

Administrator's Handbook

Embedded Software Version 7.7.4

Motorola Netopia® 2200, 3300 and 7000 Series Gateways



MOTOROLA



Copyright

Copyright © 2007 by Motorola, Inc.

All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without written permission from Motorola, Inc.

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.

Part Number

6161244-00-01

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 (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLey License

/Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (ey@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 MERCHANTABILITY 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.

Table of Contents

CHAPTER 1	<i>Introduction</i>	13
	What's New in 7.7.4	13
	About Motorola Netopia® Documentation	15
	Intended Audience	15
	Documentation Conventions	15
	General	15
	Internal Web Interface	16
	Command Line Interface	16
	Organization	17
	A Word About Example Screens	17
CHAPTER 2	<i>Basic Mode Setup</i>	19
	Important Safety Instructions	20
	POWER SUPPLY INSTALLATION	20
	TELECOMMUNICATION INSTALLATION	20
	PRODUCT VENTILATION	20
	Wichtige Sicherheitshinweise	21
	NETZTEIL INSTALLIEREN	21
	INSTALLATION DER TELEKOMMUNIKATION	21
	Setting up the Motorola Netopia® Gateway	22
	Microsoft Windows:	22
	Macintosh MacOS 8 or higher or Mac OS X:	24
	Configuring the Motorola Netopia® Gateway	25
	MiAVo VDSL and Ethernet WAN models Quickstart	25
	PPPoE Quickstart	27
	Set up the Motorola Netopia® Pocket Gateway	28
	Motorola Netopia® Gateway Status Indicator Lights	30
	Home Page - Basic Mode	31
	Manage My Account	33
	Status Details	34
	Enable Remote Management	35
	Expert Mode	36
	Update Firmware	37
	Factory Reset	38
CHAPTER 3	<i>Expert Mode</i>	39
	Accessing the Expert Web Interface	39
	Open the Web Connection	39
	Home Page - Expert Mode	41

- Home Page - Information 41
- Toolbar **43**
- Navigating the Web Interface **43**
 - Breadcrumb Trail 43
- Restart **44**
 - Alert Symbol 45
- Help **46**
- Configure **47**
 - Quickstart 47
 - How to Use the Quickstart Page 47
 - Setup Your Gateway using a PPP Connection 47
 - LAN 49
 - Wireless 53
 - Privacy 54
 - Advanced 56
 - About Closed System Mode 57
 - WPA Version Allowed 59
 - Multiple SSIDs 59
 - WiFi Multimedia 62
 - Wireless MAC Authorization 63
 - Use RADIUS Server 65
 - WAN 67
 - PPP over Ethernet interface 67
 - Advanced: 69
 - Ethernet WAN interface 70
 - WAN Ethernet and VDSL Gateways 73
 - ADSL Gateways 73
 - Advanced 78
 - IP Static Routes 79
 - IP Static ARP 81
 - Pinholes 82
 - Configure Specific Pinholes 82
 - Planning for Your Pinholes 82
 - Example: A LAN Requiring Three Pinholes 82
 - Pinhole Configuration Procedure 84
 - IPMaps 87
 - Configure the IPMaps Feature 87
 - FAQs for the IPMaps Feature 87
 - What are IPMaps and how are they used? 87
 - What types of servers are supported by IPMaps? 87
 - Can I use IPMaps with my PPPoE or PPPoA connection? 87
 - Will IPMaps allow IP addresses from different subnets to be assigned to my Gateway? 87
 - IPMaps Block Diagram 88
 - Default Server 89
 - Configure a Default Server 89
 - Typical Network Diagram 89
 - NAT Combination Application 90
 - IP-Passthrough 90
 - A restriction 91
 - Differentiated Services 92
 - DNS 95
 - DHCP Server 96
 - RADIUS Server 97

SNMP	98
IGMP (Internet Group Management Protocol)	100
UPnP	102
LAN Management	103
Ethernet Bridge	104
Configuring for Bridge Mode	105
VLAN	107
Overview	107
Ethernet Switching/Policy Setup	108
Example	116
VoIP	120
System	124
Syslog Parameters	125
Log Event Messages	126
Internal Servers	129
Software Hosting	130
List of Supported Games and Software	131
Rename a User(PC)	132
Backup	133
Manual options	133
Automatic options	134
Ethernet MAC Override	136
Clear Options	137
Time Zone	138
Security	139
Passwords	140
Create and Change Passwords	140
Firewall	142
Use a Motorola Netopia® Firewall	142
BreakWater Basic Firewall	142
Configuring for a BreakWater Setting	142
TIPS for making your BreakWater Basic Firewall Selection	143
Basic Firewall Background	143
IPSec	146
SafeHarbour IPSec VPN	147
Configuring a SafeHarbour VPN	148
Parameter Descriptions	151
Stateful Inspection	154
Stateful Inspection Firewall installation procedure	154
Exposed Addresses	155
Stateful Inspection Options	157
Open Ports in Default Stateful Inspection Installation	157
Firewall Tutorial	158
General firewall terms	158
Basic IP packet components	158
Basic protocol types	158
Firewall design rules	159
Firewall Logic	159
Implied rules	160
Example filter set page	160
Filter basics	161
Example network	161
Example filters	161
Example 1	161
Example 2	162

Example 3	162
Example 4	162
Example 5	162
Packet Filter	163
What's a filter and what's a filter set?	163
How filter sets work	164
Filter priority	164
How individual filters work	165
A filtering rule	165
Parts of a filter	165
Port numbers	165
Port number comparisons	166
Other filter attributes	166
Putting the parts together	167
Filtering example #1	167
Filtering example #2	169
Design guidelines	169
An approach to using filters	170
Working with IP Filters and Filter Sets	171
Adding a filter set	171
Adding filters to a filter set	172
Viewing filters	175
Modifying filters	175
Deleting filters	175
Moving filters	175
Deleting a filter set	175
Associating a Filter Set with an Interface	176
Policy-based Routing using Filtersets	177
TOS field matching	177
Security Log	179
Using the Security Monitoring Log	179
Timestamp Background	181
Install	182
Install Software	183
Updating Your Gateway's Motorola Netopia® Firmware Version	183
Step 1: Required Files	183
Step 2: Motorola Netopia® firmware Image File	184
Install Key	187
Use Motorola Netopia® Software Feature Keys	187
Obtaining Software Feature Keys	187
Procedure - Install a New Feature Key File	187
To check your installed features:	189
Install Certificate	190

CHAPTER 4 *Basic Troubleshooting* **193**

Status Indicator Lights	194
LED Function Summary Matrix	204
Factory Reset Switch	206

CHAPTER 5 *Advanced Troubleshooting* **207**

Home Page 208
Expert Mode 210
System Status 211
Ports: Ethernet 212
Ports: DSL 213
IP: Interfaces 214
DSL: Circuit Configuration 215
System Log: Entire 216
Diagnostics 217
Network Tools 218

CHAPTER 6 *Command Line Interface* **223**

Overview **224**
Starting and Ending a CLI Session **226**
 Logging In 226
 Ending a CLI Session 226
 Saving Settings 226
Using the CLI Help Facility **226**
About SHELL Commands **227**
 SHELL Prompt 227
 SHELL Command Shortcuts 227
SHELL Commands **228**
 Common Commands 228
 WAN Commands 239
About CONFIG Commands **240**
 CONFIG Mode Prompt 240
 Navigating the CONFIG Hierarchy 240
 Entering Commands in CONFIG Mode 241
 Guidelines: CONFIG Commands 241
 Displaying Current Gateway Settings 242
 Step Mode: A CLI Configuration Technique 242
 Validating Your Configuration 242
CONFIG Commands **243**
 Remote ATA Configuration Commands 243
 DSL Commands 245
 ATM Settings 245
 Bridging Settings 246
 Common Commands 247
 DHCP Settings 248
 Common Commands 248
 DHCP Generic Options 249
 DHCP Option Filtering 252
 Example 253
 DMT Settings 254
 DSL Commands 254
 Domain Name System Settings 255
 Common Commands 255
 Dynamic DNS Settings 256
 IGMP Settings 257

IP Settings	259
Common Settings	259
ARP Timeout Settings	259
DSL Settings	259
Ethernet LAN Settings	261
Additional subnets	262
Default IP Gateway Settings	263
IP-over-PPP Settings	263
Static ARP Settings	266
IGMP Forwarding	266
IPsec Passthrough	266
IP Prioritization	266
Differentiated Services (DiffServ)	267
Packet Mapping Configuration	269
Queue Configuration	271
Basic Queue	272
Weighted Fair Queue	273
Priority Queue	274
Funnel Queue	275
Interface Queue Assignment	275
SIP Passthrough	276
RTSP Passthrough	276
Static Route Settings	276
IPMaps Settings	277
Network Address Translation (NAT) Default Settings	278
Network Address Translation (NAT) Pinhole Settings	278
PPPoE /PPPoA Settings	279
Configuring Basic PPP Settings	279
Configuring Port Authentication	281
PPPoE with IPoE Settings	282
Ethernet WAN platforms	282
ADSL platforms	283
Ethernet Port Settings	283
802.3ah Ethernet OAM Settings	284
Command Line Interface Preference Settings	285
Port Renumbering Settings	286
Security Settings	287
Firewall Settings (for BreakWater Firewall)	287
SafeHarbour IPsec Settings	287
Internet Key Exchange (IKE) Settings	291
Stateful Inspection	292
Example:	293
Packet Filtering Settings	294
Example:	296
SNMP Settings	297
SNMP Notify Type Settings	297
System Settings	298
Syslog	301
Default syslog installation procedure	302
Wireless Settings (supported models)	303
Wireless Multi-media (WMM) Settings	306
Wireless Privacy Settings	308
Wireless MAC Address Authorization Settings	309
RADIUS Server Settings	310
VLAN Settings	311
Example 1:	312

Example 2:	313
VoIP settings	316
Example	320
UPnP settings	321
DSL Forum settings	321
TR-064	321
TR-069	322
Backup IP Gateway Settings	323
VDSL Settings	325
VDSL Parameter Defaults	325
VDSL Parameters Accepted Values	327

CHAPTER 7 *Glossary* **331**

----A----	331
----B----	332
----C----	332
----D----	333
----E----	334
----F----	335
----H----	335
----I----	336
----K----	336
----L----	336
----M----	337
----N----	337
----P----	338
----Q----	338
----R----	339
----S----	339
----T----	340
----U----	341
----V----	341
----W----	341
----X----	341

CHAPTER 8 *Technical Specifications and Safety Information* **343**

Description	343
Dimensions:	343
Communications interfaces:	343
Power requirements	343
Environment	343
Operating temperature:	343
Storage temperature:	343
Relative storage humidity:	343
Software and protocols	343
Software media:	343
Routing:	343
WAN support:	343
Security:	343
Management/configuration methods:	344
Diagnostics:	344
Agency approvals	344

North America	344
International	344
Regulatory notices	344
European Community	344
Manufacturer's Declaration of Conformance	344
United States	345
Service requirements	345
Canada	345
Declaration for Canadian users	345
Caution	346
Important Safety Instructions	346
Australian Safety Information	346
Caution	346
Caution	346
Telecommunication installation cautions	346
47 CFR Part 68 Information	347
FCC Requirements	347
FCC Statements	347
Electrical Safety Advisory	348
Copyright Acknowledgments	348

CHAPTER 9 *Overview of Major Capabilities* 351

Wide Area Network Termination	351
PPPoE/PPPoA (Point-to-Point Protocol over Ethernet/ATM)	351
Instant-On PPP	352
Simplified Local Area Network Setup	352
DHCP (Dynamic Host Configuration Protocol) Server	352
DNS Proxy	353
Management	353
Embedded Web Server	353
Diagnostics	353
Security	354
Remote Access Control	354
Password Protection	354
Network Address Translation (NAT)	354
Motorola Netopia® Advanced Features for NAT	355
Internal Servers	355
Pinholes	356
Default Server	356
Combination NAT Bypass Configuration	356
IP-Passthrough	356
VPN IPSec Pass Through	357
VPN IPSec Tunnel Termination	357
Stateful Inspection Firewall	358
SSL Certificate Support	358
VLANs	358

Index 359

CHAPTER 1 Introduction

What's New in 7.7.4

New in Motorola Netopia® Embedded Software Version 7.7.4 are the following features:

- Internet Group Management Protocol (IGMP) Version 3 support.
See [“IGMP \(Internet Group Management Protocol\)” on page 100](#).
- TR-101 Support:
 - Concurrent support for PPPoE and IPoE connections on the WAN.
See [“WAN” on page 67](#).
 - Multiple LAN IP Subnet support. See [“LAN” on page 49](#).
 - Additional DHCP range support. These ranges are associated with the additional LAN subnets on a 1-to-1 basis.
 - DHCP option filtering support. Allows DHCP option data to be used to determine the desired DHCP address range. See [“DHCP Option Filtering” on page 252](#).
 - Support for additional WAN settings to control multicast forwarding as well as if 0.0.0.0 is used as the source address for IGMP packets.
See [“Advanced:” on page 69](#).
 - Support for “unnumbered” interfaces. For IP interfaces, this allows the address to be set to 0 and the DHCP client also to be disabled. See [page 71](#).
- PPPoE/DHCP Autosensing. See [“WAN” on page 67](#).
- Wireless Multimedia Mode (WMM) support. See [“WiFi Multimedia” on page 62](#).
- Firewall: ClearSailing is automatically enabled on all 2200-Series ADSL2+ platforms. (Explicit exceptions: bonded and VDSL2, 3341, and 3387WG.) See [“Firewall” on page 142](#).
- TR-069 Remote device management is automatically enabled by default for 2200-Series Gateways. (Explicit exceptions: bonded and VDSL2, 3341, 3387WG). See [“TR-069” on page 322](#).
- Voice-over-IP (VoIP) Support using Session Initiation Protocol (SIP) for supported models. See [“VoIP” on page 120](#) and VoIP CLI [“VoIP settings” on page 316](#).
- Support of VLAN ID 0 on the Ethernet WAN and support for setting p-bits on a segment/port basis; inter-VLAN groups. See [“VLAN” on page 107](#) and CLI [“VLAN Settings” on page 311](#).
- Backup IP Gateway Support. See [“Backup” on page 133](#) and CLI [“Backup IP Gateway Settings” on page 323](#).

Corresponding commands have been added to the Command Line Interface (CLI). See [“Command Line Interface” on page 223](#).

- Reset WAN port and wireless counter and CLI command to display individual Ethernet port statistics.
See [“reset enet \[all \]” on page 231](#) and [“show enet \[all \]” on page 233](#).
- CLI for Motorola Netopia® ATA Remote Management.
See [“Remote ATA Configuration Commands” on page 243](#).

- Provide Bandwidth Management using Weighted Fair Queueing. See [“Queue Configuration” on page 271](#).
- New CLI command for disabling Dying Gasp. See [“DMT Settings” on page 254](#).
- Ethernet in the First Mile Operations Administration and Maintenance (802.3ah EFM OAM) Support. See [“802.3ah Ethernet OAM Settings” on page 284](#).
- IP multicast to layer 2 unicast mapping. See [“IGMP Settings” on page 257](#).
- Real Time Streaming Protocol (RTSP) ALG support for Video-on-Demand (VoD) Services. See [“RTSP Passthrough” on page 276](#).

About Motorola Netopia® Documentation



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.

