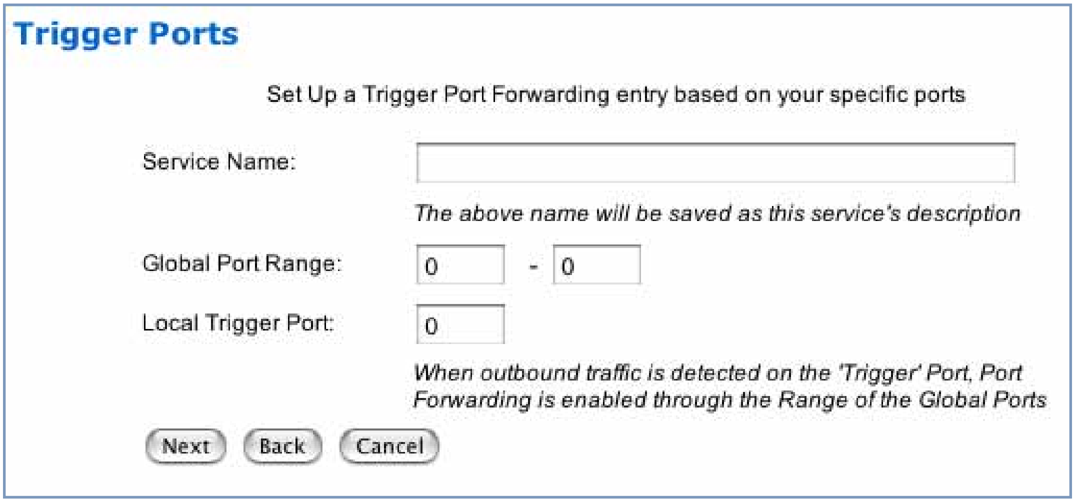
Protocol: ● TCP ○ UDP

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

Set Up a Trigger Port Forwarding entry based on your specific ports

Service Name:

The above name will be saved as this service's description

Global Port Range: 0 - 0

Local Trigger Port: 0

When outbound traffic is detected on the 'Trigger' Port, Port Forwarding is enabled through the Range of the Global Ports

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:

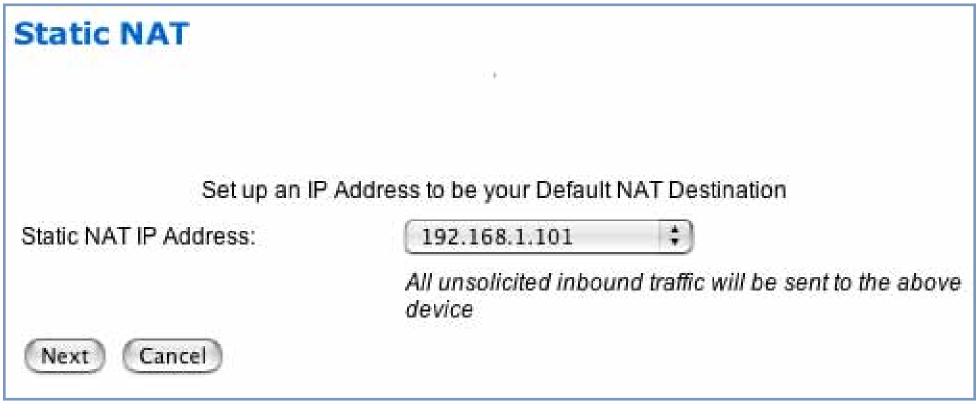
- Direct your Router to forward all externally initiated IP traffic (TCP and UDP protocols only) to a default host on the LAN.
- Enable it for certain situations:

  – 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.



Static NAT

Set up an IP Address to be your Default NAT Destination

Static NAT IP Address: 192.168.1.101

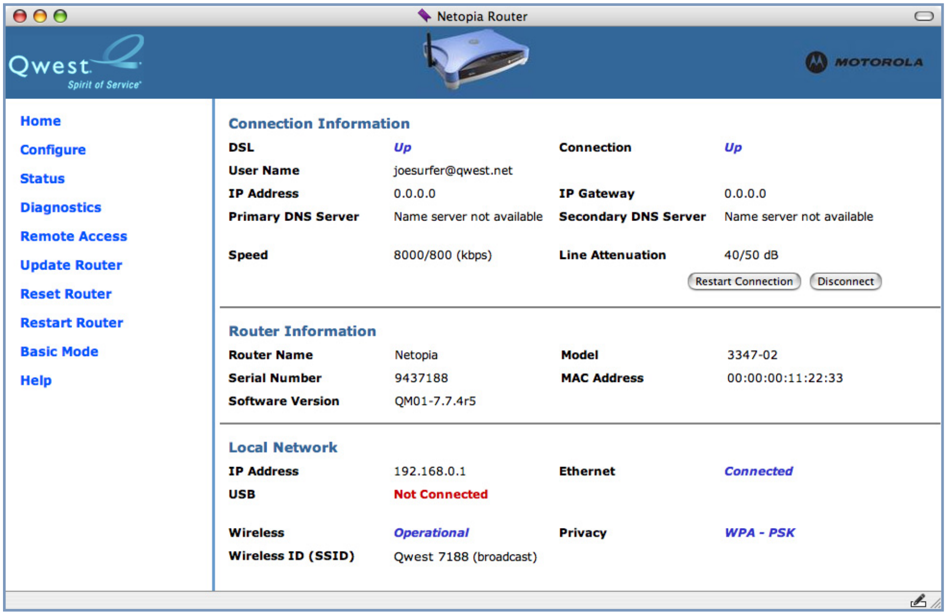
All unsolicited inbound traffic will be sent to the above device

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.

Link: Advanced Setup

Advanced Setup allows you to configure a wide variety of specific Router and networking settings. Advanced Setup is for advanced users and system administrators, and most users will not need to modify these settings. If you need to enter Advanced Setup, and click the **Advanced Setup** link, the Advanced Setup Home page displays.



Connection Information

DSL	Up	Connection	Up
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	IP Gateway	0.0.0.0
Primary DNS Server	Name server not available	Secondary DNS Server	Name server not available
Speed	8000/800 (kbps)	Line Attenuation	40/50 dB

Router Information

Router Name	Netopia	Model	3347-02
Serial Number	9437188	MAC Address	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

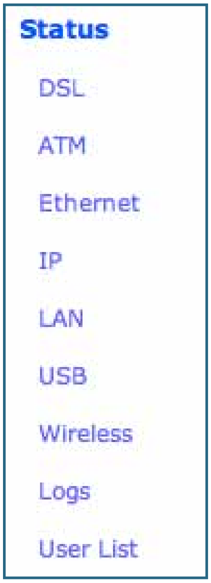
Local Network

IP Address	192.168.0.1	Ethernet	Connected
USB	Not Connected		
Wireless	Operational	Privacy	WPA - PSK
Wireless ID (SSID)	Qwest 7188 (broadcast)		

For more information, see “Advanced Setup” on page 73.

Link: Status

When you click the **Status** link, the Links Bar expands to display nine statistical sub-headings.



These screens will vary depending on your Gateway’s model and traffic activity.

- “DSL” on page 66
- “ATM” on page 67
- “Ethernet (supported models only)” on page 67
- “IP” on page 67
- “LAN” on page 68
- “USB (supported models only)” on page 68
- “Wireless (supported models only)” on page 69
- “Logs” on page 69
- “User List” on page 70

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 (supported models only)

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 (if any)

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, WAN1)

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.

USB (supported models only)

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

The USB Statistics page:

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

Wireless (supported models only)

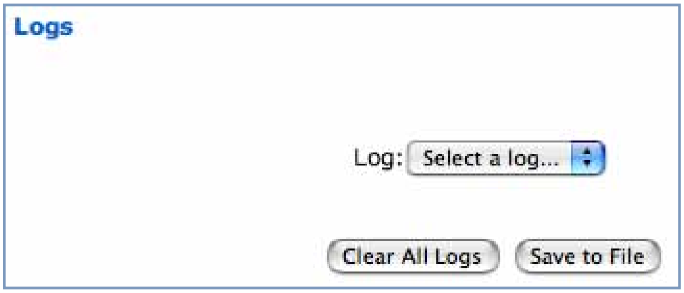
When you click **Wireless**, the Wireless Statistics page appears.

The Wireless Statistics page:

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

Logs

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



Select a log from the pull-down menu (the pull-down menu is available from every Log page):

- **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 Router STATUS** is displayed for all logs.

- To clear the individual logs, click the **Clear Log** button for that page.
- To clear all the logs, click the **Clear All Logs** button on the main Logs page.
- You can save logs to a text (.CTXT) file by clicking the **Save to File** button. This will download the file to your browser's default download location on your hard drive. The file can be opened with your favorite text editor.

Note:

Some browsers, such as Internet Explorer for Windows XP, require that you specify the Motorola Netopia® Gateway's URL as a "Trusted site" in "Internet Options: Security".

User List

When you click **User List**, the User List Statistics page appears.

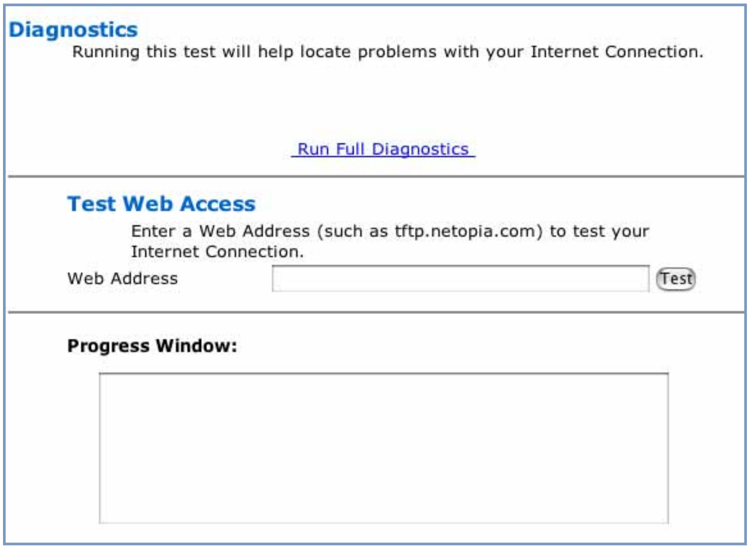
The User List Statistics page:

- displays Ethernet Users' **PC Name**, **IP Address**, and **MAC Address**.
- displays Wireless SSID Users' **PC Name**, **IP Address**, and **MAC Address**.

  If you have multiple SSIDs defined (see "Enable Multiple Wireless IDs" on page 50), Wireless SSID users are displayed by their respective SSID.

Link: 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.



Diagnostics

Running this test will help locate problems with your Internet Connection.

Run Full Diagnostics

Test Web Access

Enter a Web Address (such as tftp.netopia.com) to test your Internet Connection.

Web Address

Progress Window:

You enter a web address, such as *tftp.netopia.com*, or an IP address in the Web Address 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.

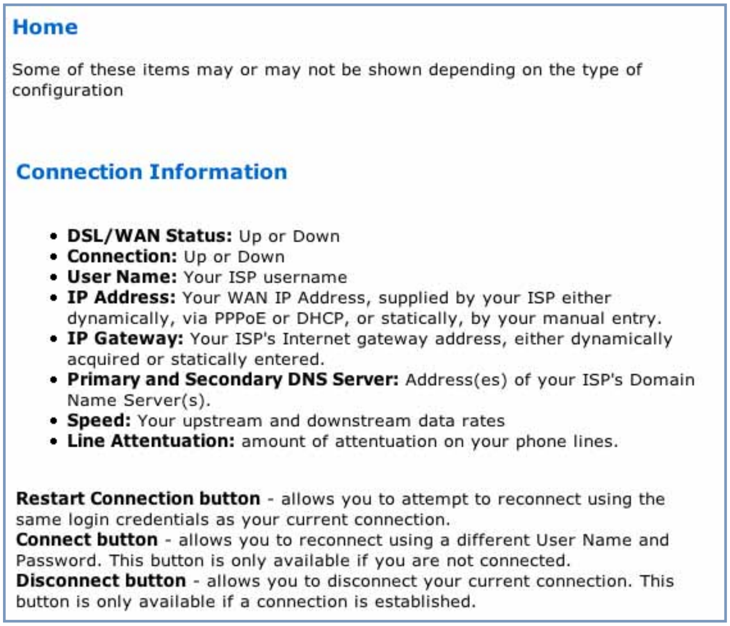
Each test generates one of the following result codes:

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.

Link: Help

When you click the **Help** link in the left-hand column of links a page of explanatory information displays. Help (*in English only*) is available for every page in the Web interface.

Here is an example from the Home page:



Home

Some of these items may or may not be shown depending on the type of configuration

Connection Information

- **DSL/WAN Status:** Up or Down
- **Connection:** Up or Down
- **User Name:** Your ISP username
- **IP Address:** Your WAN IP Address, supplied by your ISP either dynamically, via PPPoE or DHCP, or statically, by your manual entry.
- **IP Gateway:** Your ISP's Internet gateway address, either dynamically acquired or statically entered.
- **Primary and Secondary DNS Server:** Address(es) of your ISP's Domain Name Server(s).
- **Speed:** Your upstream and downstream data rates
- **Line Attentuation:** amount of attentuation on your phone lines.

Restart Connection button - allows you to attempt to reconnect using the same login credentials as your current connection.
Connect button - allows you to reconnect using a different User Name and Password. This button is only available if you are not connected.
Disconnect button - allows you to disconnect your current connection. This button is only available if a connection is established.

CHAPTER 3 Advanced Setup

Using the Web-based user interface for the Motorola Netopia® 2200 and 3300-series Gateway you can configure, troubleshoot, and monitor the status of your Gateway.

Access the Expert Web Interface

Open the Web Connection

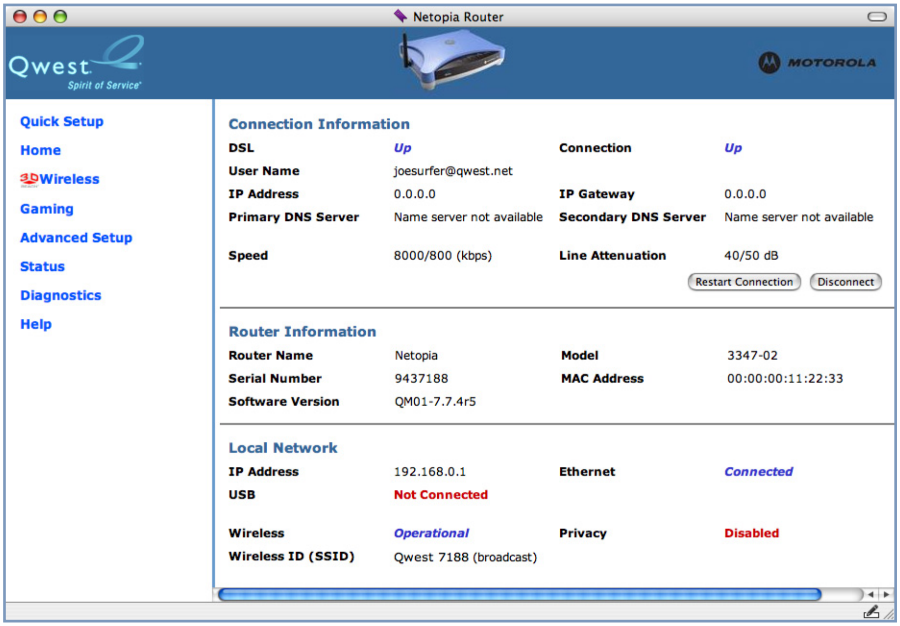
Once your Gateway is powered up, you can use any recent version of the best-known web browsers such as Netscape Navigator or Microsoft Internet Explorer from any LAN-attached PC or workstation. The procedure is:

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://192.168.0.1**.

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.



Connection Information

DSL	*Up*	Connection	*Up*
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	IP Gateway	0.0.0.0
Primary DNS Server	Name server not available	Secondary DNS Server	Name server not available
Speed	8000/800 (kbps)	Line Attenuation	40/50 dB

Router Information

Router Name	Netopia	Model	3347-02
Serial Number	9437188	MAC Address	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

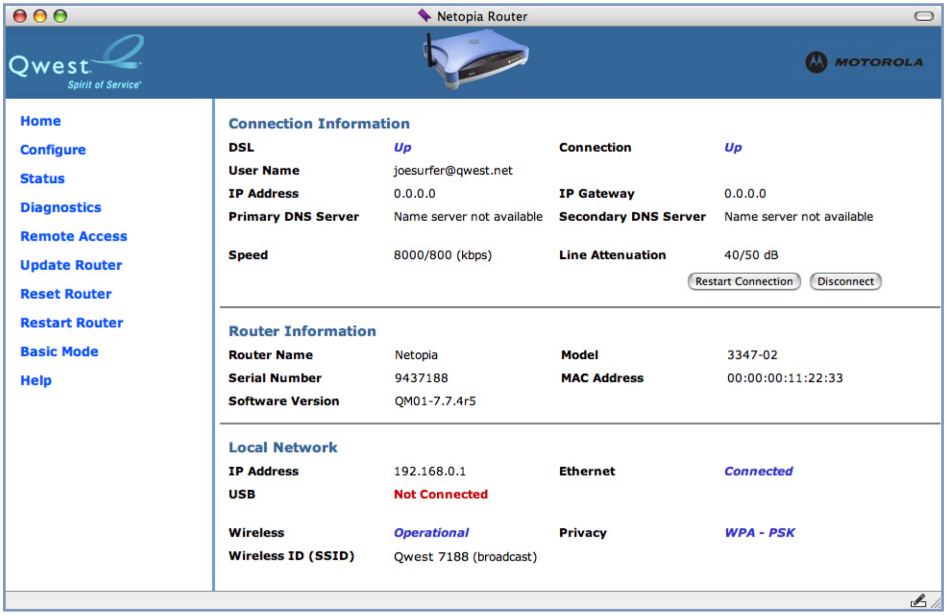
Local Network

IP Address	192.168.0.1	Ethernet	*Connected*
USB	Not Connected		
Wireless	*Operational*	Privacy	Disabled
Wireless ID (SSID)	Qwest 7188 (broadcast)		

3. **Click on the Advanced Setup link in the left-hand column of links.**
   The Home Page opens in Advanced Setup.

Home Page - Advanced Setup

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



Connection Information

DSL	Up	Connection	Up
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	IP Gateway	0.0.0.0
Primary DNS Server	Name server not available	Secondary DNS Server	Name server not available
Speed	8000/800 (kbps)	Line Attenuation	40/50 dB

Restart Connection Disconnect

Router Information

Router Name	Netopia	Model	3347-02
Serial Number	9437188	MAC Address	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

Local Network

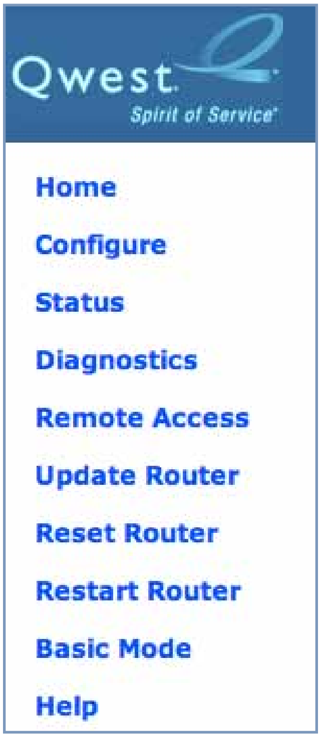
IP Address	192.168.0.1	Ethernet	Connected
USB	Not Connected		
Wireless	Operational	Privacy	WPA - PSK
Wireless ID (SSID)	Qwest 7188 (broadcast)		

Home Page - Information

The Home Page contains a **summary** of the Gateway’s configuration settings and status.

Summary Information	
Field	**Status and/or Description**
Connection Information	
DSL/WAN Status	Wide Area Network may be ***Waiting for DSL*** (or other waiting status), ***Up*** or ***Down***
Connection	***Up*** or ***Down***
User Name	Your ISP-assigned Username
IP Address	IP address assigned to the WAN port.
IP Gateway	The IP address of the gateway to which the connection defaults. If doing DHCP, this info will be acquired. If doing PPP, this info will be negotiated.
Primary and Secondary DNS Server	Address(es) of your ISP's Domain Name Server(s).
Speed	Your upstream and downstream data rates
Line Attenuation	amount of attenuation on your phone lines.
Restart Connection button	allows you to attempt to reconnect using the same login credentials as your current connection.
Connect button	allows you to reconnect using a different User Name and Password. This button is only available if you are not connected.
Disconnect button	allows you to disconnect your current connection. This button is only available if a connection is established.
Router Information	
Router Name and Model	Your Router's manufacturing information
Serial Number	Your Router's unique serial number. Usually also printed on the Router's label.
MAC Address	Your Router's unique hardware address
Software Version	The version of embedded operating system software currently running on the Gateway.
Warranty Date	Original date when your Gateway is first connected and gets the time via the network, for warranty purposes.
Local Network	
IP Address	The IP address of your Router as seen from your internal LAN
Ethernet	Status of your Ethernet network connection (if supported). ***Connected*** or ***Not Connected***.
USB	Status of your USB network connection (if supported). ***Connected*** or ***Not Connected***.

Links Bar



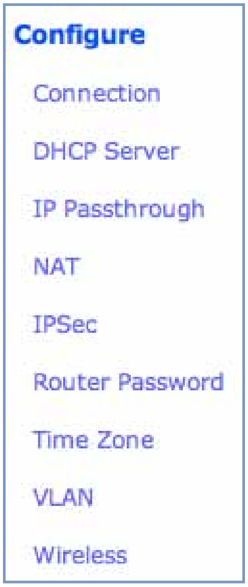
The Links Bar is the frame at the left-hand side of the page containing the major navigation links. These links are available from every page, allowing you to move freely about the site. The headings in the following table are hyperlinks. You can click on any heading to read about that feature.

This chapter covers the following:

Advanced Setup					
Configure	Connection	DHCP Server	IP Passthrough	NAT	IPSec
	Router Password	Time Zone	VLAN	Wireless	
Status	DSL	ATM	Ethernet	IP	LAN
	USB	Wireless	Logs	User List	
Diagnostics					
Update Router					
Reset Router					
Restart Router					
Basic Mode					
Help					

Note: Ethernet, **Wireless**, and **USB** links are only available on supported models.

Link: Configure



Configure

Connection

DHCP Server

IP Passthrough

NAT

IPSec

Router Password

Time Zone

VLAN

Wireless

When you click **Configure**, the Links bar expands to display the configuration options available.

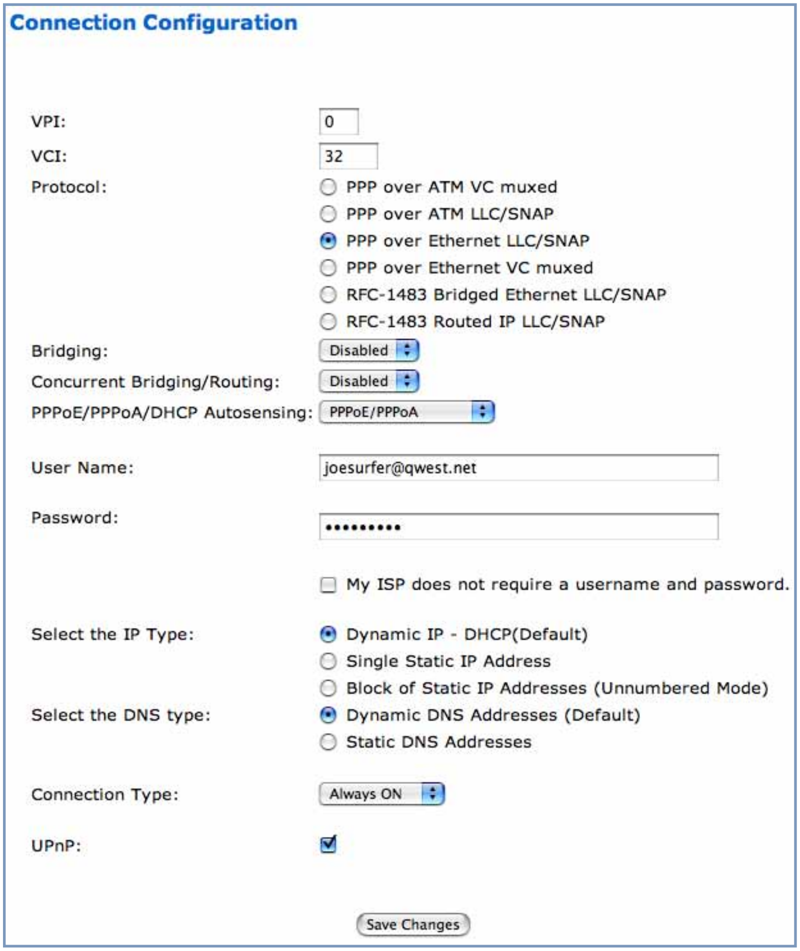
Advanced options are intended for experienced users and administrators. Exercise great caution when making any changes to Advanced Configuration options.

- "Connection" on page 79
- "DHCP Server" on page 82
- "IP Passthrough" on page 85
- "NAT" on page 87
- "IPSec" on page 94
- "Router Password" on page 104
- "Time Zone" on page 105
- "VLAN" on page 106
- "Wireless" on page 125

Link: Connection

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

Note: The appearance of this page will vary based on the model and WAN connection you have.



Connection Configuration

VPI: 0

VCI: 32

Protocol:
○ PPP over ATM VC muxed
○ PPP over ATM LLC/SNAP
● PPP over Ethernet LLC/SNAP
○ PPP over Ethernet VC muxed
○ RFC-1483 Bridged Ethernet LLC/SNAP
○ RFC-1483 Routed IP LLC/SNAP

Bridging: Disabled

Concurrent Bridging/Routing: Disabled

PPPoE/PPPoA/DHCP Autosensing: PPPoE/PPPoA

User Name: joesurfer@qwest.net

Password: ••••••••••

□ My ISP does not require a username and password.

Select the IP Type:
● Dynamic IP - DHCP(Default)
○ Single Static IP Address
○ Block of Static IP Addresses (Unnumbered Mode)

Select the DNS type:
● Dynamic DNS Addresses (Default)
○ Static DNS Addresses

Connection Type: Always ON

UPnP: ☑

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. The default setting is 8/35. With this setting, the router will match the settings your ISP is using, with no input on your part. You probably would not need to change this.
- **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 LLC, PPPOE VCMUX, ETHER LLC, IP LLC, PPPOA LLC, and PPPOA VCMUX.
- **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.
- **Concurrent Bridging/Routing**: Your Router can bridge or route traffic, depending on the IP addresses, at the same time. When this mode is enabled, the Router will also bridge traffic from the LAN if it has a valid LAN-side address.
- **PPPoE/PPPoA/DHCP Autosensing**: The pull-down menu allows you to select an autosensing feature, or to disable it. Selecting between PPPoE/DHCP or PPPoE/PPPoA enables automatic sensing of your WAN connection type. If you select **PPPoE/DHCP**, the gateway attempts to connect using PPPoE first. If the Gateway fails to connect after 60 seconds, it switches to DHCP. As soon as it can connect via DHCP, the Gateway chooses and sets DHCP as its default. Otherwise, after attempting to connect via DHCP for 60 seconds, the Gateway switches back to PPPoE. The Gateway will continue to switch back and forth in this manner until it successfully connects. Similarly, selecting **PPPoE/PPPoA** causes the Gateway to attempt to connect by trying these protocols in parallel, and using the first one that is successful. If you choose to disable the feature, select **Off**.
- **User Name** and **Password**: Provided by your ISP.
- **Confirm Password:** Repeat your Password entry for confirmation
- **Select the IP Type**:

  Dynamic IP - DHCP (Default) –

  Single Static IP Address –

  Block of Static IP Addresses (Unnumbered Mode) –
- **Static IP Address:** Your service provider may tell you that the WAN IP Address for your Router is static. If so, enter the IP Address from your service provider in this 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**: For On-Demand connections only, you can specify the time in seconds before disconnection if there is no data passing to or from the Internet.
- **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 Motorola Netopia® Gateway.

  For Windows XP users, the automatic discovery feature places an icon representing the Motorola Netopia® Gateway automatically in the "My Network Places" folder. Double-clicking this icon opens the Gateway's web UI.

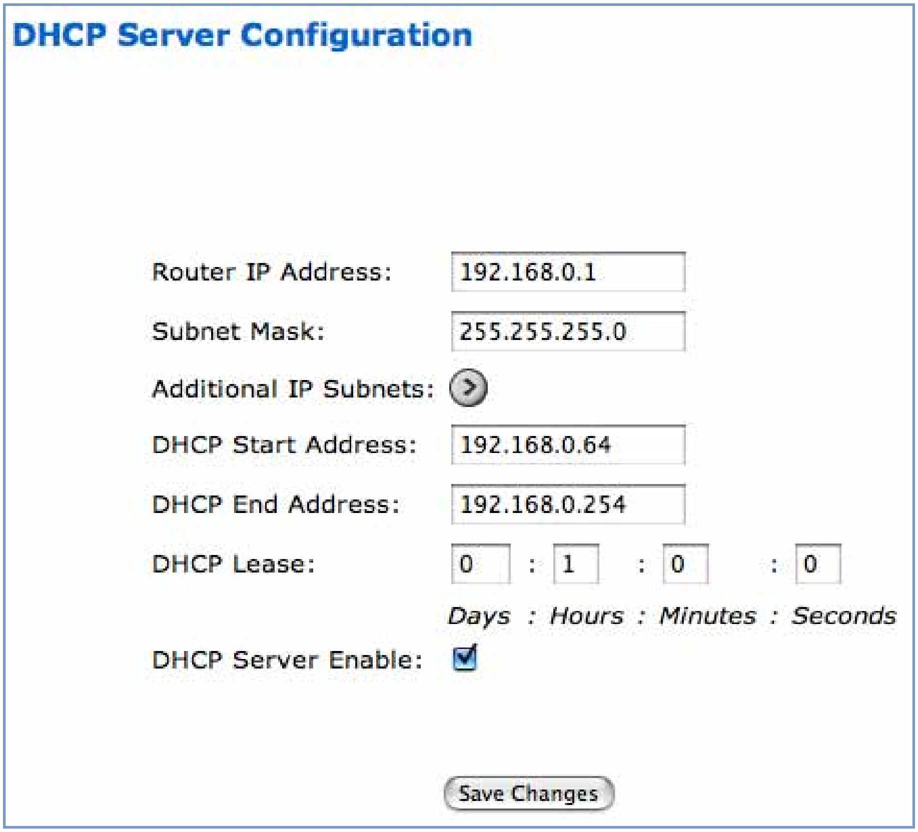
  PCs using UPnP can retrieve the Gateway's WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with a UPnP-enabled Motorola Netopia® Gateway, will not need application layer gateway support on the Motorola Netopia® Gateway to work through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

  You can disable UPnP, if you are not using any UPnP devices or applications. Uncheck the **UPnP Enabled** checkbox.

When all of your entries are made, click the **Save and Restart Connection** button.

Link: DHCP Server

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



DHCP Server Configuration

Router IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Additional IP Subnets:

DHCP Start Address: 192.168.0.64

DHCP End Address: 192.168.0.254

DHCP Lease: 0 : 1 : 0 : 0

Days : Hours : Minutes : Seconds

DHCP Server Enable: ☑

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.

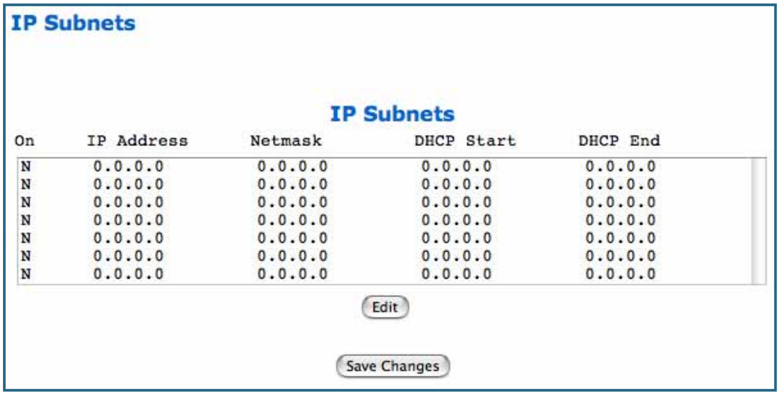
The Server configuration determines the functionality of your DHCP Settings. This functionality enables the Router to assign your LAN computer(s) a “private” IP address and other parameters that allow network communication.

- **Router IP Address:** Specifies the IP address of the Router itself.

- **Subnet Mask:** Specifies the subnet mask of the Router itself. Defaults to 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 (including up to 64 IP addresses for wireless clients) 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.

Additional IP Subnets

The Additional IP Subnets screen allows you to configure up to seven secondary subnets and their DHCP ranges, by entering IP address/subnet mask pairs:



IP Subnets

IP Subnets

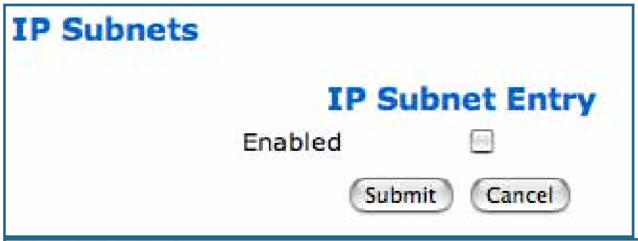
On	IP Address	Netmask	DHCP Start	DHCP End
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
N	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Note:

You need not use this screen if you have only a single Ethernet IP subnet.

This screen displays seven rows of editable columns. All seven row labels are always visible, regardless of the number of subnets configured.

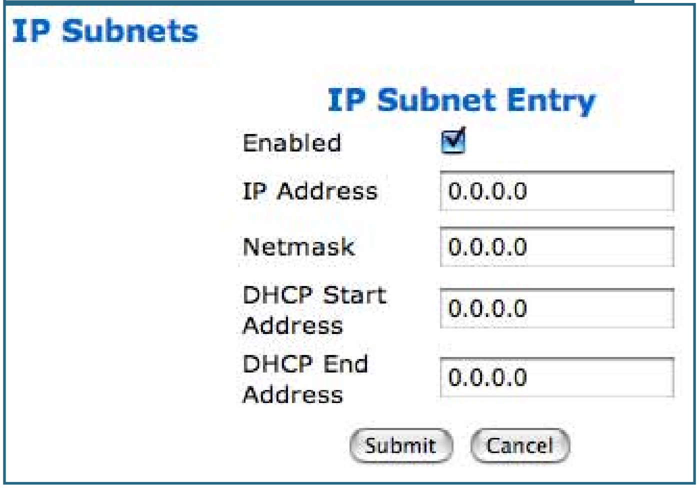
- To add an IP subnet, select one of the rows, and click the **Edit** button.


IP Subnets

IP Subnet Entry

Enabled □

Check the **Enabled** checkbox and click the **Submit** button.


IP Subnets

IP Subnet Entry

Enabled ☑

IP Address 0.0.0.0

Netmask 0.0.0.0

DHCP Start Address 0.0.0.0

DHCP End Address 0.0.0.0

The screen expands to allow you to enter subnet information.

If **DHCP Server** (see below) is not enabled, the DHCP Start Address and DHCP End Address fields do not appear.

Enter the Router's IP address on the subnet in the **IP Address** field and the subnet mask for the subnet in the **Netmask** field.

Enter the **DHCP Start Address** and **End Address** of the subnet range in their respective fields.

Ranges cannot overlap and there may be only one range per subnet.

- Click the **Submit** button.
- When you are finished adding subnets, click the **Save Changes** button, and when prompted, restart the Router.

To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and clicking the **Submit** button to commit the change.

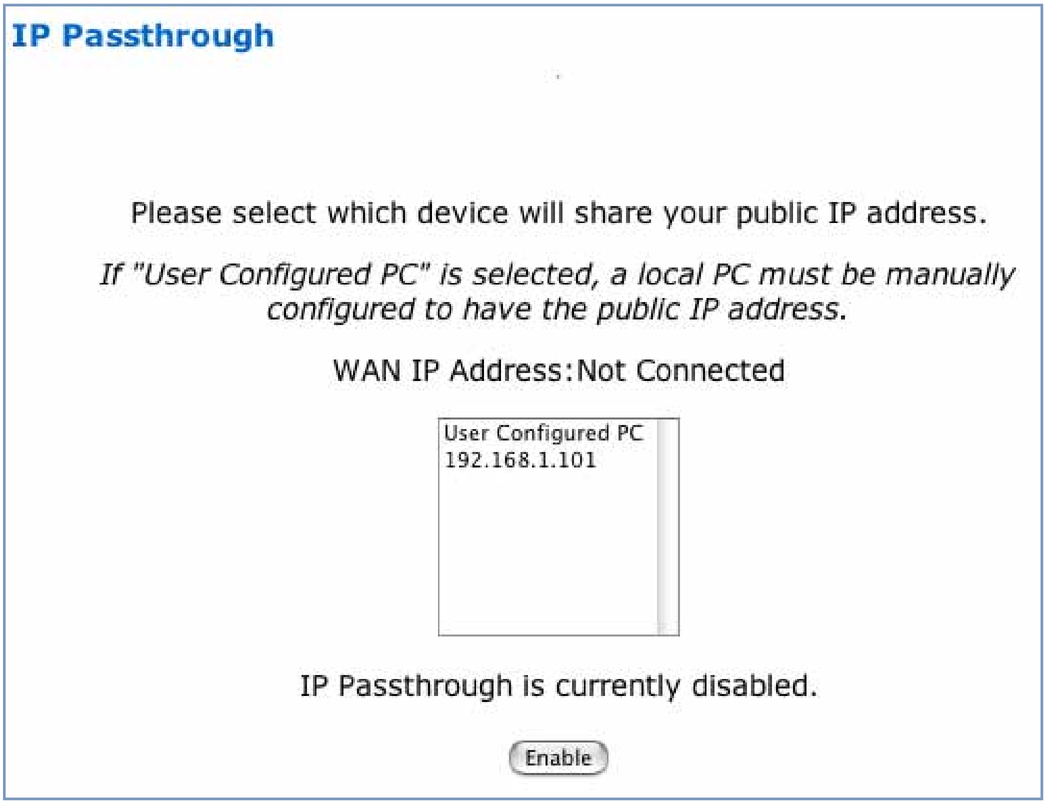
NOTE:

All additional DHCP ranges use the global lease period value. See page 82.