Motorola, Inc. provides a suite of technical information for its 2200-, 3300- and 7000-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 Motorola's Netopia website:

<http://www.netopia.com/>

Intended Audience

This guide is targeted primarily to residential service subscribers.

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

[See "Expert Mode" on page 39.](#)

Documentation Conventions

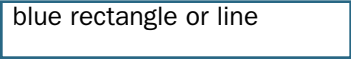

General

This manual uses the following conventions to present information:

Convention (Typeface)	Description
<i>bold italic</i>	Menu commands
<i>monospaced</i>	
<u><i>bold italic sans serif</i></u>	Web GUI page links and button names

<code>terminal</code>	Computer display text
bold terminal	User-entered text
<i>Italic</i>	Italic type indicates the complete titles of manuals.

Internal Web Interface

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

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
<i>italic terminal type face</i>	Variables for which you supply your own values

Organization

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

- **Chapter 1, “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 2, “Basic Mode Setup”** — Describes how to get up and running with your Motorola Netopia® Gateway.
- **Chapter 3, “Expert Mode”** — Focuses on the “Expert Mode” Web-based user interface for advanced users. It is organized in the same way as the Web UI is organized. As you go through each section, functions and procedures are discussed in detail.
- **Chapter 4, “Basic Troubleshooting”** — Gives some simple suggestions for troubleshooting problems with your Gateway’s initial configuration.
- **Chapter 5, “Advanced Troubleshooting”** — Gives suggestions and descriptions of expert tools to use to troubleshoot your Gateway’s configuration.
- **Chapter 6, “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 7, “Glossary”**
- **Chapter 8, “Technical Specifications and Safety Information”**
- **Chapter 9, “Overview of Major Capabilities”** — Presents a product description summary.
- **Index**

A Word About Example Screens

This manual contains many example screen illustrations. Since Motorola Netopia® 2200-, 3300- and 7000-Series Gateways offer a wide variety of features and functionality, the example screens shown may not appear exactly the same for your particular Gateway or setup as they appear in this manual. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.

CHAPTER 2 Basic Mode Setup

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

This section covers:

- [“Important Safety Instructions” on page 20](#)
- [“Wichtige Sicherheitshinweise” on page 21](#) (German)
- [“Setting up the Motorola Netopia® Gateway” on page 22](#)
- [“Configuring the Motorola Netopia® Gateway” on page 25](#)
- [“Motorola Netopia® Gateway Status Indicator Lights” on page 30](#)
- [“Home Page - Basic Mode” on page 31](#)

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.

(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.

PRODUCT VENTILATION

The Motorola Netopia® Gateway is intended for use in a consumer's home. Ambient temperatures around this product should not exceed 104°F (40°C). It should not be used in locations exposed to outside heat radiation or trapping of its own heat. The product should have at least one inch of clearance on all sides except the bottom when properly installed and should not be placed inside tightly enclosed spaces unless proper ventilation is provided.

SAVE THESE INSTRUCTIONS

Wichtige Sicherheitshinweise

NETZTEIL INSTALLIEREN

Verbinden Sie das Kabel vom Netzteil mit dem Power-Anschluss an dem Motorola Netopia® Gateway. Stecken Sie dann das Netzteil in eine Netzsteckdose.



Achtung:

Abhängig von dem mit dem Produkt gelieferten Netzteil, entweder die direkten Stecker-netzgeräte, Stecker vom Netzkabel oder der Gerätekoppler dienen als Hauptspannungsunterbrechung. Es ist wichtig, dass das Steckernetzgerät, Steckdose oder Gerätekoppler frei zugänglich sind.

(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

INSTALLATION DER TELEKOMMUNIKATION

Wenn Ihre Telefonausrüstung verwendet wird, sollten grundlegende Sicherheitsanweisungen immer befolgt werden, um die Gefahr eines Feuers, eines elektrischen Schlages und die Verletzung von Personen, zu verringern. Beachten Sie diese weiteren Hinweise:

- Benutzen Sie dieses Produkt nicht in Wassernähe wie z.B. nahe einer Badewanne, Waschschüssel, Küchenspüle, in einem nassen Keller oder an einem Swimmingpool.
- Vermeiden Sie das Telefonieren (gilt nicht für schnurlose Telefone) während eines Gewitters. Es besteht die Gefahr eines elektrischen Schlages durch einen Blitz.
- Nicht das Telefon benutzen um eine Gasleckstelle zu Melden, wenn Sie sich in der Nähe der Leckstelle befinden.

Bewahren Sie diese Anweisungen auf

Setting up the Motorola Netopia® Gateway

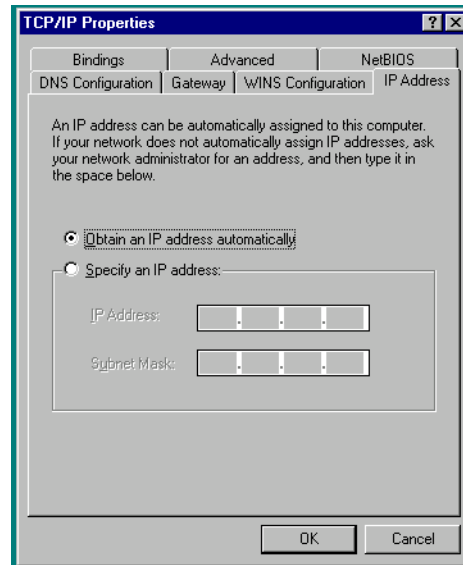
Refer to your *Quickstart Guide* for instructions on how to connect your Motorola Netopia® gateway to your power source, PC or local area network, and your Internet access point, whether it is a dedicated DSL outlet or a DSL or cable modem. Different Motorola Netopia® Gateway models are supplied for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

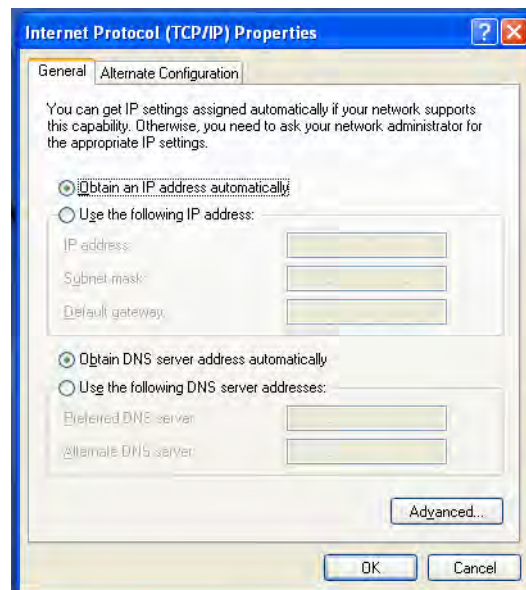
a. Some Windows versions follow a path like this:

Start menu -> **Settings** -> **Control Panel** -> **Network** (or **Network and Dial-up Connections** -> **Local Area Connection** -> **Properties**) -> **TCP/IP** [**your_network_card**] or **Internet Protocol [TCP/IP]** -> **Properties**



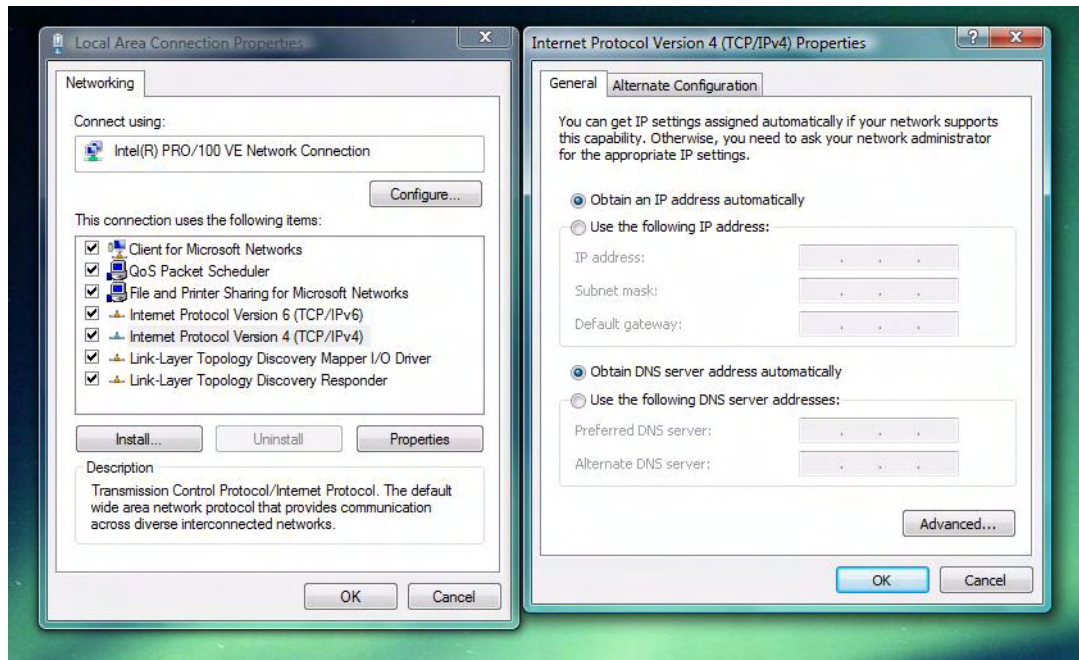
b. Some Windows versions follow a path like this:

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



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.



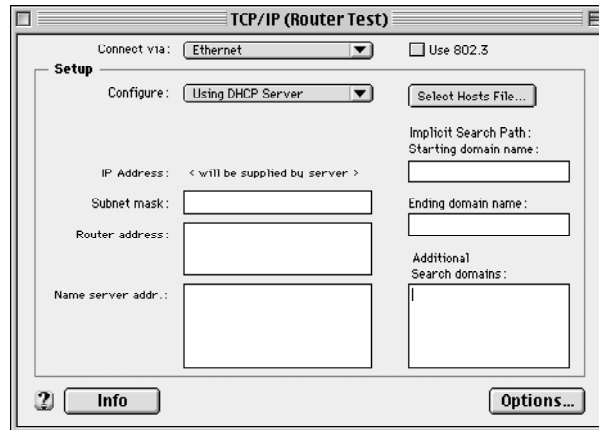
The **Internet Protocol Version 4 (TCP/IPv4) Properties** window should appear as shown.

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

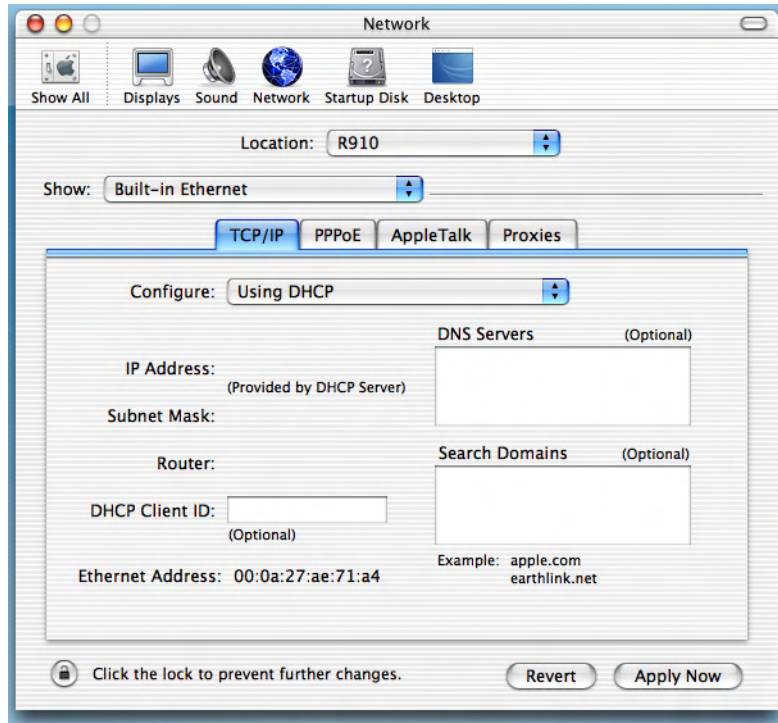
Macintosh MacOS 8 or higher or Mac OS X:

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

- a. MacOS follows a **Apple Menu -> Control Panels -> TCP/IP** Control Panel



- b. Mac OS X follows a **Apple Menu -> System Preferences -> Network** path like this:



Then go to Step 2.

Step 2. Select *Built-in Ethernet*

Step 3. Select *Configure Using DHCP*

Step 4. Close and Save, if prompted.

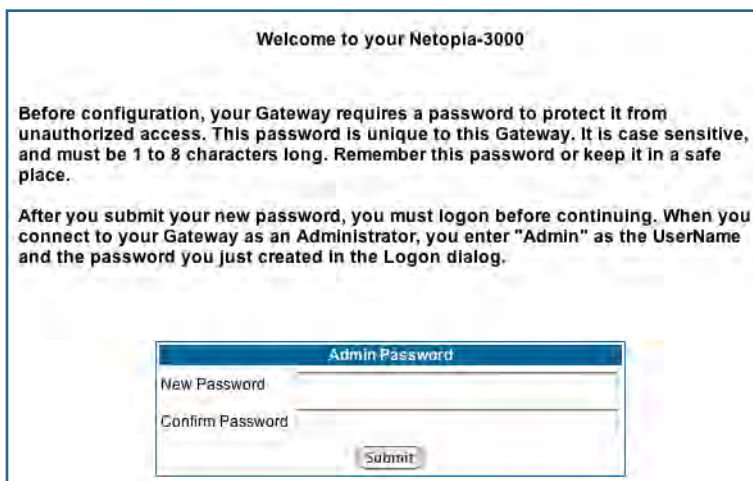
Proceed to [“Configuring the Motorola Netopia® Gateway”](#) on page 25.

Configuring 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://192.168.1.254> in the Location text box.

The Admin Password page appears.



Welcome to your Netopia-3000

Before configuration, your Gateway requires a password to protect it from unauthorized access. This password is unique to this Gateway. It is case sensitive, and must be 1 to 8 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 Gateway as an Administrator, you enter "Admin" as the UserName and the password you just created in the Logon dialog.

Admin Password

New Password

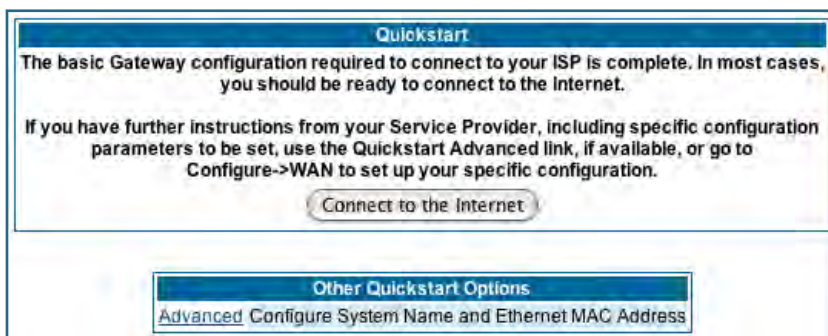
Confirm Password

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.
For the security of your connection, an Admin password must be set on the Motorola Netopia® unit.

MiAVo VDSL and Ethernet WAN models Quickstart

The browser then displays the Quickstart page.