If you make any changes, click the **Save Changes** button.

Link: IP Passthrough

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



IP Passthrough

Please select which device will share your public IP address.

If "User Configured PC" is selected, a local PC must be manually configured to have the public IP address.

WAN IP Address:Not Connected

IP Passthrough is currently disabled.

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 Router link and confirm the restart when prompted.**

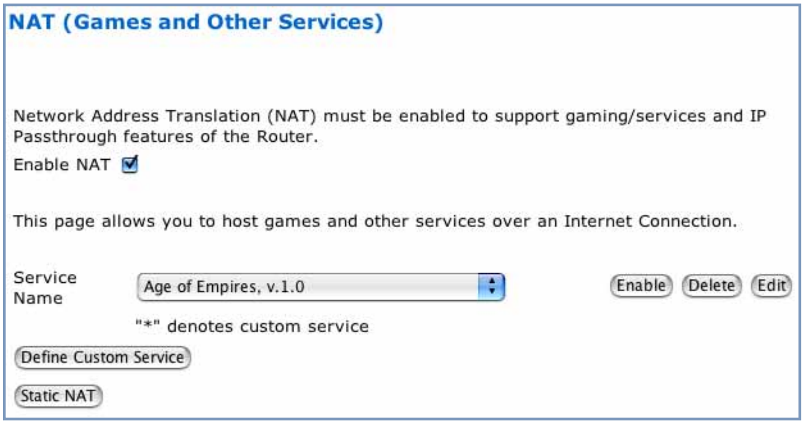
Once configured, the passthrough host's DHCP leases will be shortened to two minutes. This allows for timely updates of the host's IP address, which will be a private IP address *before* the WAN connection is established. *After* the WAN connection is established and has an address, the passthrough host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

Link: NAT

When you click **NAT**, the **NAT (Games and Other Services)** page appears.



NAT (Games and Other Services)

Network Address Translation (NAT) must be enabled to support gaming/services and IP Passthrough features of the Router.

Enable NAT ☑

This page allows you to host games and other services over an Internet Connection.

Service Name: Age of Empires, v.1.0

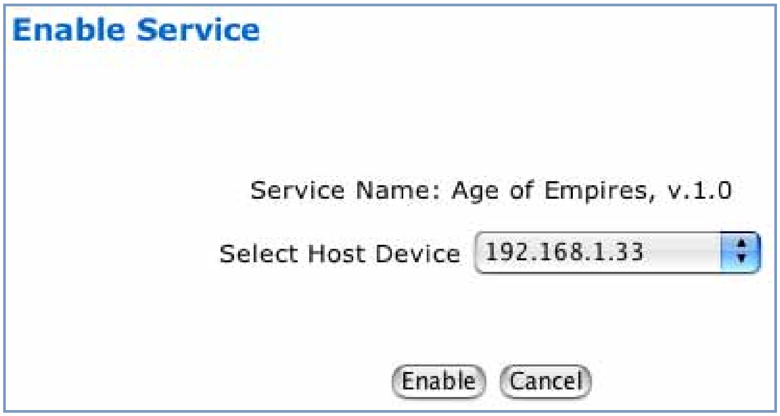
"*" denotes custom service

NAT (Games and Other Services) allows you to host internet applications when NAT is enabled. You can host different games and software on different PCs. If you uncheck the **Enable NAT** checkbox, the rest of the information on the page is hidden.

From the **Service Name** pull-down menu, you can select any of a large number of predefined games and software. (See “Supported Games and Software” on page 89.)

1. **Once you choose a software service or game, click Enable.**

   The Enable Service screen appears.



Enable Service

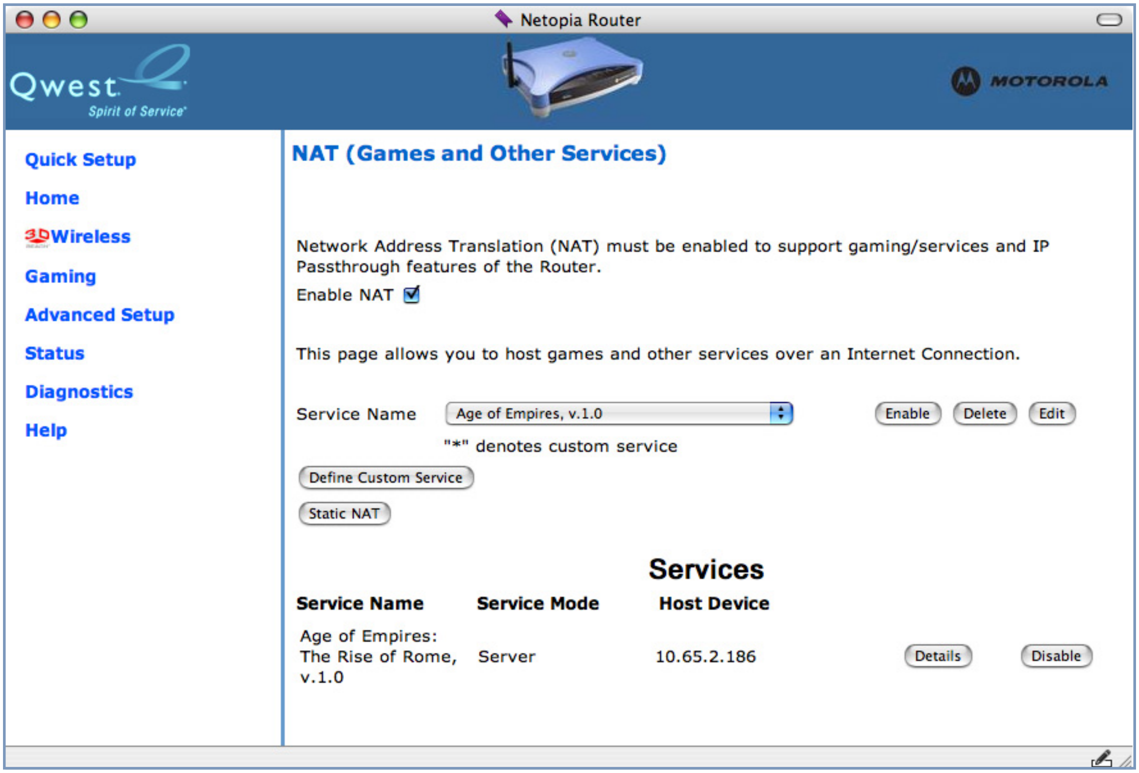
Service Name: Age of Empires, v.1.0

Select Host Device: 192.168.1.33

Select 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.



NAT (Games and Other Services)

Network Address Translation (NAT) must be enabled to support gaming/services and IP Passthrough features of the Router.

Enable NAT ☑

This page allows you to host games and other services over an Internet Connection.

Service Name: Age of Empires, v.1.0

"*" denotes custom service

Services

Service Name	Service Mode	Host Device
Age of Empires: The Rise of Rome, v.1.0	Server	10.65.2.186

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

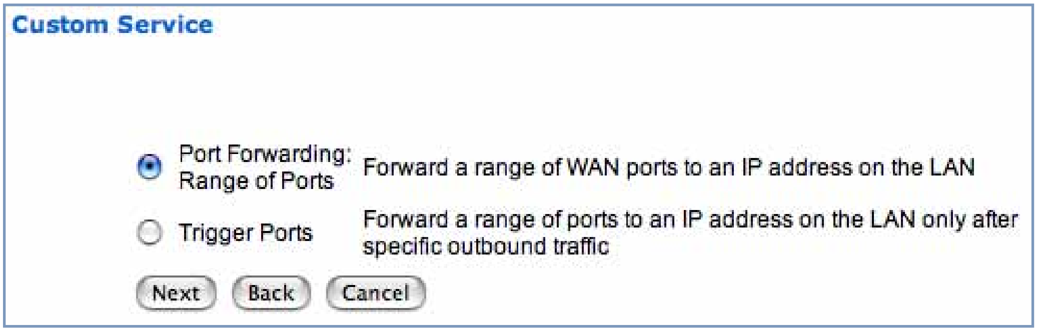
Supported Games and Software

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.



Custom Service

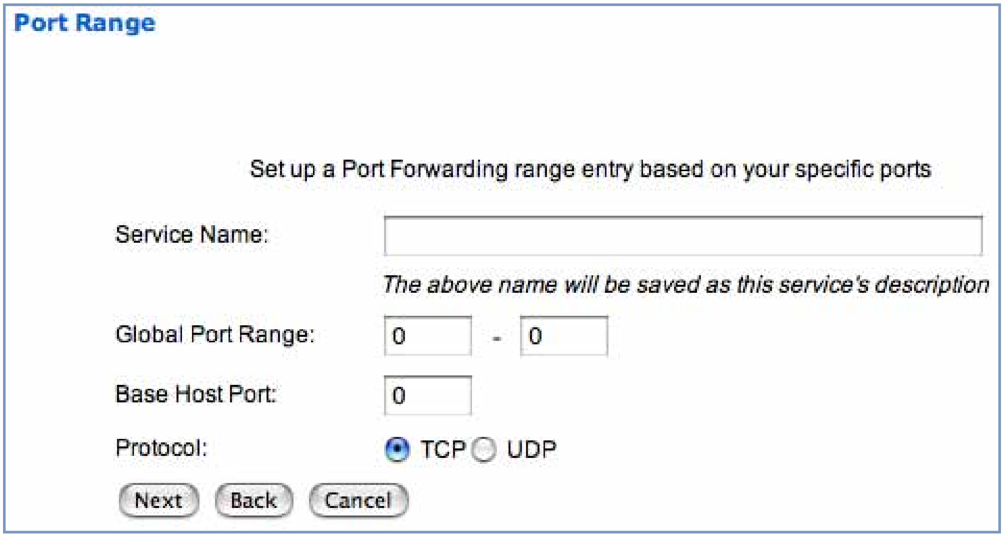
● Port Forwarding: Range of Ports — Forward a range of WAN ports to an IP address on the LAN

○ Trigger Ports — Forward a range of ports to an IP address on the LAN only after specific outbound traffic

- **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 Range

Set up a Port Forwarding range entry based on your specific ports

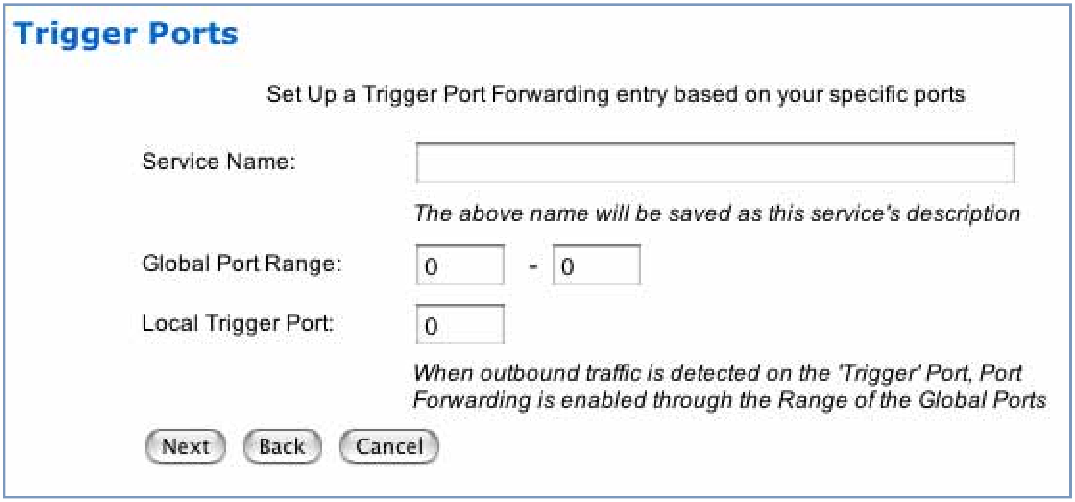
Service Name:	
	The above name will be saved as this service's description
Global Port Range:	0 - 0
Base Host Port:	0
Protocol:	● TCP ○ UDP

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

Set Up a Trigger Port Forwarding entry based on your specific ports

Service Name:

The above name will be saved as this service's description

Global Port Range: 0 - 0

Local Trigger Port: 0

When outbound traffic is detected on the 'Trigger' Port, Port Forwarding is enabled through the Range of the Global Ports

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:

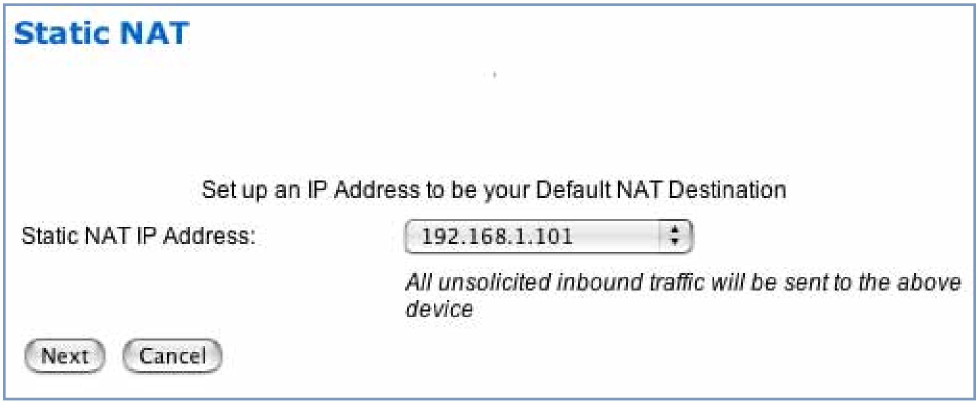
- Direct your Router to forward all externally initiated IP traffic (TCP and UDP protocols only) to a default host on the LAN.
- Enable it for certain situations:

  – 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.



Static NAT

Set up an IP Address to be your Default NAT Destination

Static NAT IP Address: 192.168.1.101

All unsolicited inbound traffic will be sent to the above device

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

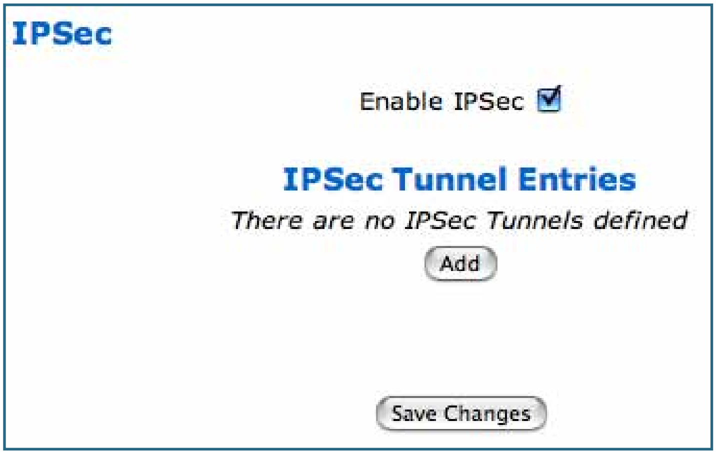
Click the **Next** button, and your choice will be so designated.

Link: IPSec

When you click on the IPSec link, the IPSec configuration screen appears.

Your Gateway can support two mechanisms for IPSec tunnels:

- **IPSec PassThrough** supports Virtual Private Network (VPN) clients running on LAN-connected computers. Normally, this feature is enabled.



IPSec

Enable IPSec ☑

IPSec Tunnel Entries

There are no IPSec Tunnels defined

You can disable it if your LAN-side VPN client includes its own NAT interoperability option. Uncheck the **Enable IPSec** checkbox.

IPSec VPN

A VPN IPSec Tunnel provides a single, encrypted tunnel to be **terminated on** the Gateway, making a secure tunnel available for **all** LAN- connected users. This implementation offers the following:

- Eliminates the need for VPN client software on individual PCs.
- Reduces the complexity of tunnel configuration.
- Simplifies the ongoing maintenance for secure remote access.

Configuring an IPSec VPN Tunnel

Use the following procedure to configure your IPSec tunnel.

1. **Obtain your configuration information from your network administrator.**

   The tables “Parameter Descriptions” on page 100 describe the various parameters that may be required for your tunnel. Not all of them need to be changed from the defaults for every VPN tunnel. Consult with your network administrator.

2. **Complete the Parameter Setup worksheet “IPSec Tunnel Details Parameter Setup Worksheet” on page 96.**

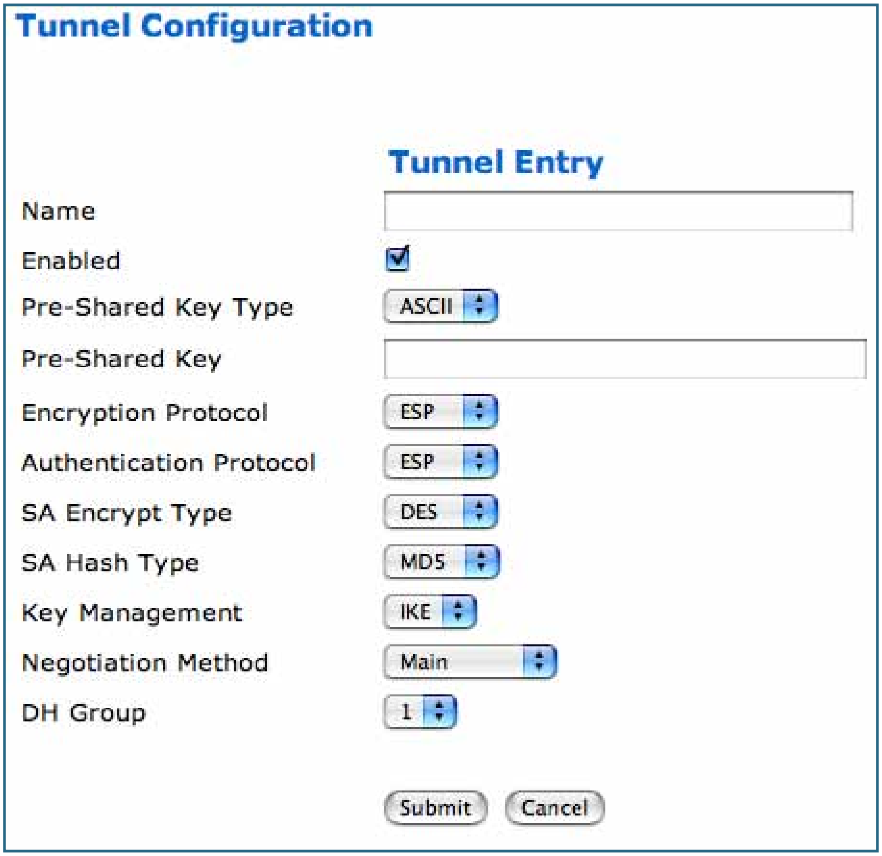
   The worksheet provides spaces for you to enter your own specific values. You can print the page for easy reference. IPSec tunnel configuration requires precise parameter setup between VPN devices. The Setup Worksheet (page 96) facilitates setup and assures that the associated variables are **identical**.

Table 1: IPSec Tunnel Details Parameter Setup Worksheet

Parameter	Motorola Netopia® Gateway	Peer Gateway
Name		
Peer Internal Network		
Peer Internal Netmask		
NAT Enable	On/Off	
PAT Address		
Negotiation Method	Main/Aggressive	
Local ID Type	IP Address Subnet Hostname ASCII	
Local ID Address/Value		
Local ID Mask		
Remote ID Type	IP Address Subnet Hostname ASCII	
Remote ID Address/Value		
Remote ID Mask		
Pre-Shared Key Type	HEX ASCII	
Pre-Shared Key		
DH Group	1/2/5	
PFS Enable	Off/On	
SA Encrypt Type	DES	
	3DES	
SA Hash Type	MD5 SHA1	
Invalid SPI Recovery	Off/On	
Soft MBytes	1 - 1000000	
Soft Seconds	60 - 1000000	
Hard MBytes	1 - 1000000	
Hard Seconds	60 - 1000000	
IPSec MTU	100 - 1500 (default)	
Xauth Enable	Off/On	
Xauth Username		
Xauth Password		

3. **Check the Enable IPSec checkbox.**
4. **Click Add.**

   The **Tunnel Configuration** page appears.



Tunnel Configuration

Tunnel Entry

Name	
Enabled	☑
Pre-Shared Key Type	ASCII
Pre-Shared Key	
Encryption Protocol	ESP
Authentication Protocol	ESP
SA Encrypt Type	DES
SA Hash Type	MD5
Key Management	IKE
Negotiation Method	Main
DH Group	1

5. **Enter the tunnel Name.**

   This parameter does not have to match the peer/remote VPN device.
6. **Enter the initial group of tunnel parameters.**

   Refer to your "IPSec Tunnel Details Parameter Setup Worksheet" on page 96 and the "Parameter Descriptions" on page 100 as required.

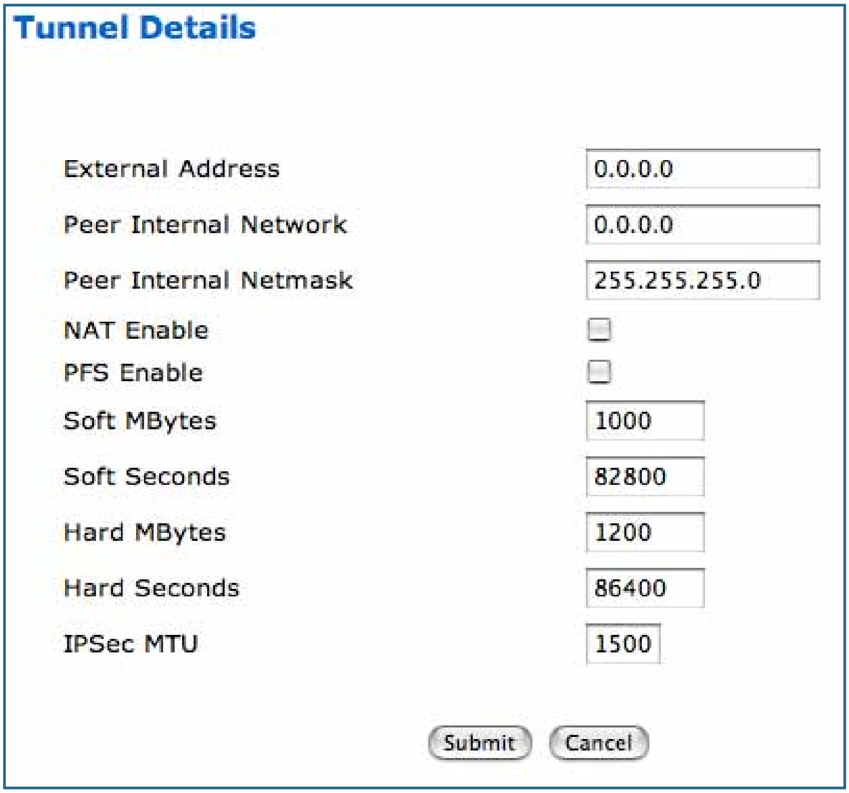
   Select the **Encryption Protocol** from the pull-down menu.

   Select the **Authentication Protocol** from the pull-down menu.

   If you choose **Aggressive** from the **Negotiation Method** pull-down menu, additional fields appear for you to supply applicable parameter information.

7. **Click the Submit button.**

   The Tunnel Details screen appears.



Tunnel Details

External Address	0.0.0.0
Peer Internal Network	0.0.0.0
Peer Internal Netmask	255.255.255.0
NAT Enable	□
PFS Enable	□
Soft MBytes	1000
Soft Seconds	82800
Hard MBytes	1200
Hard Seconds	86400
IPSec MTU	1500

8. **Make the Tunnel Details entries.**

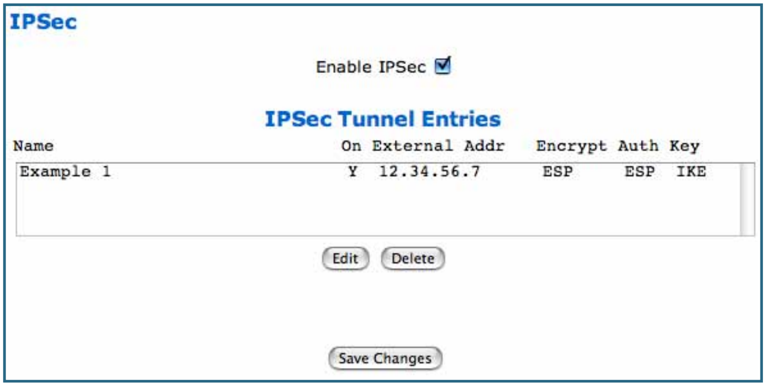
   Enter or select the required settings.

   Soft MBytes, **Soft Seconds**, **Hard MBytes**, and **Hard Seconds** values do not have to match the peer/remote VPN device.

   Refer to your "IPSec Tunnel Details Parameter Setup Worksheet" on page 96.)

9. **Click the Submit button.**

You will be returned to the IPSec configuration screen where your entries are displayed in a list. You can return to this screen at any time to edit or delete your entries.



IPSec

Enable IPSec ☑

IPSec Tunnel Entries

Name	On	External Addr	Encrypt	Auth	Key
Example 1	Y	12.34.56.7	ESP	ESP	IKE

10. **Click the Save Changes button and, when prompted, restart your Router.**

Parameter Descriptions

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

Table 2: 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 31 characters. The tunnel name 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 3: 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 31 characters. The tunnel name 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 3: 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 3: IPSec Tunnel Details page parameters

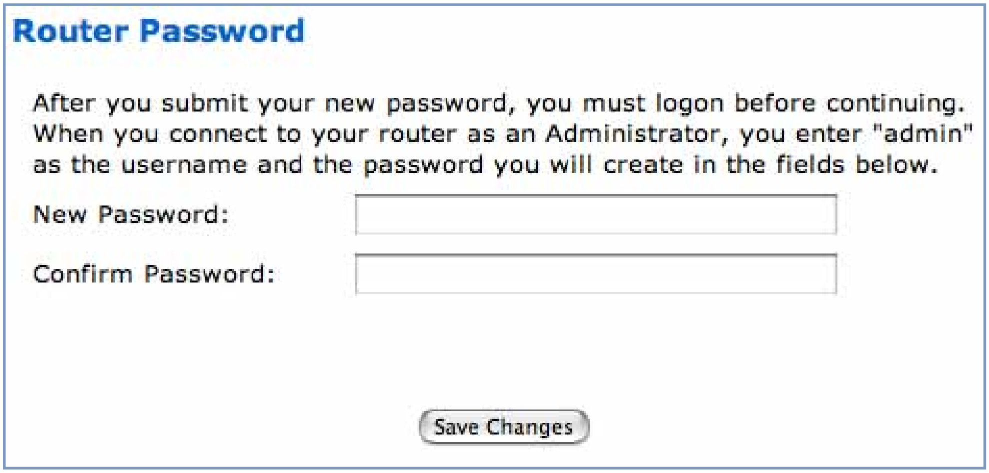
SA Hash Type	SA Hash Type refers to the Authentication Hash algorithm used during SA negotiation. Values supported include MD5 and SHA1. N/A will display if NONE is chosen for Auth Protocol.
Invalid SPI Recovery	Enabling this allows the Gateway to re-establish the tunnel if either the Netopia Gateway 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. This parameter does not need to match the peer gateway.
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. This parameter does not need to match the peer gateway.
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. This parameter does not need to match the peer gateway.
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 This parameter does not need to match the peer gateway.
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 3: 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 Motorola 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.

Link: Router Password

When you click Router Password, the **Router Password** page appears.



Router Password

After you submit your new password, you must logon before continuing. When you connect to your router as an Administrator, you enter "admin" as the username and the password you will create in the fields below.

New Password:

Confirm Password:

By default, your Gateway requires no password to access the administrative web-based user interface. If you wish to secure administrative access to your Gateway, you can optionally enable a password challenge by enabling a local **Admin** password login.

Use the following procedure to create or change an Administrative (Admin) password for your Netopia Gateway:

- Enter your new password in the New Password field.

  Motorola’s rules for a Password are:

  - It can have up to eight alphanumeric characters.

  - It is case-sensitive.

- Enter your new password again in the Confirm Password field.

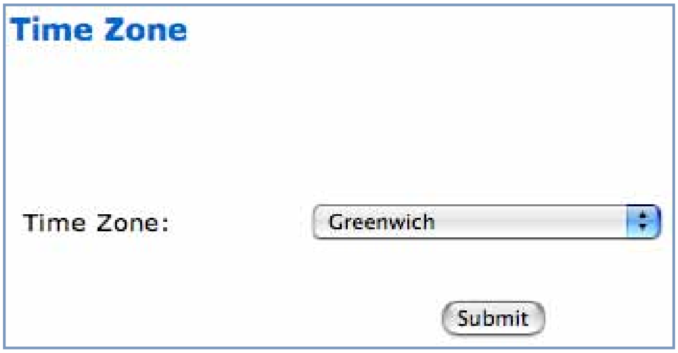
  You confirm the new password to verify that you entered it correctly the first time.

Password changes are automatically saved, and take effect immediately.

Click the Save Changes button.

Link: Time Zone

When you click the **Time Zone** link, the **Time Zone** page appears.



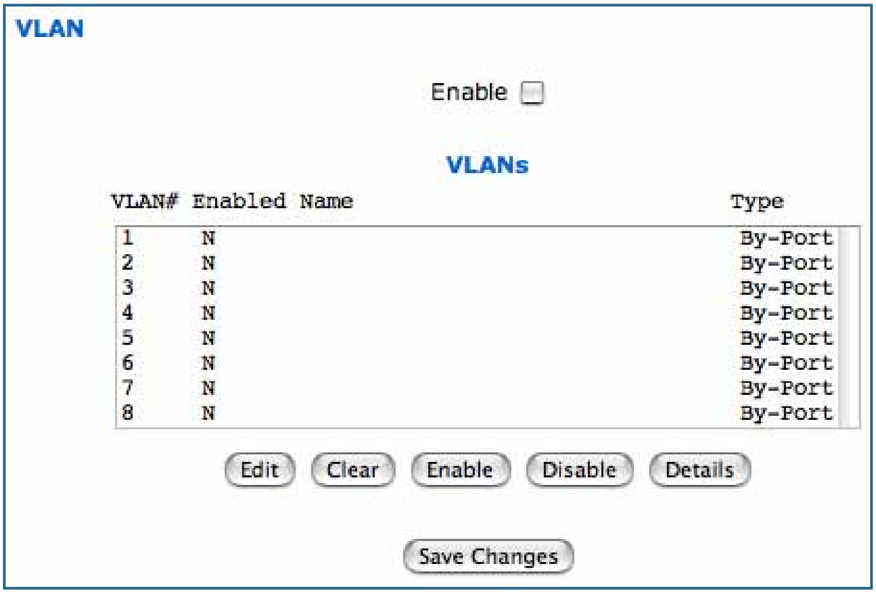
Time Zone

Time Zone: Greenwich

You can set your local time zone by selecting your time zone from the pull-down menu. This allows you to set the time zone for access controls (and in general).

Link: VLAN

When you click VLAN, the **VLANs** page appears.



VLAN

Enable □

VLANs

VLAN#	Enabled	Name	Type
1	N		By-Port
2	N		By-Port
3	N		By-Port
4	N		By-Port
5	N		By-Port
6	N		By-Port
7	N		By-Port
8	N		By-Port

Overview

A Virtual Local Area Network (VLAN) is a network of computers or other devices that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN. You set up VLANs by configuring the Gateway software rather than hardware. This makes VLANs very flexible. VLANs behave like separate and independent networks.

Beginning with Version 7.7.4, VLANs are now strictly layer 2 entities. They can be thought of as virtual Ethernet switches, into which can be added: Ethernet ports, router IP interfaces, ATM PVC/VCC interfaces, SSIDs, and any other physical port such as USB, HPNA, or MOCA. This allows great flexibility on how the components of a system are connected to each other.

VLANs are part of Motorola’s VGx Virtual Gateway technology which allows individual port-based VLANs to be treated as separate and distinct “channels.” When data is passed to a Motorola Netopia VGx-enabled broadband gateway, specific policies, routing, and prioritization parameters can be applied to each individual service, delivering that service to the appropriate peripheral device with the required level of quality of service (QoS). In effect, a single Motorola gateway acts as separate virtual gateways for each distinct service being delivered.

Motorola’s VGx technology maps multiple local VLANs to one or more specific permanent virtual circuits (PVCs) for DSL, or wide area network VLANs for a fiber network. VGx provides service segmentation and QoS controls, service management, and supports delivery of triple play applications: voice for IP Telephony, video for IPTV, and data.

Your Gateway supports the following:

- Port-based VLANs - these can be used when no trunking is required
- Global VLANs - these are used when trunking is required on any port member of the VLAN
  - Supports 802.1q and 802.1p; both are configurable
- Routed VLANs
  - WAN-side VLAN with Multiple WAN IPoE interface support and IP interface-to-VLAN binding
  - LAN-side VLAN with IP interface-to-VLAN binding
  - Inter-VLAN routing
- Bridged VLANs - these VLANs are used to bridge traffic from LAN to WAN
- Prioritization per VLAN and per port

Ethernet Switching/Policy Setup

Before you configure any VLANs, the unconfigured Gateway is set up as a router composed of a LAN switch, a WAN switch, and a router in the middle, with LAN and WAN IP interfaces connected to their respective switches. These bindings between Ethernet switch ports, IP LAN interface, IP WAN interface and WAN physical ports are automatically created.

When you configure any VLANs, the default bindings are no longer valid, and the system requires explicit binding between IP interfaces and layer 2 interfaces. Each VLAN can be thought of as a layer 2 switch, and enabling each port or interface in a VLAN is analogous to plugging it in to the layer 2 switch.

Thereafter, in order for devices to communicate on layer 2, they must be associated in the same VLAN. For devices to communicate at layer 3, the devices must be either on the same VLAN, or on VLANs that have an Inter-VLAN routing group enabled in common.

When configuring VLANs you must define how traffic needs to be forwarded:

- If traffic needs to be bridged between LAN and WAN you can create a single VLAN that encompasses the WAN port and LAN ports.
- If traffic needs to be routed then you must define four elements:
  - LAN-side VLANs
  - WAN-side VLANs
  - Associate IP Interfaces to VLANs
  - Inter-VLAN Routing Groups: configuration of routing between VLANs is done by association of a VLAN to a Routing Group. Traffic will be routed between VLANs within a routing group. The LAN IP Ethernet Interface can be bound to multiple LAN VLANs, but forwarding can be limited between an Ethernet LAN port and a WAN VLAN if you properly configure Inter-VLAN groups.

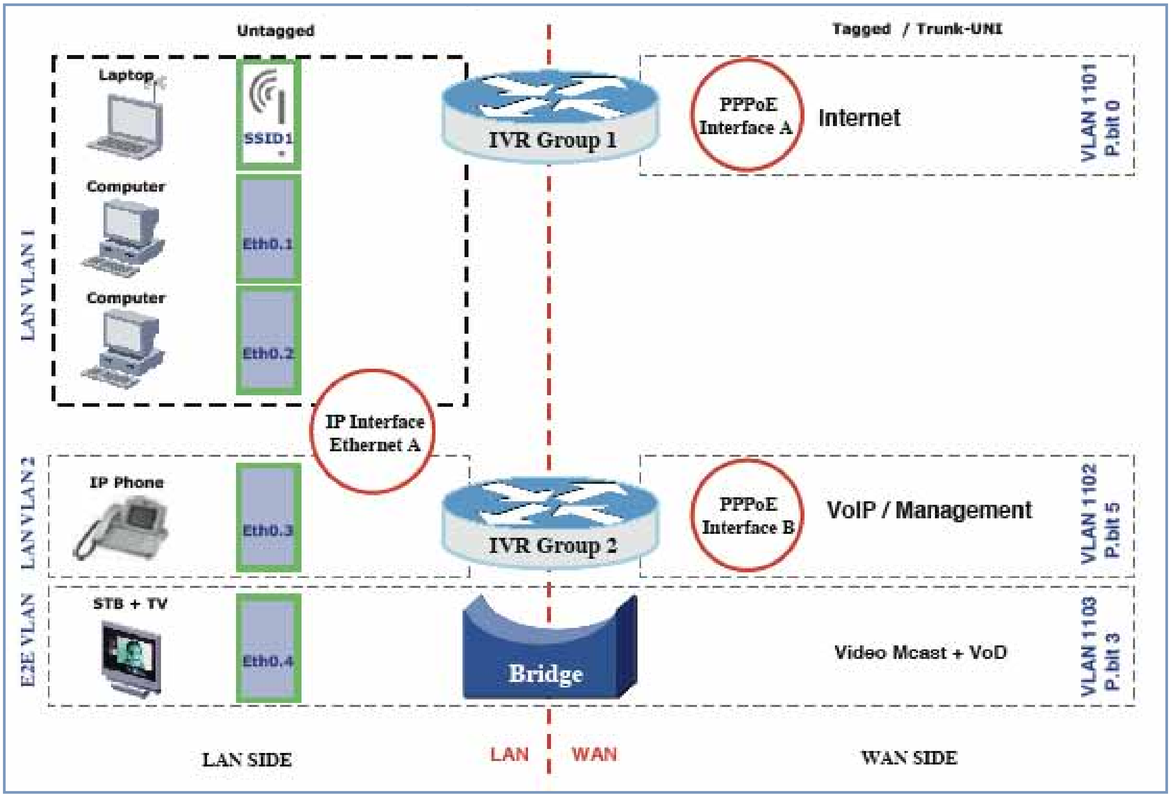
  Inter-VLAN groups are also used to block routing between WAN interfaces. If each WAN IP interface is bound to its own VLAN and if you configure a different Inter-VLAN group for each WAN VLAN then no routing between WAN IP interfaces is possible.
- Example: to route between a VCC and all the LAN ports, which effectively is similar to the default configuration without any VLANs:

  Create a VLAN named “VccWan” consisting of vcc1, ip-vcc1, routing-group 1

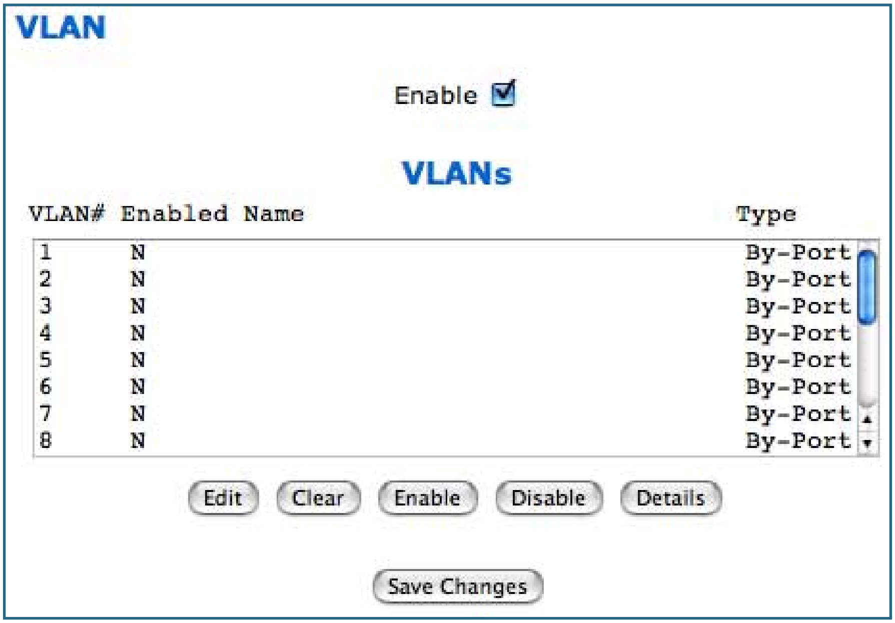
  Create a VLAN named “Lan” consisting of eth0.1, eth0.2, eth0.3, eth0.4, ssid1, ssid2, ssid3, ssid4 (etc.), ip-eth-a, routing-group 1

An example of multiple VLANs, using a Motorola Netopia® Gateway with VGx managed switch technology, is shown below:

A VLAN Model Combining Bridging and Routing



To configure VLANs check the **Enable** checkbox.



VLAN

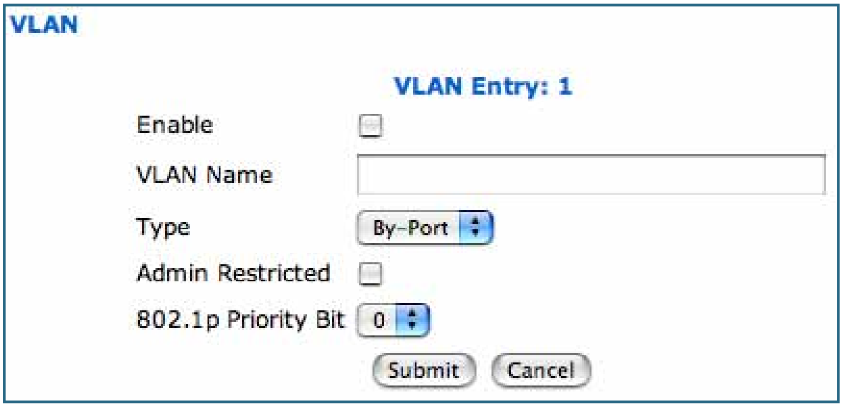
Enable ☑

VLANs

VLAN#	Enabled	Name	Type
1	N		By-Port
2	N		By-Port
3	N		By-Port
4	N		By-Port
5	N		By-Port
6	N		By-Port
7	N		By-Port
8	N		By-Port

To create a VLAN select a list item from the main VLAN page and click the **Edit** button.

The **VLAN Entry** page appears.



VLAN

VLAN Entry: 1

Enable □

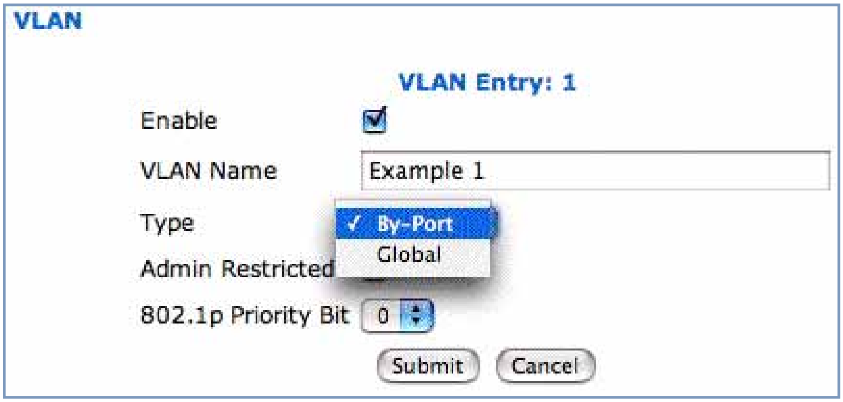
VLAN Name

Type By-Port

Admin Restricted □

802.1p Priority Bit 0

Check the **Enable** checkbox, and enter a descriptive name for the VLAN.



VLAN

VLAN Entry: 1

Enable ☑

VLAN Name: Example 1

Type: ✓ By-Port

Admin Restricted

802.1p Priority Bit: 0

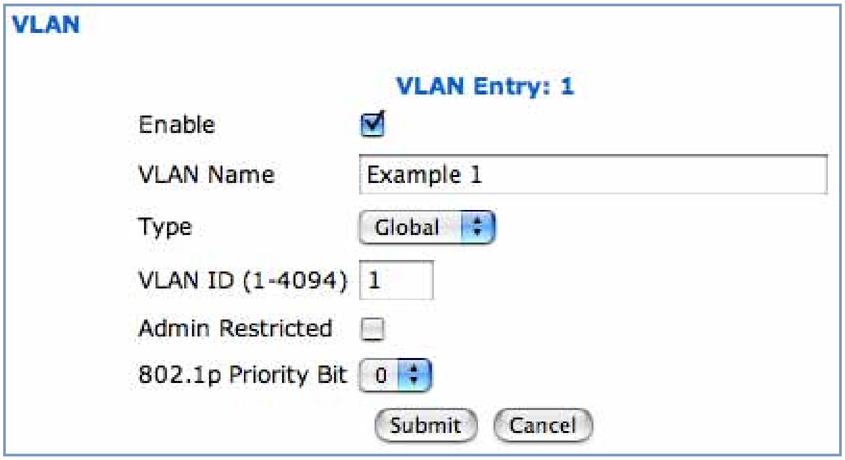
You can create up to 16 VLANs, and you can also restrict any VLAN, and the computers on it, from administering the Gateway.

- **VLAN Name** – A descriptive name for the VLAN.
- **Type** – LAN or WAN Port(s) can be enabled on the VLAN. You can choose a type designation as follows:

  By-Port: indicating that the VLAN is port-based. Traffic sent to this port will be treated as belonging to the VLAN, and will not be forwarded to other ports that are not within a common VLAN segment.

  Global: indicating that the ports joining this VLAN are part of a global 802.1q Ethernet VLAN. This VLAN includes ports on this Router and may include ports within other devices throughout the network. The VID in this case may define the behavior of traffic between all devices on the network having ports that are members of this VLAN segment.

- **VLAN ID** – If you select **Global** as the VLAN Type, the VLAN ID field appears for you to enter a VID. This must be a unique identifying number between 1 and 4094. (A VID of zero (0) is permitted on the Ethernet WAN port only.)



VLAN

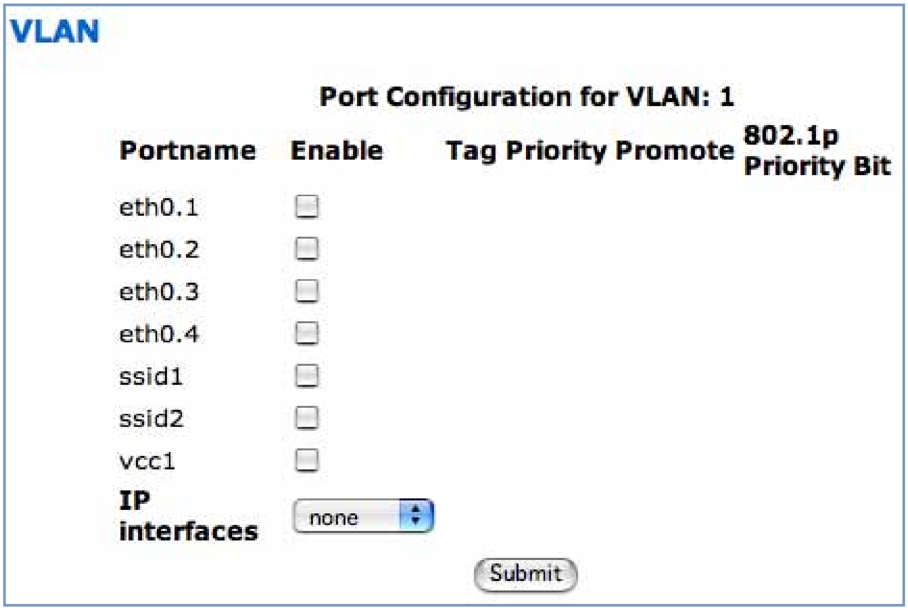
VLAN Entry: 1

Enable	☑
VLAN Name	Example 1
Type	Global
VLAN ID (1-4094)	1
Admin Restricted	□
802.1p Priority Bit	0

- **Admin Restricted** – If you want to prevent administrative access to the Gateway from this VLAN, check the checkbox.
- **802.1p Priority Bit**: If you set this from the pull-down menu to a value greater than 0, all packets of this VLAN with unmarked priority bits (pbits) will be re-marked to this priority.

  Click the **Submit** button.

The **Port Configuration** screen appears.



VLAN

Port Configuration for VLAN: 1

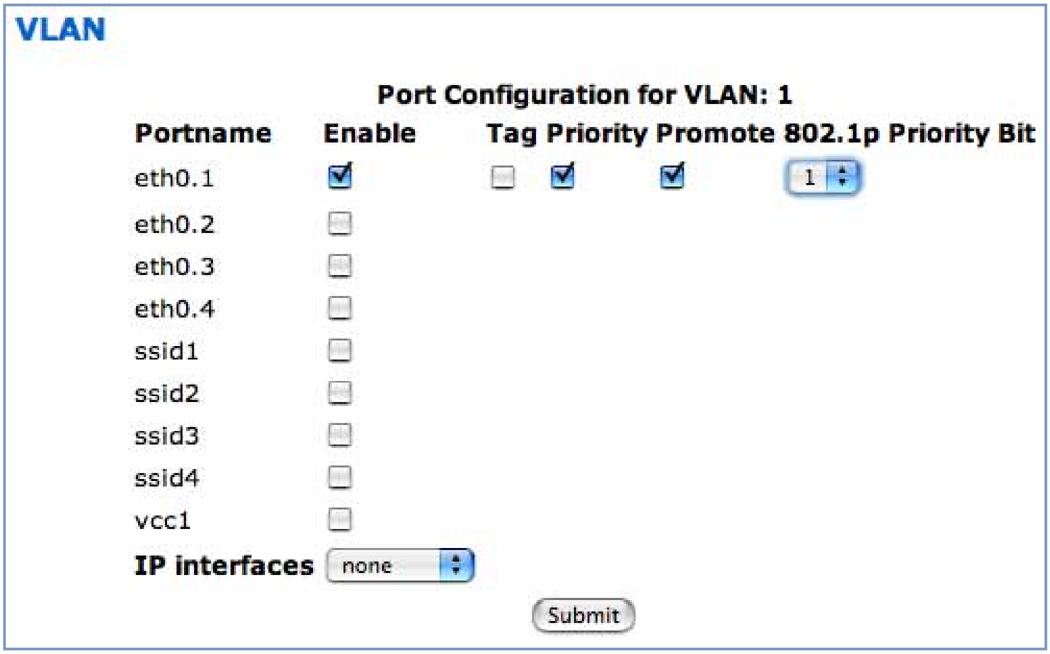
Portname	Enable	Tag Priority Promote	802.1p Priority Bit
eth0.1	□		
eth0.2	□		
eth0.3	□		
eth0.4	□		
ssid1	□		
ssid2	□		
vcc1	□		
IP interfaces	none		

- Port interfaces available for this VLAN are listed in the left hand column.
- Displayed port interfaces vary depending on the kinds of physical ports on your Gateway, for example, Ethernet, USB, and/or wireless.
- Also, if you have multiple wireless SSIDs defined, these may be displayed as well (See **Multiple Wireless IDs** on page 136)
- For Motorola Netopia® VGx technology models, separate Ethernet switch ports are displayed and may be configured.

  To enable any of them on this VLAN, check the associated **Enable** checkbox(es).

  Typically you will choose a physical port, such as an Ethernet port (example: **eth0.1**) or a wireless SSID (example: **ssid1**).

- When you enable an interface, the **Tag**, **Priority**, and **Promote** checkboxes and an **802.1p Priority Bit** pull-down menu appear for that interface.



VLAN

Port Configuration for VLAN: 1

Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	☑	□	☑	☑	1
eth0.2	□				
eth0.3	□				
eth0.4	□				
ssid1	□				
ssid2	□				
ssid3	□				
ssid4	□				
vcc1	□				
IP interfaces	none				

Tag – Packets transmitted from this port through this VLAN must be tagged with the VLAN VID. Packets received through this port destined for this VLAN must be tagged with the VLAN VID by the source. The Tag option is only available on **Global** type ports.

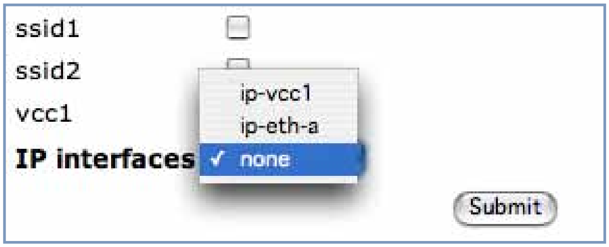
Priority – Use any 802.1p priority bits in the VLAN header to prioritize packets within the Gateway's internal queues, according to DiffServ priority mapping rules.

Promote – Write any 802.1p priority bits into the IP-TOS header bit field for received IP packets on this port destined for this VLAN. Write any IP-TOS priority bits into the 802.1p priority bit field for tagged IP packets transmitted from this port for this VLAN.

All mappings between Ethernet 802.1p and IP-TOS are made according to a pre-defined QoS mapping policy. The pre-defined mapping can now be set in the CLI. See "Queue Configuration" on page 231.

802.1p Priority Bit – If you set this field to a value greater than 0, all packets received on this port with unmarked priority bits (pbits) will be re-marked to this priority. If the port 802.1p PBit is greater than 0, the VLAN 802.1p PBit setting is ignored.

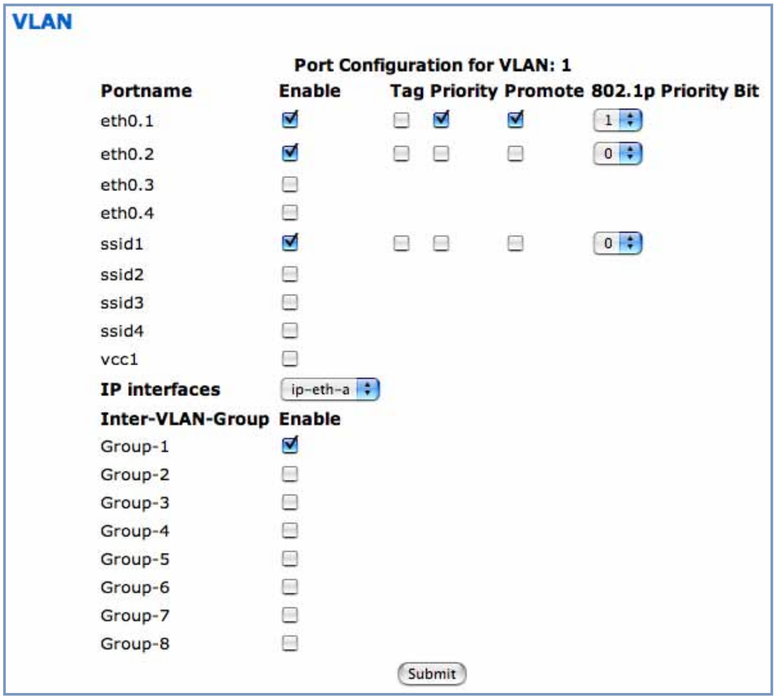
- Select an IP Interface for this VLAN. These selections will vary depending on your IP interfaces. For example, if you have set up multiple VCCs, these will appear in the list as **ip-vcc1**, **ip-vcc2**, and so forth.



ssid1	☐
ssid2	☐
vcc1	
IP interfaces	ip-vcc1 ip-eth-a ✓ none

- When you select an IP interface, the screen expands to allow you to configure **Inter-Vlan-Groups**.

  Inter-VLAN groups allow VLANs in the group to route traffic to the others; ungrouped VLANs cannot route traffic to each other.



VLAN

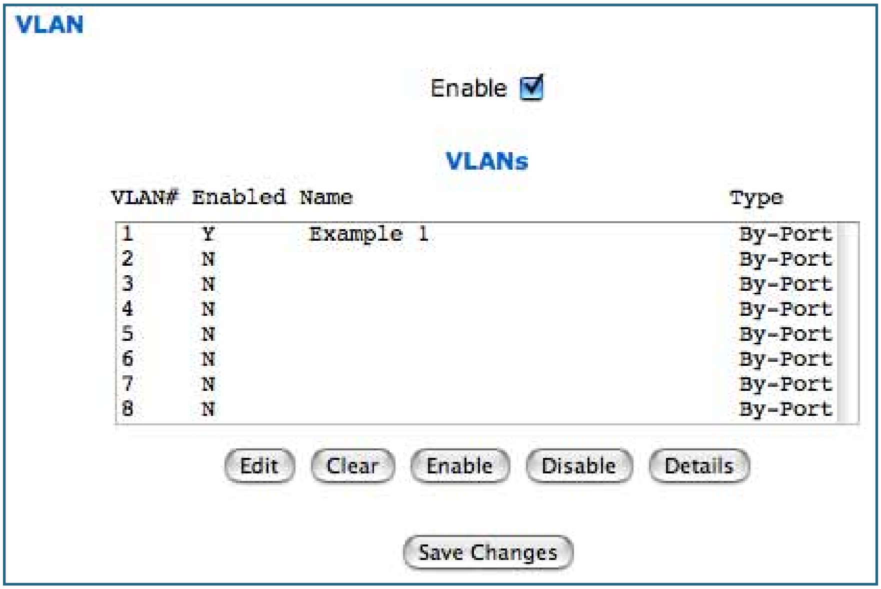
Port Configuration for VLAN: 1

Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	☑	☐	☑	☑	1
eth0.2	☑	☐	☐	☐	0
eth0.3	☐				
eth0.4	☐				
ssid1	☑	☐	☐	☐	0
ssid2	☐				
ssid3	☐				
ssid4	☐				
vcc1	☐				
IP interfaces	ip-eth-a				

Inter-VLAN-Group	Enable
Group-1	☑
Group-2	☐
Group-3	☐
Group-4	☐
Group-5	☐
Group-6	☐
Group-7	☐
Group-8	☐

- Click the **Submit** button.
- If you want to create more VLANs, repeat the process.

You can **Edit**, **Clear**, **Enable**, or **Disable** your VLAN entries by returning to the VLANs page, and selecting the appropriate entry from the displayed list.



VLAN

Enable ☑

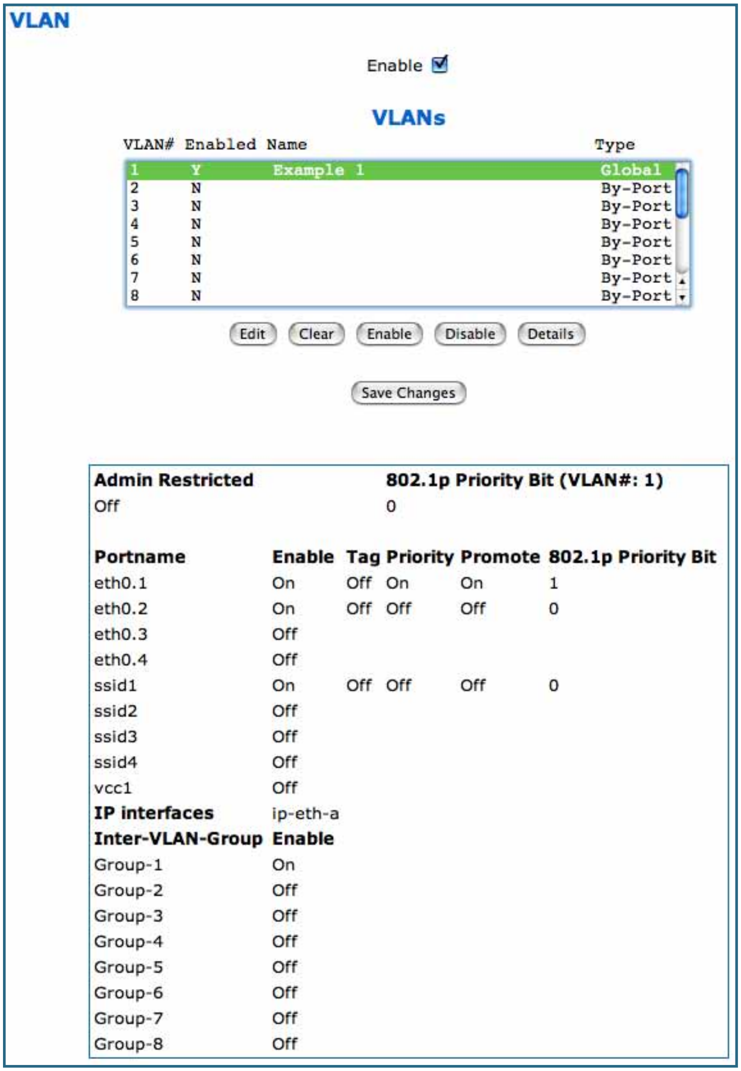
VLANs

VLAN#	Enabled	Name	Type
1	Y	Example 1	By-Port
2	N		By-Port
3	N		By-Port
4	N		By-Port
5	N		By-Port
6	N		By-Port
7	N		By-Port
8	N		By-Port

- When you are finished, click the **Save Changes** button.
- Click the **Restart Device** button.

To view the settings for each VLAN, select the desired VLAN from the list and click the **Details** button.

The screen expands to display the VLAN settings.



VLAN

Enable ☑

VLANs

VLAN#	Enabled	Name	Type
1	Y	Example 1	Global
2	N		By-Port
3	N		By-Port
4	N		By-Port
5	N		By-Port
6	N		By-Port
7	N		By-Port
8	N		By-Port

Admin Restricted	802.1p Priority Bit (VLAN#: 1)
Off	0

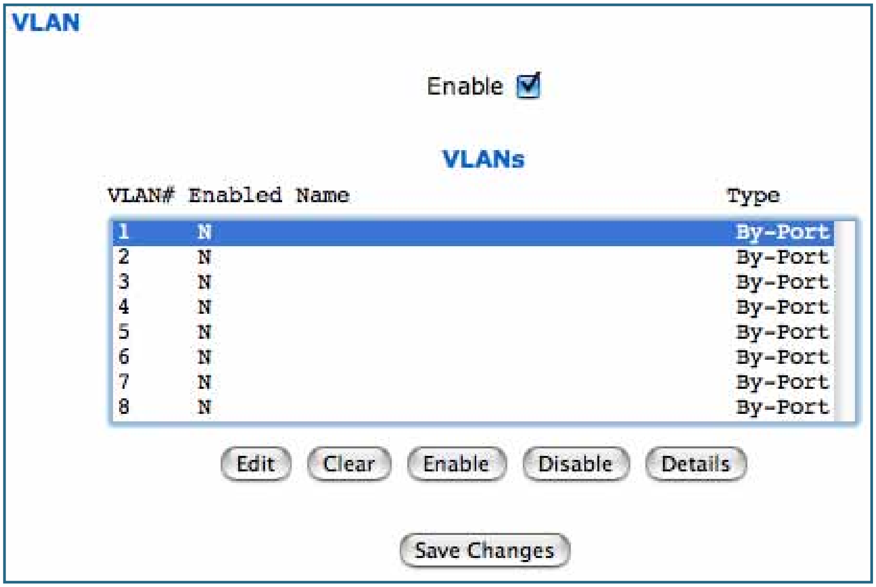
Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	On	Off	On	On	1
eth0.2	On	Off	Off	Off	0
eth0.3	Off				
eth0.4	Off				
ssid1	On	Off	Off	Off	0
ssid2	Off				
ssid3	Off				
ssid4	Off				
vcc1	Off				
IP interfaces	ip-eth-a				

Inter-VLAN-Group	Enable
Group-1	On
Group-2	Off
Group-3	Off
Group-4	Off
Group-5	Off
Group-6	Off
Group-7	Off
Group-8	Off

Example

You want to configure a 3347-02 Gateway with two SSIDs (see “Enable Multiple Wireless IDs” on page 136 for more information) for two VLANs, allowing both access to the Internet. One SSID will be in the same VLAN as the four ports of the Ethernet Switch, so that those two networks can communicate. The second VLAN will be for the other SSID. The second VLAN will also be denied access to the 3347NWG-VGx web interface and telnet interface. This setup might be useful if you have a doctor’s office or a coffee shop, and you want to keep your customers separated from the rest of the network.

1. **In the VLANs page, check the Enable checkbox, select VLAN #1 in the VLANs list, and click the Edit button.**



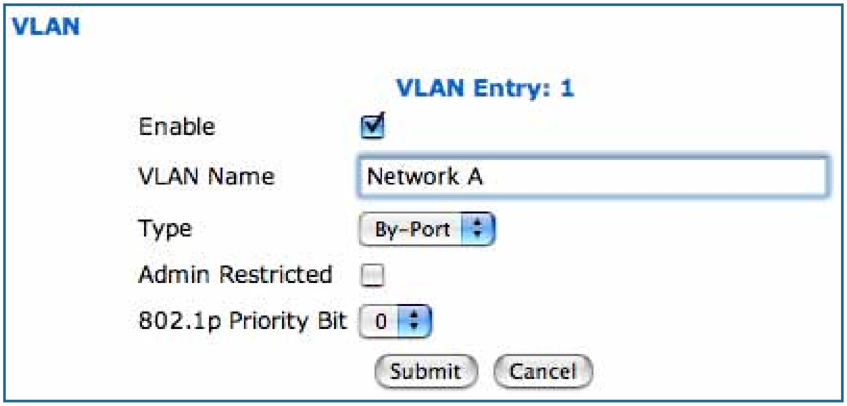
VLAN

Enable ☑

VLANs

VLAN#	Enabled	Name	Type
1	N		By-Port
2	N		By-Port
3	N		By-Port
4	N		By-Port
5	N		By-Port
6	N		By-Port
7	N		By-Port
8	N		By-Port

2. **Check the Enable checkbox, and in the VLAN Name box, enter the name you would like.**



VLAN

VLAN Entry: 1

Enable ☑

VLAN Name Network A

Type By-Port

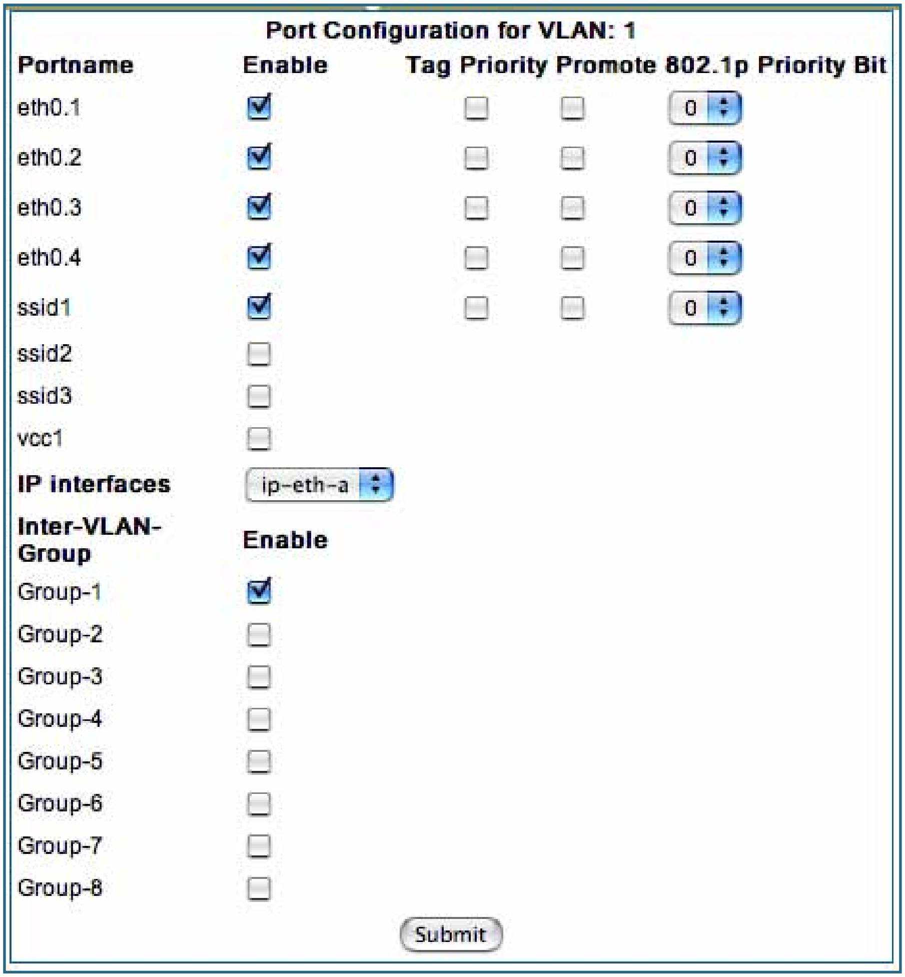
Admin Restricted □

802.1p Priority Bit 0

For example, call it ***Network A***.

Since this VLAN will be for SSID1 and the Ethernet ports, leave **Admin Restricted** unchecked. This will give this VLAN access to the Gateway.

3. **Click the Submit button.**
4. **In the Port Configuration for VLAN:1 page, you add the Port Interfaces you want associated with the VLAN.**



Port Configuration for VLAN: 1

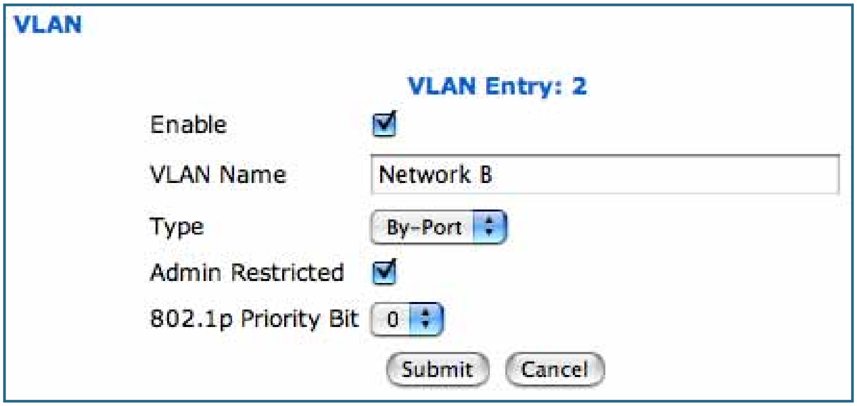
Portname	Enable	Tag	Priority Promote	802.1p Priority Bit
eth0.1	☑	□	□	0
eth0.2	☑	□	□	0
eth0.3	☑	□	□	0
eth0.4	☑	□	□	0
ssid1	☑	□	□	0
ssid2	□			
ssid3	□			
vcc1	□			

IP interfaces	ip-eth-a

Inter-VLAN-Group	Enable
Group-1	☑
Group-2	□
Group-3	□
Group-4	□
Group-5	□
Group-6	□
Group-7	□
Group-8	□

In this case, select all the physical Ethernet ports: **eth0.1** through **eth0.4**, and wireless **ssid1**. Select **ip-eth-a**, the IP interface for the group. This will be Inter-Vlan-Group #1. Check the **Group-1** checkbox. These ports will be able to communicate with each other.

5. **Click the Submit button.**
6. **In the VLAN page, select VLAN #2 in the VLANs list, and click the Edit button.**



VLAN

VLAN Entry: 2

Enable ☑

VLAN Name: Network B

Type: By-Port

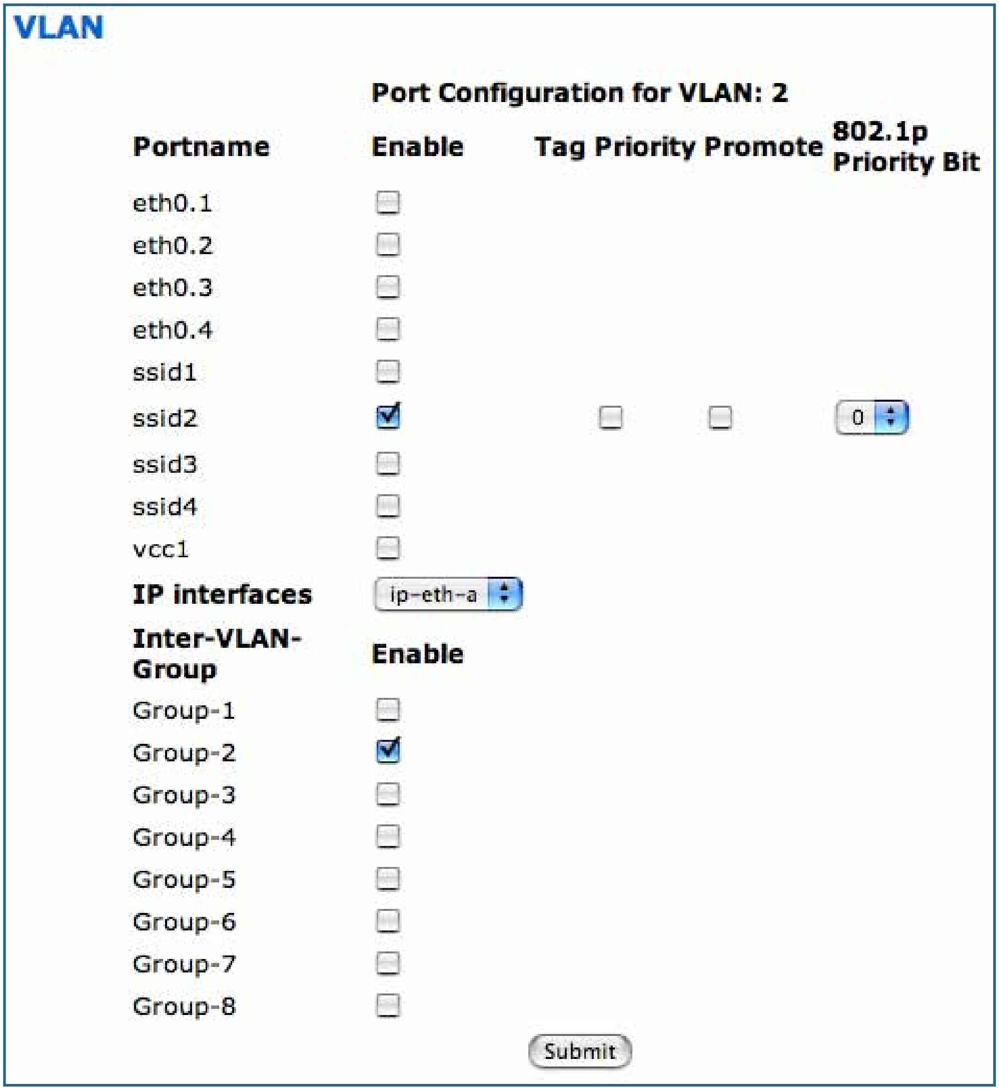
Admin Restricted ☑

802.1p Priority Bit: 0

The VLAN Name must be given another unique name. For example, call it ***Network B***. Since this is for the second SSID that we don't want to be given access to the Gateway, check the **Admin Restricted** checkbox.