Quickstart

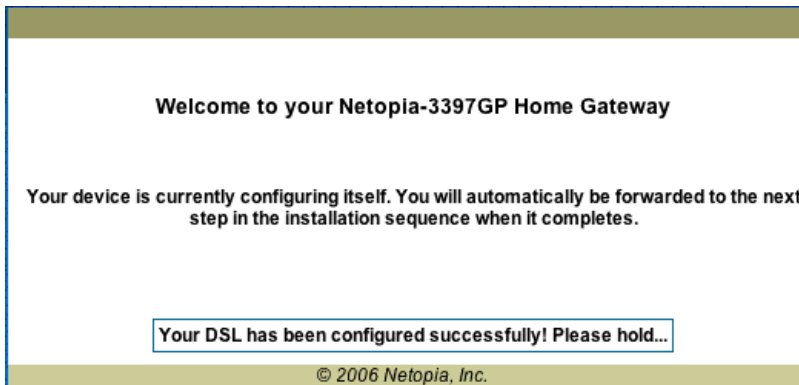
The basic Gateway configuration required to connect to your ISP is complete. In most cases, you should be ready to connect to the internet.

If you have further instructions from your Service Provider, including specific configuration parameters to be set, use the Quickstart Advanced link, if available, or go to Configure->WAN to set up your specific configuration.

Other Quickstart Options

[Advanced Configure System Name and Ethernet MAC Address](#)

2. Click the **Connect to the Internet** button.



Once a connection is established, your browser is redirected to your service provider's home page or a registration page on the Internet.



NOTE:

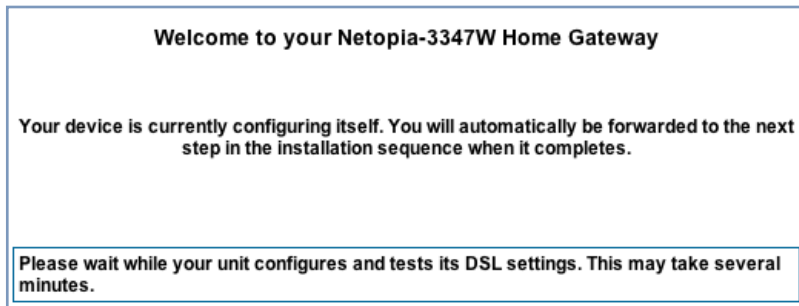
For MiAVo Series (3397GP) models, skip the rest of this section.

Congratulations! Your configuration is complete.

You can skip to [“Home Page - Basic Mode” on page 31](#).

PPPoE Quickstart

For a PPPoE connection, your browser will display a different series of web pages:



The browser then displays the Quickstart web page.

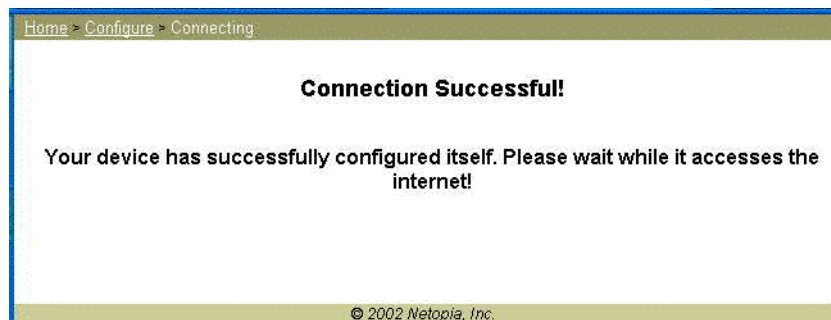
The screenshot shows a web page titled "Quickstart" with a blue header. It contains two input fields: "ISP Username" and "ISP Password". Below these fields is a button labeled "Connect to the Internet".

3. **Enter the username and password supplied by your Internet Service Provider. Click the *Connect to the Internet* button.**

Once you enter your username 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.

The Gateway displays a message while it configures itself.

4. **When the connection succeeds, your browser will display a success message.**



Once a connection is established, your browser is redirected to your service provider's home page or a registration page on the Internet.

5. **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.**

Set up the Motorola Netopia® Pocket Gateway

Your Motorola Netopia® 3342N/3352N Pocket Gateway comes with its own installation wizard.

- If you are using Windows 98, insert the CD.
- If you are using Windows XP, Windows 2000, Windows NT or Windows Vista, you don't even need the CD.

Follow these easy setup steps:

1. **Plug the Motorola Netopia® Pocket Gateway into a USB port on your PC.**
2. **Whether you use the CD (Windows 98) or not (all other Windows versions), on Windows-based PCs, the Motorola Netopia® Installation Wizard will launch automatically.**

The Motorola Netopia® Installation Wizard will assist you to configure your PC to work with the Motorola Netopia® pocket Gateway. Follow the on-screen instructions.

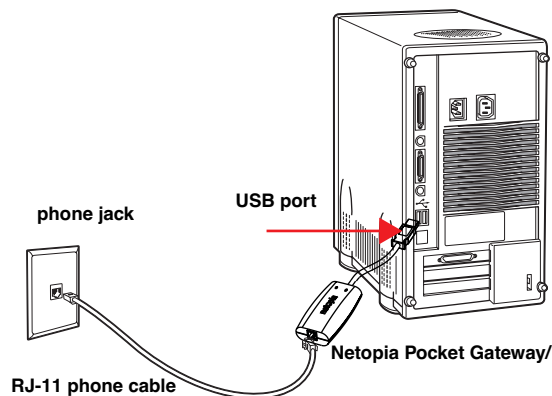


To proceed, click the [Next](#) button.

The Motorola Netopia® Installation Wizard performs a series of checks on your system and then will install USB drivers for your connection.

3. **Place the Motorola Netopia® Pocket Gateway near your PC so you can see it easily.**
Make sure any cables are kept away from power cords, fluorescent lighting fixtures, and other sources of electrical interference.
4. **When the wizard prompts you, connect the RJ-11 Telephone Cable from the DSL port on the Motorola Netopia® Pocket Gateway to the ADSL phone jack.**

The **DSL** indicator light should blink for up to two minutes and then come on solid green once the device is connected to your computer.



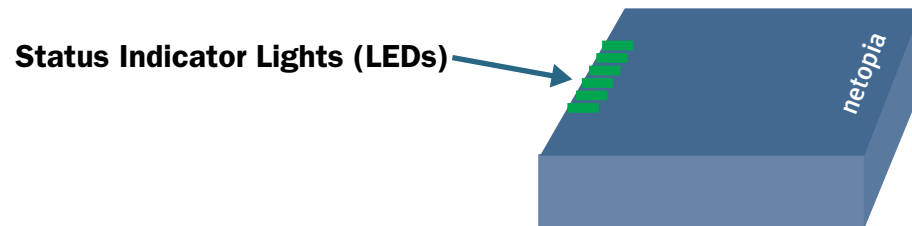
The Wizard displays a success message when the settings are configured.

5. **The Motorola Netopia® Installation Wizard will then launch your web browser and display the *Welcome* page where you configure your Motorola Netopia® Pocket Gateway.**

Motorola Netopia® Gateway Status Indicator Lights

Colored LEDs on your Motorola Netopia® Gateway indicate the status of various port activity. Different Gateway models have different ports for your connections and different indicator LEDs. The *Quickstart Guide* accompanying your Motorola Netopia® Gateway describes the behavior of the various indicator LEDs.

Example status indicator lights

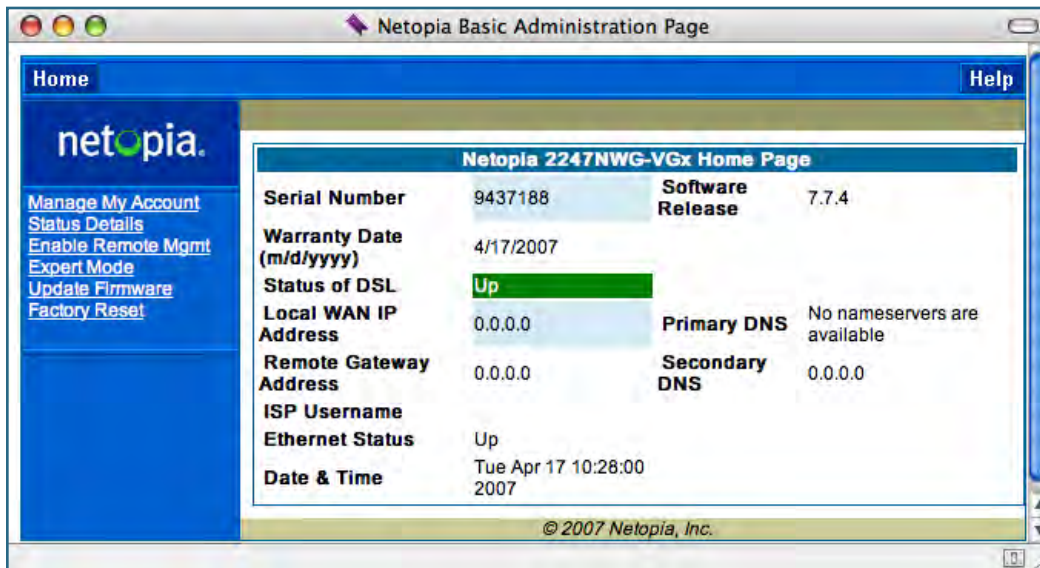


Home Page - Basic Mode

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://192.168.1.254> in your Web browser's location box.

The Basic Mode Home Page appears.



The screenshot shows a web browser window titled "Netopia Basic Administration Page". The page has a blue header with "Home" and "Help" buttons. On the left, there is a navigation menu with links: "Manage My Account", "Status Details", "Enable Remote Mgmt", "Expert Mode", "Update Firmware", and "Factory Reset". The main content area is titled "Netopia 2247NWG-VGx Home Page" and displays the following information:

Serial Number	9437188	Software Release	7.7.4
Warranty Date (m/d/yyyy)	4/17/2007		
Status of DSL	Up		
Local WAN IP Address	0.0.0.0	Primary DNS	No nameservers are available
Remote Gateway Address	0.0.0.0	Secondary DNS	0.0.0.0
ISP Username			
Ethernet Status	Up		
Date & Time	Tue Apr 17 10:28:00 2007		

© 2007 Netopia, Inc.



VoIP-enabled Gateways also display VoIP phone information, as well.

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

Item	Description
Serial Number	This is the unique serial number of your Gateway.
Software Release	This is the version number of the current embedded software in your Gateway.
Warranty Date	This is the date that your Gateway was installed and enabled.
Status of DSL	DSL connection (Internet) is either Up or Down
Status of Connection	'Waiting for DSL' is displayed while the Gateway is training. This should change to 'Up' within two minutes. 'Up' is displayed when the ADSL line is synched and the PPPoE session is established. 'Down' indicates inability to establish a connection; possible line failure.
Local WAN IP Address	This is the negotiated address of the Gateway's WAN interface. This address is usually dynamically assigned.
Remote Gateway Address	This is the negotiated address of the remote router to which this Gateway is connected.
Primary DNS Secondary DNS	These are the negotiated DNS addresses.
ISP Username	This is your PPPoE username as assigned by your service provider.
Ethernet Status	(if so equipped) Local Area Network (Ethernet) is either Up or Down
USB Status	If your Gateway is so equipped, Local Area Network (USB) is either Up or Down
Line 1/2 Registration	If your Gateway is so equipped, voice Line 1 and/or 2 is either Idle or Connected
Date & Time	This is the current UTC time; blank if this is not available due to lack of a network connection.

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.

Link: Manage My Account

You can change your ISP account information for the Motorola Netopia® Gateway. You can also manage other aspects of your account on your service provider's account management Web site.

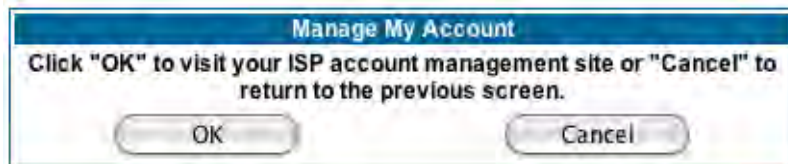
Click on the [**Manage My Account**](#) link. The Manage My Account page appears.



The screenshot shows a web form titled "My Account Update" with a blue header. Below the header, the text reads: "If you want to change your account information, please enter the new information here. Click 'Submit' to update your account username and/or password and reconnect to the Internet." The form contains a sub-section titled "ISP Account Information" with three input fields: "Username", "New Password", and "Confirm Password". A "Submit" button is located at the bottom of this section.

If you have a PPPoE account, enter your username, and then your new password. Confirm your new password. For security, your actual passwords are not displayed on the screen as you type. You must enter the new password twice to be sure you have typed it correctly.

Click the [**Submit**](#) button.



The screenshot shows a dialog box titled "Manage My Account" with a blue header. The text inside reads: "Click 'OK' to visit your ISP account management site or 'Cancel' to return to the previous screen." There are two buttons at the bottom: "OK" and "Cancel".

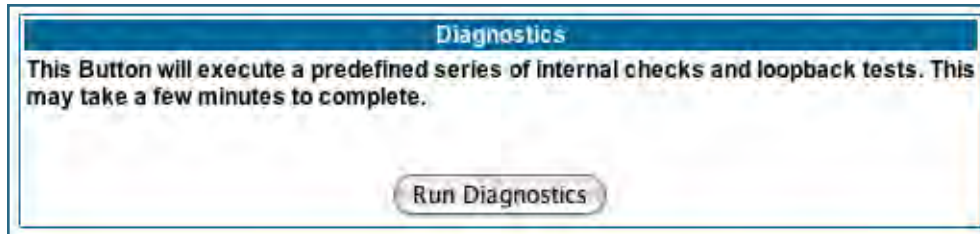
If you have a non-PPPoE account, click the [**OK**](#) button.

You will be taken to your service provider's Web site account management page.

Link: Status Details

If you need to diagnose any problems with your Motorola Netopia® Gateway or its connection to the Internet, you can run a sophisticated diagnostic tool. It checks several aspects of your physical and electronic connection and reports its results on-screen. This can be useful for troubleshooting, or when speaking with a technical support technician.

Click on the [Status Details](#) link. The Diagnostics page appears.



Click the [Run Diagnostics](#) button to run your diagnostic tests. For a detailed description of these tests, see ["Diagnostics" on page 217](#).

Link: Enable Remote Management

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.

Click the [Enable Rmt Mgmt](#) link. The Enable Remote Management page appears.

Enable Remote Management

Please enter a password for administrator access to this device, as well as a timeout value for the management session. You may leave the password entries blank to use the current administrator password. Click "OK" to enable administrator access, or "Cancel" to return to the previous screen.

Temporary Admin Password

Old Password

New Password

Confirm Password

Password Timeout 20 minutes

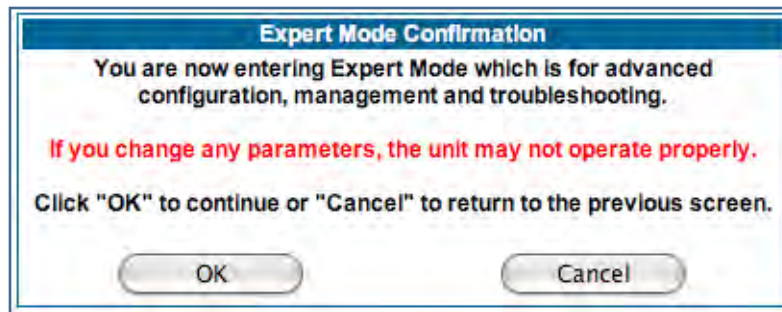
Since you've already has entered an Admin password, you can use that Admin password or enter a new password. If you enter a new password, it becomes the temporary Admin password. After the time-out period has expired, the Admin password reverts to the original Admin password you entered.