7. **Click the Submit button.**

8. **In the Port Configuration for VLAN: 2 page, you add the Port Interfaces you want associated with the VLAN.**



VLAN

Port Configuration for VLAN: 2

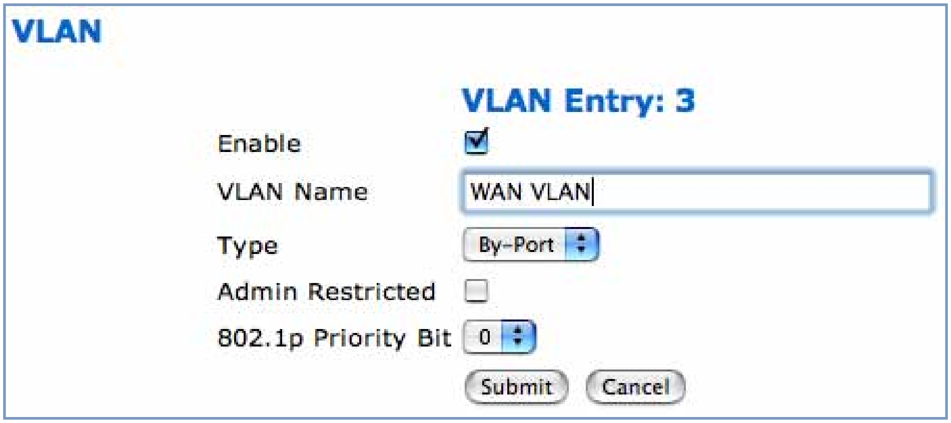
Portname	Enable	Tag	Priority Promote	802.1p Priority Bit
eth0.1	□			
eth0.2	□			
eth0.3	□			
eth0.4	□			
ssid1	□			
ssid2	☑	□	□	0
ssid3	□			
ssid4	□			
vcc1	□			
IP interfaces	ip-eth-a			

Inter-VLAN-Group	Enable
Group-1	□
Group-2	☑
Group-3	□
Group-4	□
Group-5	□
Group-6	□
Group-7	□
Group-8	□

Select the **ip-eth-a** port interface and check the **ssid2** port interface. Make this VLAN a member of Inter-Vlan-Group **Group-2**.

9. **Click the Submit button.**

10. **Next, create a VLAN to provide the Inter-Vlan-Groups access to the Internet (WAN).**



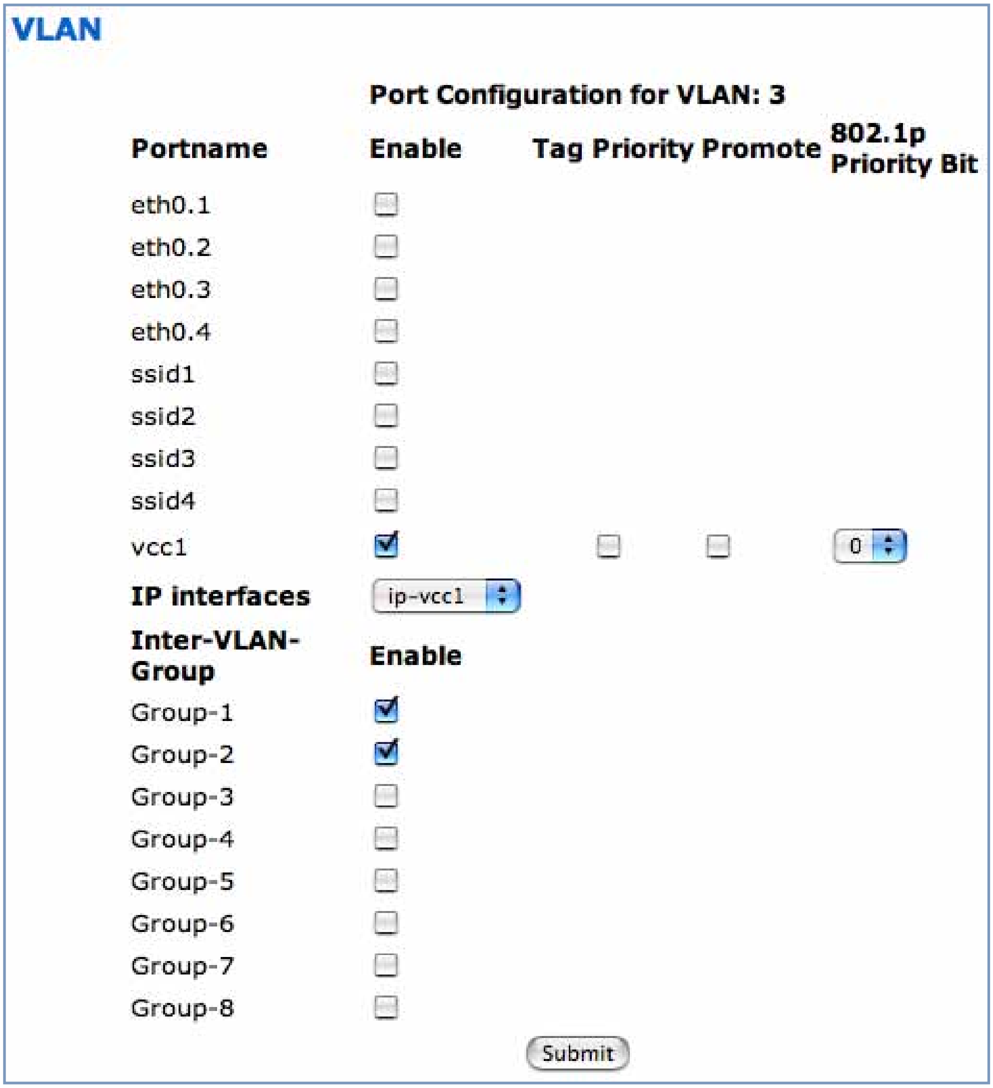
VLAN

VLAN Entry: 3

Enable	☑
VLAN Name	WAN VLAN
Type	By-Port
Admin Restricted	□
802.1p Priority Bit	0

For example, call it ***WAN VLAN***.

11. **Click the Submit button.**



VLAN

Port Configuration for VLAN: 3

Portname	Enable	Tag	Priority Promote	802.1p Priority Bit
eth0.1	□			
eth0.2	□			
eth0.3	□			
eth0.4	□			
ssid1	□			
ssid2	□			
ssid3	□			
ssid4	□			
vcc1	☑	□	□	0

IP interfaces: ip-vcc1

Inter-VLAN-Group	Enable
Group-1	☑
Group-2	☑
Group-3	□
Group-4	□
Group-5	□
Group-6	□
Group-7	□
Group-8	□

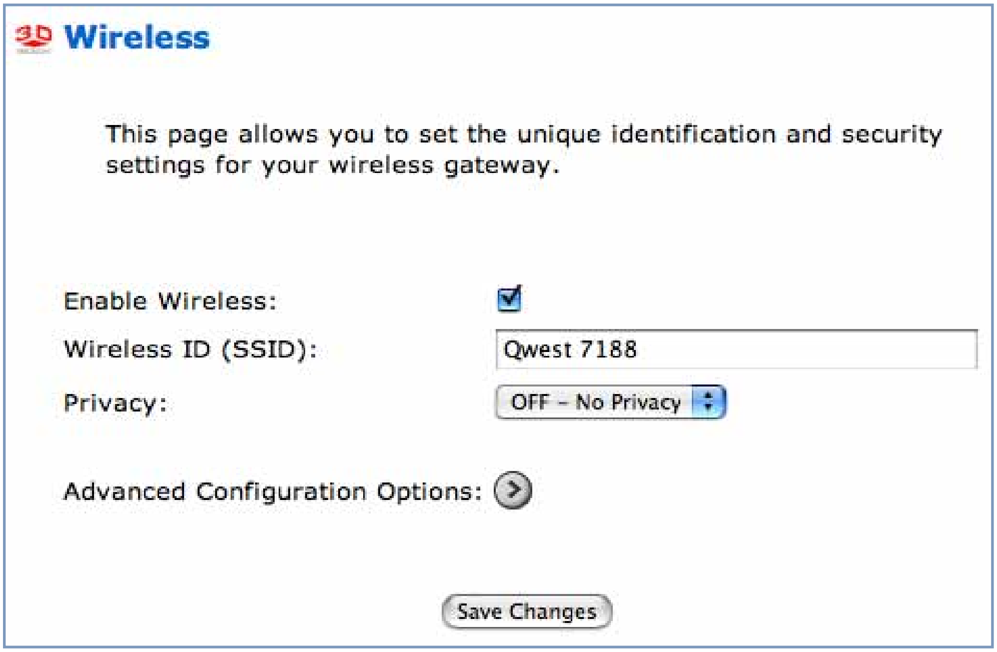
Check the **vcc1** checkbox, select the **ip-vcc1** IP interface, and check the Inter-Vlan-Group **Group-1** and **Group-2** checkboxes. Members of Groups 1 and 2 will now be able to communicate with the Internet (WAN), but not with each other.

12. **When you are finished, click the Submit button, then the Save Changes button.**
13. **When prompted to Save and Restart Connection, click the Yes button.**

Link: Wireless

(supported models only)

When you click Wireless, the 3-D Reach **Wireless** configuration page appears.



Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless: ☑

Wireless ID (SSID): Qwest 7188

Privacy: OFF - No Privacy

Advanced Configuration Options:

Enable Wireless

The wireless function is automatically enabled by default. If you uncheck the **Enable Wireless** checkbox, the Wireless Options are disabled, and the Gateway will not provide or broadcast any wireless LAN services.

Wireless ID (SSID)

The Wireless ID is preset to a number unique to your unit. You can either leave it as is, or change it by entering a freeform name of up to 32 characters, for example “Hercule’s Wireless LAN”. On client PCs’ software, this might also be called the *Network Name*. The Wireless ID is used to identify this particular wireless LAN. Depending on their operating system or client wireless card, users must either:

- select from a list of available wireless LANs that appear in a scanned list on their client

- or enter this name on their clients in order to join this wireless LAN.

Privacy

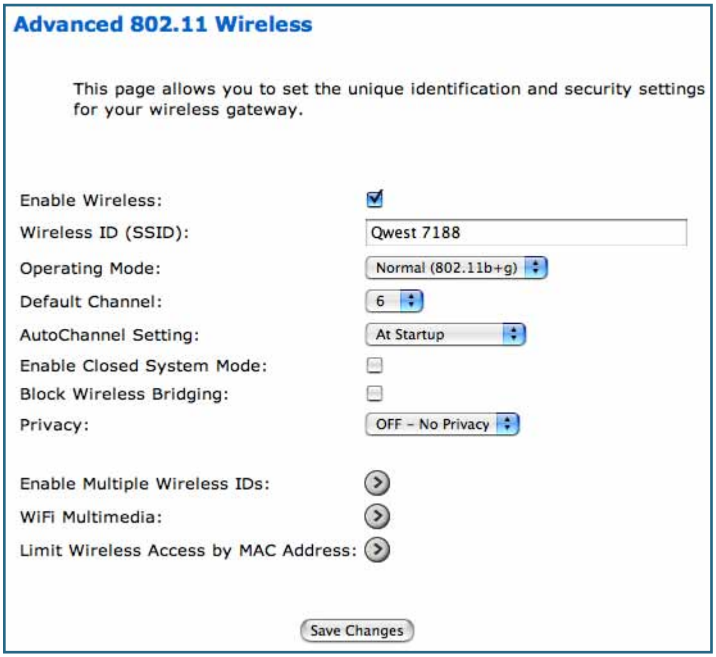
The pull-down menu for enabling **Privacy** offers four settings: **WPA-802.1x, WPA-PSK**, **WEP-Manual**, and **Off - No Privacy.**

IT IS STRONGLY RECOMMENDED THAT YOU ENABLE SOME FORM OF PRIVACY FOR THE SECURITY OF YOUR WIRELESS NETWORK.

See “Privacy” on page 130 for more information.

Advanced Configuration Options (optional)

When you click the Advanced Configuration Options button, the **Advanced 802.11 Wireless** screen appears. This screen varies its options depending on which form of wireless Privacy you have selected.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	□
Block Wireless Bridging:	□
Privacy:	OFF – No Privacy
Enable Multiple Wireless IDs:	>
WiFi Multimedia:	>
Limit Wireless Access by MAC Address:	>

Operating Mode

The pull-down menu allows you to select and lock the Gateway into the wireless transmission mode you want. For compatibility with clients using 802.11**b** (up to 11 Mbps transmission) and 802.11**g** (up to 20+ Mbps), select **Normal (802.11b + g)**. To limit your wireless LAN to one mode or the other, select **802.11b Only**, or **802.11g Only**.

NOTE:

If you choose to limit the operating mode to 802.11b or 802.11g only, clients using the mode you excluded will not be able to connect.

Default Channel

(1 through 11, for North America) on which the network will broadcast. This is a frequency range within the 2.4Ghz band. Channel selection depends on government regulated radio frequencies that vary from region to region. The widest range available is from 1 to 14. Europe, France, Spain and Japan differ. Channel selection can have a significant impact on performance, depending on other wireless activity close to this Router. Channel selection is not necessary at the client computers; the clients will scan the available channels seeking access points using the same SSID as the client.

AutoChannel Setting

For 802.11G models, AutoChannel is a feature that allows the Netopia Gateway to determine the best channel to broadcast automatically.

Three settings are available from the pull-down menu: **Off-Use default**, **At Startup**, and **Continuous**.

- **Off-Use default**: the Netopia Gateway will use the configured default channel selected from the previous pull-down menu.
- **At Startup** – the default setting – causes the Netopia Gateway at startup to briefly initialize on the default channel, then perform a full two- to three-second scan, and switch to the best channel it can find, remaining on that channel until the next reboot.
- **Continuous** performs the at-startup scan, and will continuously monitor the current channel for any other Access Point beacons. If an Access Point beacon is detected on the same channel, the Netopia Gateway will initiate a three- to four-minute scan of the channels, locate a better one, and switch. Once it has switched, it will remain on this channel for at least 30 minutes before switching again if another Access Point is detected.

Enable Closed System Mode

If enabled, Closed System Mode hides the wireless network from the scanning features of wireless client computers. Unless both the wireless clients and the Router share the same Wireless ID in Closed System mode, the Router’s wireless LAN will not appear as an available network when scanned for by wireless-enabled computers. Members of the Closed System WLAN must log onto the Router’s wireless network with the identical SSID as that configured in the router.

Closed System mode is an ideal way to increase wireless security and to prevent casual detection by unwanted neighbors, office users, or malicious users such as hackers.

If you do not enable Closed System Mode, it is more convenient, but potentially less secure, for clients to access your WLAN by scanning available access points. You must decide based on your own network requirements.

About Closed System Mode and Wireless Encryption

Enabling Closed System Mode on your wireless Router provides another level of security, since your wireless LAN will no longer appear as an available access point to client PCs that are casually scanning for one.

Your own wireless network clients, however, must log into the wireless LAN by using the exact SSID of the Motorola Netopia® Router.

In addition, if you have enabled WEP or WPA encryption on the Motorola Netopia® Router, your network clients must also have WEP or WPA encryption enabled, and must have the same WEP or WPA encryption key as the Motorola Netopia® Router.

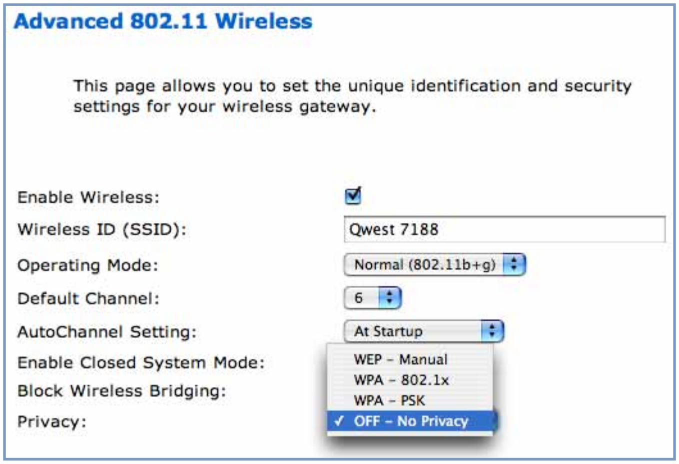
Once the Motorola Netopia® Gateway is located by a client computer, by setting the client to a matching SSID, the client can connect immediately if WEP or WPA is not enabled. If WEP or WPA is enabled then the client must also have WEP or WPA enabled and a matching WEP or WPA key.

Wireless client cards from different manufacturers and different operating systems accomplish connecting to a wireless LAN and enabling WEP or WPA in a variety of ways. Consult the documentation for your particular wireless card and/or operating system.

Block Wireless Bridging

Check the checkbox to block wireless clients from communicating with other wireless clients on the LAN side of the Gateway.

Privacy



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless: ☑

Wireless ID (SSID): Qwest 7188

Operating Mode: Normal (802.11b+g)

Default Channel: 6

AutoChannel Setting: At Startup

Enable Closed System Mode:

Block Wireless Bridging:

Privacy: ✓ OFF – No Privacy

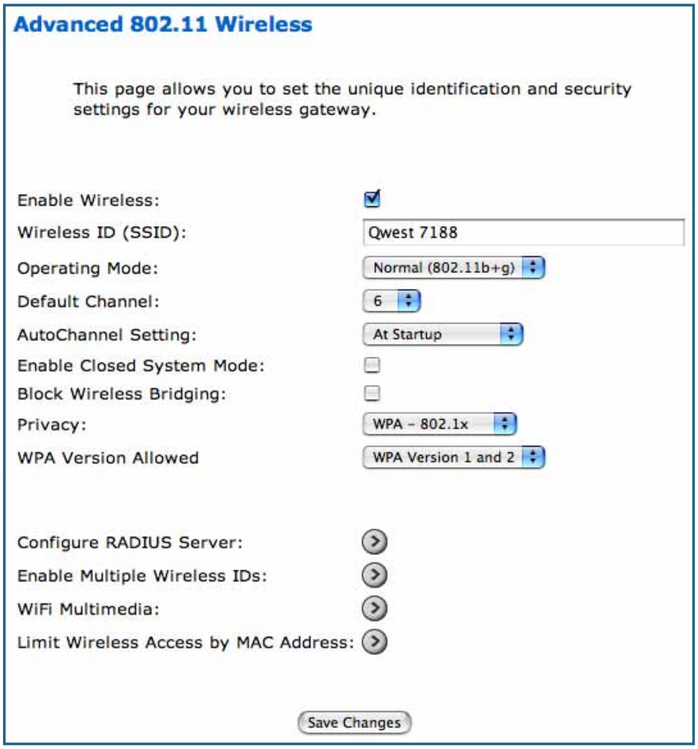
- **OFF - No Privacy:** This mode disables privacy on your network, allowing any wireless users to connect to your wireless LAN. Use this option if you are using alternative security measures such as VPN tunnels, or if your network is for public use.
- **WEP - Manual:** WEP Security is a Privacy option that is based on encryption between the Router and any PCs ("clients") you have with wireless cards. If you are not using WPA-PSK Privacy, you can use WEP Encryption instead. For this encryption to work, both your Router and each client must share the same Wireless ID, and both must be using the same encryption keys.
- **WPA-802.1x** provides RADIUS server authentication support. See RADIUS Server authentication below.
- **WPA-PSK** provides Wireless Protected Access, the most secure option for your wireless network. See "WPA-PSK" on page 133. This mechanism provides the best data protection and access control.

  Be sure that your Wi-Fi client adapter supports this option. Not all Wi-Fi clients support WPA-PSK.

RADIUS Server authentication

RADIUS servers allow external authentication of users by means of a remote authentication database. The remote authentication database is maintained by a Remote Authentication Dial-In User Service (RADIUS) server. In conjunction with Wireless User Authentication, you can use a RADIUS server database to authenticate users seeking access to the wireless services, as well as the authorized user list maintained locally within the Gateway.

If you select **WPA-802.1x**, the screen expands.



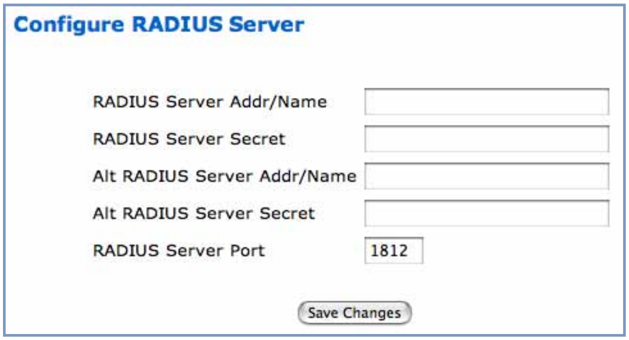
Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	□
Block Wireless Bridging:	□
Privacy:	WPA - 802.1x
WPA Version Allowed	WPA Version 1 and 2
Configure RADIUS Server:	⊙
Enable Multiple Wireless IDs:	⊙
WiFi Multimedia:	⊙
Limit Wireless Access by MAC Address:	⊙

Click the Configure RADIUS Server button.

The Configure RADIUS Server screen appears.



Configure RADIUS Server

RADIUS Server Addr/Name

RADIUS Server Secret

Alt RADIUS Server Addr/Name

Alt RADIUS Server Secret

RADIUS Server Port 1812

Enter your RADIUS Server information in the appropriate fields:

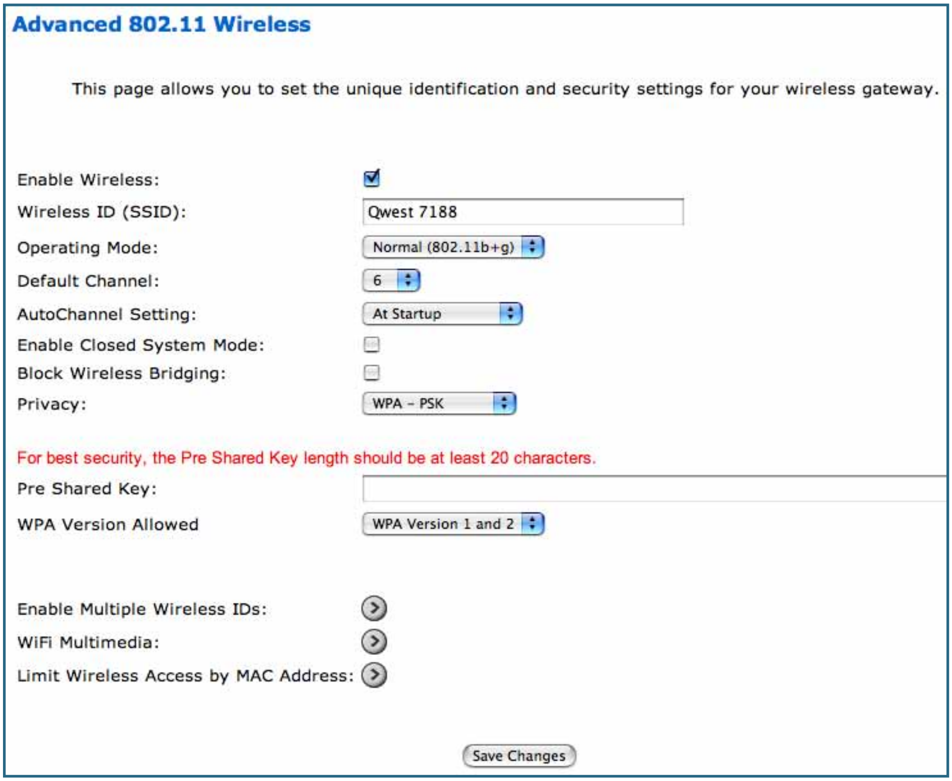
- **RADIUS Server Addr/Name:** The default RADIUS server name or IP address that you want to use.
- **RADIUS Server Secret:** The RADIUS secret key used by this server. The shared secret should have the same characteristics as a normal password.
- **Alt RADIUS Server Addr/Name:** An alternate RADIUS server name or IP address, if available.
- **Alt RADIUS Server Secret:** The RADIUS secret key used by this alternate server. The shared secret should have the same characteristics as a normal password.
- **RADIUS Server Port:** The port on which the RADIUS server is listening, typically, the default 1812.

Click the **Save Changes** button.

WPA-PSK

One of the easiest ways to enable Privacy on your Wireless network is by selecting **WPA-PSK** (Wi-Fi Protected Access) from the pull-down menu.

The screen expands to allow you to enter a **Pre Shared Key**. The key can be between 8 and 63 characters, but for best security it should be at least 20 characters. When you have entered your key, click the **Save Changes** button.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	□
Block Wireless Bridging:	□
Privacy:	WPA - PSK

For best security, the Pre Shared Key length should be at least 20 characters.

Pre Shared Key:	
WPA Version Allowed	WPA Version 1 and 2

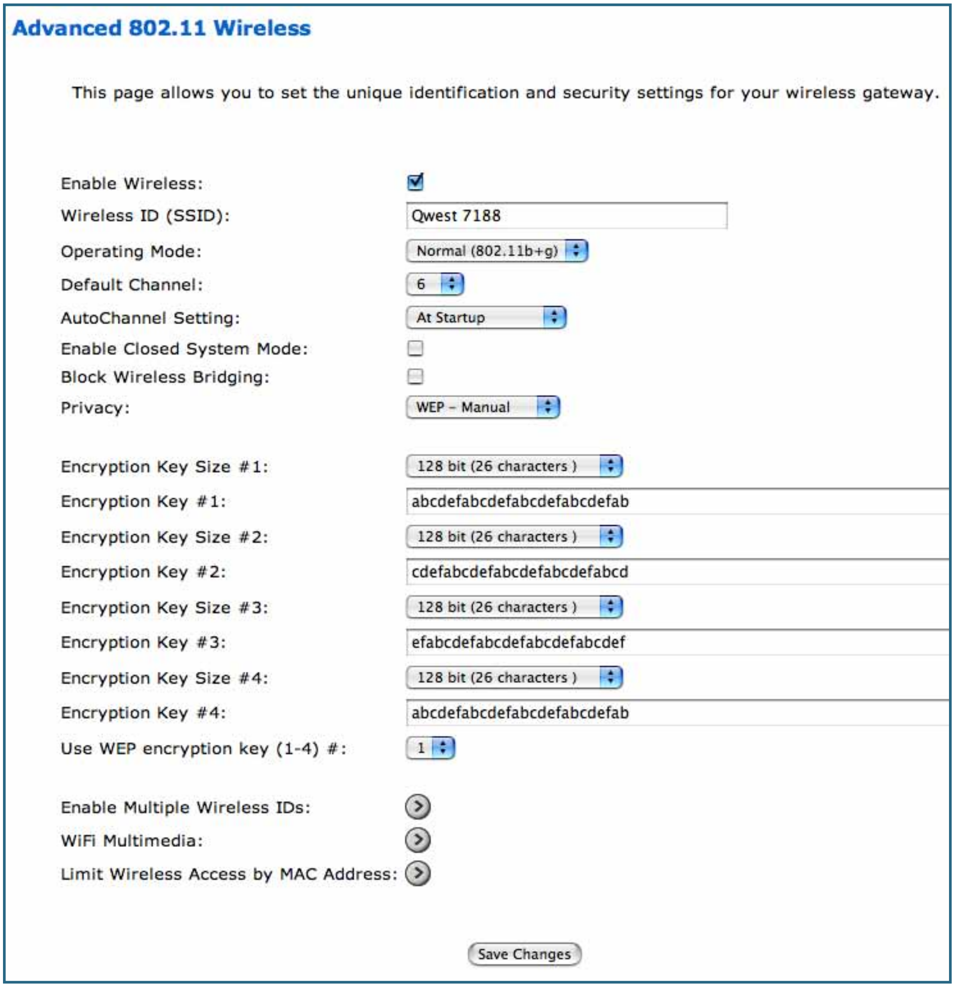
Enable Multiple Wireless IDs:

WiFi Multimedia:

Limit Wireless Access by MAC Address:

WEP-Manual

Alternatively, you can enable WEP (Wired Equivalent Privacy) encryption by selecting **WEP-Manual** from the Privacy pull-down menu.



Advanced 802.11 Wireless

This page allows you to set the unique identification and security settings for your wireless gateway.

Enable Wireless:	☑
Wireless ID (SSID):	Qwest 7188
Operating Mode:	Normal (802.11b+g)
Default Channel:	6
AutoChannel Setting:	At Startup
Enable Closed System Mode:	☐
Block Wireless Bridging:	☐
Privacy:	WEP – Manual
Encryption Key Size #1:	128 bit (26 characters)
Encryption Key #1:	abcdefabcdefabcdefabcdefab
Encryption Key Size #2:	128 bit (26 characters)
Encryption Key #2:	cdefabcdefabcdefabcdefabcd
Encryption Key Size #3:	128 bit (26 characters)
Encryption Key #3:	efabcdefabcdefabcdefabcdef
Encryption Key Size #4:	128 bit (26 characters)
Encryption Key #4:	abcdefabcdefabcdefabcdefab
Use WEP encryption key (1-4) #:	1
Enable Multiple Wireless IDs:	›
WiFi Multimedia:	›
Limit Wireless Access by MAC Address:	›

You can provide a level of data security by enabling WEP (Wired Equivalent Privacy) for encryption of network data. You can enable 40-, 128-, or 256-bit WEP Encryption (depending on the capability of your client wireless card) for IP traffic on your LAN.

WEP - Manual allows you to enter your own encryption keys manually. This is a difficult process, but only needs to be done once. Avoid the temptation to enter all the same characters.

Encryption Key Size #1 – #4: Selects the length of each encryption key. The longer the key, the stronger the encryption and the more difficult it is to break the encryption.

Encryption Key #1 – #4: The encryption keys. You enter keys using hexadecimal digits. For 40/64bit encryption, you need ten digits; 26 digits for 128bit, and 58 digits for 256bit WEP. Hexadecimal characters are 0 – 9, and a – f.

Examples:

- 40bit: 02468ACE02
- 128bit: 0123456789ABCDEF0123456789
- 256bit: 592CA140F0A238B0C61AE162F592CA140F0A238B0C61AE162F21A09C

Use WEP encryption key (1 – 4) #: Specifies which key the Gateway will use to encrypt transmitted traffic. The default is key #1.

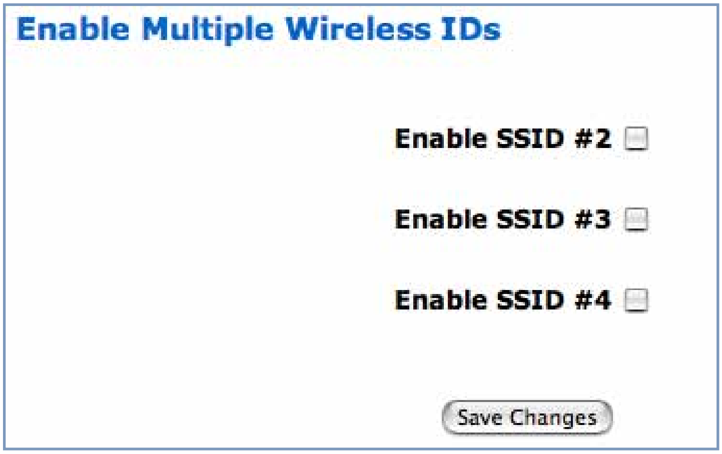
Click the click **Save Changes** button.

Any WEP-enabled client must have an identical key of the same length as the Router, in order to successfully receive and decrypt the traffic. Similarly, the client also has a ‘default’ key that it uses to encrypt its transmissions. In order for the Router to receive the client’s data, it must likewise have the identical key of the same length.

Enable Multiple Wireless IDs

This feature allows you to add additional network identifiers (SSIDs or *Network Names*) for your wireless network. To enable Multiple Wireless IDs, click the button.

The **Enable Multiple Wireless IDs** screen appears to allow you to add up to three additional Wireless IDs.



Enable Multiple Wireless IDs

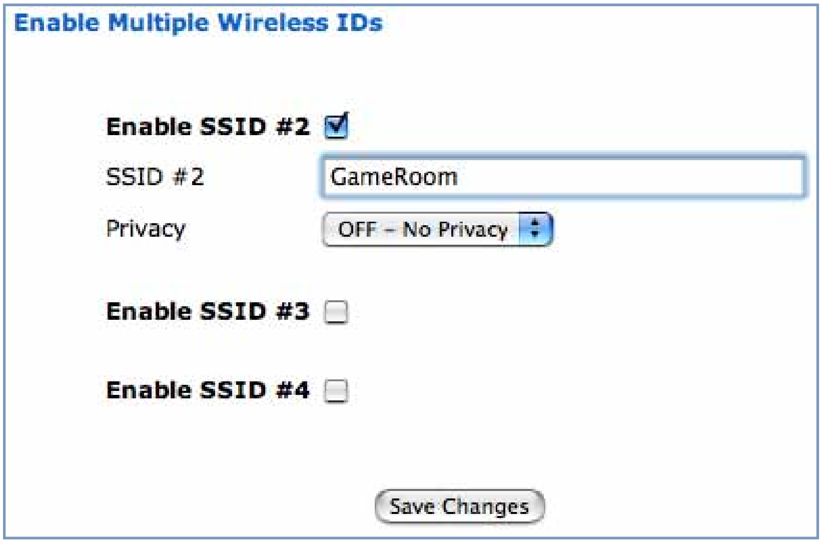
Enable SSID #2 □

Enable SSID #3 □

Enable SSID #4 □

When the Multiple Wireless SSIDs screen appears, check the **Enable SSID** checkbox for each SSID you want to enable.

The screen expands to allow you to name each additional Wireless ID, and specify a Privacy mode for each one.



Enable Multiple Wireless IDs

Enable SSID #2 ☑

SSID #2 GameRoom

Privacy OFF – No Privacy

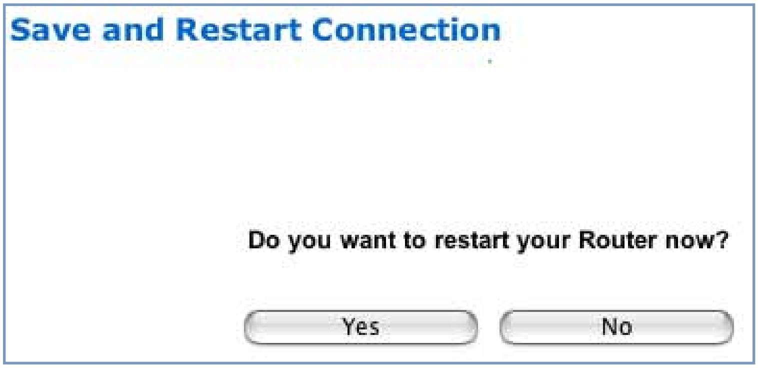
Enable SSID #3 □

Enable SSID #4 □

Privacy modes available from the pull-down menu for the multiple SSIDs are: **WPA-PSK**, **WPA-802.1x**, or **Off-No Privacy**.

These additional Wireless IDs are “Closed System Mode” Wireless IDs (see below) that will not be shown by a client scan, and therefore must be manually configured at the client. In addition, wireless bridging between clients is disabled for all members of these additional network IDs.

Click the **Save Changes** button. The Gateway will prompt you to restart it.



Save and Restart Connection

Do you want to restart your Router now?

Click the **Yes** button, and the Gateway will restart with your new settings.

NOTES:

The Gateway supports up to 4 different SSIDs:

- One SSID is broadcast by default and has wireless bridging enabled by default.
- Three additional SSIDs are in “Closed System Mode” and have wireless bridging disabled.
- These network IDs cannot be configured separately in terms of MAC Address filtering.
- You can configure privacy on one SSID and disable it on another SSID.

WiFi Multimedia

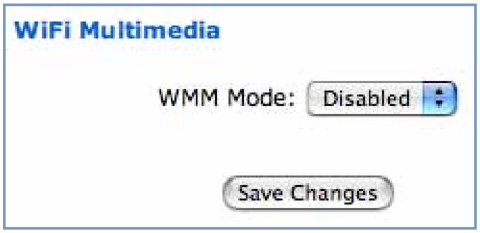
WiFi Multimedia is an advanced feature that allows you to prioritize various types of data travelling over the wireless network. Certain types of data that are sensitive to delays, such as voice or video, must be prioritized ahead of other, less delay-sensitive types, such as email.

WiFi Multimedia currently implements wireless Quality of Service (QoS) by transmitting data depending on Diffserv priority settings. These priorities are mapped into four Access Categories (AC), in increasing order of priority:

- Background (BK),
- Best Effort (BE),
- Video (VI), and
- Voice (VO).

It requires WiFi Multimedia (WMM)-capable clients, usually a separate feature enabled at the client network settings, and client PC software that makes use of Differentiated Services (Diffserv). Refer to your operating system instructions for enabling Diffserv QoS.

When you click the **WiFi Multimedia** button the **WiFi Multimedia** page appears.