Enter a temporary password for the person you want to authorize, and confirm it by typing it again. You can select a time-out period for this password, from 5 to 30 minutes, from the pull-down menu. Be sure to tell the authorized person what the password is, and for how long the time-out is set. Click the [OK](#) button.

[Link: Expert Mode](#)

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

Click the [Expert Mode](#) link to display the Expert Mode Confirmation page.



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

Once you click the **OK** button you will be taken to the Expert Mode Home Page.

The Expert Mode Home Page is the main access point for configuring and managing the advanced features of your Gateway. See ["Expert Mode" on page 39](#) for information.

[Link: Update Firmware](#)

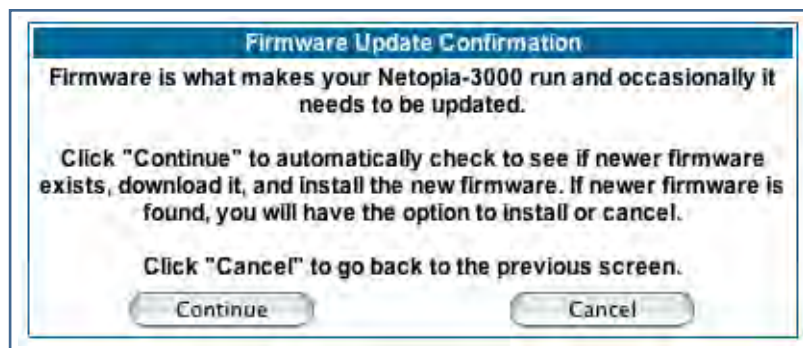


NOTE:

(This link is not available on the 3342/3352 models, since firmware updates must be upgraded via the USB host driver. 3342N/3352N models *do* support this feature.)

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

Click the [Update Firmware](#) link. The Firmware Update Confirmation page appears.

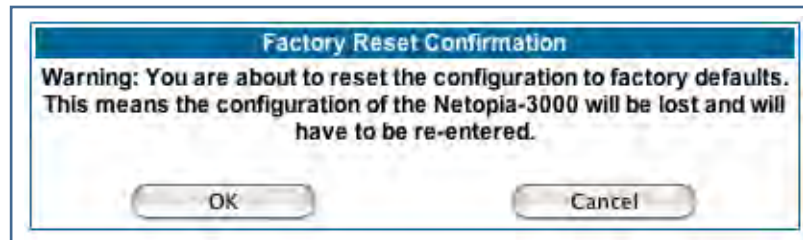


If you click the [Continue](#) button, the Gateway will check a remote Firmware Server for the latest firmware revision. If a newer version is found, your firmware will be automatically updated once you confirm the installation.

[Link: Factory Reset](#)

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

Click on [Factory Reset](#) to reset the Gateway back to its original factory default settings.



NOTE:

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

CHAPTER 3 Expert Mode

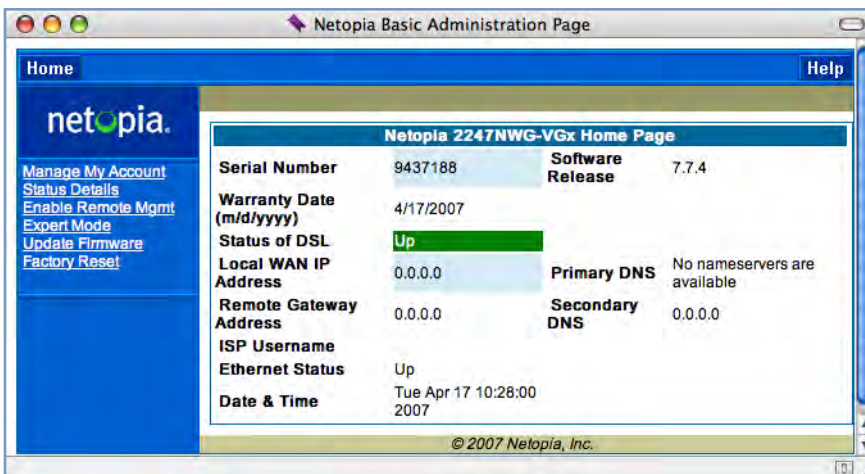
Using the Expert Mode Web-based user interface for the Motorola Netopia® 2200-, 3300- and 7000-series Gateway you can configure, troubleshoot, and monitor the status of your Gateway.

Accessing the Expert Web Interface

Open the Web Connection

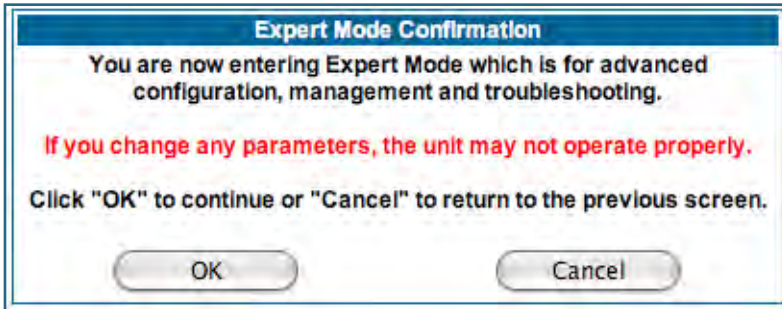
Once your Gateway is powered up, you can use any recent version of the best-known web browsers such as Netscape Navigator or Microsoft Internet Explorer from any LAN-attached PC or workstation. The procedure is:

1. **Enter the name or IP address of your Motorola Netopia® Gateway in the Web browser's window and press Return.**
For example, you would enter <http://192.168.1.254>.
2. **If an administrator or user password has been assigned to the Motorola Netopia® Gateway, enter *Admin* or *User* as the username and the appropriate password and click [OK](#).**
The Basic Mode Home Page opens.



3. **Click on the [Expert Mode](#) link in the left-hand column of links.**

You are challenged to confirm your choice.



Click **OK**.

The Home Page opens in Expert Mode.

Home Page - Expert Mode

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

General Information			
Hardware	Netopia Model 2247-41-10NA ADSL2 WIAD		
Serial Number	9437188		
Software Version	7.7.4	BreakWater Firewall	ClearSailing
Product ID	1225		
Date & Time	Fri Jun 1 10:07:20 2007	Safe Harbour	On
WAN			
Status	Up	Data Rate (Kbps)	Downstream: 8000 Upstream: 800
Local Address	0.0.0.0	Peer Address	0.0.0.0
Connection Type	Always On		
NAT	On	WAN Users	Unlimited
LAN			
IP Address	192.168.1.254		
Netmask	255.255.255.0		
DHCP Server	On	Ethernet Status	Up
		DHCP Leases	0 out of 253 leases in use
VoIP			
Line 1 Registration	Registered	Line 2 Registration	Registered
Line 1 Account	4004	Line 2 Account	4005

Home Page - Information

The Home page's center section contains a summary of the Gateway's configuration settings and operational status.

Summary Information	
Field	Status and/or Description
General Information	
Hardware	Model number and summary specification
Serial Number	Unique serial number, located on label attached to bottom of unit
Software Version	Release and build number of running Motorola Netopia® Operating System.
Product ID	Refers to internal circuit board series; useful in determining which software upgrade applies to your hardware type.
Date & Time	This is the current UTC time; blank if this is not available due to lack of a network connection.
Breakwater Firewall	<i>If the optional feature key is installed:</i> Status of the Breakwater Firewall: ClearSailing, SilentRunning, or LANdLocked.
Safe Harbour	<i>If the optional feature key is installed:</i> SafeHarbour VPN IPsec Tunnel option (if installed): either On or Off.
WAN	

Status	Wide Area Network may be Waiting for DSL (or other waiting status), Up or Down
Data Rate (Kbps)	Once connected, displays DSL speed rate, Downstream and Upstream
Local Address	IP address assigned to the WAN port.
Peer Address	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.
Connection Type	May be either Instant On or Always On.
NAT	On or Off . <i>ON</i> if using Network Address Translation to share the IP address across many LAN users.
WAN Users	Displays the number of users allotted and the total number available for use.

LAN

IP Address	Internal IP address of the Motorola Netopia® Gateway.
Netmask	Defines the IP subnet for the LAN Default is 255.255.255.0 for a Class C device
DHCP Server	On or Off . <i>ON</i> if using DHCP to get IP addresses for your LAN client machines.
DHCP Leases	A "lease" is held by each LAN client that has obtained an IP address through DHCP.
Ethernet (or USB) Status	Status of your Ethernet network connection (if supported). Up or Down .

VoIP

Line 1/2 Registration	If your Gateway is so equipped, voice Line 1 and/or 2 is either Idle or Registered
-----------------------	--

Toolbar

The toolbar is the dark blue bar at the top of the page containing the major navigation buttons. These buttons are available from almost every page, allowing you to move freely about the site.

Home	Configure	Troubleshoot	Security	Install	Restart	Help
	Quickstart	System Status	Passwords	Install Certificate		
	LAN	Network Tools	Firewall	Install Key		
	WAN	Diagnostics	IPSec	Install Software		
	Advanced		Stateful Inspection			
			Packet Filter			
			Security Log			

Navigating the Web Interface

[Link: Breadcrumb Trail](#)

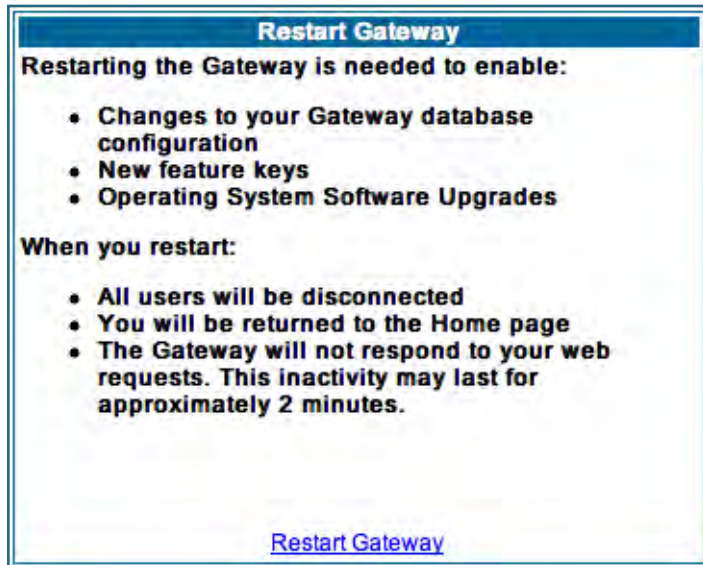
The breadcrumb trail is built in the light brown area beneath the toolbar. As you navigate down a path within the site, the trail is built from left to right. To return anywhere along the path from which you came, click on one of the links.



Restart

Button: Restart

The Restart button on the toolbar allows you to restart the Gateway at any time. You will be prompted to confirm the restart before any action is taken. The Restart Confirmation message explains the consequences of and reasons for restarting the Gateway.

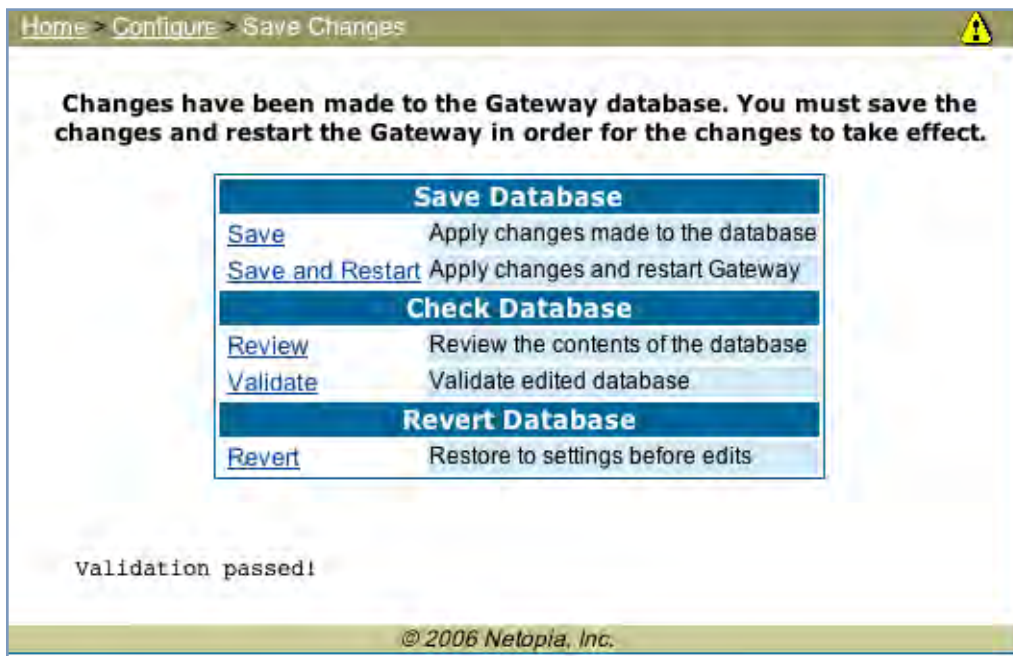


[Link: Alert Symbol](#)

The Alert symbol appears in the upper right corner if you make a database change; one in which a change is made to the Gateway's configuration. The Alert serves as a reminder that you must **Save** the changes and **Restart** the Gateway before the change will take effect. You can make many changes on various pages, and even leave the browser for up to 5 minutes, but if the Gateway is restarted before the changes are applied, they will be lost. When you click on the Alert symbol, the Save Changes page appears. Here you can select various options to save or discard these changes.



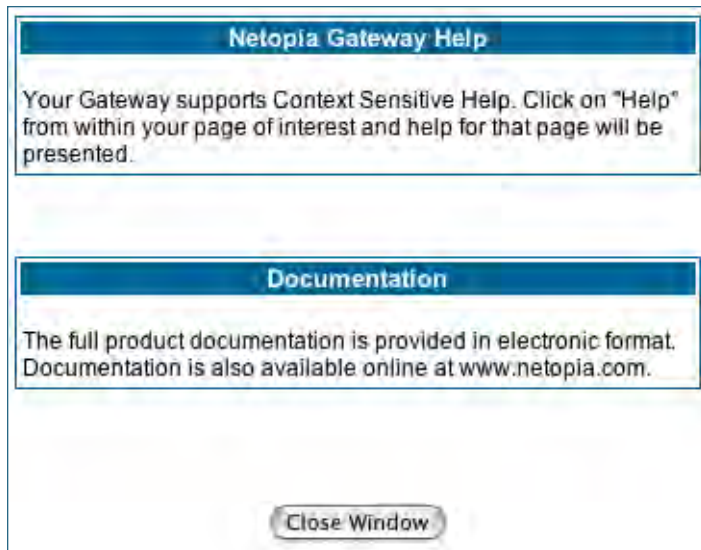
If more than one Alert is triggered, you will need to take action to clear the first Alert before you can see the second Alert.



Help

Button: [Help](#)

Context-sensitive Help is provided in your Gateway. The page shown here is displayed when you are on the Home page or other transitional pages. To see a context help page example, go to [Security -> Pass-words](#), then click [Help](#).