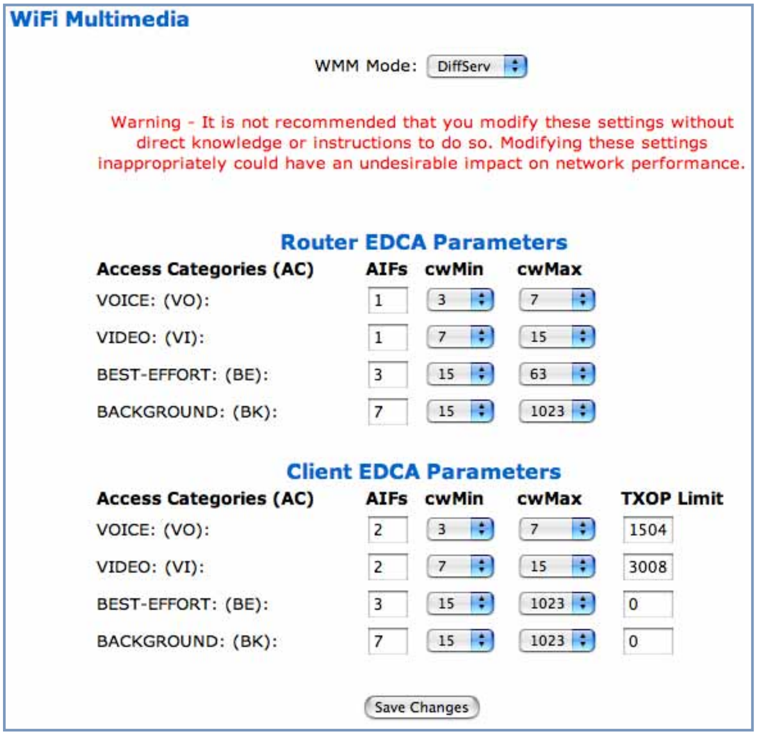


WiFi Multimedia

WMM Mode: Disabled

To enable the WiFi Multimedia custom settings, select **Diffserv** from the pull-down menu.

The screen expands.



WiFi Multimedia

WMM Mode: DiffServ

Warning - It is not recommended that you modify these settings without direct knowledge or instructions to do so. Modifying these settings inappropriately could have an undesirable impact on network performance.

Router EDCA Parameters

Access Categories (AC)	AIFs	cwMin	cwMax
VOICE: (VO):	1	3	7
VIDEO: (VI):	1	7	15
BEST-EFFORT: (BE):	3	15	63
BACKGROUND: (BK):	7	15	1023

Client EDCA Parameters

Access Categories (AC)	AIFs	cwMin	cwMax	TXOP Limit
VOICE: (VO):	2	3	7	1504
VIDEO: (VI):	2	7	15	3008
BEST-EFFORT: (BE):	3	15	1023	0
BACKGROUND: (BK):	7	15	1023	0

Router EDCA Parameters (Enhanced Distributed Channel Access) govern wireless data from your Gateway to the client; **Client EDCA Parameters** govern wireless data from the client to your Gateway.

NOTE:

It is not recommended that you modify these settings without direct knowledge or instructions to do so. Modifying these settings inappropriately could seriously degrade network performance.

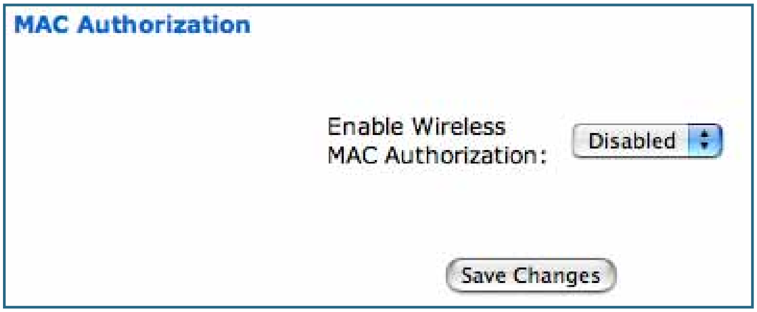
- **AIFs**: (Arbitration Interframe Spacing) the wait time in milliseconds for data frames.
- **cwMin**: (Minimum Contention Window) upper limit in milliseconds of the range for determining initial random backoff. The value you choose must be lower than cwMax.

- **cwMax**: (Maximum Contention Window) upper limit in milliseconds of the range of determining final random backoff. The value you choose must be higher than cwMin.
- **TXOP Limit**: Time interval in microseconds that clients may initiate transmissions. (When **Operating Mode** is **B-only**, default values are used and this field is not configurable.)

Click the **Save Changes** button.

Wireless MAC Authorization (optional)

MAC Authorization allows you to specify which client PCs are allowed to join the wireless LAN by unique hardware (MAC) address. To enable this feature, click the **Limit Wireless Access by MAC Address** button. The MAC Authorization screen appears.

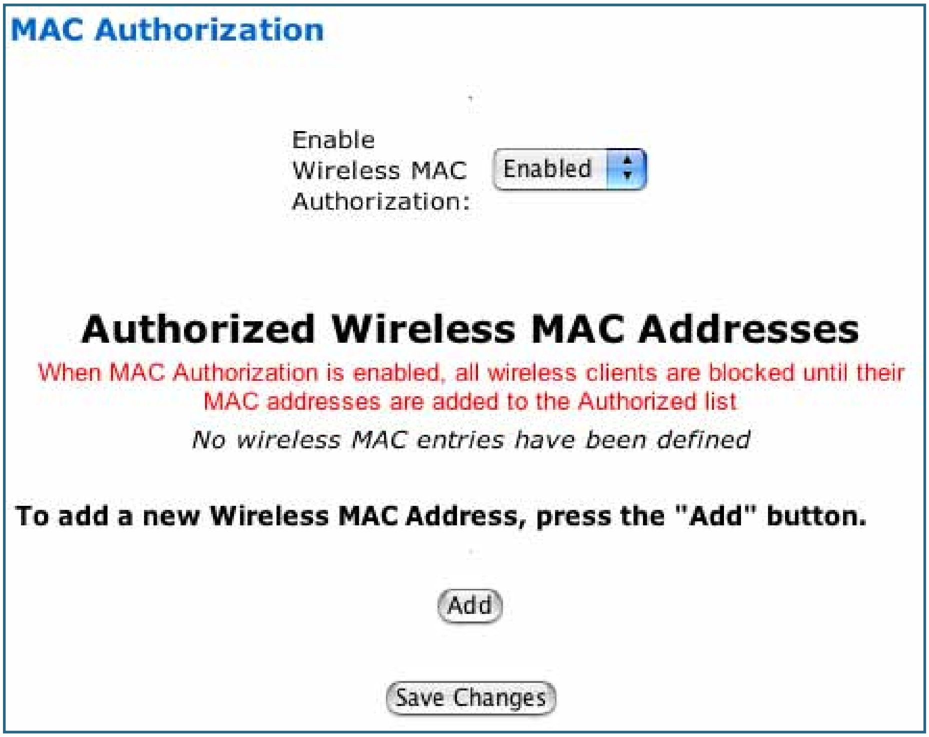


MAC Authorization

Enable Wireless MAC Authorization: Disabled

Select **Enabled** from the pull-down menu.

The screen expands to permit you to add MAC addresses.



MAC Authorization

Enable Wireless MAC Authorization: Enabled

Authorized Wireless MAC Addresses

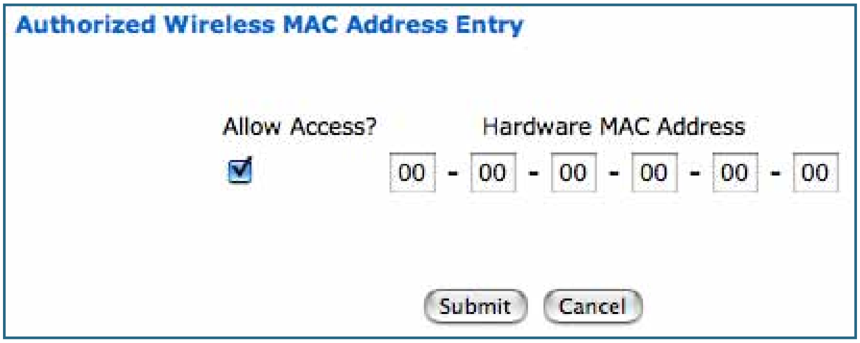
When MAC Authorization is enabled, all wireless clients are blocked until their MAC addresses are added to the Authorized list

No wireless MAC entries have been defined

To add a new Wireless MAC Address, press the "Add" button.

Click the **Add** button.

Once it is enabled, only entered MAC addresses that have been set to ***Allow*** will be accepted onto the wireless LAN. All unlisted addresses will be blocked, in addition to the listed addresses with *Allow* disabled.

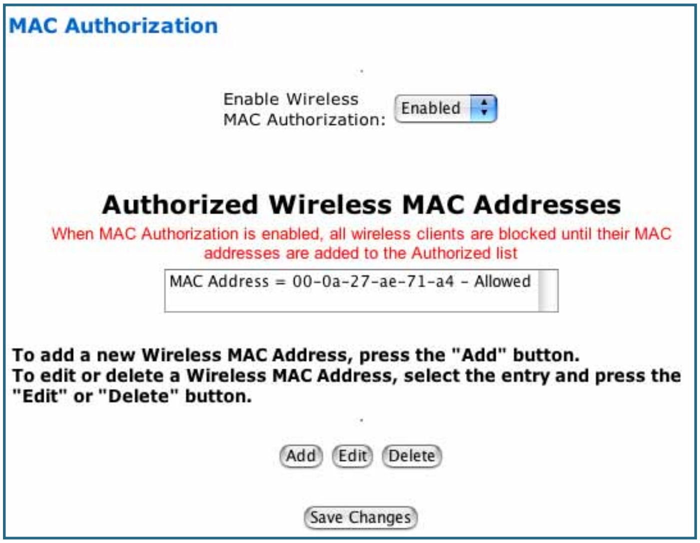


Authorized Wireless MAC Address Entry

Allow Access? ☑

Hardware MAC Address 00 - 00 - 00 - 00 - 00 - 00

Click the **Submit** button.



MAC Authorization

Enable Wireless MAC Authorization: Enabled

Authorized Wireless MAC Addresses

When MAC Authorization is enabled, all wireless clients are blocked until their MAC addresses are added to the Authorized list

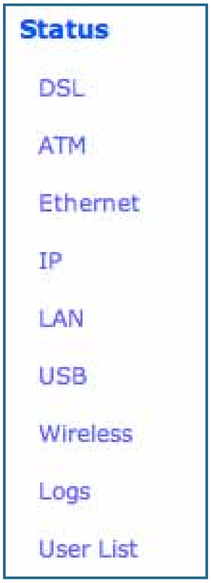
MAC Address = 00-0a-27-ae-71-a4 - Allowed

To add a new Wireless MAC Address, press the "Add" button.
To edit or delete a Wireless MAC Address, select the entry and press the "Edit" or "Delete" button.

When you are finished adding MAC addresses click the **Save Changes** button. You will be returned to the 802.11 Wireless page. You can **Add**, **Edit**, or **Delete** any of your entries later by returning to this page.

Link: Status

When you click the **Status** link, the Links Bar expands to display nine statistical sub-headings.



These screens will vary depending on your Gateway’s model and traffic activity:

- “DSL” on page 144
- “ATM” on page 145
- “Ethernet” on page 145
- “IP” on page 145
- “LAN” on page 146
- “USB” on page 147
- “Wireless” on page 146
- “Logs” on page 147
- “User List” on page 148

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 (if any)

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.

Wireless

(supported models only)

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

The Wireless Statistics page:

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

USB

(supported models only)

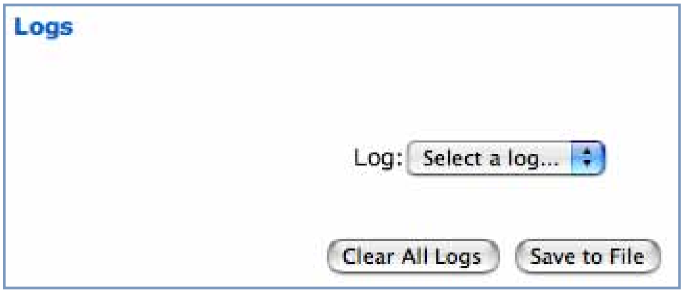
When you click **USB**, the USB Statistics page appears.

The USB Statistics page:

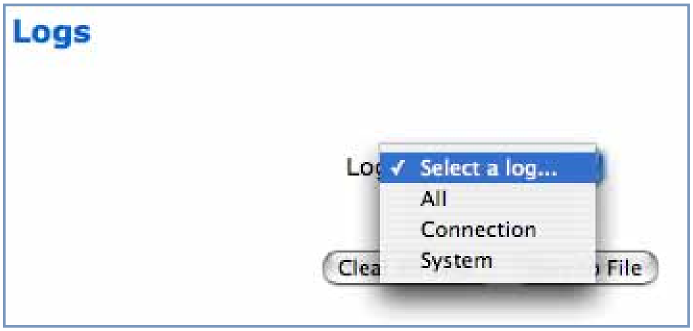
- displays your Router's unique hardware (MAC) address.
- displays detailed statistics about your LAN data traffic, upstream and downstream.

Logs

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



Select a log from the pull-down menu (the pull-down menu is available from every Log page):



- **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 Router STATUS** is displayed for all logs.

- To clear the individual logs, click the **Clear Log** button for that page.
- To clear all the logs, click the **Clear All Logs** button on the main Logs page.
- You can save logs to a text (.CTXT) file by clicking the **Save to File** button. This will download the file to your browser's default download location on your hard drive. The file can be opened with your favorite text editor.

Note:

Some browsers, such as Internet Explorer for Windows XP, require that you specify the Motorola Netopia® Gateway's URL as a "Trusted site" in "Internet Options: Security".

User List

When you click **User List**, the User List Statistics page appears.

The User List Statistics page:

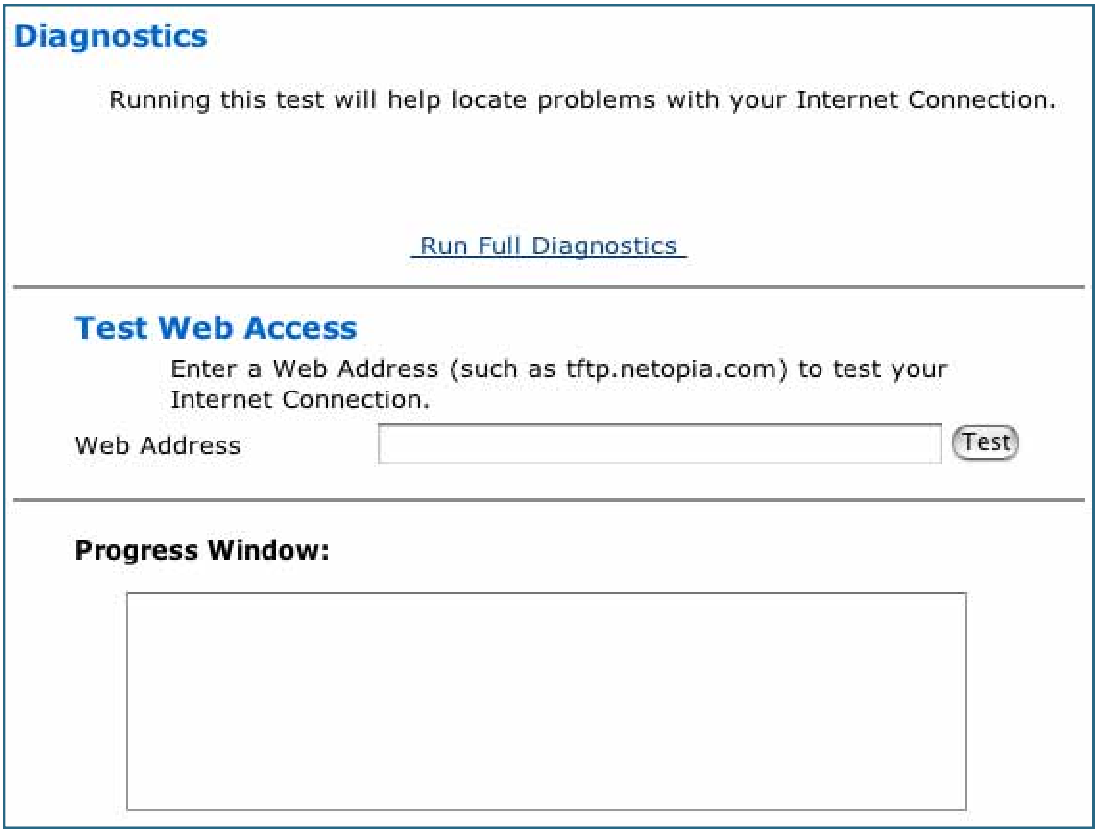
- displays Ethernet Users' **PC Name**, **IP Address**, and **MAC Address**.
- displays Wireless SSID Users' **PC Name**, **IP Address**, and **MAC Address**.

  If you have multiple SSIDs defined (see "Enable Multiple Wireless IDs" on page 136), Wireless SSID users are displayed by their respective SSID.

Link: Diagnostics

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

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.



Diagnostics

Running this test will help locate problems with your Internet Connection.

Test Web Access

Enter a Web Address (such as tftp.netopia.com) to test your Internet Connection.

Web Address

Progress Window:

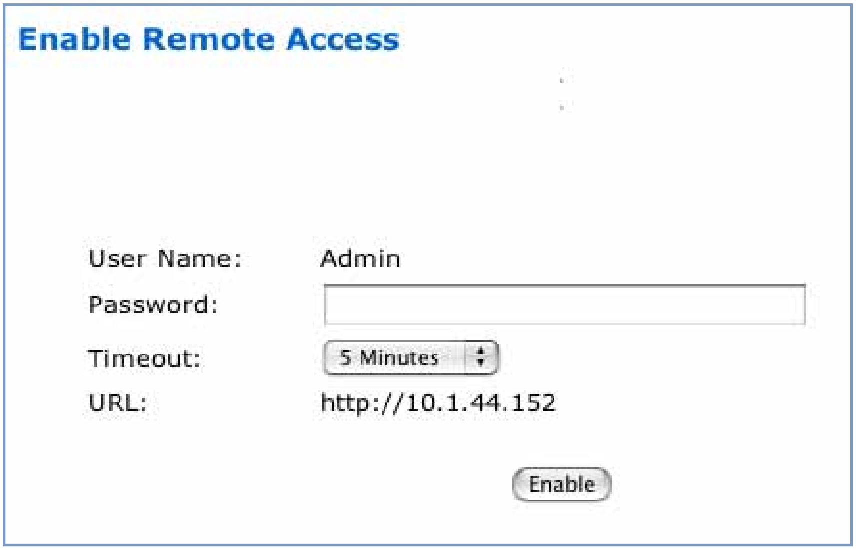
You enter a web address, such as *tftp.netopia.com*, or a known IP address, in the Web Address field and click the **Test** button. Results will be displayed in the **Progress Window** as they are generated.

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.

Link: Remote Access

When you click **Remote Access**, the **Enable Remote Access** page appears.



Enable Remote Access

User Name: Admin

Password:

Timeout: 5 Minutes

URL: http://10.1.44.152

This link allows you to authorize a remotely-located person, such as a support technician, to directly access your Motorola Netopia® Gateway. This is useful for fixing configuration problems when you need expert help. You can limit the amount of time such a person will have access to your Gateway. This will prevent unauthorized individuals from gaining access after the time limit has expired.

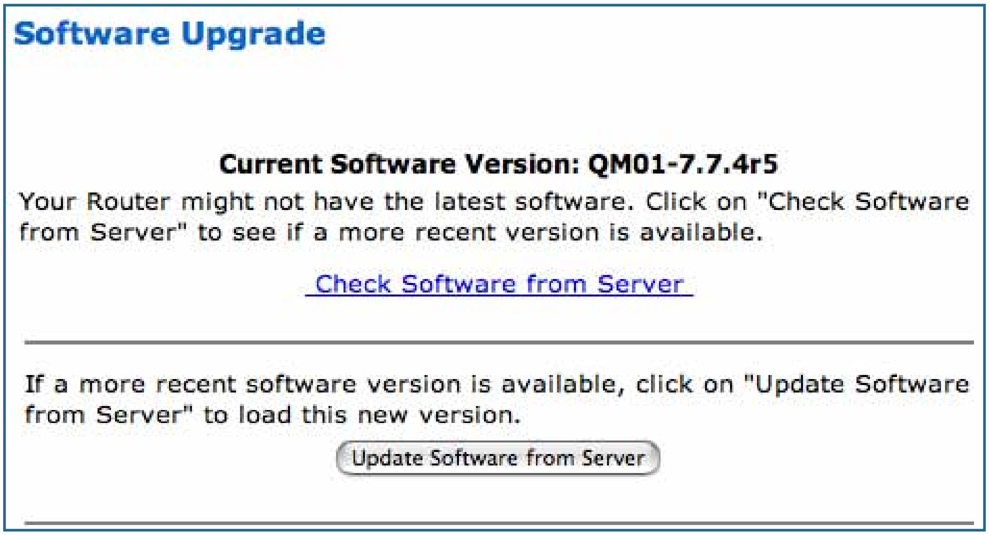
- Enter a temporary password for the person you want to authorize.
- Select a **Timeout** period for this password, from the pull-down menu (5 – 30 minutes, or Unlimited). Remote Access authorization lasts for a selected period of inactivity, after which it is automatically disabled again, to protect against unauthorized access attempts to your Router. Selecting *Unlimited* will enable remote access until the Router is rebooted. Be sure to tell the authorized person what the password is, and for how long the time-out is set.
- “Permanent” remote access to the router (i.e. access which is not disabled after the router is rebooted) may be configured in the CLI. See the command “set ip dsl vccn restrictions { admin-disabled l none }” on page 216. To make remote access “permanent,” you would use the option **none**. **This is not a recommended practice**, but may be needed for some applications.
  Click the **Enable** button. You can manually disable it, before the timeout period ends, by clicking the **Disable** button, or by restarting the Router.

Link: Update Router

When you click **Update Router**, 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.

(example screen – your screen may vary)



Software Upgrade

Current Software Version: QM01-7.7.4r5

Your Router might not have the latest software. Click on "Check Software from Server" to see if a more recent version is available.

Check Software from Server

If a more recent software version is available, click on "Update Software from Server" to load this new version.

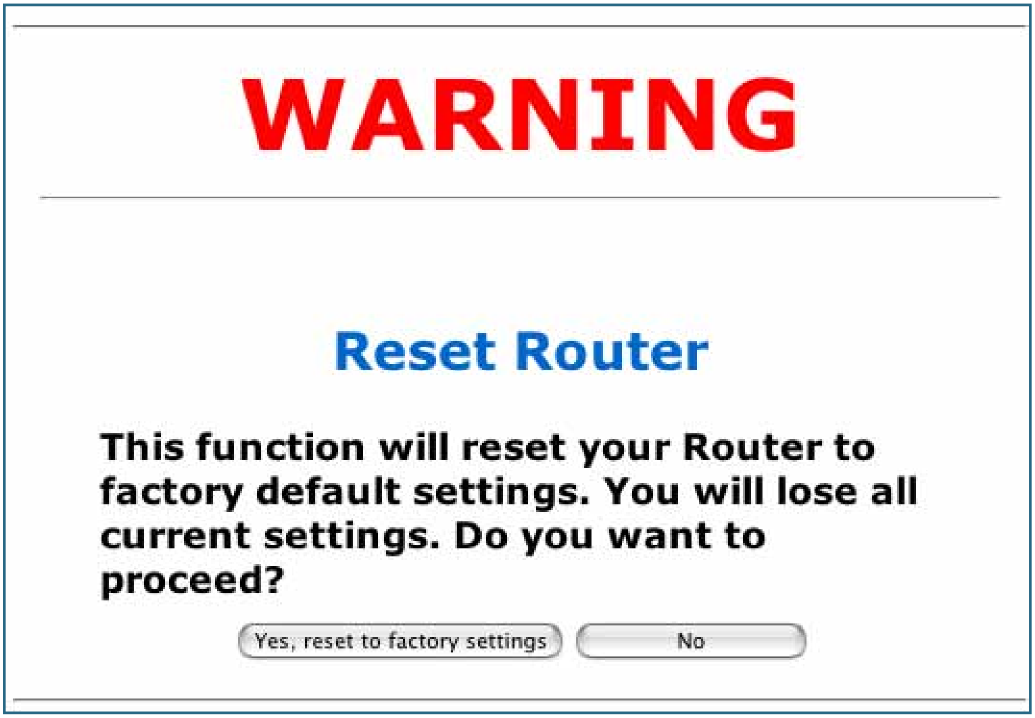
If you want to check for an updated version without installing it, click the **Check Software from Server** link.

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.

Link: Reset Router

You might need to reset your Router to its factory default state, and clear all of your previous settings. The **Reset Router** link allows you to do that. When you click the link, you will be challenged to confirm that this is what you want to do.



WARNING

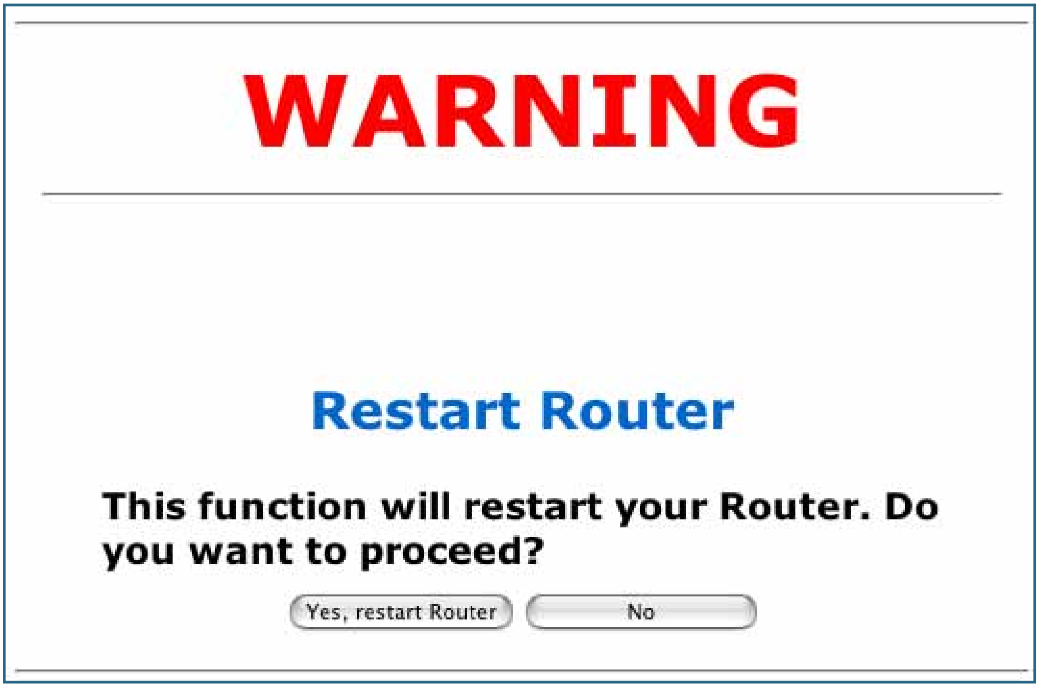
Reset Router

This function will reset your Router to factory default settings. You will lose all current settings. Do you want to proceed?

If you want to clear your settings, click the **Yes, reset to factory settings** button. The Router configuration will be reset to the factory default. Any configuration information you have entered will be lost and will have to be re-entered. The Router is restarted automatically.

Link: Restart Router

When the Gateway is restarted, it will disconnect all users, initialize all its interfaces, and copy the Operating System Software and feature keys from its internal storage.



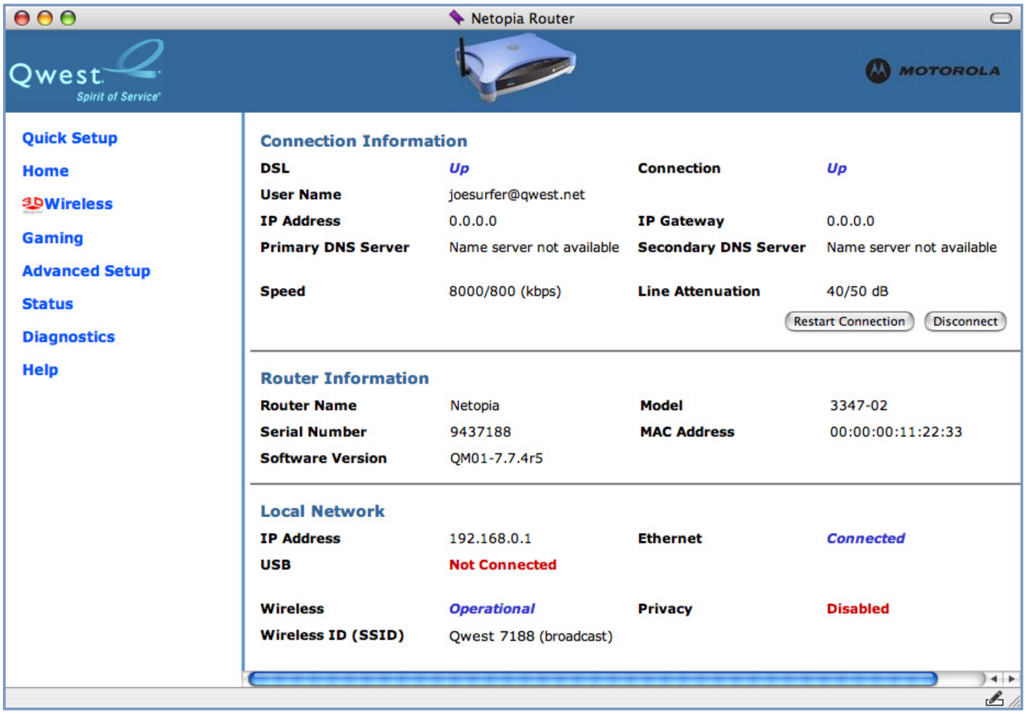
WARNING

Restart Router

This function will restart your Router. Do you want to proceed?

Basic Mode

When you click **Basic Mode**, you will be returned to the Basic Mode Home Page.



Connection Information

DSL	*Up*	**Connection**	*Up*
User Name	joesurfer@qwest.net		
IP Address	0.0.0.0	**IP Gateway**	0.0.0.0
Primary DNS Server	Name server not available	**Secondary DNS Server**	Name server not available
Speed	8000/800 (kbps)	**Line Attenuation**	40/50 dB

Router Information

Router Name	Netopia	**Model**	3347-02
Serial Number	9437188	**MAC Address**	00:00:00:11:22:33
Software Version	QM01-7.7.4r5		

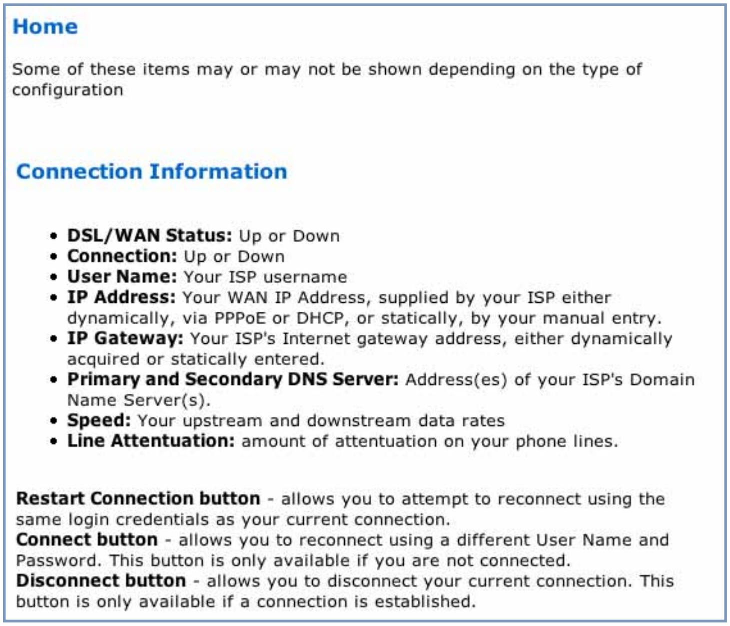
Local Network

IP Address	192.168.0.1	**Ethernet**	*Connected*
USB	**Not Connected**		
Wireless	*Operational*	**Privacy**	**Disabled**
Wireless ID (SSID)	Qwest 7188 (broadcast)		

Help

When you click the **Help** link in the left-hand column of links a page of explanatory information displays. Help is available for every page in the Web interface.

Here is an example from the Home page:



Home

Some of these items may or may not be shown depending on the type of configuration

Connection Information

- **DSL/WAN Status:** Up or Down
- **Connection:** Up or Down
- **User Name:** Your ISP username
- **IP Address:** Your WAN IP Address, supplied by your ISP either dynamically, via PPPoE or DHCP, or statically, by your manual entry.
- **IP Gateway:** Your ISP's Internet gateway address, either dynamically acquired or statically entered.
- **Primary and Secondary DNS Server:** Address(es) of your ISP's Domain Name Server(s).
- **Speed:** Your upstream and downstream data rates
- **Line Attentuation:** amount of attentuation on your phone lines.

Restart Connection button - allows you to attempt to reconnect using the same login credentials as your current connection.
Connect button - allows you to reconnect using a different User Name and Password. This button is only available if you are not connected.
Disconnect button - allows you to disconnect your current connection. This button is only available if a connection is established.

CHAPTER 4 Basic Troubleshooting

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

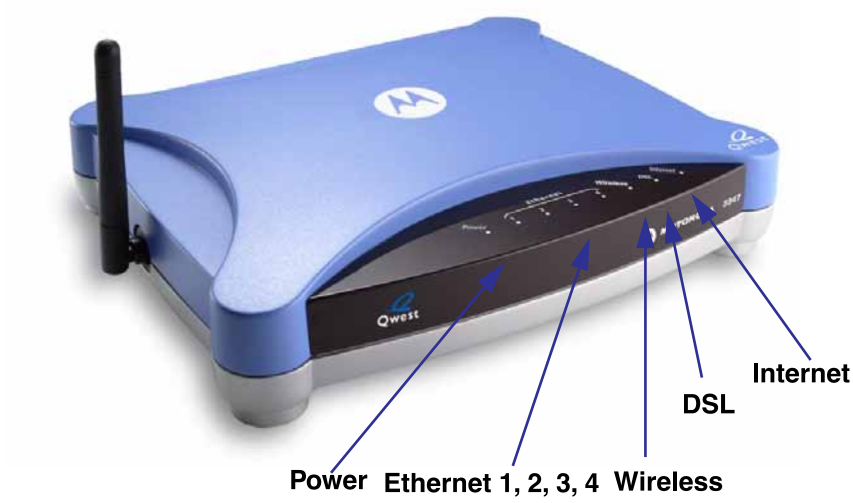
Before troubleshooting, make sure you have

- 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 in the following section.

Motorola Netopia® Gateway 3347-02 status indicator lights



LED	Action
Power	**Green** when power is on. **Red** when updating embedded software, or for system failure.
Ethernet 1, 2, 3, 4	Solid **green** when connected. Flash **green** when there is activity on the LAN. **Red** when bad userid and password are entered.
Wireless	Flashes **green** when there is activity on the wireless LAN.
DSL	Solid **green** when Internet connection is established.
Internet	Solid **green** when router is connected. Flashes **green** when transmitting or receiving data.

LED Function Summary Matrix

	Power	DSL	Internet	Ethernet	Wireless
Unlit	No power	No signal	No signal	No signal	No signal
Solid Green	Power on	Internet connection is established.	Router is connected.	Synched with Ethernet card	Synched with WLAN
Flashing Green	N/A	Activity on the DSL cable	Transmitting or receiving data.	Activity on the Ethernet cable	Activity on the WLAN
Red	Updating embedded software, or for system failure.	N/A	N/A	Bad userid and password are entered.	N/A

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

If LED is not Lit	Possible problems
Power	• Make sure the power switch is in the ON position. • Make sure the power adapter is plugged into the DSL Router properly. • Try a known good wall outlet. • Replace the power supply and/or unit.
DSL	• Make sure that any telephone has a microfilter installed. • Make sure the you are using the correct cable. The DSL cable is the thinner standard telephone cable. • Make sure the DSL cable is plugged into the correct wall jack. • Make sure the DSL cable is plugged into the DSL port on the DSL Router. • Make sure the DSL line has been activated at the central office DSLAM. • Make sure the DSL Router is not plugged into a micro filter. • Launch a browser and try to browse the Internet. If the DSL Active light still does not flash, then proceed to Advanced Troubleshooting.

Ethernet	• Make sure the you are using the Ethernet cable, not the DSL cable. The Ethernet cable is thicker than the standard telephone cable. • Make sure the Ethernet cable is securely plugged into the Ethernet jack on the PC. • Make sure the Ethernet cable is securely plugged into the Ethernet port on the DSL Router. • Try another Ethernet cable if you have one available. • Make sure you have Ethernet drivers installed on the PC. • Make sure the PC's TCP/IP Properties for the Ethernet Network Control Panel is set to obtain an IP address via DHCP. • Make sure the PC has obtained an address in the 192.168.1.x range. (You may have changed the subnet addressing.) • Make sure the PC is configured to access the Internet over a LAN. • Disable any installed network devices (Ethernet, HomePNA, wireless) that are not being used to connect to the DSL Router.
Wireless	• Make sure your client PC(s) have their wireless cards correctly installed and configured. • Check your client PC(s) TCP/IP settings to make sure they are receiving an IP address from the wireless Router. • Check the Router's log for wireless driver failure messages.