Configure

Button: [Configure](#)

The Configuration options are presented in the order of likelihood you will need to use them. **Quickstart** is typically accessed during the hardware installation and initial configuration phase. **Often, these settings should be changed only in accordance with information from your Service Provider. LAN and WAN** settings are available to fine-tune your system. **Advanced** provides some special capabilities typically used for gaming or small office environments, or where LAN-side servers are involved.



This button will not be available if you log on as *User*.

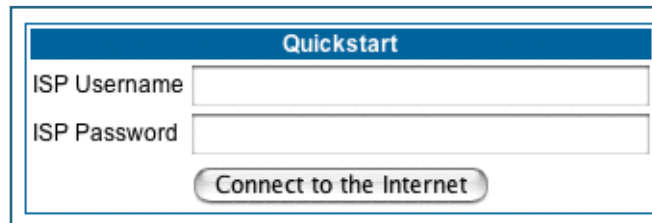
Link: [Quickstart](#)

How to Use the Quickstart Page. Quickstart is normally used immediately after the new hardware is installed. When you are first configuring your Gateway, Quickstart appears first.

(Once you have configured your Gateway, logging on displays the Home page. Thereafter, if you need to use Quickstart, choose it from the Expert Mode Configure menu.)

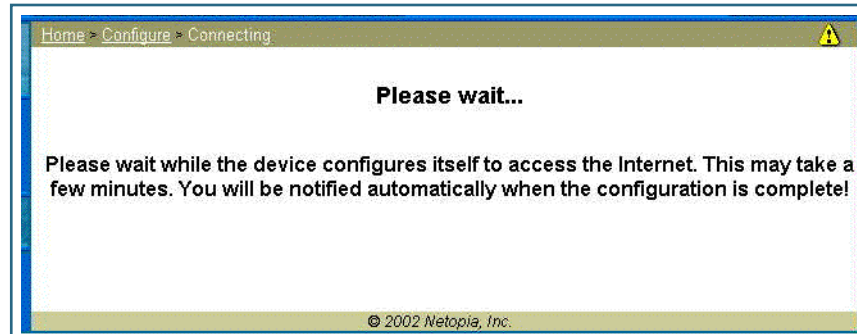
Setup Your Gateway using a PPP Connection.

This example screen is the for a **PPP Quickstart** configuration. Your gateway authenticates with the Service Provider equipment using the ISP Username and Password. These values are given to you by your Service Provider.



1. Enter your ISP Username and ISP Password.
2. Click [Connect to the Internet](#).

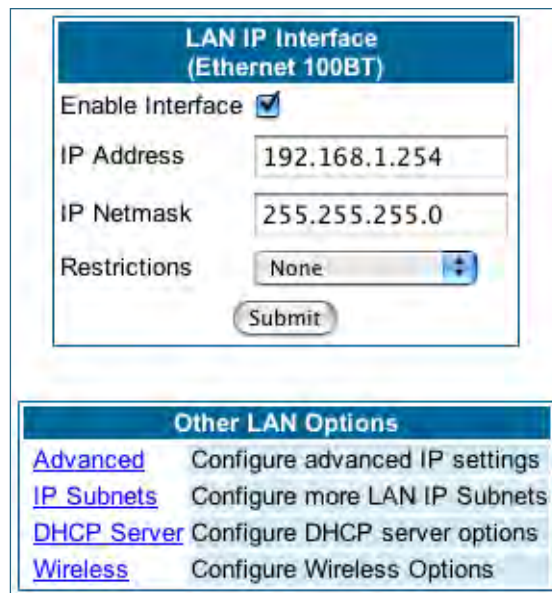
A brief message is displayed while the Gateway attempts to establish a connection.



3. **When the connection succeeds, your browser will display your Service Provider's home page.**

If you encounter any problems connecting, refer to the chapters "[Basic Troubleshooting](#)" on page 193 or "[Advanced Troubleshooting](#)" on page 207.

[Link: LAN](#)



The screenshot shows two sections of a web interface. The top section is titled "LAN IP Interface (Ethernet 100BT)" and contains the following fields: "Enable Interface" with a checked checkbox, "IP Address" with the value "192.168.1.254", "IP Netmask" with the value "255.255.255.0", and "Restrictions" with a dropdown menu set to "None". A "Submit" button is located below these fields. The bottom section is titled "Other LAN Options" and contains four links: "Advanced" (Configure advanced IP settings), "IP Subnets" (Configure more LAN IP Subnets), "DHCP Server" (Configure DHCP server options), and "Wireless" (Configure Wireless Options).

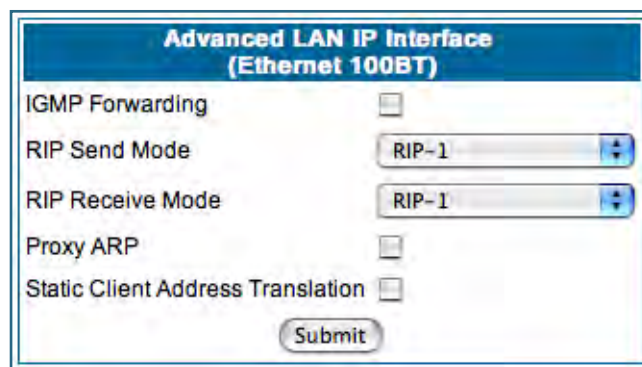
* **Enable Interface:** Enables all LAN-connected computers to share resources and to connect to the WAN. The Interface should always be enabled unless you are instructed to disable it by your Service Provider during troubleshooting.

* **IP Address:** The LAN IP Address of the Gateway. The IP Address you assign to your LAN interface must not be used by another device on your LAN network.

* **IP 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 represent network information. The default subnet mask for most networks is 255.255.255.0 (Class C subnet mask.)

* **Restrictions:** Specifies whether an administrator can open a Web Administrator or Telnet connection to the Gateway over the LAN interface in order to monitor and configure the Gateway. On the LAN Interface, you can enable or disable administrator access. By default, administrative restrictions are turned off, meaning an administrator can open a Web Administrator or Telnet connection through the LAN Interface.

• **Advanced:** Clicking on the Advanced link displays the Advanced LAN IP Interface page.



The screenshot shows the "Advanced LAN IP Interface (Ethernet 100BT)" configuration page. It contains the following fields: "IGMP Forwarding" with an unchecked checkbox, "RIP Send Mode" with a dropdown menu set to "RIP-1", "RIP Receive Mode" with a dropdown menu set to "RIP-1", "Proxy ARP" with an unchecked checkbox, and "Static Client Address Translation" with an unchecked checkbox. A "Submit" button is located at the bottom of the form.

- **IGMP Forwarding:** The default setting is Disabled. If you check this option, it will enable Internet Group Management Protocol (IGMP) multicast forwarding. IGMP allows a router to determine which host groups have members on a given network segment. See [“IGMP \(Internet Group Management Protocol\)” on page 100](#) for more information.
- **RIP Send Mode:** Specifies whether the gateway should use Routing Information Protocol (RIP) broadcasts to advertise its routing tables to other routers on your network. You may choose from the following protocols:
 - RIP-1: Routing Information Protocol version 1
 - RIP-2: RIP Version 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 new 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-1 compatibility: Compatible with RIP version 1
 - RIP-2 with MD5: MD5 authentication is an extension of RIP-2 that increases security by requiring an authentication key when routes are advertised.
 - RIP MD5 Key: Secret password when using RIP-2 with MD5.
- **RIP Receive Mode:** Specifies whether the Gateway should use Routing Information Protocol (RIP) broadcasts to update its routing tables with information received from other routers on your network. The protocol choices are the same as for the RIP send mode.
- **Proxy ARP:** Specifies whether you want the Gateway to respond when it receives an address resolution protocol for devices behind it. This is a way to make a computer that is physically located on one network appear to be part of a different physical network connected to the same Gateway. It allows you to hide a computer with a public IP address on a private network behind your Gateway, and still have the computer appear to be on the public network “in front of” the Gateway.
- **Static Client Address Translation:** If you check this checkbox, this feature allows a statically addressed computer whose IP address falls outside of the LAN subnet(s) to simply plug in and get online without any manual configuration on either the host or the Motorola Netopia® Gateway. If enabled, statically addressed LAN hosts that have an address outside of LAN subnets will be able to communicate via the Router’s WAN interface to the Internet. Supported static IP address values *must* fall *outside* of the Router's LAN subnet(s).
- **IP Subnets:** The IP Subnets screen allows you to configure up to seven secondary subnets and their DHCP ranges, by entering IP address/subnet mask pairs:

To edit an IP subnet entry, select the entry and press the "Edit" button.

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.

The screenshot shows a small window titled "IP Subnet Entry". It contains a label "Enabled" followed by an unchecked checkbox. Below this is a "Submit" button.

Check the **Enabled** checkbox and click the [Submit](#) button.

The screen expands to allow you to enter subnet information.

The screenshot shows the expanded "IP Subnet Entry" form. It has a title bar "IP Subnet Entry". The "Enabled" checkbox is now checked. Below it are four input fields: "IP Address" (0.0.0.0), "Netmask" (0.0.0.0), "DHCP Start Address" (0.0.0.0), and "DHCP End Address" (0.0.0.0). A "Submit" button is at the bottom.

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 **Alert** icon at the upper right, and in the resulting page, click the [Save and Restart](#) link.

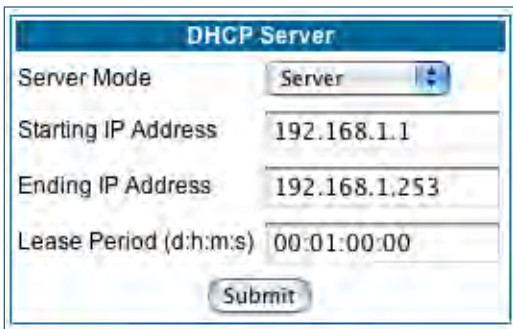
To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and clicking the [Submit](#) button to commit the change.



NOTE:

All additional DHCP ranges use the global lease period value. See [page 52](#).

• **DHCP Server:** Your Gateway can provide network configuration information to computers on your LAN, using the Dynamic Host Configuration Protocol (DHCP).



If you already have a DHCP server on your LAN, you should turn this service off.

If you want the Gateway to provide this service, click the **Server Mode** pull-down menu, choose **Server**, then configure the range of IP addresses that you would like the Gateway to hand out to your computers.

You can also specify the length of time the computers can use the configuration information; DHCP calls this period the lease time.

Your Service Provider may, for certain services, want to provide configuration from its DHCP servers to the computers on your LANs. In this case, the Gateway will relay the DHCP requests from your computers to a DHCP server in the Service Provider's network. Click the relay-agent and enter the IP address of the Service Provider's DHCP server in the Server Address field. This address is furnished by the Service Provider.



NOTE:

The **Relay-agent** option only works when NAT is off and the Gateway is in router mode.

Wireless (supported models)

If your Gateway is a wireless model (such as a 3347W) you can enable or disable the wireless LAN (WLAN) by clicking the [Wireless](#) link.

Wireless functionality is enabled by default.



802.11 Wireless Settings

Enable Wireless

SSID (Network ID) 5440 4401

Privacy OFF - No Privacy

Submit

Other Wireless Options

[Advanced Configuration Options](#)

If you uncheck the **Enable Wireless** checkbox, the Wireless Options are disabled, and the Gateway will not provide or broadcast any wireless LAN services.

SSID (Network ID): The SSID is preset to a number that is 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 “Ed’s Wireless LAN”. On client PCs’ software, this might also be called the *Network Name*. The SSID 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, if you are in Closed System Mode (see **Enable Closed System Mode** below), enter this name on their clients in order to join this wireless LAN.

The pull-down menu for enabling **Privacy** offers four settings: **WPA-802.1x**, **WPA-PSK**, **WEP - Automatic**, and **Off - No Privacy**. **WEP-Manual** is also available on the Advanced Configuration Options page. [See “Privacy” on page 54.](#)



NOTE:

On the 2200-Series Gateways, **WEP-Manual** privacy is enabled by default. Use the Motorola Netopia® Installation Wizard on the accompanying Motorola Netopia® CD to generate WEP keys for connecting wireless client computers.

Privacy

- **Off - No Privacy** provides no encryption on your wireless LAN data.
- **WPA-802.1x** provides RADIUS server authentication support.
- **WPA-PSK** provides Wireless Protected Access, the most secure option for your wireless network. This mechanism provides the best data protection and access control.

The **Pre Shared Key** is a passphrase shared between the Router and the clients and is used to generate dynamically changing keys. The passphrase can be 8-63 characters or up to 64 hex characters. It is recommended to use at least 20 characters for best security.

- **WEP - Automatic** is a passphrase generator. You enter a passphrase that you choose in the **Passphrase** field. The passphrase can be any string of words or numbers.

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.

You select a single key for encryption of outbound traffic. The WEP-enabled client must have an identical key of the same length, in the identical slot (1 – 4) as the Gateway, 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 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 Gateway and its clients need only enter, share, and use the first key.

802.11 Wireless Settings

Enable Wireless

SSID (Network ID) 4414 0400

Privacy WEP - Automatic

Select a key size and enter a passphrase below; then click Submit

Encryption Key Size 40/64 bit (10 characters)

Passphrase howdydoodo

Encryption Key **abcdefabcd**

Default Key 1

Submit

Click the [Submit](#) button. The Alert icon appears.

Click the Alert icon, and then the [Save and Restart](#) link.

Advanced

If you click the [Advanced](#) link, the advanced **802.11 Wireless Settings** page appears.

802.11 Wireless Settings

Enable Wireless

Wireless ID (SSID)

Operating Mode

Default Channel

AutoChannel Setting

Enable Closed System Mode

Block Wireless Bridging

Privacy

Enter a passphrase below, and click Submit to make keys.

WEP key passphrase

Encryption Key Size #1

Encryption Key #1

Encryption Key Size #2

Encryption Key #2

Encryption Key Size #3

Encryption Key #3

Encryption Key Size #4

Encryption Key #4

Use WEP encryption key(1-4) #

Other Wireless Options

[Multiple SSIDs](#) Enable and Configure Multiple SSIDs.

[WiFi Multimedia](#) Enable and Configure WMM.

[MAC Authorization](#) Limit Wireless Access by MAC Address.

Note: This page displays different options depending on which form of Privacy or other options you have enabled.

You can then configure:

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: 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. However, in North America only 1 to 11 may be selected. Europe,

France, Spain and Japan will differ. Channel selection can have a significant impact on performance, depending on other wireless activity close to this Gateway. 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** is the default setting; the Motorola Netopia® Gateway will use the configured default channel selected from the previous pull-down menu.
- **At Startup** 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 SSID 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

Enabling Closed System Mode on your wireless Gateway 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® Gateway.

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

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 is not enabled. If WEP is enabled then the client must also have WEP enabled and a matching WEP key.

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



NOTE:

While clients may also have a passphrase feature, these are vendor-specific and may not necessarily create the same keys. You can passphrase generate a set of keys on one, and manually enter them on the other to get around this.

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

- **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.