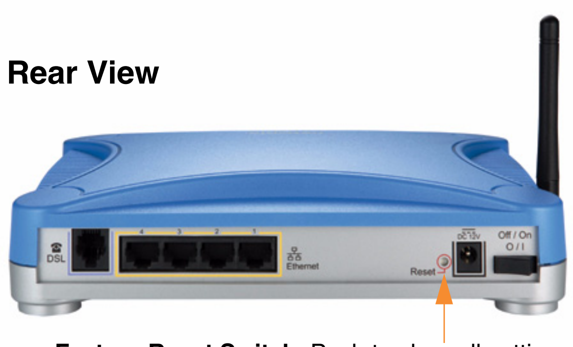
Factory Reset Switch

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 following diagram, 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.**
3. **Hold the button in until the “Power” LED turns RED and then hold it in until it turns GREEN again.**

   If you don't hold it this long, the normal configuration will be cleared, but not all the configuration info (default settings, etc.) – in some cases you may NOT want to clear all the default settings, as well. This entire process takes approximately 10 seconds: approximately five seconds for the Gateway to reboot and the LED to turn RED; then approximately three seconds for it to turn GREEN again.
4. **This will reset the unit to factory defaults and you will now be able to reprogram the Netopia Gateway.**

CHAPTER 5 Command Line Interface

The Motorola Netopia® Gateway operating software includes a command line interface (CLI) that lets you access your Motorola 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:

CONFIG Commands

CONFIG Commands

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
etheroam	to show Ethernet OAM info
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

view	to show configuration information
voip	to show VoIP info
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	
ata	ATA remote config options
atm	ATM options (DSL only)
backup	Backup gateway options
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 client options
ethernet	Ethernet options
ethernet-MAC-override	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
wan-over-ether	PPP over Ethernet options
preferences	Shell environment settings
queue	bandwidth queueing options
radius	RADIUS Server options
security	Security options
servers	Internal Server options

snmp	SNMP management options
system	Gateway’s system options
upnp	UPnP options
vdsl	VDSL tuning options
vlan	VLAN options
wireless	Wireless LAN 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 Motorola Netopia® Gateway before you can make a telnet connection to it. By default, your Motorola Netopia® Gateway uses 192.168.0.1 as the IP address for its LAN interface. You can use a Web browser to configure the Motorola 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 Motorola Netopia® Gateway settings.
- Entering a user password lets you display (but not update) Motorola 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 Motorola Netopia® Gateway:

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

SHELL Prompt

When you are in SHELL mode, the CLI prompt is the name of the Motorola Netopia® Gateway followed by a right angle bracket (>). For example, if you open a CLI connection to the Motorola Netopia® Gateway named "Netopia-3000/9437188," you would see ***Netopia-3000/9437188>*** 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 Motorola 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 Motorola Netopia® Gateway with Config commands. Config commands are described starting on page 167.

diagnose

Runs a diagnostic utility to conduct a series of internal checks and loopback tests to verify network connectivity over each interface on your Motorola 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 Motorola 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 Motorola 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.

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]

(Not supported on model 3342/3352)

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

The *server_address* argument identifies the IP address of the TFTP server on which your Motorola 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 Motorola Netopia® Gateway diagnostic log.

loglevel [*level*]

Displays or modifies the types of log messages you want the Motorola 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 Motorola Netopia® Gateway.

netstat -r

Displays the IP routes stored in your Motorola 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 Motorola 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 Motorola Netopia® Gateway’s own IP address.

quit

Exits the Motorola 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 cdmode

This command will set up one boot flag so that the next time a 3342**N**/3352**N** restarts or reboots (power cycle), the Gateway will boot into CD-ROM mode instead of Gateway mode.

This command is only for the 3342**N**/3352**N**. If the Gateway is not a 3342**N**/3352**N** this command does nothing but returns the message: “CD mode is not supported on this platform.”

reset crash

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

reset dhcp server

Clears the DHCP lease table in the Motorola Netopia® Gateway.

reset diffserv

Resets the Differentiated Services (diffserv) statistics.

reset enet [all]

Resets Ethernet statistics to zero. Resets individual LAN switch port statistics as well as wireless and WAN Ethernet statistics (where applicable).

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 Motorola 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.

reset wan

This function resets WAN interface statistics.

reset wepkeys

This function allows you to force your wireless WEP key settings back to the default values, if there are default values. For example, on some models, the WEP keys are based on the serial number. This allows you to get back those default settings if you have changed them without the need to reset the entire configuration of the unit.

restart [*seconds*]

Restarts your Motorola Netopia® Gateway. If you include the optional *seconds* argument, your Motorola 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 Motorola Netopia® Gateway.

show backup

Displays the status of the Backup port, Up or Down, and reports the current port in use.

show bridge interfaces

Displays bridge interfaces maintained by the Motorola Netopia® Gateway.

show bridge table

Displays the bridging table maintained by the Motorola Netopia® Gateway.

show config

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

show crash

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

show dhcp agent

Displays DHCP relay-agent leases.

show dhcp server leases

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

show diffserv

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

show dslf device-association

Displays LAN devices that conform with the TR111 Gateway requirement. It displays - IP Address, Manufacture OUI and Serial number.

show enet [all]

Displays Ethernet interface statistics maintained by the Motorola Netopia® Gateway. Beginning with Firmware Version 7.7, supports display of individual LAN switch port statistics as well as WAN Ethernet statistics (where applicable).

Example:

```
show enet status all
10/100 Ethernet 1

Port Status:  Link down
 Transmit OK            : 0
 Transmit unicastpkts   : 0
 Receive  OK            : 0
 Receive unicastpkts    : 0
 Tx Octets              : 0
 Rx Octets              : 0

10/100 Ethernet 2

Port Status:  Link down
 Transmit OK            : 0
 Transmit unicastpkts   : 0
 Receive  OK            : 0
 Receive unicastpkts    : 0
 Tx Octets              : 0
 Rx Octets              : 0

10/100 Ethernet 3
```

```
Port Status:  Link up
Duplex:  Full-duplex not active
Speed:  100BASE-X
 Transmit OK           : 3309
 Transmit unicastpkts  : 31
 Receive  OK           : 5588
 Receive unicastpkts   : 1976
 Tx Octets             : 31
 Rx Octets             : 1976

10/100 Ethernet 4

Port Status:  Link down
 Transmit OK           : 0
 Transmit unicastpkts  : 0
 Receive  OK           : 0
 Receive unicastpkts   : 0
 Tx Octets             : 0
 Rx Octets             : 0
```

show etheroam ah

Displays OAM internal information, such as OAM mode, state, configurations, events and OAM statistics.

show features

Displays standard and keyed features installed in the Motorola Netopia® Gateway.

show group-mgmt

Displays the IGMP Snooping Table.

show ip arp

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

show ip igmp

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

show ip interfaces

Displays the IP interfaces for your Motorola 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 Motorola 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 ipmap

Displays IPMap table (NAT).

show log

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

show pppoe

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

show rtsp

Displays RTSP ALG session activity data.

show security-log

Displays blocks of information from the Motorola Netopia® Gateway security log.

show status

Displays the current status of a Motorola Netopia® Gateway, the device's hardware and software revision levels, a summary of errors encountered, and the length of time the Motorola 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 vlan

Displays detail of VLAN status and statistics.

Example:

```
show vlan

Displaying vlan segment interfaces
==== vlan mode ====
==== segment 0 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 1 port masks ====
PortPort   : 00001006-00000001
GlobalPort : 00000000-00000000
SumPort    : 00001006-00000001
==== segment 2 port masks ====
PortPort   : 0000003c-00000000
GlobalPort : 00000000-00000000
SumPort    : 0000003c-00000000
==== segment 3 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 4 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 5 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 6 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 7 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
```

```
SumPort    : 00000000-00000000
==== segment 8 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 9 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
==== segment 10 port masks ====
PortPort   : 00000000-00000000
GlobalPort : 00000000-00000000
SumPort    : 00000000-00000000
  ==== vlan active segment ====
  Type  : 1
  Index : 1
  Vid : 1
  PortMask     : 00001006-00000001
  SwitchMask   : 00000004
  WirelessMask : 00001000
    ==== vlan active link ====
    namePtr   : eth-lan-uplink
    portType  : 1
    portIndex : 1
    ifId      : 45
    ==== vlan active link ====
    namePtr   : ethernet0/0
    portType  : 3
    portIndex : 2
    ifId      : 46
    ==== vlan active link ====
    namePtr   : ssid1
    portType  : 5
    portIndex : 12
    ifId      : 56
    ==== vlan active link ====
    namePtr   : eth-ip0
    portType  : 7
    portIndex : 32
    ifId      : 76
  ==== vlan active segment ====
  Type  : 1
  Index : 2
  Vid : 3
  PortMask     : 0000003c-00000000
  SwitchMask   : 0000003c
  WirelessMask : 00000000
    ==== vlan active link ====
    namePtr   : ethernet0/0
    portType  : 3
    portIndex : 2
    ifId      : 90
    ==== vlan active link ====
    namePtr   : ethernet0/1
    portType  : 3
    portIndex : 3
    ifId      : 91
    ==== vlan active link ====
    namePtr   : ethernet0/2
    portType  : 3
    portIndex : 4
    ifId      : 92
    ==== vlan active link ====
    namePtr   : ethernet0/3
    portType  : 3
    portIndex : 5
    ifId      : 93
```

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 Motorola 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 Motorola 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 Motorola 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.

view config

Dumps the Motorola Netopia® Gateway’s configuration just as the **view** command does in config mode.

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 Motorola Netopia® Gateway is currently using to acquire the IP settings for the specified DSL port. The ***vcc-id*** identifier is an “index” letter in the range B-I, and does not directly map to the VCC in use. Enter the **reset dhcp client release** command without the variable to see the letter assigned to each virtual circuit.

reset dhcp client renew [*vcc-id*]

Releases the DHCP lease the Motorola Netopia® Gateway is currently using to acquire the IP settings for the specified DSL port. The ***vcc-id*** identifier is an “index” letter in the range B-I, and does not directly map to the VCC in use. 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 Motorola Netopia® Gateway. The optional **all** argument displays a more detailed set of ATM statistics.

show dsl [all]

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.

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 Motorola 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 **`Netopia-3000/9437188 (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 **`Netopia-3000/9437188 (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.

```
Netopia-3000/9437188 (top)>> quit
Netopia-3000/9437188 >
```

- **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.

```
            Netopia-3000/9437188 (top)>> ip
            Netopia-3000/9437188 (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 b, you could enter one letter ("**b**") to move to the bridge 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 Motorola Netopia® Gateway.

Displaying Current Gateway Settings

You can use the ***view*** command to display the current CONFIG settings for your Motorola 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 Motorola 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:

```
Netopia-3000/9437188 (top)>> set system
...
system
   name (“Netopia-3000/9437188”): 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 Motorola Netopia® Gateway verifies that all required settings for all services are present and that settings are consistent.

```
Netopia-3000/9437188 (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 Motorola 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.

Remote ATA Configuration Commands

Motorola Netopia® firmware supports configuration of a maximum of four Motorola Netopia® ATA profiles, which are stored in the Gateway's configuration database. When a Motorola Netopia® ATA is discovered, the Gateway compares the MAC address of the ATA with one of the existing profiles stored in the database. If there is a match, the configuration is downloaded to the Motorola Netopia® ATA, and the ATA is restarted. Once the Motorola Netopia® ATA is restarted, it comes up with the newly downloaded configuration.

set ata profile [0... 3] ata-option [on l off]

Enables or disables the remote ATA configuration option for the specified ATA configuration profile to be stored in the Gateway.

set ata profile [0... 3] ata-mac-addr *MAC_addr*

Specifies the MAC address of the ATA for the specified configuration profile.

set ata profile [0... 3] ata-qos-enable [on l off]

Enables or disables QoS for the specified profile.

set ata profile [0... 3] ata-dhcpc-enable [on l off]

Enables or disables DHCP client service for the specified profile.

set ata profile [0... 3] ata-dhcpc-hostname *string*

Specifies a DHCP client hostname for the specified profile.

set ata profile [0... 3] ata-dhcpc-vid-enable [off l on]

Enables or disables a DHCP client vendor ID for the specified profile.

set ata profile [0... 3] ata-dhcpc-vid *string*

Specifies a vendor ID for the specified profile when **ata-dhcpc-vid-enable** is **on**.

set ata profile [0... 3] ata-static-wan-ip *ip_addr*

Specifies a static WAN IP address for the specified profile.

set ata profile [0... 3] ata-static-wan-subnet-mask *subnet_mask*

Specifies a static WAN IP subnet mask for the specified profile.

set ata profile [0... 3] ata-static-wan-gateway *ip_addr*

Specifies a static gateway WAN IP address for the specified profile.

set ata profile [0... 3] ata-proxy-server *ip_addr*

Specifies a SIP proxy server hostname or IP address for the specified profile.

set ata profile [0... 3] ata-proxy-port *port*

Specifies a SIP proxy server port, typically 5060, for the specified profile.

set ata profile [0... 3] ata-registrar-server *ip_addr*

Specifies a registrar server hostname or IP address for the specified profile.

set ata profile [0... 3] ata-registrar-port *port*

Specifies a registrar server port, typically 5060, for the specified profile.

set ata profile [0... 3] ata-outproxy-server *ip_addr*

Specifies an outbound proxy server hostname or IP address for the specified profile.

set ata profile [0... 3] ata-outproxy-port *port*

Specifies an outbound proxy server port, typically 5060, for the specified profile.

set ata profile [0... 3] ata-auth-id *value*

Specifies an authorization ID for the specified profile.

set ata profile [0... 3] ata-user-name *string*

Specifies the ISP-supplied user name for the specified profile.

set ata profile [0... 3] ata-user-display-name *string*

Specifies the a user “display” or “screen” name for the specified profile.

set ata profile [0... 3] ata-user-password *string*

Specifies the user password for the specified profile.

DSL Commands

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

set atm option {on I off }

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

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

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

set atm [vcc *n*] qos service-class { cbr I ubr I 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 l ppp-llc l ether-llc l ip-llc l ppoe-vcmux l 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 Motorola Netopia® Gateway use MAC (Ethernet hardware) addresses to forward non-TCP/IP traffic from one network to another. When bridging is enabled, the Motorola 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 3341 (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 I off }

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

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

Enables or disables Concurrent Bridging/Routing.

set bridge dhcp-filterset "*string*"

Assigns a filterset named ***string*** to the bridge configuration.

NOTE:

A filterset can only be configured for the bridge if the system bridge or concurrent bridging/routing is enabled.

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 (.5–100 mins).

DHCP Settings

As a Dynamic Host Control Protocol (DHCP) server, your Motorola 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 Motorola Netopia® Gateway can use the information for a fixed period of time (called the DHCP lease).

Common Commands

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

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

If you turn off DHCP services and save the new configuration, the Motorola 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 Motorola 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 Motorola Netopia® Gateway. Enter lease time in **`dd:hh:mm:ss`** (day/hour/minute/second) format.

set dhcp option-group *name*

Specifies a name for one of up to eight DHCP Option Groups. Each Option Group can have a name of between 1 and 15 characters. The name is used in the DHCP filterset syntax to choose what group of gen-options is to be served to a particular DHCP Client. See "DHCP Generic Options" on page 200 and "DHCP Option Filtering" on page 204.

Option Groups refer to *gen-options*; they do not contain them. Deleting a gen-option from an option group does not delete the option. Adding a gen-option to an option-group does not preclude it from being added to another option-group.

set dhcp default-option-group *name*

Sets the option group specified by ***name*** as the default.

set dhcp server-address *ip_address*

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

set dhcp range [2... 8] start-address *ip_address*

Specifies the starting IP address of DHCP range ***n*** when **subnet *n* option** is **on**. See "Additional subnets" on page 220.

set dhcp range [2... 8] end-address *ip_address*

Specifies the ending IP address of DHCP range ***n*** when **subnet *n* option** is **on**. See "Additional subnets" on page 220.

set dhcp reserved ip-address *x.x.x.x* mac-address *y-y-y-y-y-y*

If you selected **`server`**, reserves the specified IP address from the DHCP pool to the specified MAC address. These are list items; a total of 16 reserved addresses are supported. Secondary ranges will all make use of the **`dhcp lease-time`** value.

DHCP Generic Options

You can specify DHCP Generic Options which allow you to configure the content to be served for particular option numbers.

set dhcp gen-option name *name*

Specifies a DHCP generic option set named *name* of one to 15 characters. You can specify up to 20 **gen-option**s. Each can contain up to 100 bytes of data, up to a maximum of 912 bytes of options data total. An option will be served only if the client requests it.

set dhcp gen-option option [1 – 255]

Specifies the DHCP option by number, 1 – 255. The following table shows the formats and sizes for known options, and whether or not you can configure a **gen-option** of that type.

Option	Data Format	Data Size (bytes)	Can Configure
0	Empty	0	No
1	IP mask	4	Yes
2	Unsigned 4 byte integer	4	Yes
3 - 11	IP address list	Multiples of 4	Yes
12	String (up to 100 characters)	N	Yes
13	Unsigned 2 byte integer	2	Yes
14 - 15	String (up to 100 characters)	N	Yes
16	Unsigned 4 byte integer	4	Yes
17	String (up to 100 characters)	N	Yes
18	String (up to 100 characters)	N	Yes
19 - 20	Flag	1	Yes
21	IP address & mask list	Multiples of 8	Yes
22	Unsigned 2 byte integer	2	Yes
23	Unsigned 1 byte integer	1	Yes
24	Unsigned 4 byte integer	4	Yes
25	Unsigned 2 byte integer list	Multiples of 2	Yes
26	Unsigned 2 byte integer	2	Yes
27	Flag	1	Yes

Option	Data Format	Data Size (bytes)	Can Configure
28	IP address	4	Yes
29 - 31	Flag	1	Yes
32	IP address	4	Yes
33	IP address and mask list	Multiples of 8	Yes
34	Flag	1	Yes
35	Unsigned 4 byte integer	4	Yes
36	Flag	1	Yes
37	Unsigned 1 byte integer	1	Yes
38	Unsigned 4 byte integer	4	Yes
39	Flag	1	Yes
40	String (up to 100 characters)	N	Yes
41 - 42	IP address list	Multiples of 4	Yes
43	Vendor-specific	String	Yes
44 - 45	IP address list	Multiples of 4	Yes
46	Unsigned 1 byte integer	1	Yes
47	String (up to 100 characters)	N	Yes
48 - 49	IP address list	Multiples of 4	Yes
50	IP address	4	No
51	Unsigned 4 byte integer	4	No
52	Unsigned 1 byte integer	1	No
53	Unsigned 1 byte integer	1	Yes
54	IP address	4	Yes
55	String (up to 100 characters)	N	No
56	String (up to 100 characters)	N	Yes
57	Unsigned 2 byte integer	2	Yes
58 - 59	Unsigned 4 byte integer	4	No
60	String (up to 100 characters)	N	Yes
61	String (up to 100 characters)	N	No
62	String (up to 100 characters)	N	Yes
63	Complex	N	No

Option	Data Format	Data Size (bytes)	Can Configure
64	String (up to 100 characters)	N	Yes
65	IP address list	Multiples of 4	Yes
66 - 67	String (up to 100 characters)	N	Yes
68 - 76	IP address list	Multiples of 4	Yes
77	Pascal string list (length byte + data)	N	Yes
78 - 79	Complex	N	No
80	Empty	0	No
81	Complex	N	No
82	Sub-option list	N	Yes
83	Complex	N	No
84	Undefined	??	Yes
85	IP address list	Multiples of 4	Yes
86 - 87	Unicode String	Multiples of 2	Yes
88	Encoded DN list	N	Yes
89	IP address list	Multiples of 4	Yes
90	Complex	N	No
91 - 97	Undefined/Weakly defined	??	Yes
98	String (up to 100 characters)	N	Yes
99 - 115	Undefined/Weakly defined	??	Yes
116	Flag	1	Yes
117	Unsigned 2 byte integer list	Multiples of 2	Yes
118	IP address	4	Yes
119	Encoded DN list 2	N	Yes
120	Encoded DN list or IP Address list	N	Yes
121 - 125	Complex	N	No
126 - 127	Undefined	N	Yes
128	IP address list	Multiples of 4	Yes
129 - 223	Undefined/Weakly defined	??	Yes
224 - 254	Private Use	N	Yes

Option	Data Format	Data Size (bytes)	Can Configure
249 (note)	Microsoft uses this instead of 121	N	Yes
255	Empty	0	No

set dhcp gen-option data-type [ascii | hex | dotted-decimal]

Specifies the DHCP gen-option data type: **ascii**, **hex** or **dotted-decimal**.

set dhcp gen-option data *data*

Specifies the **gen-option** data.

- If the **data-type** is **ascii**, then any printable character + octal representations (e.g.”\0007”) and hex representations (e.g. “\xA4”).
- If the **data-type** is **hex**, then an even number of hex characters (e.g. “0123456789AbcdEf”
- If the **data-type** is **dotted-decimal**, then a series of numbers between 0 and 255, separated by a period (.). IP addresses are generally represented in this form.

DHCP Option Filtering

Beginning with Firmware Version 7.7, support for DHCP option filtering is provided via the filterset settings.

set dhcp filterset name "*string*" rule *n* type [dhcp-option | hw-address | requested-option]

Specifies a DHCP filterset named string as one of three possible types:

The rule can either specify an option and option contents, **dhcp-option**; a client hardware address range, **hw-address**; or an option the client is requesting, **requested-option**. For **hw-address**, you will need to enter **start-address** and **end-address** values; for the others a **dhcp-option** parameter must be set.

By default a rule is of type **dhcp-option**, for backwards compatibility.

set dhcp filterset name "*string*" rule *n* dhcp-option [0... 255]

Creates a DHCP filterset named ***string***, for example “settopbox,” with rule number ***n***.

Up to two filtersets can be added. Your Gateway supports a single LAN DHCP server instance, but an additional filterset is available for use when bridging, to block undesired DHCP traffic. Up to 8 **rules** can be created in the filterset, which are evaluated in order.

dhcp-option determines which DHCP option should be compared. A typical value would be to use option 60 data for comparison, but allowing this value to be configured permits more flexibility.

```
set dhcp filterset name "settopbox" rule 1 type dhcp-option
```

set dhcp filterset name "*string*" rule *n* match-action [pass | discard | continue]

Assigns a match action to the filterset. If set to **pass** the **match-pool** address is shown.

set dhcp filterset name "*string*" rule *n* absent-action

[pass l discard l continue]

Assigns an absent action to the filterset. If set to **pass** the **absent-pool** address is hidden.

set dhcp filterset name "*string*" rule *n* match-option-group "*option_group*"

Assigns the option group named ***option_group*** to match.

set dhcp filterset name "*string*" rule *n* match-str "*match_string*"

Assigns a match string to the filterset. The **match-str** string will be compared against the DHCP DISCOVER option data. This string can contain multiple "*" and "?" wildcard substitutions.

set dhcp filterset name "*string*" rule *n* match-pool *ip_address*

Specifies the start IP address of the range within a DHCP pool where that range will be used to allocate an address if the wildcard matches.

The value 0.0.0.0 means regular processing; 255.255.255.255 means discard.

set dhcp filterset name "*string*" rule *n* absent-pool *ip_address*

Specifies the start IP address of the range within a DHCP pool where that range will be used to allocate an address if the option in the DHCP packet is not present.

The value 0.0.0.0 means regular processing; 255.255.255.255 means discard.

Example

```
Netopia-3000/9450000 (dhcp)>> sc
set dhcp option server
set dhcp start-address 192.168.1.33
set dhcp end-address 192.168.1.63
set dhcp lease-time 01:00:00:00
set dhcp filterset name "settopbox" rule 1 dhcp-option 60
set dhcp filterset name "settopbox" rule 1 match-str "STB*"
set dhcp filterset name "settopbox" rule 1 match-pool
```

```
192.168.6.100
set dhcp filterset name "settopbox" rule 1 absent-pool
0.0.0.0
Netopia-3000/9450000 (dhcp)>>
```

set dhcp assigned-filterset "*string*"

Assigns the filterset named ***string*** created above to the DHCP configuration.

DMT Settings

DSL Commands

set dmt dsl-annex-support [off | on]

This controls whether other annex support (just as Annex M) is enabled. Default is **off**.

set dmt type [lite | dmt | ansi | multi | adsl2 | adsl2+ | readsl2 | adsl2anxm | adsl2+anxm]

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

The **type** value also supports the following settings on certain model units: **adsl2**, **adsl2+**, **readsl2**, **adsl2anxm**, **adsl2+anxm**.

NOTE:

Some **dmt type** settings are now supported for many Annex B (335x***N***) platforms. 2200 Series and 33xx**N** Series models are supported. Currently, **adsl2anxm** and **adsl2+anxm** are not supported in Annex B.

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 dmt dying-gasp [default | off | on]

Enables or disables Gateway “dying gasp” behavior in cases of power failure. Default is **off**.

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.

set dmt metallic-termination [auto | disabled | always_on]

(not supported on all models) This command allows you to apply a sealing current to “dry” DSL lines so that the wiring doesn’t corrode.

- **auto** - The device will scan for standard telephone service (POTS). If it finds POTS, it disables metallic termination. If it does not find POTS during the search period, then metallic termination is enabled.
- **disabled** - There is no POTS detection, and metallic termination is disabled.
- **always_on** - The device will scan for POTS for information only. Metallic termination is always enabled.

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.

set dns configured-dns-priority [0 - 255]

Sets the configured DNS priority relative to acquired DNS. These server addresses may be acquired via DHCP (client), PPP, or statically configured. A “DNS learned-server-priority” is assigned to each configured interface. By default, configured DNSes have the highest priority (lowest number), then PPP-acquired DNSes, and DHCP-acquired DNSes have lowest priority (highest number).

The default priorities for each type are:

- Configured DNSes: 10
- PPP-acquired: 20
- DHCP-acquired: 30

Dynamic DNS Settings

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

Multicasting is a method for transmitting large amounts of information to many, but not all, computers over an internet. One common use is to distribute real time voice, video, and data services to the set of computers which have joined a distributed conference. Other uses include updating the address books of mobile computer users in the field, or sending out company newsletters to a distribution list.

Since a router should not be used as a passive forwarding device, Motorola Netopia® Gateways use a protocol for forwarding multicasting: Internet Group Management Protocol (IGMP).

Motorola Netopia® Gateways support IGMP Version 1, Version 2, or, beginning with Motorola Netopia® Firmware Version 7.7, Version 3.

IGMP “Snooping” is a feature of Ethernet layer 2 switches that “listens in” on the IGMP conversation between computers and multicast routers. Through this process, it builds a database of where the multicast routers reside by noting IGMP general queries used in the querier selection process and by listening to other router protocols.

From the host point of view, the snooping function listens at a port level for an IGMP report. The switch then processes the IGMP report and starts forwarding the relevant multicast stream onto the host's port. When the switch receives an IGMP *leave* message, it processes the leave message, and if appropriate stops the multicast stream to that particular port. Basically, customer IGMP messages although processed by the switch are also sent to the multicast routers.

In order for IGMP snooping to function with IGMP Version 3, it must always track the full source filter state of each host on each group, as was previously done with Version 2 only when *Fast Leave* support was enabled.

IGMP Version 3 supports:

IGMP Source Filtering: the ability for group memberships to incorporate source address filtering. This allows “Source-Specific Multicast” (SSM). By adding source filtering, a Gateway that proxies IGMP can more selectively join the specific multicast group for which there are interested LAN multicast receivers.

These features require no user configuration on the Gateway.

You can set the following options:

- **IGMP Snooping** – enables the Motorola 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.
- **Robustness** – 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.
- **Query Interval**– the amount of time in seconds between IGMP General Query messages sent by the querier gateway. The default query interval is 125 seconds.
- **Query Response Interval** – the maximum amount of time in tenths of a second that the IGMP router waits to receive a response to a General Query message. The default query response interval is 10 seconds and must be less than the query interval.
- **Unsolicited Report Interval** – the amount of time in seconds between repetitions of a particular computer's initial report of membership in a group. The default unsolicited report interval is 10 seconds.
- **Querier Version** – select a version of the IGMP Querier: version **1**, version **2**, or version **3**. If you know you will be communicating with other hosts that are limited to v1 or v2, for backward compatibility, select accordingly; otherwise, allow the default v3.

NOTE:

IGMP Querier version is relevant only if the router is configured for IGMP forwarding. If any IGMP v1 routers are present on the subnet, the querier **must** use IGMP v1. The use of IGMP v1 must be administratively configured, since there is no reliable way of dynamically determining whether IGMP v1 routers are present on a network. IGMP forwarding is enabled per IP Profile and WAN Connection Profile.

- **Last Member Query Interval** – the amount of time in tenths of a second that the IGMP gateway waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 1 second (10 deciseconds).
- **Last Member Query Count** – the number of Group-Specific Query messages sent before the gateway assumes that there are no members of the host group being queried on this interface. The default last member query count is 2.
- **Fast Leave** – set to **off** by default, fast leave enables a non-standard expedited leave mechanism. The querier keeps track of which client is requesting which channel by IP

address. When a leave message is received, the querier can check its internal table to see if there are any more clients on this group. If there are none, it immediately sends an IGMP leave message to the upstream querier.

- **Log Enable** – If set to on, all IGMP messages on both the LAN and the WAN will be logged.
- **Wireless Multicast to Unicast conversion** – Only available if **IGMP Snooping** is enabled. If set to **on**, the Gateway replaces the multicast MAC-address with the physical MAC-address of the wireless client. If there is more than one wireless client interested in the same multicast group, the router will revert to multicasting the stream immediately. When one or more wireless clients leave a group, and the router determines that only a single wireless client is interested in the stream, it will once again unicast the stream.

set igmp snooping [off I on]

Enables IGMP Snooping.

set igmp robustness *value*

Sets IGMP robustness range: from 2 – 255. The default 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.

set igmp unsol-report-intvl *value*

Sets the unsolicited report interval: the amount of time in seconds between repetitions of a particular computer’s initial report of membership in a group. The default is 10 seconds.

set igmp version [1 | 2 | 3]

Sets the IGMP querier version: version **1**, version **2**, or version **3**. If you know you will be communicating with other hosts that are limited to v1, for backward compatibility, select **1**; otherwise, allow the default **3**.

set igmp last-member-query-intvl *value*

Sets the last member query interval: the amount of time in tenths of a second that the IGMP gateway waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default is 1 second (10 deci-seconds).

set igmp last-member-query-count *value*

Sets the last member query count: the number of Group-Specific Query messages sent before the gateway assumes that there are no members of the host group being queried on this interface. The default is 2.

set igmp fast-leave [off | on]

Sets fast leave on or off. Set to **off** by default, fast leave enables a non-standard expedited leave mechanism. The querier keeps track of which client is requesting which channel by IP address. When a leave message is received, the querier can check its internal table to see if there are any more clients on this group. If there are none, it immediately sends an IGMP leave message to the upstream querier.

set igmp wireless-m2u [on | off]

This command allows you enable or disable wireless multicast-to-unicast if **igmp snooping** is set to **on**.

set igmp log-enable [on | off]

If set to **on**, all IGMP messages on both the LAN and the WAN will be logged. Default is **off**.

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 Motorola 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 l off }

Enables or disables TCP/IP services in the Motorola Netopia® Gateway. You must enable TCP/IP services before you can enter other TCP/IP settings for the Motorola Netopia® Gateway. If you turn off TCP/IP services and save the new configuration, the Motorola 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* restrictions { admin-disabled | none }

Specifies restrictions on the types of traffic the Motorola 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 Motorola 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 auto-sensing [off | dhcp/pppoe | pppoe/pppoa]

Enables or disables DHCP/PPPoE or PPPoE/PPPoA autosensing on the specified interface. Setting this to **DHCP/PPPoE** enables automatic sensing of your WAN connection type: PPPoE or DHCP. The gateway attempts to connect using PPPoE first. If the Gateway fails to connect after 60 seconds, it switches to DHCP. As soon as it can connect via DHCP, the Gateway chooses and sets DHCP as its default. Otherwise, after attempting to connect via DHCP for 60 seconds, the Gateway switches back to PPPoE. The Gateway will continue to switch back and forth in this manner until it successfully connects. Similarly, selecting

PPPoE/PPPoA causes the Gateway to attempt to connect by trying these protocols in parallel, and using the first one that is successful.

set ip dsl vccn mcast-fwd [on I off }

Enables or disables multi-cast forwarding on the specified interface. If set to **on**, this interface acts as an IGMP proxy host, and IGMP packets are transmitted and received on this interface on behalf of IGMP hosts on the LAN interface.

set ip dsl vccn igmp-null-source-addr { on I off }

Specifies whether you want the Motorola Netopia® Gateway to identify the source IP address of every IGMP packet transmitted from this interface as 0.0.0.0 when **mcast-fwd** is set to **on**. This complies with the requirements of TR-101, and removes the need for a publicly advertised IP address on the WAN interface.

set ip dsl vccn unnumbered [on I off }

Specifies whether you want the Motorola Netopia® Gateway to have its WAN interface unnumbered, i.e. set to 0. **unnumbered** option is only available if the address is set to 0 for the interface. Enables or disables unnumbered IP addressing (where an address of 0 is allowed AND the DHCP client is disabled) on the specified interface. This setting applies to native IP as well as PPP interfaces to support running an IPoE interface without an address.

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

Specifies whether the Motorola 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 Motorola 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 Motorola 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 A 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 Motorola 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 Motorola Netopia® Gateway uses 192.168.0.1 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 restrictions { none l admin-disabled }

Specifies whether an administrator can open a telnet connection to a Motorola Netopia® Gateway over an Ethernet interface (**A** = the LAN) 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 l v1 l v2 l v1-compat l v2-MD5 }

Specifies whether the Motorola 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 Motorola 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 Motorola 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.

Additional subnets

See “DHCP Settings” on page 198 for subnet range configuration commands.

set ip ethernet A subnet [2 ... 8] option [on | off]

Enables or disables additional LAN subnets. Up to seven additional subnets may be configured.

set ip ethernet A subnet *n* address *ip_address*

Specifies an IP address for the subnet ***n***, when **subnet *n* option** is **on**.

set ip ethernet A subnet *n* netmask *netmask*

Specifies the subnet mask for the subnet ***n***, when **subnet *n* option** is **on**.

Default IP Gateway Settings

set ip gateway option { on | off }

Specifies whether the Motorola 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 Motorola 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 Motorola 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 | 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 Motorola 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 Motorola 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 Motorola 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 Motorola 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*] restrictions { admin-disabled | none }

Specifies restrictions on the types of traffic the Motorola 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. RIP and ICMP traffic is still accepted. The **none** argument means that all traffic is accepted.

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

Specifies whether you want the Motorola 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 ip-ppp [*vccn*] auto-sensing [off | dhcp/pppoe | pppoe/pppoa]

Enables or disables DHCP/PPPoE or PPPoE/PPPoA autosensing on the specified interface. Setting this to **DHCP/PPPoE** enables automatic sensing of your WAN connection type: PPPoE or DHCP. The gateway attempts to connect using PPPoE first. If the Gateway fails to connect after 60 seconds, it switches to DHCP. As soon as it can connect via DHCP, the Gateway chooses and sets DHCP as its default. Otherwise, after attempting to connect via DHCP for 60 seconds, the Gateway switches back to PPPoE. The Gateway will continue to switch back and forth in this manner until it successfully connects. Similarly, selecting **PPPoE/PPPoA** causes the Gateway to attempt to connect by trying these protocols in parallel, and using the first one that is successful.

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

Specifies whether the Motorola 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 Motorola 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.

set ip ip-ppp vcc*n* igmp-null-source-addr [on | off]

Specifies whether you want the Motorola Netopia® Gateway to identify the source IP address of every IGMP packet transmitted from this interface as 0.0.0.0 when **mcast-fwd** is set to **on**. This complies with the requirements of TR-101, and removes the need for a publicly advertised IP address on the WAN interface.

set ip ip-ppp vcc*n* mcast-fwd [on | off]

Specifies whether you want the Motorola Netopia® Gateway interface to act as an IGMP proxy host.

set ip ip-ppp vcc*n* unnumbered [on | off]

Specifies whether you want the Motorola Netopia® Gateway to have its WAN interface unnumbered, i.e. set to 0.

set ip ip-ppp vcc*n* dns acquired-dns-priority [0 - 255]

Sets the priority for DNS acquired via PPP. See “Domain Name System Settings” on page 208 for more information.

Static ARP Settings

Your Motorola Netopia® Gateway maintains a dynamic Address Resolution Protocol (ARP) table to map IP addresses to Ethernet (MAC) addresses. Your Motorola 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 Motorola Netopia® Gateway. Use the following commands to add static ARP entries to the Motorola 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 I on]

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

IPsec Passthrough

set ip ipsec-passthrough [off I 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)

set diffserv option [off I 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.

NOTE:

diffserv lohi-ratio has been removed for VDSL, ADSL bonded units.

set diffserv custom-flows name *name*
protocol [TCP | UDP | ICMP | other]
direction [outbound | inbound | both]
start-port [0 - 65535]
end-port [0 - 65535]
inside-ip *inside-ip-addr*
inside-ip-mask *inside-ip-netmask*
outside-ip *outside-ip-addr*
outside-ip-mask *outside-ip-netmask*
qos [off | assure | expedite | network-control]

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/mask** – If you want packets originating from a certain LAN IP address to be marked, enter the IP address and subnet mask 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/mask** – If you want packets destined for and originating from a certain WAN IP address to be marked, enter this address and subnet mask 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.

  Note:
  When setting the Inside/Outside IP Address/Netmask settings, note that a netmask value can be used to configure for a network rather than a single IP address.

- **qos** – Allows you to specify the Quality of Service for the flow: **off**, **assure**, **expedite** or **network-control**. 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.

QoS Setting	TOS Bit Value	Behavior
Off	TOS=000	This custom flow is disabled. You can activate it by selecting one of the two settings below. This setting allows you to pre-define flows without actually activating them.
Assure	TOS=001	Use normal queuing and throughput rules, but do not drop packets if possible. Appropriate for applications with no guaranteed delivery mechanism.
Expedite	TOS=101	Use minimum delay. Appropriate for VoIP and video applications.
Network Control	TOS=111	Use highest possible priority.

Packet Mapping Configuration

set diffserv qos [network-control-queue I expedite-queue I assured-queue I best-effort-queue] *queue_name*

Specifies the Diffserv QoS queue mapping associations.

- ***queue_name*** - the basic queue name to which classified packets are directed.

By default the following mappings are created:

```
set diffserv qos network-control-queue basic_q0
set diffserv qos expedite-queue basic_q1
set diffserv qos assured-queue basic_q2
set diffserv qos best-effort-queue basic_q3
```

set diffserv qos dscp-map [default I custom]

- **default** – the default DSCP-queue mappings are used
- **custom** – allows you to set up customized mappings between DSCP code points and queue types.

If **custom** is selected, the following can be configured:

set diffserv qos dscp-map-0 [best-effort I assured I expedite I network-control]

set diffserv qos dscp-map-1
[best-effort | assured | expedite | network-control]
...
set diffserv qos dscp-map-31
[best-effort | assured | expedite | network-control]

By default, the following settings are used in custom mode:

```
set diffserv qos dscp-map-0 best-effort
set diffserv qos dscp-map-1 best-effort
set diffserv qos dscp-map-2 best-effort
set diffserv qos dscp-map-3 best-effort
set diffserv qos dscp-map-4 best-effort
set diffserv qos dscp-map-5 assured
set diffserv qos dscp-map-6 best-effort
set diffserv qos dscp-map-7 best-effort
set diffserv qos dscp-map-8 best-effort
set diffserv qos dscp-map-9 assured
set diffserv qos dscp-map-10 best-effort
set diffserv qos dscp-map-11 best-effort
set diffserv qos dscp-map-12 best-effort
set diffserv qos dscp-map-13 assured
set diffserv qos dscp-map-14 best-effort
set diffserv qos dscp-map-15 best-effort
set diffserv qos dscp-map-16 best-effort
set diffserv qos dscp-map-17 assured
set diffserv qos dscp-map-18 best-effort
set diffserv qos dscp-map-19 best-effort
set diffserv qos dscp-map-20 best-effort
set diffserv qos dscp-map-21 best-effort
set diffserv qos dscp-map-22 best-effort
set diffserv qos dscp-map-23 expedite
set diffserv qos dscp-map-24 network-control
set diffserv qos dscp-map-25 network-control
set diffserv qos dscp-map-26 network-control
set diffserv qos dscp-map-27 network-control
set diffserv qos dscp-map-28 network-control
set diffserv qos dscp-map-29 network-control
set diffserv qos dscp-map-30 network-control
set diffserv qos dscp-map-31 network-control
```

Queue Configuration

Beginning with Firmware Version 7.7.4, the queuing characteristics of all “N” and “-02” model Gateway’s WAN interface can now be configured for:

- strict priority queuing (as currently)
- weighted fair queuing
- rate-limiting funnel

Note:

The configuration mechanism is designed to be flexible enough to accommodate complex queuing requirements. Configurations not supported by the Gateway will be flagged during configuration verification.

You configure the WAN outbound queue as follows:

- create and configure one or more queues, which can be a basic queue or a priority queue comprising a group of basic queues, a weighted fair queue comprising a group of basic queues, or a funnel comprising a group of basic queues;
- assign a queue instance to the Ethernet WAN interface;
- map packet attributes to a queue.

The same queue name can be assigned to multiple interfaces which require identical queue configuration, however currently the only interface available for queueing configuration is ethernet 1.

To help you configure queues, and to maintain compatibility with previous firmware releases, several queues are set up automatically on upgrade to Version 7.7, or upon a factory reset.

set queue name *queue_name* option [on l off] type [basic l wfq l priority l funnel]

Creates a queue named ***queue_name*** and assigns a **type**:

- **basic** – Basic Queue
- **wfq** – Weighted Fair Queue
- **priority** – Priority Queue
- **funnel** – Funnel Queue

Basic Queue

set queue name *basic_queue_name* option [on l off]
set queue name *basic_queue_name* type basic

Specifies the Basic Queue named ***basic_queue_name*** attributes. Basic queues have one input and one output. The basic queue is assigned an ID, with the following attribute: when the queue is full, discard.

By default, the following Basic Queues are created:

- basic_q0
- basic_q1
- basic_q2
- basic_q3

Weighted Fair Queue

set queue name wfq option [on l off]
set queue name *wf_queue_name* type wfq
set queue name *wf_queue_name* weight-type [relative l bps]
set queue name *wf_queue_name* entry *n* input input_queue_name
set queue name *wf_queue_name* entry *n* weight *weight*
set queue name *wf_queue_name* entry *n* share-bw [on l off]
set queue name *wf_queue_name* entry *n* default-input *queue_name*

Specifies the attributes of the Weighted Fair Queue named ***wf_queue_name***.

- ***wf_queue_name*** – name of weighted fair queue

A weighted fair queue can contain up to 8 input queues. For each input queue, the following is configured:

- **weight-type** – the weighted fair queue configuration allows you to set the rate in bits per second (**bps**) or percentage of the line rate (**relative**). **bps** is the default.
- ***n*** – entry number for this input queue
- ***input_queue_name*** – name of input queue
- ***weight_value*** – numeric relative weight of queue
- **share-bw** – if enabled, the bandwidth for this queue can be shared between other queues when idle.
- **default-input** – specifies the default input queue name.

The default special queuing configuration shapes the rate of a custom flow toward the Remote Management Server.

By default, the following WFQ is created:

```
set queue name "wfq" option on
set queue name "wfq" type wfq
set queue name "wfq" weight-type bps
set queue name "wfq" entry 1 input "basic_q0"
set queue name "wfq" entry 1 weight 10000
set queue name "wfq" entry 1 share-bw off
set queue name "wfq" entry 2 input "basic_q1"
set queue name "wfq" entry 2 weight 20000
set queue name "wfq" entry 2 share-bw off
set queue name "wfq" entry 3 input "basic_q2"
set queue name "wfq" entry 3 weight 30000
set queue name "wfq" entry 3 share-bw off
set queue name "wfq" entry 4 input "basic_q3"
set queue name "wfq" entry 4 weight 40000
set queue name "wfq" entry 4 share-bw off
set queue name "wfq" default-input "basic_q0"
```

Priority Queue

set queue name *priority_queue_name* option [off I on]
set queue name *priority_queue_name* type priority
set queue name *priority_queue_name* default-input *queue_name*

A priority queue can contain up to 8 input queues. For each input queue, the following is configured:

set queue name *priority_queue_name* entry *n* input *input_queue_name*
set queue name *priority_queue_name* entry *n* priority *priority_value*

Specifies the Priority Queue named ***priority_queue_name*** attributes.

- ***priority_queue_name*** – name of priority queue
- ***input_queue_name*** – name of input queue
- ***priority_value*** – numeric relative priority of queue. The higher the number, the higher the priority of the queue.
- **default-input** – specifies the default input queue name.

By default, the following priority queue is created:

```
set queue name "pq" option on
set queue name "pq" type priority
set queue name "pq" entry 1 input "basic_q0"
set queue name "pq" entry 1 priority 10
set queue name "pq" entry 2 input "basic_q1"
set queue name "pq" entry 2 priority 20
set queue name "pq" entry 3 input "basic_q2"
set queue name "pq" entry 3 priority 30
set queue name "pq" entry 4 input "basic_q3"
set queue name "pq" entry 4 priority 40
set queue name "pq" default-input "basic_q0"
```

Funnel Queue

A funnel queue is used to limit the rate of the transmission below the actual line rate:

set queue name *funnel_queue_name* option [on | off]
set queue name *funnel_queue_name* type funnel
set queue name *funnel_queue_name* input *input_queue_name*
set queue name *funnel_queue_name* bps *bps*

Specifies the Funnel Queue named ***funnel_queue_name*** attributes.

- ***funnel_queue_name*** – name of funnel queue
- ***input_queue_name*** – name of input queue
- ***bps*** – max bits per second permitted through funnel queue

By default, the following funnel queues are created:

Rate-limiting priority queue to 100Kbps:

```
set queue name pq-100kbps option on
set queue name pq-100kbps type funnel
set queue name pq-100kbps input pq
set queue name pq-100kbps bps 100000
```

Rate-limiting weighted fair queue to 100Kbps:

```
set queue name wfq-100kbps option on
set queue name wfq-100kbps type funnel
set queue name wfq-100kbps input wfq
set queue name wfq-100kbps bps 100000
```

Interface Queue Assignment

The WAN ethernet queue is assigned as follows:

set [ethernet ethernet | ip ethernet B | ip-ppp vcc*n*] tx-queue *queue_name*

By default, the WAN ethernet interface is assigned the default priority queue:

```
set ethernet ethernet B tx-queue pq
```

Other interfaces may likewise be assigned **tx-queue** values.

SIP Passthrough

set ip sip-passthrough [on I 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.

RTSP Passthrough

set ip ethernet B rtsp-passthrough [off I on]

Turns Real Time Streaming Protocol application layer gateway client passthrough **on** or **off**. RTSP is a protocol used for streaming media. It allows a client remotely to control a streaming media server. A typical application is Video-on-Demand (VoD). The default is **on**.

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 Motorola Netopia® Gateway. Use the following commands to maintain static routes to the Motorola 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 Motorola 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 l always l 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 Motorola 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 Motorola Netopia® Gateway should be directed to a specific hosts.

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

Specifies whether you want your Motorola 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*

Specifies the IP address of the NAT default server.

set nat-default host-hardware-address *MAC_address* }

Specifies the hardware (MAC) address of the IP passthrough host. If the MAC address is specified as all-zeroes, the first DHCP client that requests an IP address gets the passthrough address.

Network Address Translation (NAT) Pinhole Settings

NAT pinholes let you pass specific types of network traffic through the NAT interfaces on the Motorola 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 Motorola 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 l 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 [0 - 65535]

Specifies the port number your Motorola 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 Motorola 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 l off }

Enables or disables PPP on the Motorola Netopia® Gateway.

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

Enables or disables LCP magic number negotiation.

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

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

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

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

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

Specifies the number of seconds the Motorola 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 Motorola 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 Motorola Netopia® Gateway will send. The integer argument can be any number between 1 and 20.

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

Specifies the maximum number of unacknowledged termination requests that your Motorola 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 Motorola 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 I always-on }

Specifies whether a PPP connection is maintained by the Motorola Netopia® Gateway when it is unused for extended periods. If you specify **`always-on`**, the Motorola Netopia® Gateway never shuts down the PPP link. If you specify **`instant-on`**, the Motorola 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 Motorola 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 Motorola Netopia® Gateway should respond when it receives an authentication request from a remote peer.

The settings for port authentication on the local Motorola 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 Motorola Netopia® Gateway, you must enable CHAP and specify the same name and secret on the Motorola Netopia® Gateway before the link can be established.

set ppp module [vccn] port-authentication option [off I on I pap-only I 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 – 128 alphanumeric characters. The information you enter must match the password used by the PPP peer.

PPPoE with IPoE Settings

Ethernet WAN platforms

set wan-over-ether pppoe [on | off]

Enables or disables PPPoE on the Ethernet WAN interface.

set wan-over-ether pppoe-with-ipoe [on | off]

Enables or disables the PPPoE with IPoE support on Ethernet WAN, including VDSL, platforms when **pppoe option** is set to **on**.

When **pppoe-with-ipoe** is set to **on**, an additional interface, "ethernet C," becomes available.

set wan-over-ether ipoe-sessions [1 - 4]

Sets the number of IPoE sessions, up to four, on Ethernet WAN, including VDSL, platforms.

NOTE:

Enabling pppoe-with-ipoe disables support for multiple PPPoE sessions.

Example:

```
set ip ethernet C option on
set ip ethernet C address 0.0.0.0
set ip ethernet C broadcast 0.0.0.255
set ip ethernet C netmask 255.255.255.0
set ip ethernet C restrictions admin-disabled
set ip ethernet C addr-mapping on
set ip ethernet C dns acquired-dns-priority 20
set ip ethernet C mcast-fwd on
set ip ethernet C igmp-null-source-addr off
set ip ethernet C tx-queue "none"
set ip ethernet C unnumbered off
set ip ethernet C rip-receive off
set ip ethernet C proxy-arp off
set ip ip-ppp enet-B option on
set ip ip-ppp enet-B address 0.0.0.0
set ip ip-ppp enet-B peer-address 0.0.0.0
set ip ip-ppp enet-B restrictions admin-disabled
set ip ip-ppp enet-B addr-mapping on
set ip ip-ppp enet-B dns acquired-dns-priority 20
set ip ip-ppp enet-B igmp-null-source-addr off
set ip ip-ppp enet-B tx-queue "none"
set ip ip-ppp enet-B mcast-fwd on
set ip ip-ppp enet-B unnumbered off
set ip ip-ppp enet-B rip-receive off
```

ADSL platforms

You must configure two VCCs with the *same* VPI/VCI to enable concurrent PPPoE and IPoE support, and you will need to configure the individual settings for each interface for proper operation.

set atm vcc *n* encap pppoe-llc

Specifies that the VCC will allow a second VCC with the same VPI/VCI values as the first. **pppoe-llc** denotes this special case.

Example:

```
set atm option on
set atm vcc 1 option on
set atm vcc 1 vpi 0
set atm vcc 1 vci 35
set atm vcc 1 encap pppoe-llc
set atm vcc 2 option on
set atm vcc 2 vpi 0
set atm vcc 2 vci 35
set atm vcc 2 encap ether-llc
```

This will allow you to configure the second WAN interface.

```
set atm vcc 2 vpi 0
set atm vcc 2 vci 35
set atm vcc 2 encap ether-llc
...
```

set ip ip-ppp vcc1 mcast-fwd [on | off }

Enables or disables multi-cast forwarding on the specified interface. If set to **on**, this interface acts as an IGMP proxy host, and IGMP packets are transmitted and received on this interface on behalf of IGMP hosts on the LAN interface. See “IGMP Settings” on page 211 for more information.

set ip ip-ppp vcc1 igmp-null-source-addr [off | on]

Enables or disables IGMP null source address, if **mcast-fwd** is set to **on**. If enabled, the source IP address of every IGMP packet transmitted from this interface is set to 0.0.0.0. This complies with the requirements of TR-101, and removes the need for a publicly advertised IP address on the WAN interface.

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**.

802.3ah Ethernet OAM Settings

802.3ah Ethernet in the First Mile (EFM) Operations Administration and Maintenance (OAM) is a group of network management functions that provide network fault indication, performance information, and diagnosis using special-purpose Ethernet OAM frames. These are exchanged between your Gateway and service provider Access Node (AN) devices for network fault management, performance analysis and fault isolation.

All VDSL and Ethernet WAN Motorola Netopia Gateways support Ethernet OAM options.

More Ethernet Packet-Transfer-Mode (PTM) enabled xDSL Motorola Netopia Gateways will support 802.3ah Ethernet OAM options in future releases.

802.3ah Ethernet OAM exchanges periodic Ethernet OAM heartbeat frames between the endpoints of the physical link being monitored, and thus discovers and keeps-alive the Link connectivity and reports faults if the link goes down. Supported OAM request and response types are: remote loopback enable, remote loopback disable, variable request, variable response.

set ethernet oam ah option [off I on]

Enables or disables Ethernet OAM. Default is **off**.

set ethernet oam ah pass-through [off I on]

Enable or disable Ethernet OAM pass-through mode. Default is **off**.

Warning: This is a DEBUG feature. Leave it off unless you know exactly what you are doing.

set ethernet oam ah mode [active I passive]

Specifies the Ethernet OAM mode. Default is **active**.

set ethernet oam ah pdu-size-max [64 - 1518]

Specifies the Maximum Protocol Data Unit (PDU) size. Default is **1518**.

set ethernet oam ah discovery-timer [1 - 300]

Specifies the discovery timer value for continuity check in seconds. Range is 1 – 300 seconds. Default is **1**.

set ethernet oam ah keepalive-timer [5 - 305]

Specifies the keep-alive timer value in seconds. Range is 5 – 305 seconds. Default is **5**.

etheroam ah ping

Sends OAM remote loopback request in active mode.

Command Line Interface Preference Settings

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

set preference verbose { on l 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 1000 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 Motorola Netopia® Gateway to an internal host, you must change the port numbers the Motorola 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 Motorola 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 Motorola Netopia® Gateway uses for its configuration traffic, you must use those port numbers instead of the standard numbers when configuring the Motorola 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 Motorola 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 Motorola Netopia® Gateway.

set servers web-http [1 - 65534]

Specifies the port number for HTTP (web) communication with the Motorola 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 Motorola 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 Motorola 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 Motorola 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, Packet Filtering, Stateful Inspection, and IPSec parameters. Some of the security functionality is keyed.

Firewall Settings (for BreakWater Firewall)

set security firewall option [ClearSailing | SilentRunning | LANdLocked]

BreakWater Basic Firewall. BreakWater delivers an easily selectable set of pre-configured firewall protection levels. For simple implementation these settings (comprised of three levels) are readily available through Motorola Netopia®'s embedded web server interface.

BreakWater Basic Firewall's three settings are:

- **ClearSailing**

  ClearSailing, BreakWater's default setting, supports both inbound and outbound traffic. It is the only basic firewall setting that fully interoperates with all other Motorola Netopia® software features.
- **SilentRunning**

  Using this level of firewall protection allows transmission of outbound traffic on pre-configured TCP/UDP ports. It disables any attempt for inbound traffic to identify the Gateway. This is the Internet equivalent of having an *unlisted number*.
- **LANdLocked**

  The third option available turns off all inbound and outbound traffic, isolating the LAN and disabling all WAN traffic.

NOTE:

BreakWater Basic Firewall operates independent of the NAT functionality on the Gateway.

TIPS for making your BreakWater Basic Firewall Selection

Application	Select this Level	Other Considerations
Typical Internet usage (browsing, e-mail)	SilentRunning	
Multi-player online gaming	ClearSailing	**Set Pinholes**; once defined, pinholes will be active whenever ClearSailing is set. **Restore SilentRunning** when finished.
Going on vacation	LANdLocked	Protects your connection while your away.
Finished online use for the day	LANdLocked	This protects you instead of disconnecting your Gateway connection.
Chatting online or using instant messaging	ClearSailing	**Set Pinholes**; once defined, pinholes will be active whenever ClearSailing is set. **Restore SilentRunning** when finished.

Basic Firewall Background

As a device on the Internet, a Motorola Netopia® Gateway requires an IP address in order to send or receive traffic.

The IP traffic sent or received have an associated application port which is dependent on the nature of the connection request. In the IP protocol standard the following session types are common applications:

- ICMP
- SNMP
- HTTP
- telnet
- FTP
- DHCP

By receiving a response to a scan from a port or series of ports (which is the expected behavior according to the IP standard), hackers can identify an existing device and gain a potential opening for access to an internet-connected device.

To protect LAN users and their network from these types of attacks, BreakWater offers three levels of increasing protection.

The following tables indicate the **state of ports associated with session types**, both on the WAN side and the LAN side of the Gateway.

This table shows how inbound traffic is treated. *Inbound* means the traffic is coming from the WAN into the WAN side of the Gateway.

Gateway: WAN Side				
	BreakWater Setting >>	**ClearSailing**	**SilentRunning**	**LANdLocked**
Port	**Session Type**	**-------------Port State----------------------**		
20	ftp data	Enabled	Disabled	Disabled
21	ftp control	Enabled	Disabled	Disabled
23	telnet external	Enabled	Disabled	Disabled
23	telnet Motorola Netopia® server	Enabled	Disabled	Disabled
80	http external	Enabled	Disabled	Disabled
80	http Motorola Netopia® server	Enabled	Disabled	Disabled
67	DHCP client	Enabled	Enabled	Disabled
68	DHCP server	Not Applicable	Not Applicable	Not Applicable
161	snmp	Enabled	Disabled	Disabled
	ping (ICMP)	Enabled	Disabled	Disabled

This table shows how outbound traffic is treated. *Outbound* means the traffic is coming from the LAN-side computers into the LAN side of the Gateway.

Gateway: LAN Side				
	BreakWater Setting >>	**ClearSailing**	**SilentRunning**	**LANdLocked**
Port	**Session Type**	**-------------Port State----------------------**		
20	ftp data	Enabled	Enabled	Disabled
21	ftp control	Enabled	Enabled	Disabled
23	telnet external	Enabled	Enabled	Disabled
23	telnet Motorola Netopia® server	Enabled	Enabled	Enabled
80	http external	Enabled	Enabled	Disabled
80	http Motorola Netopia® server	Enabled	Enabled	Enabled
67	DHCP client	Not Applicable	Not Applicable	Not Applicable

68	DHCP server	Enabled	Enabled	Enabled
161	snmp	Enabled	Enabled	Enabled
	ping (ICMP)	Enabled	Enabled	**WAN** - Disabled **LAN** - Local Address Only

NOTE:

The Gateway's WAN DHCP client port in SilentRunning mode is **enabled.** This feature allows end users to continue using DHCP-served IP addresses from their Service Providers, while having no identifiable presence on the Internet.

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 Motorola Netopia® unit or another IPsec/IKE based security product. For VPN you can choose to have traffic authenticated, encrypted, or both.

When connecting the Motorola Netopia® unit in a telecommuting scenario, the corporate VPN settings will dictate the settings to be used in the Motorola 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.

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

Turns on the SafeHarbour IPsec tunnel capability. Default is off. See "IPSec" on page 94 for more information.

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 I 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 I none }

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

See page 94 for details about SafeHarbour IPsec tunnel capability.

Example: **0x1234**

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

See page 94 for details about SafeHarbour IPsec tunnel capability.

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 I 2 I 5}

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

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 I SHA1}

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

See page 94 for details about SafeHarbour IPsec tunnel capability.

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

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

set security ipsec tunnels name "123" xauth enable {off I 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 I 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 I Subnet I Hostname I ASCII }

Specifies the NAT local ID type for the specified IPsec tunnel, when Aggressive Mode is set.

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, when Aggressive Mode is set.

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 I Subnet I Hostname I ASCII }

Specifies the NAT remote ID type for the specified IPsec tunnel, when Aggressive Mode is set.

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, when Aggressive Mode is set.

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 *begins* to negotiate a new key. For example, after 82800 seconds (23 hours) or 1 Gbyte has been transferred (whichever comes first) the key will begin to 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 l dsl] vcc*n* option [off l on]
set security state-insp ethernet [A l B] option [off l 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 l dsl] vcc*n* default-mapping [off l on]
set security state-insp ethernet [A l B] default-mapping [off l on]

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

set security state-insp [ip-ppp l dsl] vcc*n* tcp-seq-diff [0 - 65535]
set security state-insp ethernet [A l 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 l dsl] vcc*n* deny-fragments [off l on]
set security state-insp ethernet [A l B] deny-fragments [off l 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 dos-detect [off | on]

Enables or disables the stateful inspection Denial of Service detection feature. If set to **on**, the device will monitor packets for Denial of Service (DoS) attack. Offending packets may be discarded if it is determined to be a DoS attack.

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 l udp l both l 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]

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 Motorola Netopia® Gateway.

set snmp community read *name*

Adds the specified name to the list of communities associated with the Motorola Netopia® Gateway. By default, the Motorola 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 Motorola Netopia® Gateway.

set snmp community trap *name*

Adds the specified name to the list of communities associated with the Motorola 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 Motorola 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 Motorola 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

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.

SNMP V3 Settings

SNMP V3 is supported beginning with Firmware Version 7.4.

SNMPv3 supports two users, the Read-Only user and the Read-Write user. The read-only account will have read-only access to all objects known to the agent, while the read-write account will have read-write access to all objects known to the agent. SNMPv3 adds the ability to authenticate and/or encrypt management traffic.

For security reasons, enabling SNMPv3 will disable SNMPv1/v2.

- If SNMPv3 is enabled, the firmware will no longer respond to SNMPv1/SNMPv2 traffic, nor generate SNMPv1/v2 traps in SNMPv1/SNMPv2 packets. If it receives v1 or v2 packets when v3 is enabled, it behaves as if it does not support v1/v2, and silently discards the incoming packet.
- If SNMPv3 is disabled, the firmware will not respond to SNMPv3 traffic, nor generate SNMPv3 notifications. The firmware behaves as if it does not support v3 and silently discards the incoming packet.

set snmp v3 enable [off | on]

Turns SNMPv3 off or on.

set snmp v3 ro-account security-name *string*

Adds the specified 1 – 32 character name *string* as the name of the Read-Only user.

set snmp v3 ro-account security-model [none l auth l auth+priv]

Sets the security model for the Read-Only account: none, authentication, or authentication plus privacy.

- **none** specifies no authentication or encryption;
- **auth** (authentication, no encryption) requires a security name and authentication password, and a specified authentication protocol;
- **auth+priv** (authentication plus privacy DES encryption) requires authentication plus a privacy password.

set snmp v3 ro-account auth-protocol [md5 l sha]

Specifies the authentication protocol for the Read-Only account: **md5** (HMAC-MD5 authentication) or **sha** (HMAC-SHA authentication), if the security model is set to **auth** or **auth+priv**.

set snmp v3 ro-account auth-password

Specifies the authentication password, a 1 – 32 character *string*, for the Read-Only account, if the security model is set to **auth** or **auth+priv**. You are prompted for a new password and then to repeat the password. If there is an existing password, the user must enter the old password, then the new password, and repeat it.

set snmp v3 ro-account priv-password

Specifies the privacy password, a 1 – 32 character *string*, for the Read-Only account, if the security model is set to **auth+priv**. You are prompted for a new password and then to repeat the password. If there is an existing password, the user must enter the old password, then the new password, and repeat it.

set snmp v3 ro-account localize-keys [off l on]

Determines whether or not the generated keys should be localized (hashed) with the Engine ID for the Read-Only account, if the security model is set to **auth+priv**.

set snmp v3 rw-account security-name *string*

Adds the specified 1 – 32 character name *string* as the name of the Read-Write user.

set snmp v3 rw-account security-model [none I auth I auth+priv]

Sets the security model for the Read-Write account: none, authentication, or authentication plus privacy.

- **none** specifies no authentication or encryption;
- **auth** (authentication, no encryption) requires a security name and authentication password, and a specified authentication protocol;
- **auth+priv** (authentication plus privacy DES encryption) requires authentication plus a privacy password.

set snmp v3 rw-account auth-protocol [md5 I sha]

Specifies the authentication protocol for the Read-Write account: **md5** (HMAC-MD5 authentication) or **sha** (HMAC-SHA authentication), if the security model is set to **auth** or **auth+priv**.

set snmp v3 rw-account auth-password

Specifies the authentication password, a 1 – 32 character *string*, for the Read-Write account, if the security model is set to **auth** or **auth+priv**. You are prompted for a new password and then to repeat the password. If there is an existing password, the user must enter the old password, then the new password, and repeat it.

set snmp v3 rw-account priv-password

Specifies the privacy password, a 1 – 32 character *string*, for the Read-Write account, if the security model is set to **auth+priv**. You are prompted for a new password and then to repeat the password. If there is an existing password, the user must enter the old password, then the new password, and repeat it.

set snmp v3 rw-account localize-keys [off I on]

Determines whether or not the generated keys should be localized (hashed) with the Engine ID for the Read-Write account, if the security model is set to **auth+priv**.

show snmp v3 engine-id

Displays the router's SNMP Engine ID. This is not editable.

System Settings

You can configure system settings to assign a name to your Motorola 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 Motorola Netopia® Gateway. Each Motorola Netopia® Gateway is assigned a name as part of its factory initialization. The default name for a Motorola 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 Motorola Netopia® Gateway, you can enter that name in the ***Address*** text field of your browser to open a connection to your Motorola 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 Motorola 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 ftp-server option [off I on]

Enables or disables a simple FTP server in the Gateway. If enabled, the Gateway will accept binary embedded software images ('.bin') files or command line configuration files.

Supported FTP commands

MODE	(data transfer mode (only Streaming supported)
NOOP	(send back ok)
PORT	(specify client address:port for data)
QUIT	(quit)
STOR	(send file to FTP server)
SYST	(get system info about FTP server)
TYPE	(set data representation type, ASCII and IMAGE (BIN) only supported)
USER	(send username for authentication)

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 I on]

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

set system idle-timeout { telnet [1...120] I 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* I 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 Motorola 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 Motorola Netopia® Gateway for the password to take effect. Assigning an administrator or user password to a Motorola 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* | *dns_name*]
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 lay-

out, 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 (north-america.pool.ntp.org)
alt-server-address (pool.ntp.org):
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. The NTP **server-address** and **alt-server-address** can be entered as DNS names as well as IP addresses. 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 Motorola Netopia® Gateway. The Motorola 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.

Syslog

set system syslog option [off I on]

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

set system syslog host-nameip [*ip_address* I *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 I on]

Specifies whether violations are logged or ignored.

set system syslog log-accepted [off I on]

Specifies whether acceptances are logged or ignored.

set system syslog log-attempts [off I 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 ip-ppp vcc1 option on
   ```

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

   ```
   set security state-insp ip-ppp vcc1 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 Motorola Netopia® Gateway to determine the best channel to broadcast automatically. For details, see "AutoChannel Setting" on page 128.

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 }

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 }

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 { off | WEP | WPA-PSK | WPA-802.1x }
set wireless multi-ssid third-ssid-privacy { off | WEP | WPA-PSK | WPA-802.1x }
set wireless multi-ssid fourth-ssid-privacy { off | WEP | WPA-PSK | WPA-802.1x }

Specifies the type of privacy enabled on multiple SSIDs when **multi-ssid option** is set to **on**. off = no privacy; WEP = WEP encryption; WPA-PSK = Wireless Protected Access/Pre-Shared Key; WPA-802.1x = Wireless Protected Access/802.1x authentication. See “Wireless Privacy Settings” on page 284 for more information.

NOTE:

WEP is supported on only one SSID at a time, and will not be available if another SSID already has it configured.

set wireless multi-ssid second-ssid-wpa-ver { all | WPA1-only | WPA2-only }
set wireless multi-ssid third-ssid-wpa-ver { all | WPA1-only | WPA2-only }
set wireless multi-ssid fourth-ssid-wpa-ver { all | WPA1-only | WPA2-only }

Specifies the type of WPA version enabled on multiple SSIDs when **multi-ssid option** is set to **on** and privacy is set to **WPA-PSK**. See “Wireless Privacy Settings” on page 284 for more information.

set wireless multi-ssid second-ssid-psk { *string* }
set wireless multi-ssid third-ssid-psk { *string* }
set wireless multi-ssid fourth-ssid-psk { *string* }

Specifies a WPA passphrase for the multiple SSIDs, when **second-**, **third-**, or **fourth-ssid-privacy** is set to **WPA-PSK**. The Pre Shared Key is a passphrase shared between the Gateway and the clients and is used to generate dynamically changing keys. The passphrase can be 8 – 63 characters. It is recommended to use at least 20 characters for best security.

set wireless multi-ssid second-ssid-weplen [40/64bit | 128bit | 256bit]
set wireless multi-ssid third-ssid-weplen [40/64bit | 128bit | 256bit]
set wireless multi-ssid fourth-ssid-weplen [40/64bit | 128bit | 256bit]

Specifies the WEP key length for the multiple SSIDs, when **second-**, **third-**, or **fourth-ssid-privacy** is set to **WEP**. **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 multi-ssid second-ssid-wepkey { *hexadecimal digits* }
set wireless multi-ssid third-ssid-wepkey { *hexadecimal digits* }
set wireless multi-ssid fourth-ssid-wepkey { *hexadecimal digits* }

Specifies a WEP key for the multiple SSIDs, when **second-**, **third-**, or **fourth-ssid-privacy** is set to **WEP**. 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.

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 802.11 spectrum, it helps to size the Gateway's cell to match the location. This allows you to install a router to cover a small “hole” without conflicting with other routers nearby.

Wireless Multi-media (WMM) Settings

Router EDCA Parameters (Enhanced Distributed Channel Access) govern wireless data from your Gateway to the client; **Client EDCA Parameters** govern wireless data from the client to your Gateway.

set wireless wmm option [off I on]

Enables or disables wireless multi-media settings option, which allows you to fine tune WiFi Multimedia Quality of Service (QoS) by transmitting data depending on Diffserv priority settings. These priorities are mapped into four Access Categories (AC), in increasing order of priority: Background (BK), Best Effort (BE), Video (VI), and Voice (VO). It requires WiFi Multimedia-capable clients, usually a separate feature enabled at the client.

- **aifs**: (Arbitration Interframe Spacing) the wait time in milliseconds for data frames. Valid values are: 1 – 255
- **cwmin**: (Minimum Contention Window) upper limit in milliseconds of the range for determining initial random backoff. The value you choose must be lower than **cwmax**. Valid ***value***s are: 1, 3, 7, 15, 31, 63, 127, 255, or 511.
- **cwmax**: (Maximum Contention Window) upper limit in milliseconds of the range of determining final random backoff. The value you choose must be higher than **cwmin**. Valid ***value***s are: 3, 7, 15, 31, 63, 127, 255, 511, or 1023.
- **txoplimit**: Time interval in microseconds that clients may initiate transmissions. Valid values are: 0 – 9999.

NOTE:

It is not recommended that you modify these settings without direct knowledge or instructions to do so. Modifying these settings inappropriately could seriously degrade network performance.

set wireless wmm router-edca voice { aifs 1... 255 }
set wireless wmm router-edca voice { cwmin *value* }
set wireless wmm router-edca voice { cwmax *value* }

Sets values for Gateway WMM voice parameters.

set wireless wmm router-edca video { aifs 1... 255 }
set wireless wmm router-edca video { cwmin *value* }
set wireless wmm router-edca video { cwmax *value* }

Sets values for Gateway WMM video parameters.

set wireless wmm router-edca best-effort { aifs 1... 255 }
set wireless wmm router-edca best-effort { cwmin *value* }
set wireless wmm router-edca best-effort { cwmax *value* }

Sets values for Gateway WMM best effort parameters.

set wireless wmm router-edca background { aifs 1... 255 }
set wireless wmm router-edca background { cwmin *value* }
set wireless wmm router-edca background { cwmax *value* }

Sets values for Gateway WMM background parameters.

set wireless wmm client-edca voice { aifs 1... 255 }
set wireless wmm client-edca voice { cwmin *value* }
set wireless wmm client-edca voice { cwmax *value* }
set wireless wmm client-edca voice { txoplimit 0... 9999 }

Sets values for client WMM voice parameters.

set wireless wmm client-edca video { aifs 1... 255 }
set wireless wmm client-edca video { cwmin *value* }
set wireless wmm client-edca video { cwmax *value* }
set wireless wmm client-edca video { txoplimit 0... 9999 }

Sets values for client WMM video parameters.

set wireless wmm client-edca best-effort { aifs 1... 255 }
set wireless wmm client-edca best-effort { cwmin *value* }
set wireless wmm client-edca best-effort { cwmax *value* }
set wireless wmm client-edca best-effort { txoplimit 0... 9999 }

Sets values for client WMM best effort parameters.

set wireless wmm client-edca background { aifs 1... 255 }
set wireless wmm client-edca background { cwmin *value* }
set wireless wmm client-edca background { cwmax *value* }
set wireless wmm client-edca background { txoplimit 0... 9999 }

Sets values for client WMM background parameters.

Wireless Privacy Settings

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. See “Privacy” on page 126 for a discussion of these options.

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 successfully 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 l 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

You can create up to 8 VLANs, and you can also restrict any VLAN, and the computers on it, from administering the Gateway. See “VLAN” on page 106 for more information.

set vlan name *name*

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.

set vlan name *name* type [by-port | global]

Specifies VLAN **type**: **by-port** or **global**. Default is **by-port**.

set vlan name *name* id *VID*

Specifies VLAN **id** (VID), when type is set to **global**. The numerical range of possible VIDs is 1 - 4094. (A VID of zero (0) is permitted on the Ethernet WAN port only.)

set vlan name *name* admin-restricted [off | on]

Turns **admin-restricted off** or **on**. Default is **off**. If you select **on**, administrative access to the Gateway is blocked from the specified VLAN.

set vlan name *name* seg-pbits [0 - 7]

Specifies the 802.1p priority bit. If you set this to a value greater than 0, all packets of this VLAN with unmarked priority bits (pbits) will be re-marked to this priority.

set vlan name *name* ports *port* option [off | on]

Enables or disables the Gateway’s physical Ethernet, USB or VCC ***port*** or wireless SSID for the specified VLAN.

set vlan name *name* ports *port* tag [off l on]

If set to **on**, packets transmitted from this port through this VLAN must be tagged with the VLAN VID. Packets received through this port destined for this VLAN must be tagged with the VLAN VID by the source. The **tag** option is only available on **global** type ports.

set vlan name *name* ports *port* priority [off l on]

Enables or disables the **priority** for the port assigned to the specified VLAN allowing packet prioritization based on any 802.1p priority bits in the VLAN header to prioritize packets within the Gateway's internal queues, according to DiffServ priority mapping rules.

set vlan name *name* ports *port* promote [off l on]

Enables or disables the **promote** setting allowing writing any 802.1p priority bits into the IP-TOS header bit field for received IP packets on this port destined for this VLAN. Write any IP-TOS priority bits into the 802.1p priority bit field for tagged IP packets transmitted from this port for this VLAN. All mappings between Ethernet 802.1p and IP-TOS are made via **diffserv dscp-map** settings.

set vlan name *name* ports *port* port-pbits [0 - 7]

Specifies the 802.1p priority bit for this port associated with the specified VLAN. If you set this to a value greater than 0, all packets of this port with unmarked priority bits (pbits) will be re-marked to this priority.

set vlan name *name* ip-interface *ip_interface*

Associates this VLAN with the specified IP interface. By default the **ip-vcc1** and **ip-eth-a** interfaces are available, but others may be defined.

set vlan name *name* inter-vlan-routing [group-1... group-8] [off l on]

When set to **on**, **inter-vlan-routing** allows VLANs in the specified group to route traffic to the others; ungrouped VLANs cannot route traffic to each other.

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

Example 1:

- A simple example using the “Step” method – Navigate to the VLAN item:

```
Netopia-3000/9437188 (top)>> vlan
Netopia-3000/9437188 (vlan)>> set
  vlan

(vlan) node list ...
Select (name) node to modify from list,
or enter new (name) to create.
  vlan name (?): vlan1
(vlan1) has been added to the (vlan) list
    name "vlan1"
      type (by-port) [ by-port | global ]: by-port
      admin-restricted (off) [ off | on ]: off
      seg-pbits (0) [ 0 - 7 ]: 0
      ports
```

- At this point you have created a VLAN. It is called **vlan1**, without any admin restrictions.
- Next, add the port **eth0.1** port to this VLAN:

```
      ports
        eth0.1
          option (off) [ off | on ]: on
          priority (off) [ off | on ]: on
          promote (off) [ off | on ]: on
          port-pbits (0) [ 0 - 7 ]: 1
        eth0.2
          option (off) [ off | on ]:
        eth0.3
          option (off) [ off | on ]:
        eth0.4
          option (off) [ off | on ]:
        ssid1
          option (off) [ off | on ]:
        vcc1
          option (off) [ off | on ]:
```

- Assign an IP interface:

```
        ip-vcc1
          option (off) [ off | on ]:
        ip-eth-a
          option (off) [ off | on ]: on
        ipsec-mgmt1
          option (off) [ off | on ]:
Netopia-3000/9437188 (vlan)>>
```

Example 2:

- An example of a “Triple-Play” setup:

```
set vlan name "LanPorts" type by-port
set vlan name "LanPorts" admin-restricted off
set vlan name "LanPorts" seg-pbits 0
set vlan name "LanPorts" ports eth0.1 option off
set vlan name "LanPorts" ports eth0.2 option on
set vlan name "LanPorts" ports eth0.2 priority off
set vlan name "LanPorts" ports eth0.2 promote off
set vlan name "LanPorts" ports eth0.2 port-pbits 0
set vlan name "LanPorts" ports eth0.3 option on
set vlan name "LanPorts" ports eth0.3 priority off
set vlan name "LanPorts" ports eth0.3 promote off
set vlan name "LanPorts" ports eth0.3 port-pbits 0
set vlan name "LanPorts" ports eth0.4 option on
set vlan name "LanPorts" ports eth0.4 priority off
set vlan name "LanPorts" ports eth0.4 promote off
set vlan name "LanPorts" ports eth0.4 port-pbits 0
set vlan name "LanPorts" ports ssid1 option on
set vlan name "LanPorts" ports ssid1 priority off
set vlan name "LanPorts" ports ssid1 promote off
set vlan name "LanPorts" ports ssid1 port-pbits 0
set vlan name "LanPorts" ports eth1 option off
set vlan name "LanPorts" ip-interfaces ip-ppp-a option off
set vlan name "LanPorts" ip-interfaces ip-eth-b option off
set vlan name "LanPorts" ip-interfaces ip-eth-c option off
set vlan name "LanPorts" ip-interfaces ip-eth-a option on
set vlan name "LanPorts" inter-vlan-routing group-1 on
set vlan name "LanPorts" inter-vlan-routing group-2 off
set vlan name "LanPorts" inter-vlan-routing group-3 off
set vlan name "LanPorts" inter-vlan-routing group-4 off
set vlan name "Voip_217" type global
set vlan name "Voip_217" id 217
set vlan name "Voip_217" admin-restricted off
set vlan name "Voip_217" seg-pbits 7
set vlan name "Voip_217" ports eth0.1 option off
set vlan name "Voip_217" ports eth0.2 option off
set vlan name "Voip_217" ports eth0.3 option off
set vlan name "Voip_217" ports eth0.4 option off
set vlan name "Voip_217" ports ssid1 option off
set vlan name "Voip_217" ports eth1 option on
set vlan name "Voip_217" ports eth1 tag on
set vlan name "Voip_217" ports eth1 priority off
set vlan name "Voip_217" ports eth1 promote off
set vlan name "Voip_217" ports eth1 port-pbits 0
set vlan name "Voip_217" ip-interfaces ip-ppp-a option off
set vlan name "Voip_217" ip-interfaces ip-eth-b option on
set vlan name "Voip_217" ip-interfaces ip-eth-c option off
set vlan name "Voip_217" ip-interfaces ip-eth-a option off
set vlan name "Voip_217" inter-vlan-routing group-1 on
set vlan name "Voip_217" inter-vlan-routing group-2 off
set vlan name "Voip_217" inter-vlan-routing group-3 off
set vlan name "Voip_217" inter-vlan-routing group-4 off
set vlan name "PPPoE_11" type global
set vlan name "PPPoE_11" id 11
set vlan name "PPPoE_11" admin-restricted off
set vlan name "PPPoE_11" seg-pbits 0
set vlan name "PPPoE_11" ports eth0.1 option off
set vlan name "PPPoE_11" ports eth0.2 option off
set vlan name "PPPoE_11" ports eth0.3 option off
set vlan name "PPPoE_11" ports eth0.4 option off
set vlan name "PPPoE_11" ports ssid1 option off
set vlan name "PPPoE_11" ports eth1 option on
set vlan name "PPPoE_11" ports eth1 tag on
set vlan name "PPPoE_11" ports eth1 priority off
set vlan name "PPPoE_11" ports eth1 promote off
set vlan name "PPPoE_11" ports eth1 port-pbits 0
set vlan name "PPPoE_11" ip-interfaces ip-ppp-a option on
set vlan name "PPPoE_11" ip-interfaces ip-eth-b option off
set vlan name "PPPoE_11" ip-interfaces ip-eth-c option off
set vlan name "PPPoE_11" ip-interfaces ip-eth-a option off
set vlan name "PPPoE_11" inter-vlan-routing group-1 on
set vlan name "PPPoE_11" inter-vlan-routing group-2 off
set vlan name "PPPoE_11" inter-vlan-routing group-3 off
set vlan name "PPPoE_11" inter-vlan-routing group-4 off
set vlan name "Mgmt_2017" type global
set vlan name "Mgmt_2017" id 2017
set vlan name "Mgmt_2017" admin-restricted off
set vlan name "Mgmt_2017" seg-pbits 3
set vlan name "Mgmt_2017" ports eth0.1 option off
set vlan name "Mgmt_2017" ports eth0.2 option off
set vlan name "Mgmt_2017" ports eth0.3 option off
set vlan name "Mgmt_2017" ports eth0.4 option off
set vlan name "Mgmt_2017" ports ssid1 option off
set vlan name "Mgmt_2017" ports eth1 option on
set vlan name "Mgmt_2017" ports eth1 tag on
set vlan name "Mgmt_2017" ports eth1 priority off
set vlan name "Mgmt_2017" ports eth1 promote off
set vlan name "Mgmt_2017" ports eth1 port-pbits 0
set vlan name "Mgmt_2017" ip-interfaces ip-ppp-a option off
set vlan name "Mgmt_2017" ip-interfaces ip-eth-b option off
set vlan name "Mgmt_2017" ip-interfaces ip-eth-c option on
set vlan name "Mgmt_2017" ip-interfaces ip-eth-a option off
set vlan name "Mgmt_2017" inter-vlan-routing group-1 off
set vlan name "Mgmt_2017" inter-vlan-routing group-2 off
set vlan name "Mgmt_2017" inter-vlan-routing group-3 off
set vlan name "Mgmt_2017" inter-vlan-routing group-4 off
set vlan name "Video_31" type global
set vlan name "Video_31" id 31
set vlan name "Video_31" admin-restricted off
set vlan name "Video_31" seg-pbits 5
set vlan name "Video_31" ports eth0.1 option on
set vlan name "Video_31" ports eth0.1 tag off
set vlan name "Video_31" ports eth0.1 priority off
set vlan name "Video_31" ports eth0.1 promote off
set vlan name "Video_31" ports eth0.1 port-pbits 0
set vlan name "Video_31" ports eth0.2 option off
set vlan name "Video_31" ports eth0.3 option off
set vlan name "Video_31" ports eth0.4 option off
set vlan name "Video_31" ports ssid1 option off
set vlan name "Video_31" ports eth1 option on
set vlan name "Video_31" ports eth1 tag on
set vlan name "Video_31" ports eth1 priority off
set vlan name "Video_31" ports eth1 promote off
set vlan name "Video_31" ports eth1 port-pbits 0
set vlan name "Video_31" ip-interfaces ip-ppp-a option off
set vlan name "Video_31" ip-interfaces ip-eth-b option off
set vlan name "Video_31" ip-interfaces ip-eth-c option off
set vlan name "Video_31" ip-interfaces ip-eth-a option off
set vlan name "Video_31" inter-vlan-routing group-1 off
set vlan name "Video_31" inter-vlan-routing group-2 off
set vlan name "Video_31" inter-vlan-routing group-3 off
set vlan name "Video_31" inter-vlan-routing group-4 off
```

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

VoIP settings

(supported models only)

Voice-over-IP (VoIP) refers to the ability to make voice telephone calls over the Internet. This differs from traditional phone calls that use the Public Switched Telephone Network (PSTN). VoIP calls use an Internet protocol, Session Initiation Protocol (SIP), to transmit sound over a network or the Internet in the form of data packets. Certain Motorola Netopia® Gateway models have two separate voice ports for connecting telephone handsets. These models support VoIP. If your Gateway is a VoIP model, you can configure the VoIP features.

set voip phone [0 | 1] sip-option [off | on]

Turns SIP on or off for the specified phone. Default is **off**.

set voip phone [0 | 1] sip-proxy-server [*server_name* | *ip_address*]

Specifies the SIP proxy server for the specified phone by fully qualified server name or IP address.

set voip phone [0 | 1] sip-proxy-server-domain *domain_name*

Specifies the SIP proxy server domain name or IP address for the specified phone.

set voip phone [0 | 1] sip-proxy-server-transport [UDP | TCP | TLS]

Specifies the SIP proxy server transport protocol for the specified phone. Default is **UDP**.

set voip phone [0 | 1] sip-registrar-setting sip-registrar-server [*server_name* | *ip_address*]

Specifies the SIP registration server for the specified phone by fully qualified server name or IP address.

set voip phone [0 | 1] sip-registrar-setting sip-registrar-server-transport [UDP | TCP | TLS]

Specifies the SIP registration server transport protocol for the specified phone. Default is **UDP**.

set voip phone [0 | 1] sip-registrar-setting sip-expires-time [0 - 65535]

Specifies the SIP registration server time-out duration from 0 – 65535 seconds for the specified phone. Default is **3600** (1 hour).

set voip phone [0 | 1] sip-out-proxy-server [*server_name* | *ip_address*]

Specifies the SIP outbound proxy server for the specified phone by fully qualified server name or IP address.

set voip phone [0 | 1] sip-user-display-name *name*

Specifies the user name that is displayed on the web UI Home page, or other caller-id displays for the specified phone.

set voip phone [0 | 1] sip-user-name *username*

Specifies the user name that authenticates the user to SIP for the specified phone.

set voip phone [0 | 1] sip-user-password *password*

Specifies the password that authenticates the user to SIP for the specified phone.

set voip phone [0 | 1] auth-id *string*

Specifies the authorization ID that authenticates the user to SIP for the specified phone. Most SIP Servers expect this to be the username itself but some may use **auth-id**.

set voip phone [0 | 1] codec G711A priority [1 | 2 | 3 | 4 | 5 | 6 | 7 | none]

Assigns a priority to the ***alaw*** codec, the common analog voice encoding method used *outside* North America.

set voip phone [0 | 1] codec G711U priority

[1 l 2 l 3 l 4 l 5 l 6 l 7 l none]

Assigns a priority to the ***ulaw*** codec, the common analog voice encoding method used *in* North America.

set voip phone [0 l 1] codec G729A priority [1 l 2 l 3 l 4 l 5 l 6 l 7 l none]

Assigns a priority to the ***G729 annex A*** codec, the common analog voice compression implementation used in North America.

set voip phone [0 l 1] codec G726_16 priority [1 l 2 l 3 l 4 l 5 l 6 l 7 l none]

Assigns a priority to the ***G726-16*** codec, a common audio media type implementation at 16 kbit/s.

set voip phone [0 l 1] codec G726_24 priority [1 l 2 l 3 l 4 l 5 l 6 l 7 l none]

Assigns a priority to the ***G726-24*** codec, a common audio media type implementation at 24 kbit/s.

set voip phone [0 l 1] codec G726_32 priority [1 l 2 l 3 l 4 l 5 l 6 l 7 l none]

Assigns a priority to the ***G726-32*** codec, a common audio media type implementation at 32 kbit/s.

set voip phone [0 l 1] codec G726_40 priority [1 l 2 l 3 l 4 l 5 l 6 l 7 l none]

Assigns a priority to the ***G726-40*** codec, a common audio media type implementation at 40 kbit/s.

set voip phone [0 l 1] sip-advanced-setting sip-dtmf-mode [inband l rfc2833 l info]

sip-dtmf-mode – sets the Dual Tone Multi-Frequency Mode:

- **inband**: sends the DTMF digits as a normal inband tone.
- **rfc2833**: sends the DTMF digits as an event as part of the RTP packet header information.
- **info**: sends the DTMF digits in the SIP INFO message.

set voip phone [0 l 1] sip-advanced-setting sip-end-of-dial-marker [off l on]

sip-end-of-dial-marker – turns an “end of dial” (#) signal that indicates that the dialed number is complete **on** or **off**.

set voip phone [0 l 1] sip-advanced-setting call-feature call-forwarding-all-option [off l on]

call-forwarding-all-option – turns unconditional call forwarding **on** or **off**.

set voip phone [0 l 1] sip-advanced-setting call-feature call-forwarding-all-number *phone_number*

call-forwarding-all-number – specifies the number to which calls are to be forwarded when **call-forwarding-all-option** is **on**.

set voip phone [0 l 1] sip-advanced-setting call-feature call-forwarding-on-busy-option [off l on]

call-forwarding-on-busy-option – turns call forwarding when the line is busy **on** or **off**.

set voip phone [0 l 1] sip-advanced-setting call-feature call-forwarding-on-no-answer-option [off l on]

call-forwarding-on-no-answer-option – turns call forwarding when there is no answer **on** or **off**.

set voip phone [0 l 1] sip-advanced-setting call-feature call-forwarding-on-no-answer-number *phone_number*

call-forwarding-on-no-answer-number – specifies the number to which calls are to be forwarded when **call-forwarding-on-no-answer-option** is **on**.

set voip phone [0 | 1] sip-advanced-setting call-feature call-waiting-option [off | on]

call-waiting-option – enables or disables call waiting.

set voip phone [0 | 1] sip-advanced-setting call-feature call-conferencing-option [off | on]

call-conferencing-option – enables or disables 3-way call conferencing.

set voip phone [0 | 1] sip-advanced-setting call-feature subscribe-do-not-disturb-option [off | on]

subscribe-do-not-disturb-option – enables or disables option to prevent the phone from ringing.

set voip phone [0 | 1] sip-advanced-setting call-feature subscribe-mwi-option [off | on]

subscribe-mwi-option – if set to **on**, the Message Waiting Indicator is enabled when new voice mail is received.

set voip phone [0 | 1] sip-advanced-setting dsp-settings echo-option [echo-off | echo-on | echo-on-nlp | echo-on-cng-nlp]

echo-option – specifies under what conditions the system invokes or disables echo cancellation. Default is **echo-on-cng-nlp** (Comfort Noise Generation with non-linear processor).

set voip phone [0 | 1] sip-advanced-setting dsp-settings echo-start-attenuation [0 - 65535]

echo-start-attenuation – specifies the minimum attenuation level at which to invoke echo cancellation. Default is **8192**.

set voip phone [0 | 1] sip-advanced-setting dsp-settings

echo-max-attenuation [0 - 65535]

echo-max-attenuation – specifies the maximum attenuation level at which to invoke echo cancellation. Default is **16384**.

set voip phone [0 l 1] sip-advanced-setting dsp-settings echo-tail-length [0 - 65535]

echo-tail-length – specifies the duration of an echo tail required to invoke cancellation. Default is **0**.

set voip phone [0 l 1] sip-advanced-setting dsp-settings vad-option [off l on]

vad-option – turns Voice Activity Detection on or off. Default is **off**.

set voip phone [0 l 1] sip-advanced-setting dsp-settings vad-setting [vad-cn l vad-std-sid l vad-suppress-sid]

When **vad-option** is set to **on**:

- **vad-cn** – enables Voice Activity Detection/Comfort Noise Generation. When speech is not present, the CNG algorithm generates a noise signal at the level sent from the transmit side.
- **vad-std-sid** – enables Voice Activity Detection with standard Silence Insertion Descriptor support.
- **vad-suppress-sid** – enables Voice Activity Detection but suppresses standard Silence Insertion Descriptor support.

Example

```
set voip phone: 0 sip-option on
set voip phone: 0 sip-proxy-server "10.3.1.129"
set voip phone: 0 sip-proxy-server-domain ""
set voip phone: 0 sip-proxy-server-transport UDP
set voip phone: 0 sip-registrar-setting sip-registrar-server "10.3.1.129"
set voip phone: 0 sip-registrar-setting sip-registrar-server-transport UDP
set voip phone: 0 sip-registrar-setting sip-expires-time 3600
set voip phone: 0 sip-out-proxy-server "10.3.1.129"
set voip phone: 0 sip-user-display-name "4004"
set voip phone: 0 sip-user-name "4004"
set voip phone: 0 sip-user-password "4004"
set voip phone: 0 auth-id "4004"
set voip phone: 0 codec G711A priority 1
set voip phone: 0 codec G711U priority 2
set voip phone: 0 codec G729A priority 3
set voip phone: 0 codec G726_16 priority 4
set voip phone: 0 codec G726_24 priority 5
set voip phone: 0 codec G726_32 priority 6
set voip phone: 0 codec G726_40 priority 7
set voip phone: 0 sip-advanced-setting sip-dtmf-mode rfc2833
set voip phone: 0 sip-advanced-setting sip-end-of-dial-marker off
set voip phone: 0 sip-advanced-setting call-feature call-forwarding-all-
option off
set voip phone: 0 sip-advanced-setting call-feature call-forwarding-on-busy-
option off
set voip phone: 0 sip-advanced-setting call-feature call-forwarding-on-no-
answer-option off
set voip phone: 0 sip-advanced-setting call-feature call-waiting-option off
set voip phone: 0 sip-advanced-setting call-feature call-conferencing-option
off
set voip phone: 0 sip-advanced-setting call-feature subscribe-do-not-
disturb-option off
set voip phone: 0 sip-advanced-setting call-feature subscribe-mwi-option off
set voip phone: 0 sip-advanced-setting dsp-settings echo-option echo-on-cng-
nlp
set voip phone: 0 sip-advanced-setting dsp-settings echo-start-attenuation
8192
set voip phone: 0 sip-advanced-setting dsp-settings echo-max-attenuation
16384
set voip phone: 0 sip-advanced-setting dsp-settings echo-tail-length 0
set voip phone: 0 sip-advanced-setting dsp-settings vad-option off
set voip phone: 1 sip-option on
set voip phone: 1 sip-proxy-server "10.3.1.129"
set voip phone: 1 sip-proxy-server-domain ""
set voip phone: 1 sip-proxy-server-transport UDP
set voip phone: 1 sip-registrar-setting sip-registrar-server "10.3.1.129"
set voip phone: 1 sip-registrar-setting sip-registrar-server-transport UDP
set voip phone: 1 sip-registrar-setting sip-expires-time 3600
set voip phone: 1 sip-out-proxy-server "10.3.1.129"
set voip phone: 1 sip-user-display-name "4005"
set voip phone: 1 sip-user-name "4005"
set voip phone: 1 sip-user-password "4005"
set voip phone: 1 auth-id "4005"
set voip phone: 1 codec G711A priority 1
set voip phone: 1 codec G711U priority 2
set voip phone: 1 codec G729A priority 3
set voip phone: 1 codec G726_16 priority 4
set voip phone: 1 codec G726_24 priority 5
set voip phone: 1 codec G726_32 priority 6
set voip phone: 1 codec G726_40 priority 7
set voip phone: 1 sip-advanced-setting sip-dtmf-mode rfc2833
set voip phone: 1 sip-advanced-setting sip-end-of-dial-marker off
set voip phone: 1 sip-advanced-setting call-feature call-forwarding-all-
option off
set voip phone: 1 sip-advanced-setting call-feature call-forwarding-on-busy-
option off
set voip phone: 1 sip-advanced-setting call-feature call-forwarding-on-no-
answer-option off
set voip phone: 1 sip-advanced-setting call-feature call-waiting-option off
set voip phone: 1 sip-advanced-setting call-feature call-conferencing-option
off
set voip phone: 1 sip-advanced-setting call-feature subscribe-do-not-
disturb-option off
set voip phone: 1 sip-advanced-setting call-feature subscribe-mwi-option off
set voip phone: 1 sip-advanced-setting dsp-settings echo-option echo-on-cng-
nlp
set voip phone: 1 sip-advanced-setting dsp-settings echo-start-attenuation
8192
set voip phone: 1 sip-advanced-setting dsp-settings echo-max-attenuation
16384
set voip phone: 1 sip-advanced-setting dsp-settings echo-tail-length 0
set voip phone: 1 sip-advanced-setting dsp-settings vad-option off
```

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 Motorola Netopia® Gateway, will not need application layer gateway support on the Motorola Netopia® Gateway to work through NAT. The default is **on**.

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

set upnp log [off | on]

Enables or disables UPnP logging.

set upnp read-only [off | on]

Enables or disables

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 Motorola 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 Motorola 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 Motorola 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*”

Turns TR-069 WAN side management services on or off. For 3300-Series Gateways, the default is **off**; for 2200-Series Gateways, the default is **on**. 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
```

Backup IP Gateway Settings

The purpose of Backup is to provide a recovery mechanism in the event that the primary connection fails. A failure can be either line loss, for example by central site switch failure or physical cable breakage, or loss of end-to-end connectivity. Detection of one of these failures causes the Gateway to switch from using the primary DSL WAN connection to an alternate gateway on the Ethernet LAN. In the event of a loss of primary connectivity you have the option of switching back to the primary circuit automatically once it has recovered its connection.

A typical application would be to have a LAN connection from your Gateway to another Gateway that has, for example, another DSL modem or Gateway connection to the Internet, and designating the second gateway as the backup gateway. Should the primary WAN connection fail, traffic would be automatically redirected through your alternate gateway device to maintain Internet connectivity.

set backup option [disabled | manual | automatic]

Specifies whether backup to an IP gateway is **disabled** or enabled as **manual** or **automatic**. Default is **disabled**.

set backup failure-timeout [1 - 10]

Specifies the number of minutes you want the system to wait before the backup port becomes enabled in the event of primary line failure, when **backup option** is set to **automatic**. Sets the Default is **1**.

set backup ping-host [1 | 2] [name | address]

Specifies whether the Gateway will ping an IP address or resolvable DNS name, when **backup option** is set to **automatic**. These are optional items that are particularly useful for testing if the remote end of a VPN connection has gone down.

The Gateway will ping both addresses simultaneously at five-second intervals, recording the ping responses from each host. The Gateway will proceed into backup mode only if neither of the configured remote hosts responds.

set backup ping-host [1 l 2] [name *hostname* l ip-address *ip_address*]

Specifies an IP address or resolvable DNS name for the Gateway to ping.

set backup auto-recovery [off l on]

Turns automatic recovery **off** or **on**. Default is **off**.

set backup recovery-timeout [1 - 10]

If **auto-recovery** is set to **on**, specifies the number of minutes for the system to wait before attempting to switch back to the WAN connection. This allows you to be sure that the WAN connection is well re-established before the gateway switches back to it from the backup mode. Default is **1**.

set ip backup-gateway option [on l off]

Turns the backup gateway option **on** or **off**. Default is **off**.

set ip backup-gateway interface ip-address

Specifies the backup gateway interface ip address to which you want to direct the backup connection.

set ip backup-gateway default *ip_address*

Specifies the ip address of the default gateway.

VDSL Settings

CAUTION!

These settings are for very advanced users and lab technicians. Exercise extreme caution when modifying any of these settings.

```
set vdsl sys-option [ 0x00 - 0xff ]
         sys-bandplan [ 0x00 - 0xff ]
         psd-mask-level [ 0x00 - 0xff ]
         pbo-k1_1 [ 0x00000000 - 0xffffffff ]
         pbo-k1_2 [ 0x00000000 - 0xffffffff ]
         pbo-k1_3 [ 0x00000000 - 0xffffffff ]
         pbo-k2_1 [ 0x00000000 - 0xffffffff ]
         pbo-k2_2 [ 0x00000000 - 0xffffffff ]
         pbo-k2_3 [ 0x00000000 - 0xffffffff ]
         line-type [ 0x00 - 0xff ]
         us-max-inter-delay [ 0x00 - 0xff ]
         ds-max-inter-delay [ 0x00 - 0xff ]
         us-target-noise-margin [ 0x0000 - 0xffff ]
         ds-target-noise-margin [ 0x0000 - 0xffff ]
         min-noise-margin [ 0x0000 - 0xffff ]
         port-bandplan [ 0x00 - xff ]
         framing-mode [ 0x00 - 0xff ]
         band-mod [ 0x00 - 0xff ]
         port-option [ 0x00 - 0xff ]
         power-mode [ 0x00 - 0xff ]
         tx-filter [ 0x00 - 0xff ]
         rx-filter [ 0x00 - 0xff ]
         dying-gasp [ off l on ]
```

VDSL Parameter Defaults

Parameter	Default	Meaning
sys-option	0x00	VDSL system option(bit0=ntr, 1=margin, 2=ini, 3=pbo, 4=tlan, 5=pbo)
sys-bandplan	0x02	VDSL system bandplan(bp_3_998_4=2, bp4_997_3=3, bp5_997_3=4…)
psd-mask-level	0x00	VDSL system psd mask(def=0, 1=ansim1cab, 2=ansim2cab, 3=etsim1cab, 4=etsim2cab)
pbo-k1_1	0x00	VDSL system power back-off k1_1
pbo-k1_2	0x00	VDSL system power back-off k1_2
pbo-k1_3	0x00	VDSL system power back-off k1_3
pbo-k2_1	0x00	VDSL system power back-off k2_1
pbo-k2_2	0x00	VDSL system power back-off k2_2
pbo-k2_3	0x00	VDSL system power back-off k2_3
line-type	0x81	VDSL port line type(auto=0x80, vdsl=0x81, vdsl_etsi=0x82)
us-max-inter-delay	0x04	VDSL port upstream max inter delay
ds-max-inter-delay	0x04	VDSL port downstream max inter delay
us-target-noise-margin	0x0C	VDSL port upstream target noise margin
ds-target-noise-margin	0x0C	VDSL port downstream target noise margin
min-noise-margin	0x0A	VDSL port minimum noise margin
port-bandplan	0x02	VDSL port bandplan
framing-mode	0x90	DSL port frame mode(0-ATM; 0x80-PTM; 0x90-Auto(EFM/PTM)
band-mod	0x11	VDSL port band mod
port-option	0x0A - Annex B 0x06 - Annex A	VDSL port portoption(bit0=I43, bit1=v43, bit2=a43, bit3=b43)
power-mode	0x01	VDSL port power mode
tx-filter	0x02	VDSL port txPathFilterMode
rx-filter	0x02	VDSL port rxPathFilterMode
dying-gasp	off	Dying Gasp On/Off

VDSL Parameters Accepted Values

Parameter	Accepted Values
sys-option	Bit[0]: NTR_DISABLE Bit[1]: ALW_MARGIN_ADJUST. 1: the SNR margin for the optional band is reduced by up to 2.5 dB, but never below a minimum of 4 dB. Bit[2]: SUPPORT_INI Bit[4]: TLAN Enable Bit[5]: PBO Weak mode Enable (Applicable only when PBO Bit[3]=0. Bit[6]: ADSL_SAFE_MODE Enable Bit[7]: TLAN_SAFE_MODE Enable (Applicable only when TLAN Enable Bit[4] is set. If TLAN_SAFE_MODE not set, line will attempt to retrain at higher rates, but less stable line)

VDSL Parameters Accepted Values

Parameter	Accepted Values
sys-bandplan	BP1_998_3 (0x00)
	BP2_998_3 (0x01)
	BP998_3B_8_5M (0x01)
	BP3_998_4 (0x02)
	BP998_4B_12M (0x02)
	BP4_997_3 (0x03)
	BP997_3B_7_1M (0x03)
	BP5_997_3 (0x04)
	BP6_997_4 (0x05)
	BP997_4B_7_1M (0x05)
	BP7_MXU_3 (0x06)
	FLEX_3B_8_5M (0x06)
	BP8_MXU_2 (0x07)
	BP9_998_2 (0x08)
	BP10_998_2 (0x09)
	BP998_2B_3_8M (0x09)
	BP11_998_2 (0x0A)
	BP12_998_2 (0x0B)
	BP13_MXU_3 (0x0C)
	BP14_MXU_3 (0x0D)
	BP15_MXU_3 (0x0E)
	BP16_997_4B_4P (0x0F)
	BP17_998_138_4400 (0x10)
	BP18_997_138_4400(0x11)
	BP19_997_32_4400(0x12)
	BP20_998_138_4400_opBand (0x15)
	BP21_997_138_4400_opBand (0x16)
	BP22_998_138_4400_opBand(0x16)
	BP23_998_138_16000 (0x17)
	BP24_998_3B_8KHZ (0x18)
	BP25_998_138_17600 (0x19)
	BP26_CH1_3 (0x1A)
	BP27_CH1_4 (0x1B)

VDSL Parameters Accepted Values

Parameter	Accepted Values
psd-mask-level	0x00 -- default mask (old gains from before) 0x01 -- ANSI M1 CAB 0x02 -- ANSI M2 CAB 0x03 -- ETSI M1 CAB 0x04 -- ETSI M2 CAB 0x05 -- ITU-T Annex F (Japan) 0x06 - ANSI M1 Ex 0x07 - ANSI M2 Ex 0x08 -- ETSI M1 Ex 0x09 - ETSI M2 Ex 0x0A - RESERVED 0x0B - PSD_K (Korean M1 FTTCab -59dBm/Hz)
pbo-k1_1 pbo-k1_2 pbo-k1_3 pbo-k2_1 pbo-k2_2 pbo-k2_3	K1 and K2 parameters allow the user more flexibility in using Upstream Power Back-Off (UPBO) on CPE modem. Changing K1 and K2 values will affect the CPE TX PSD. Refer to VDSL standards for exact relation between K1, K2 parameters and TX PSD. There is an individual set of K1/K2 parameters associated with each upstream band in the PSD: Upstream Band 0 or Optional band, Upstream band 1, Upstream band 2 and Upstream Band 3. Setting all K2 parameters to 0 and all K1 to a high power level(ie low number) will essentially disable UPBO.
line-type	VDSL_AUTO_DETECT – (0x80) VDSL – (0x81) VDSL_ETSI – (0x82)
us-max-inter-delay	Maximum upstream interleave delay. Provisioned in steps of 0.5 ms. User defined.
ds-max-inter-delay	Maximum downstream interleave delay. Provisioned in steps of 0.5 ms. User defined.
us-target-noise-margin	Range 0-31.0dB, increments of 0.5dB (e.g., 0 = 0dB, 1 = 0.5dB, ...)
ds-target-noise-margin	Range 0-31.0dB, increments of 0.5dB (e.g., 0 = 0dB, 1 = 0.5dB, ...)
min-noise-margin	Range 0-31.0dB, increments of 0.5dB (e.g., 0 = 0dB, 1 = 0.5dB, ...)

VDSL Parameters Accepted Values

Parameter	Accepted Values
port-bandplan	BP1_998_3 (0x00)
	BP2_998_3 (0x01)
	BP998_3B_8_5M (0x01)
	BP3_998_4 (0x02)
	BP998_4B_12M (0x02)
	BP4_997_3 (0x03)
	BP997_3B_7_1M (0x03)
	BP5_997_3 (0x04)
	BP6_997_4 (0x05)
	BP997_4B_7_1M (0x05)
	BP7_MXU_3 (0x06)
	FLEX_3B_8_5M (0x06)
	BP8_MXU_2 (0x07)
	BP9_998_2 (0x08)
	BP10_998_2 (0x09)
	BP998_2B_3_8M (0x09)
	BP11_998_2 (0x0A)
	BP12_998_2 (0x0B)
	BP13_MXU_3 (0x0C)
	BP14_MXU_3 (0x0D)
	BP15_MXU_3 (0x0E)
	BP16_997_4B_4P (0x0F)
	BP17_998_138_4400 (0x10)
	BP18_997_138_4400(0x11)
	BP19_997_32_4400(0x12)
	BP20_998_138_4400_opBand (0x15)
	BP21_997_138_4400_opBand (0x16)
	BP22_998_138_4400_opBand(0x16)
	BP23_998_138_16000 (0x17)
	BP24_998_3B_8KHZ (0x18)
	BP25_998_138_17600 (0x19)
	BP26_CH1_3 (0x1A)
	BP27_CH1_4 (0x1B)

VDSL Parameters Accepted Values

Parameter	Accepted Values
framing-mode	HDLC – 0x80 AUTO – 0x90 ATM – 0x00
band-mod	Bit 0, 1: Tx Cfg band 1- All tones on 2- All tones below 640 Khz are turned off 3- All tones below 1.1 Mhz are turned off Bit 2,3: Not used Bit 4,5: Rx Cfg band 1- All tones on 2- All tones below 640 Khz are turned off 3- All tones below 1.1 Mhz are turned off Bit 6, 7:Optional band 0- No Optional band 1- ANNEX_A_6_32 (ie. 25KHz to 138 KHz) 2- ANNEX_B_32_64 (ie. 138 KHz to 276 KHz) 3- ANNEX_B_6_64 (ie. 25KHz to 276 KHz)
port-option	Bit [0]: I 43 G.hs carrier set. Bit [1]: V 43 G.hs carrier set. Bit [2]. A 43 G.hs carrier set. Bit [3]: B 43 G.hs carrier set. Bit[4:7]: shall be set to 0.
power-mode	0: 8.5dBm power output 1: 11.5 dBm power output
tx-filter	0: using internal filter in Tx path 1: using K1 external filter in Tx path (for Korea VLR Application) 2: using U1 external filter in Tx path (for US / Korea VLR Application) 3: using H1 external filter in Tx path (for 100/100 Application)

VDSL Parameters Accepted Values

Parameter	Accepted Values
rx-filter	0: using internal filter in Rx path 1: using K1 external filter in Rx path (for Korea VLR Application) 2: using U1 external filter in Rx path (for US / Korea VLR Application) 3: using H1 external filter in Rx path (for 100/100 Application)
dying-gasp	Dying Gasp is a message sent from CPE to CO using the indicator bit. It indicates that the CPE is experiencing an impending loss of power. Off: Dying Gasp off (don't send a message to CO). On: Dying Gasp on.

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 Motorola 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.

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.

-----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. **H**ash-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.

-----I-----

IKE. **I**nternet **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 Motorola 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. **I**nternet **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.

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.

STATEFUL. The Motorola 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 Motorola 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 Motorola 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.

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.

-----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.

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 Pocket Modems: 8.5 cm (w) x 4.5 cm (d) x 2 cm (h); 3.375” (w) x 1.75” (d) x .875” (h)
2200-Series Modems: 1.06"(2.69 cm) H, 4.36" (11.07 cm) W, 5.71"(14.50 cm) L
2200-Series Wireless Models: 1.2"(3.0cm) H, 8.7" (22.0 cm) W, 5.2"(13.2cm) L

Communications interfaces: The Motorola Netopia® 2200 and 3300 Series 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 802.11 wireless LAN transmitter.

Power requirements

- 12 VDC input
- **USB-powered models only:** For Use with Listed I.T.E. Only

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: PPPoE, DHCP, static IP address

Security: PAP, CHAP, UI password security, IPsec, Secure Sockets Layer (SSL) certificates

Management/configuration methods: HTTP (Web server), Telnet, SNMP, TR-069

Diagnostics: Ping, event logging, routing table displays, statistics counters, web-based management

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 Motorola 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 Motorola Netopia® 2200 and 3300 Series 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 Motorola, 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.

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 Motorola Netopia® 2200 or 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 Motorola Netopia® 2200 or 3300 Series router, for repair or warranty information, please contact:

Motorola 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 Motorola 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 Motorola Netopia® 2200 or 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.

Copyright Acknowledgments

Because Motorola has included certain software source code in this product, Motorola includes the following text required by the respective copyright holders:

Portions of this software are based in part on the work of the following:

Copyright (c) 1998-2005 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

(http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project

for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Portions of this software are based in part on the work of the following:

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are based in part on the work of the following:

Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.

<<RSA Data Security, Inc. MD5 Message-Digest Algorithm>>

License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message Digest Algorithm” in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.

<<RSA Data Security, Inc. MD4 Message-Digest Algorithm>>

License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD4 Message Digest Algorithm” in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm” in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Portions of this software are based in part on the work of the following:

Copyright (c) 1989 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are based in part on the work of the following:

Copyright 2000, 2001 Shane Kerr. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

Motorola Netopia® 2200-, 3300- or 7000-series

Motorola, Inc.
6001 Shellmound Street
Emeryville, CA 94608

October, 2007