802.11 Wireless Settings

Enable Wireless

Wireless ID (SSID) 4414 0400

Operating Mode Normal (802.11b+g)

Default Channel 6

AutoChannel Setting OFF - Use default

Enable Closed System Mode

Block Wireless Bridging

Privacy WEP - Manual

Encryption Key Size #1 40/64 bit (10 characters)

Encryption Key #1 abcdefabcd

Encryption Key Size #2 40/64 bit (10 characters)

Encryption Key #2 efabcdefab

Encryption Key Size #3 40/64 bit (10 characters)

Encryption Key #3 cdefabcdef

Encryption Key Size #4 40/64 bit (10 characters)

Encryption Key #4 abcdefabcd

Use WEP encryption key (1-4) # 1

Submit

Other Wireless Options:

- [Multiple SSIDs](#) Enable and Configure Multiple SSIDs
- [WiFi Multimedia](#) Enable and Configure WMM
- [MAC Authorization](#) Limit Wireless Access by MAC Address

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

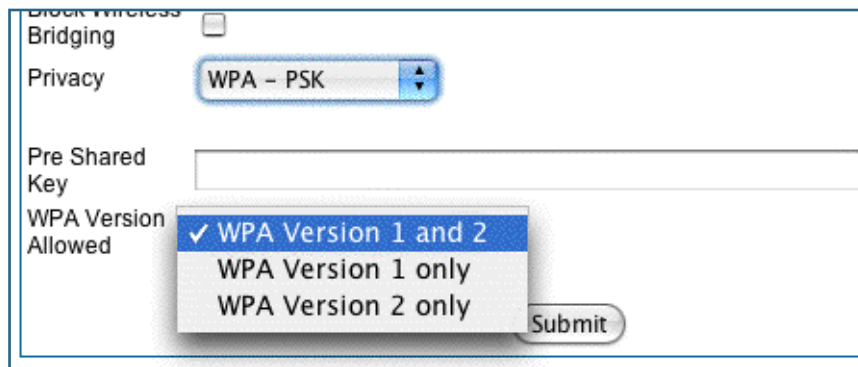
Use WEP encryption key (1 – 4) #: Specifies which key the Gateway will use to encrypt transmitted traffic. The default is key #1.

You disable the wireless LAN by unchecking the Enable Wireless checkbox, clicking the [Submit](#) button, followed by the [Save and Restart](#) link.

WPA Version Allowed

If you select either **WPA-802.1x** or **WPA-PSK** as your privacy setting, the **WPA Version Allowed** pull-down menu appears to allow you to select the WPA version(s) that will be required for client connections. Choices are:

- **WPA Version 1 and 2**, for maximum interoperability,
- **WPA Version 1 Only**, for backward compatibility,
- **WPA Version 2 Only**, for maximum security.



All clients must support the version(s) selected in order to successfully connect.

Multiple SSIDs

The **Multiple Wireless SSIDs** feature allows you to add additional network identifiers (SSIDs or *Network Names*) for your wireless network.

To enable Multiple Wireless SSIDs, click the [Multiple SSIDs](#) link.

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

Multiple Wireless SSIDs

Enable SSID #2

Enable SSID #3

Enable SSID #4

Submit

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

Multiple Wireless SSIDs

Enable SSID #2

SSID #2: David's Game Room

Privacy: WPA - PSK

Pre Shared Key:

WPA Version Allowed: WPA Version 1 and 2

Enable SSID #3


Enable SSID #4

Submit

Privacy modes available from the pull-down menu for the multiple SSIDs are: **WPA-PSK**, **WPA-802.1x**, or **Off-No Privacy. WEP** can also be selected on the additional SSIDs as long as it is not used on the primary SSID. WEP can only be used on one SSID, so any others will not have WEP available.

These additional Wireless IDs are “Closed System Mode” Wireless IDs 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 **Submit** button.

After your first entry, the Alert icon  will appear in the upper right corner of your screen. When you are finished adding SSIDs, click the Alert icon, and Save your changes and restart the Gateway.

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](#) link the **WiFi Multimedia** page appears.



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

The screen expands.

WiFi Multimedia

WMM Mode:

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):	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>
VIDEO: (VI):	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>
BEST-EFFORT: (BE):	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>
BACKGROUND: (BK):	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>

Client EDCA Parameters

Access Categories (AC)	AIFs	cwMin	cwMax	TXOP Limit
VOICE: (VO):	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1504"/>
VIDEO: (VI):	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="3008"/>
BEST-EFFORT: (BE):	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>
BACKGROUND: (BK):	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="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.)

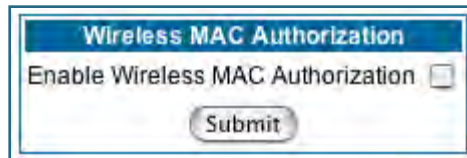
Wireless MAC Authorization

Wireless MAC Authorization allows you to specify which client PCs are allowed to join the wireless LAN by specific hardware address. 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.

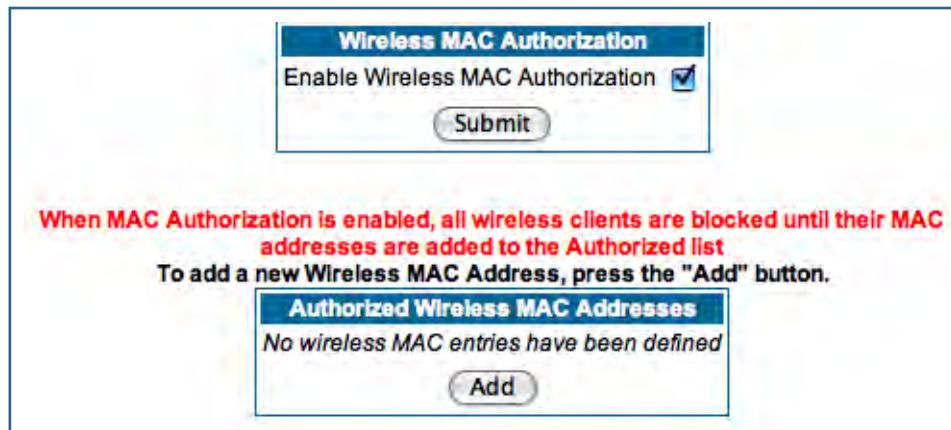
To enable Wireless MAC Authentication, click the [MAC Authorization](#) link.

When the Wireless MAC Authentication screen appears, check the **Enable Wireless MAC Authorization** checkbox:




The screenshot shows a window titled "Wireless MAC Authorization". Inside, there is a checkbox labeled "Enable Wireless MAC Authorization" which is currently unchecked. Below the checkbox is a "Submit" button.

The screen expands as follows:



The screenshot shows the expanded "Wireless MAC Authorization" window. The "Enable Wireless MAC Authorization" checkbox is now checked. Below the "Submit" button, there is a red warning message: "When MAC Authorization is enabled, all wireless clients are blocked until their MAC addresses are added to the Authorized list. To add a new Wireless MAC Address, press the 'Add' button." Below this message is a section titled "Authorized Wireless MAC Addresses" with the text "No wireless MAC entries have been defined" and an "Add" button.

Click the [Add](#) button. The **Authorized Wireless MAC Address Entry** screen appears.



The screenshot shows the "Authorized Wireless MAC Address Entry" window. It has two columns: "Allow Access?" and "Hardware MAC Address". The "Allow Access?" checkbox is checked. The "Hardware MAC Address" field contains the address "00 - 0a - 27 - ae - 71 - a3". A "Submit" button is at the bottom.

Enter the MAC (hardware) address of the client PC you want to authorize for access to your wireless LAN. The **Allow Access?** checkbox is enabled by default. Unchecking this checkbox specifically denies access from this MAC address. Click the [Submit](#) button.



Note:


When MAC Authorization is enabled, all wireless clients are blocked until their MAC addresses

are added to the Authorized list.

Your entry will be added to a list of up to 32 authorized addresses as shown:

The screenshot shows a web interface for configuring wireless MAC authentication. At the top, there is a section titled "Wireless MAC Authentication" with a checkbox labeled "Enable Wireless MAC Authentication:" which is checked. Below this is a "Submit" button. In the center, there is instructional text: "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." Below this text is a section titled "Authorized Wireless MAC Addresses" containing a table with one entry: "Wireless MAC Address = 00-0a-27-ae-71-a3 - Allowed". At the bottom of this section are three buttons: "Add", "Edit", and "Delete".

You can continue to [Add](#), [Edit](#), or [Delete](#) addresses to the list by clicking the respective buttons.

After your first entry, the Alert icon  will appear in the upper right corner of your screen. When you are finished adding addresses to the list, click the Alert icon, and Save your changes and restart the Gateway.

Use RADIUS Server

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 click the [RADIUS](#) link, the screen expands to allow you to enter your RADIUS server information.

The screenshot shows a web interface for configuring RADIUS servers. The title is "Radius Servers". It contains five input fields: "RADIUS Server Addr/Name", "RADIUS Server Secret", "Alt RADIUS Server Addr/Name", "Alt RADIUS Server Secret", and "Radius Server Port". The "Radius Server Port" field has the value "1812" entered. At the bottom right is a "Submit" button.

- **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.
- **RADIUS Server Port:** The port on which the RADIUS server is listening, typically, the default 1812.

Click the [Submit](#) button.

You can also configure alternate RADIUS servers from the Advanced Network Configuration page, by clicking the [Advanced](#) link.

The **Advanced Network Configuration** page appears.

Network Configuration	
IP Static Routes	Build IP static route table
IP Static ARP	Build IP static ARP table
NAT	
Pinholes	Set up pinholes through NAT
IPMaps	Set up NAT one-to-one IP address mappings
Default Server	Set up NAT default server options
Services	
Differentiated Services	Set up Differentiated Service options
DNS	Set up DNS options
DHCP Server	Set up DHCP server and relay-agent options
RADIUS Server	Set up RADIUS server options
SNMP	Set up SNMP community, trap and system group options
IGMP	Set up IGMP options
UPnP	Enable or disable Universal Plug'n'Play
LAN Management (TR-064)	Enable or disable DSL Forum LAN-Side DSL CPE Configuration services
Ethernet Bridge	Set up ethernet MAC bridge
VLAN	Set up VLAN Configuration
VoIP	Set up VoIP Configuration
Miscellaneous	
System	Configure System parameters
Syslog Parameters	Set up Syslog
Internal Servers	Configure internal web and telnet ports
Software Hosting	Set up Software Hosting
Backup	Set up Backup options
Clear Options	Restore the Gateway to its factory configuration
Time Zone	Time Zone settings

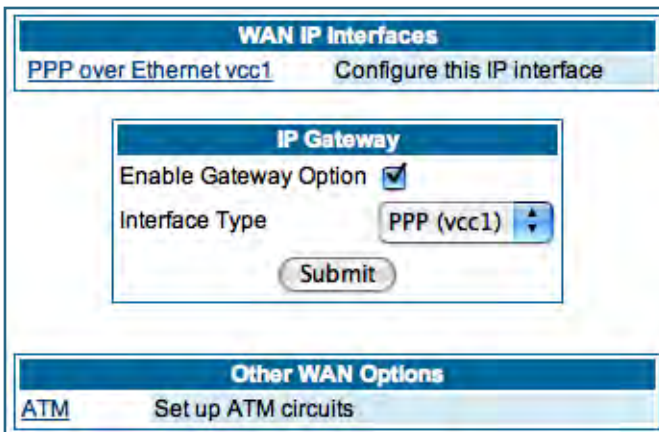
You access the RADIUS Server configuration screen from the Advanced Network Configuration web page, by clicking the [RADIUS Server](#) link.

[Link: WAN](#)

When you click the [WAN](#) link, the WAN IP configuration page appears. This page varies depending on the WAN interface of your Motorola Netopia® Gateway.

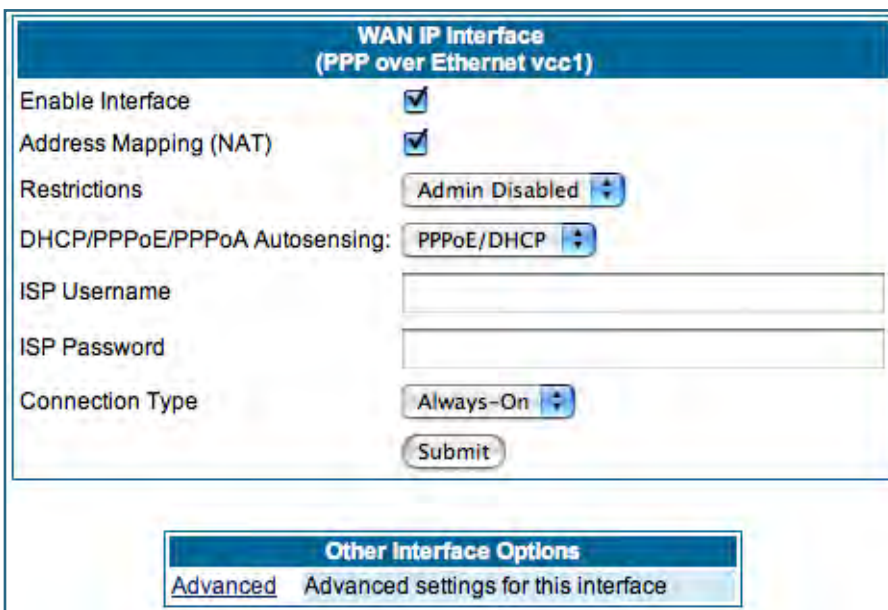
WAN IP Interfaces: Your IP interfaces are listed.

PPP over Ethernet interface



Click the [PPP over Ethernet](#) link to configure it.

The **WAN IP Interface** page appears.

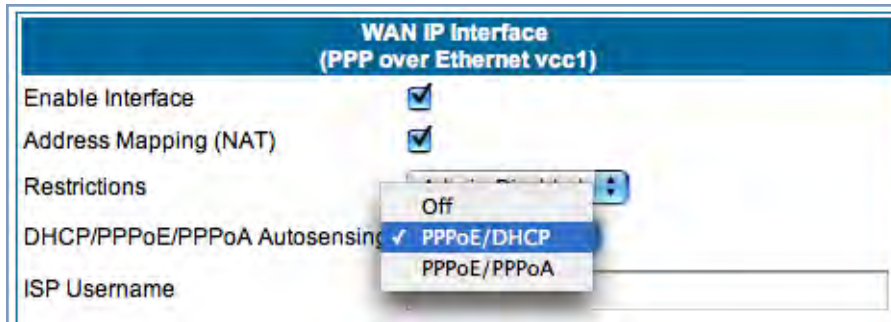


Enable Interface: You can disable the interface by unchecking the checkbox. However, doing so will disable all ability for your LAN users to connect to the WAN using the Gateway.

Address Mapping (NAT): Specifies whether you want the Gateway to use network address translation (NAT) when communicating with remote routers. NAT lets you conceal details of your network from remote routers. By default, address mapping is enabled.

Restrictions: This setting determines the types of traffic the Gateway accepts from the WAN. **Admin Disabled** means that Gateway traffic is accepted but administrative commands are ignored. **None** means that all traffic is accepted. When PPP is enabled, **Admin Disabled** is the default.

DHCP/PPPoE/PPPoA 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**.

ISP Username: This is the username used to authenticate your Gateway with the Service Provider's network. This value is given to you by your Service Provider.

ISP Password: This is the password used to authenticate your Gateway with the Service Provider's network. This value is given to you by your Service Provider.

Connection Type: The pull-down menu allows you to choose to have either an uninterrupted connection or an as-needed connection.

- **Always On:** This setting provides convenience, but it leaves your network permanently connected to the Internet.
- **Instant On** 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.

Timeout: (only appears if Instant-On Connection Type is selected) Specifies the time in seconds before disconnect if there is no traffic over the Internet link.

Advanced:

If you click the [Advanced](#) link, the **Advanced WAN IP Interface** configuration page appears.

Advanced WAN IP Interface (PPP over Ethernet voc1)	
Local Address	0.0.0.0
Peer Address	0.0.0.0
RIP Receive Mode	Off
Multicast Forward	<input checked="" type="checkbox"/>
IGMP Null Source Address	<input type="checkbox"/>

LCP Settings	
Authentication	PAP and/or CHAP
MRU	1492
Magic Number	<input checked="" type="checkbox"/>
Protocol Compression	<input type="checkbox"/>
LCP Echo Requests	<input checked="" type="checkbox"/>
Max Failures	10
Max Configures	10
Max Terminates	2
Restart Timer	3

Submit

Local Address: If this value is 0.0.0.0, the Gateway will acquire its IP address from your ISP. Otherwise this address is assigned to the virtual PPP interface.

Peer Address: Address of the server on the Service Provider side of the ppp link. This peer will attempt to negotiate the local IP address if IP Address = 0.0.0.0. If the remote peer does not accept the IP address, the link will not come up.

RIP Receive Mode: Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Motorola Netopia® Gateway needs to recognize. Set to **Off**, Netopia Embedded Software Version 7.7.4 will not accept information from either RIP-1 nor RIP-2 routers. With Receive RIP Mode set to **RIP-1**, the Motorola Netopia® Gateway will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to **RIP-2**, Netopia Embedded Software Version 7.7.4 will accept routing information provided by RIP packets from other routers that use different subnet masks.

From the pull-down menu, choose **Off**, **RIP-1**, **RIP-2**, **RIP-1 compatibility**, or **RIP-2 with MD5**.

RIP Receive MD5 Key: (Only appears if RIP-2 with MD5 RIP Receive Mode is selected) The purpose of MD5 authentication is to provide an additional level of confidence that a RIP packet received was generated by a reliable source. In other words, MD5 authentication provides an enhanced level of security that information that your PC receives does not originate from a malicious source posing as part of your network. This field allows you to enter an MD5 encryption key of from 1 – 16 ASCII characters for authenticating RIP receipts.

Multicast Forward: If you check this checkbox, 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.

IGMP Null Source Address: If you check this checkbox, 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. This checkbox is only available if “Multicast Forward” is checked.

LCP Settings:

Authentication: Select **Off**, **PAP and/or CHAP**, **PAP only**, or **CHAP only** from the pull-down menu. The settings for port authentication on the Gateway must match the authentication expected by the remote system. The username and passwords are available on the WAN IP Interfaces page.

MRU: Specifies the Maximum Receive Unit for the PPP Interface.

Magic Number: Enables or disables LCP magic number negotiation.

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

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

Max Failures: Specifies the maximum number of Configure-NAK messages the PPP module can send without having sent a Configure-ACK message.

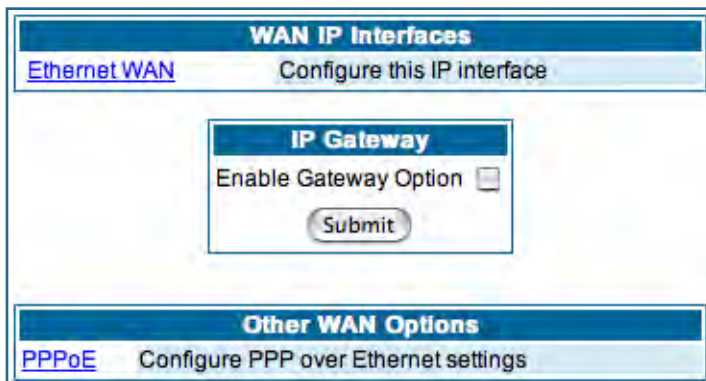
Max Configures: Specifies the maximum number of unacknowledged configuration requests that your Gateway will send.

Max Terminates: Specifies the maximum number of unacknowledged termination requests that your Gateway will send before terminating the PPP link.

Restart Timer: The number of seconds the Gateway should wait before retransmitting a configuration or termination request.

Click the [Submit](#) button when you are finished.

Ethernet WAN interface



Click the [Ethernet WAN](#) link to configure it.

The **WAN IP Interface** page appears.

The screenshot shows the configuration page for a WAN IP Interface (Ethernet WAN). It includes the following options:

- Enable Interface:
- Obtain IP Address Automatically:
- Address Mapping (NAT):
- Restrictions: Admin Disabled (dropdown menu)

A Submit button is located at the bottom of the form.

This section is titled "Other Interface Options" and contains a link for "Advanced" settings, which are described as "Advanced settings for this interface".

Enable Interface: You can disable the interface by unchecking the checkbox. However, doing so will disable all ability for your LAN users to connect to the WAN using the Gateway.

Obtain IP Address Automatically: Your service provider may tell you that the WAN IP Address for your Gateway is static. In this case, disable this checkbox and enter the IP Address and IP Netmask from your Service Provider in the appropriate fields.

The screenshot shows the configuration page for a WAN IP Interface (RFC-1483 Bridged Ethernet vcc1). It includes the following options:

- Enable Interface:
- Obtain IP Address Automatically:
- IP Address: 0.0.0.1
- IP Netmask: 255.255.255.0
- Address Mapping (NAT):
- Restrictions: Admin Disabled (dropdown menu)

A Submit button is located at the bottom of the form.

IP Address: This is the IP Address from your Service Provider when using static IP addressing.

IP Netmask: This is the Netmask from your Service Provider when using static IP addressing.



NOTE:

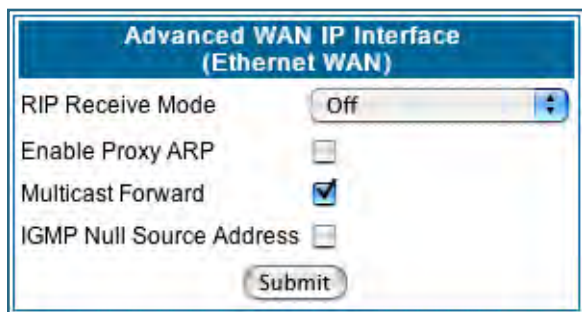
Beginning with Firmware Version 7.7, you can now run an IPoE interface without an IP address (“unnumbered” interface), if you un-check “Obtain IP Address Automatically” and set the IP Address to 0.

Address Mapping (NAT): Specifies whether you want the Gateway to use network address translation (NAT) when communicating with remote routers. NAT lets you conceal details of your network from remote routers. By default, address mapping is enabled.

Restrictions: This setting determines the types of traffic the Gateway accepts from the WAN. **Admin Disabled** means that Gateway traffic is accepted but administrative commands are ignored. **None** means that all traffic is accepted. **Admin Disabled** is the default.

Advanced:

If you click the [Advanced](#) link the **Advanced WAN IP Interface** configuration page appears.



RIP Receive Mode: Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Motorola Netopia® Gateway needs to recognize. Set to **Off**, Netopia Embedded Software Version 7.7.4 will not accept information from either RIP-1 nor RIP-2 routers. With Receive RIP Mode set to **RIP-1**, the Motorola Netopia® Gateway will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to **RIP-2**, Netopia Embedded Software Version 7.7.4 will accept routing information provided by RIP packets from

other routers that use different subnet masks.

From the pull-down menu, choose **Off**, **RIP-1**, **RIP-2**, **RIP-1 compatibility**, or **RIP-2 with MD5**.

Enable Proxy ARP: Checking the checkbox will enable the Gateway to respond when it receives an Address Resolution Protocol message for devices behind it.

Multicast Forward: If you check this checkbox, 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.

IGMP Null Source Address: If you check this checkbox, 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. This checkbox is only available if “Multicast Forward” is checked.

IP Gateway

Enable Gateway Option: You can configure the Gateway to send packets to a default gateway if it does not know how to reach the destination host.

Interface Type: If you have PPPoE enabled, you can specify that packets destined for unknown hosts will be sent to the gateway being used by the remote PPP peer. If you select ip-address, you must enter the IP address of a host on a local or remote network to receive the traffic.

Default Gateway: The IP Address of the default gateway.

Other WAN Options

PPPoE: You can enable or disable PPPoE. This link also allows configuration of NAT, admin restrictions, PPPoE username/password, and connection type.

WAN Ethernet and VDSL Gateways

To allow for concurrent PPPoE and IPoE support on WAN Ethernet Gateways, including VDSL units, **PPPoE with IPoE** is available on the PPPoE configuration page. Checking the checkbox will provide this concurrent support. When you enable PPPoE with IPoE, the additional WAN interface becomes available for configuration.



NOTE:

Enabling pppoe-with-ipoe disables support for multiple PPPoE sessions.

ADSL Gateways

ATM Circuits: You can configure the ATM circuits and the number of Sessions. The IP Interface(s) should be reconfigured after making changes here.

Available Encapsulation types:

PPP over Ethernet (PPPoE)
 PPP over ATM (PPPoA)
 RFC-1483 Bridged Ethernet
 RFC-1483 Routed IP
 None

Available Multiplexing types:

LLC/SNAP
 VC muxed

ATM Circuits						
VCC	VPI	VCI	Encapsulation	Multiplexing	PPPoE Sessions	
1	0	0	PPP over Ethernet	LLC/SNAP	1	

To turn off a VCC, set its encapsulation to **None**.
 To turn on another VCC, [Click Here](#).

Other ATM Options

[ATM Traffic Shaping](#) Configure ATM Traffic Shaping Options

Your Motorola Netopia® ADSL Gateway supports VPI/VCI autodetection by default. If VPI/VCI autodetection is enabled, the ATM Circuits page displays VPI/VCI = 0. If you configure a new ATM VPI/VCI pair, upon saving and restarting, autodetection is disabled and only the new VPI/VCI pair configuration will be enabled.

VPI/VCI Autodetection consists of eight static VPI/VCI pair configurations. These are 0/35, 8/35, 0/32, 8/32, 1/35, 1/1, 1/32, 2/32. These eight VPI/VCI pairs will be created if the Gateway is configured for autodetection. the Gateway does not establish a circuit using any of these preconfigured VPI/VCI pairs, then you can manually enter a VPI/VCI pair in the ATM Circuits page.

PPPoE with IPoE: For ADSL Gateways, you must configure two VCCs with the **same** VPI/VCI settings to provide concurrent PPPoE with IPoE support.

You must use fixed VPI/VCI values for PPPoE with IPoE. You cannot have both VPI/VCI values set to 0/0; autodetection does not work in this mode.

ATM Circuits						
VCC	VPI	VCI	Encapsulation	Multiplexing	PPPoE Sessions	
1	0	36	PPP over Ethernet	LLC/SNAP	1	
1	0	36	RFC-1483 Bridged Ethernet	LLC/SNAP		

To turn off a VCC, set its encapsulation to **None**.
 To turn on another VCC, [Click Here](#).

Other ATM Options

[ATM Traffic Shaping](#) Configure ATM Traffic Shaping Options


WAN IP Interfaces

[PPP over Ethernet vcc1](#) Configure this IP interface

[RFC-1483 Bridged Ethernet vcc1](#) Configure this IP interface

IP Gateway

Enable Gateway Option

Interface Type 

Other WAN Options

[ATM](#) Set up ATM circuits

Once the VCCs have been configured, the WAN IP Interfaces screen displays the additional interface which you can then configure as required.

ATM Traffic Shaping: You can prioritize delay-sensitive data by configuring the Quality of Service (QoS) characteristics of the virtual circuit. Click the [ATM Traffic Shaping](#) link.

VCC	Service Class	Peak Cell Rate	Sustained Cell Rate	Maximum Burst Size
1	UBR	0		

Submit

You can choose UBR (Unspecified Bit Rate), CBR (Constant Bit Rate), or VBR (Variable Bit Rate) from the pull-down menu and set the Peak Cell Rate (PCR) in the editable field.

UBR (Unspecified Bit Rate) guarantees no minimum transmission rate. Cells are transmitted on a “best effort” basis. However, there is a cap on the maximum transmission rate for UBR VCs. In a practical situation:

- UBR VCs should be transmitted at a priority lower than CBR.
- Bandwidth should be shared equally among UBR VCs.

UBR applications are non-real-time traffic such as IP data traffic.

CBR (Constant Bit Rate) guarantees a certain transmission rate (although the application may underutilize this bandwidth). A Peak Cell Rate (PCR) characterizes CBR. CBR is most suited for real time applications such as real time voice / video, although it can be used for other applications.

VBR (Variable Bit Rate) This class is characterized by:

- a **Peak Cell Rate** (PCR), which is a temporary burst, not a sustained rate, and
- a **Sustained Cell Rate** (SCR),
- a Burst Tolerance (BT), specified in terms of **Maximum Burst Size** (MBS). The MBS is the maximum number of cells that can be transmitted at the peak cell rate and should be less than, or equal to the Peak Cell Rate, which should be less than, or equal to the line rate.

VBR has two sub-classes:

a. VBR non-real-time (VBR-nrt): Typical applications are non-real-time traffic, such as IP data traffic. This class yields a fair amount of Cell Delay Variation (CDV).

b. VBR real time (VBR-rt): Typical applications are real-time traffic, such as compressed voice over IP and video conferencing. This class transmits cells with a more tightly bounded Cell Delay Variation. The applications follow CBR.

VCC	Service Class	Peak Cell Rate	Sustained Cell Rate	Maximum Burst Size
1	VBR	0	0	0

Submit



Note:

The difference between VBR-rt and VBR-nrt is the tolerated Cell Delay Variation range and the provisioned Maximum Burst Size.

Class	PCR	SCR	MBS	Transmit Priority	Comments
UBR	X	N/A	N/A	Low	PCR is a cap
CBR	X	N/A	N/A	High	PCR is a guaranteed rate
VBR	X	X	X	High	PCR > SCR. SCR is a guaranteed rate. PCR is a cap.

[Link: Advanced](#)

Selected Advanced options are discussed in the pages that follow. Many are self-explanatory or are dictated by your service provider.

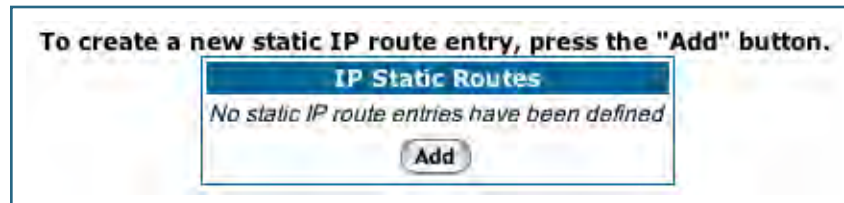
The following are typical links under Configure -> Advanced (some models offer other links):

Network Configuration	
IP Static Routes	Build IP static route table
IP Static ARP	Build IP static ARP table
NAT	
Pinholes	Set up pinholes through NAT
IPMaps	Set up NAT one-to-one IP address mappings
Default Server	Set up NAT default server options
Services	
Differentiated Services	Set up Differentiated Service options
DNS	Set up DNS options
DHCP Server	Set up DHCP server and relay-agent options
RADIUS Server	Set up RADIUS server options
SNMP	Set up SNMP community, trap and system group options
IGMP	Set up IGMP options
UPnP	Enable or disable Universal Plug'n'Play
LAN Management (TR-064)	Enable or disable DSL Forum LAN-Side DSL CPE Configuration services
Ethernet Bridge	Set up ethernet MAC bridge
VLAN	Set up VLAN Configuration
VoIP	Set up VoIP Configuration
Miscellaneous	
System	Configure System parameters
Syslog Parameters	Set up Syslog
Internal Servers	Configure internal web and telnet ports
Software Hosting	Set up Software Hosting
Backup	Set up Backup options
Clear Options	Restore the Gateway to its factory configuration
Time Zone	Time Zone settings

[Link: IP Static Routes](#)

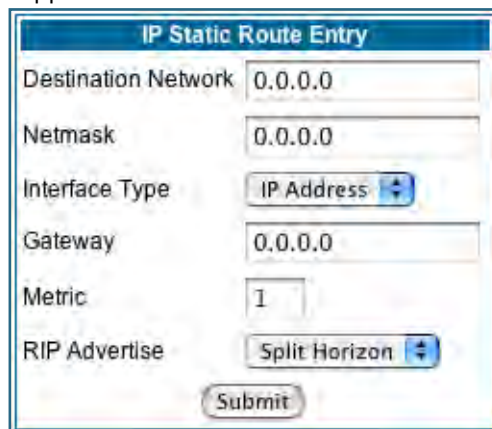
A static route identifies a manually configured pathway to a remote network. Unlike dynamic routes, which are acquired and confirmed periodically from other routers, static routes do not time out. Consequently, static routes are useful when working with PPP, since an intermittent PPP link may make maintenance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

When you click the [Static Routes](#) link, the **IP Static Routes** page appears.




You can configure as many as 32 static IP routes for the Gateway. To add a static route, click the [Add](#) button.

The **IP Static Route Entry** page appears.



- **Destination Network:** Enter the IP address of the static route. It may not be 0.0.0.0.
- **Netmask:** Enter the subnet mask for the IP network at the other end of the static route. 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 or class B network number) to be valid.
- **Interface Type:** Choose **PPP (vcc1)** – depending on the interface; typically vcc1 for DSL – or **IP Address** from the pull-down menu to specify whether the static route is accessible through PPP or IP address.
- **Gateway:** Enter the IP address of the gateway for the static route. The default gateway must be located on a network connected to your Motorola Netopia® Gateway configured interface.
- **Metric:** Specifies the hop count for the static route. Enter a number from 1 to 15 to indicate the number of routes (actual or best guess) a packet must traverse to reach the remote network. Some metric or a value of 1 will be used to indicate:
 - 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.


- **RIP Advertise:** From the pull-down menu, choose how the static route should be advertised via RIP:
 - **Split Horizon:** Do not advertise route if the gateway is on the same subnet.
 - **Always:** Advertise route in all RIP messages.
 - **Never:** Do not advertise route.

Click the [Submit](#) button. The Alert icon  will appear, so that you can switch to the **Save Changes** page, when you are finished.

Once you save your changes, you will be returned to the IP Static Routes entry screen.



- You can continue to **Add**, **Edit**, or **Delete** Static Routes from this screen.

When you are finished, click the Alert icon , switch to the **Save Changes** page, and click the [Save Changes](#) link.

Link: IP Static ARP

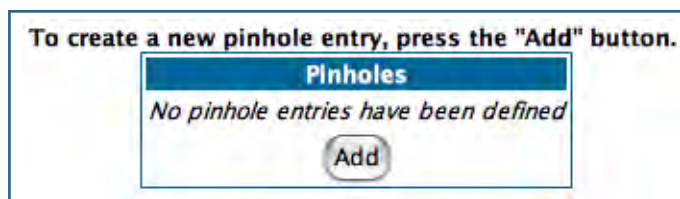
Your Gateway maintains a dynamic Address Resolution Protocol (ARP) table to map IP addresses to Ethernet (MAC) addresses. It populates this ARP table dynamically, by retrieving IP address/MAC address pairs only when it needs them. Optionally, you can define static ARP entries to map IP addresses to their corresponding Ethernet MAC addresses. Unlike dynamic ARP table entries, static ARP table entries do not time out. The IP address cannot be 0.0.0.0. The Ethernet MAC address entry is in nn-nn-nn-nn-nn-nn (hexadecimal) format.

IP Static ARP Entry	
IP Address	Hardware MAC Address
<input type="text" value="0.0.0.0"/>	<input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/>
<input type="button" value="Submit"/>	

Link: Pinholes

Pinholes allow you to transparently route selected types of network traffic, such as FTP requests or HTTP (Web) connections, to a specific host behind the Gateway. Creating a pinhole allows access traffic originating from a remote connection (WAN) to be sent to the internal computer (LAN) that is specified in the Pinhole page.

Pinholes are common for applications like multiplayer online games. Refer to software manufacturer application documentation for specific traffic types and port numbers.



Configure Specific Pinholes. Planning for Your Pinholes. Determine if any of the service applications that you want to provide on your LAN stations use TCP or UDP protocols. If an application does, then you must configure a pinhole to implement port forwarding. This is accessed from the **Advanced -> Pinholes** page.

Example: A LAN Requiring Three Pinholes . The procedure on the following pages describes how you set up your NAT-enabled Motorola Netopia® Gateway to support three separate applications. This requires passing three kinds of specific IP traffic through to your LAN.

Application 1: You have a Web server located on your LAN behind your Motorola Netopia® Gateway and would like users on the Internet to have access to it. With NAT "On", the only externally visible IP address on your network is the Gateway's WAN IP (supplied by your Service Provider). All traffic intended for that LAN Web server must be directed to that IP address.

Application 2: You want one of your LAN stations to act as the "central repository" for all email for all of the LAN users.

Application 3: One of your LAN stations is specially configured for game applications. You want this specific LAN station to be dedicated to games.

A sample table to plan the desired pinholes is:

WAN Traffic Type	Protocol	Pinhole Name	LAN Internal IP Address
Web	TCP	my-webserver	192.168.1.1
Email	TCP	my-mailserver	192.168.1.2
Games	UDP	my-games	192.168.1.3

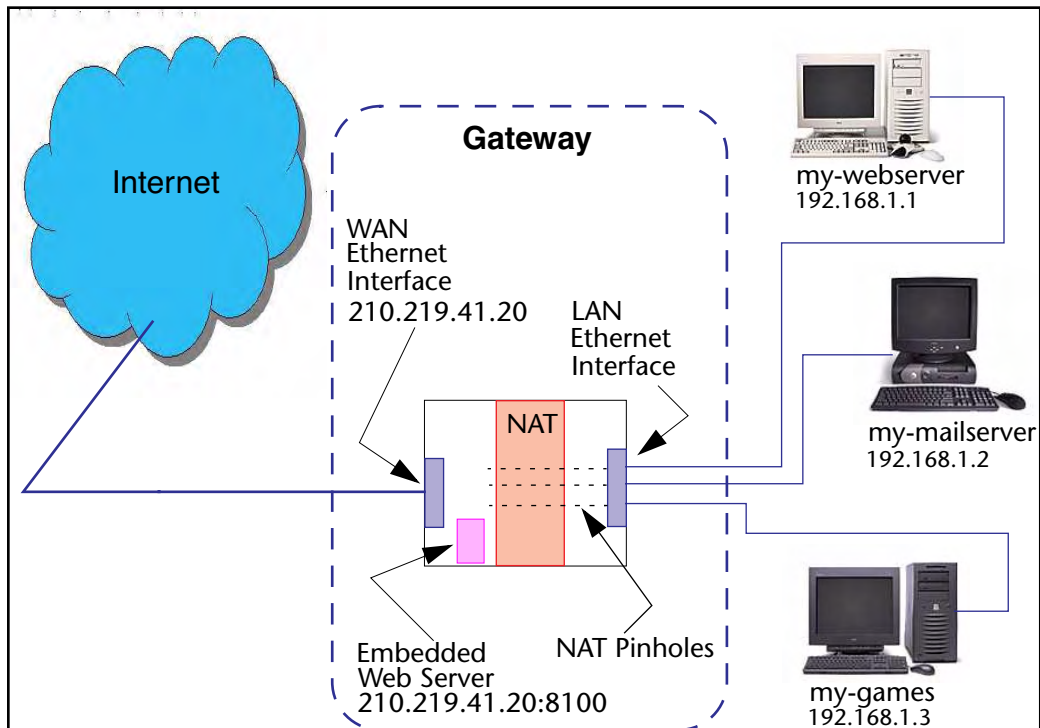
For this example, Internet protocols TCP and UDP must be passed through the NAT security feature and the Gateway's embedded Web (HTTP) port must be re-assigned by configuring new settings on the Internal Servers page.



TIPS for making Pinhole Entries:

1. If the port forwarding feature is required for Web services, ensure that the embedded Web server's port number is re-assigned PRIOR to any Pinhole data entry.
2. Enter data for one Pinhole at a time.
3. Use a unique name for each Pinhole. If you choose a duplicate name, it will overwrite the previous information without warning.

A diagram of this LAN example is:



You can also use the LAN-side address of the Gateway, 192.168.1.x:8100 to access the web and 192.168.1.x:23 to access the telnet server.

Pinhole Configuration Procedure. Use the following steps:

1. From the [Configure](#) toolbar button -> [Advanced](#) link, select the [Internal Servers](#) link.

Since Port Forwarding is required for this example, the Motorola Netopia® embedded Web server is configured first.



NOTE:

The two text boxes, **Web (HTTP) Server Port** and **Telnet Server Port**, on this page refer to the port numbers of the Motorola Netopia® Gateway's *embedded administration ports*.

To pass Web traffic through to your LAN station(s), select a Web (HTTP) Port number that is greater than 1024. In this example, you choose 8100.

2. Type **8100** in the **Web (HTTP) Server Port** text box.

Internal Servers	
Enter a value from 1 to 65534, 0 to disable the server	
Web (HTTP) Server Port	8100
Telnet Server Port	23
<input type="button" value="Submit"/>	

3. Click the [Submit](#) button.
4. Click [Advanced](#). Select the [Pinholes](#) link to go to the Pinhole page.
5. Click [Add](#). Type your specific data into the Pinhole Entries table of this page. Click [Submit](#).

Pinhole Entry	
Pinhole Name	my-webserver
Protocol	TCP
External Port Start	80
External Port End	80
Internal IP Address	192.168.1.1
Internal Port	80
<input type="button" value="Submit"/>	
Add or Edit more Pinholes	

-
6. Click on the [Add or Edit more Pinholes](#) link. Click the [Add](#) button. Add the next Pinhole. Type the specific data for the second Pinhole.



The screenshot shows a web form titled "Pinhole Entry". The fields are filled with the following values: Pinhole Name: my-mailserver; Protocol: TCP (selected from a dropdown); External Port Start: 25; External Port End: 25; Internal IP Address: 192.168.1.2; Internal Port: 25. At the bottom of the form, there is a "Submit" button and a link that says "Add or Edit more Pinholes".

7. Click on the [Add or Edit more Pinholes](#) link. Click the [Add](#) button. Add the next Pinhole. Type the specific data for the third Pinhole.



The screenshot shows a web form titled "Pinhole Entry". The fields are filled with the following values: Pinhole Name: my-games; Protocol: UDP (selected from a dropdown); External Port Start: 1100; External Port End: 1200; Internal IP Address: 192.168.1.3; Internal Port: 1100. At the bottom of the form, there is a "Submit" button and a link that says "Add or Edit more Pinholes".

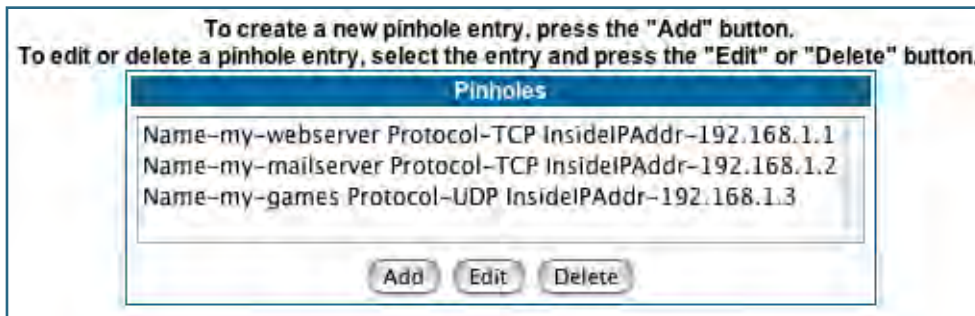


NOTE:

Note the following parameters for the “my-games” Pinhole:

1. The Protocol ID is UDP.
 2. The external port is specified as a range.
 3. The Internal port is specified as the lower range entry.
-

8. Click on the [Add or Edit more Pinholes](#) link. Review your entries to be sure they are correct.



9. Click the [Alert](#) icon.
10. Click the [Save and Restart](#) link to complete the entire Pinhole creation task and ensure that the parameters are properly saved.



NOTE:

REMEMBER: When you have re-assigned the port address for the embedded Web server, you can still access this facility.

Use the Gateway's WAN address plus the new port number.

In this example it would be

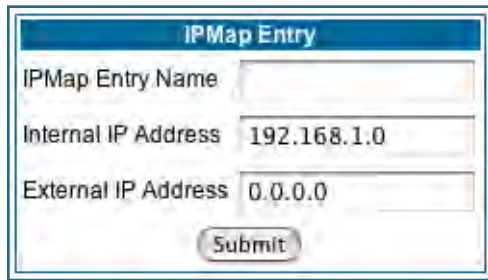
<WAN Gateway address>:<new port number> or, in this case, 210.219.41.20:8100

You can also use the LAN-side address of the Gateway, 192.168.1.x:8100 to access the web and 192.168.1.x:23 to access the telnet server.

[Link: IPMaps](#)

IPMaps supports one-to-one Network Address Translation (NAT) for IP addresses assigned to servers, hosts, or specific computers on the LAN side of the Motorola Netopia® Gateway.

A single static or dynamic (DHCP) WAN IP address must be assigned to support other devices on the LAN. These devices utilize Motorola Netopia®'s default NAT/PAT capabilities.



The screenshot shows a web-based configuration window titled "IPMap Entry". It features three text input fields: "IPMap Entry Name" (empty), "Internal IP Address" (containing "192.168.1.0"), and "External IP Address" (containing "0.0.0.0"). A "Submit" button is located at the bottom center of the form.

Configure the IPMaps Feature

FAQs for the IPMaps Feature

Before configuring an example of an IPMaps-enabled network, review these frequently asked questions.

What are IPMaps and how are they used? The IPMaps feature allows **multiple static** WAN IP addresses to be assigned to the Motorola Netopia® Gateway.

Static WAN IP addresses are used to support specific services, like a web server, mail server, or DNS server. This is accomplished by mapping a separate static WAN IP address to a specific internal LAN IP address. All traffic arriving at the Gateway intended for the static IP address is transferred to the internal device. All outbound traffic from the internal device appears to originate from the static IP address.

Locally hosted servers are supported by a public IP address while LAN users behind the NAT-enabled IP address are protected.

IPMaps is compatible with the use of NAT, with either a statically assigned IP address or DHCP/PPP served IP address for the NAT table.

What types of servers are supported by IPMaps? IPMaps allows a Motorola Netopia® Gateway to support servers behind the Gateway, for example, web, mail, FTP, or DNS servers. VPN servers are not supported at this time.

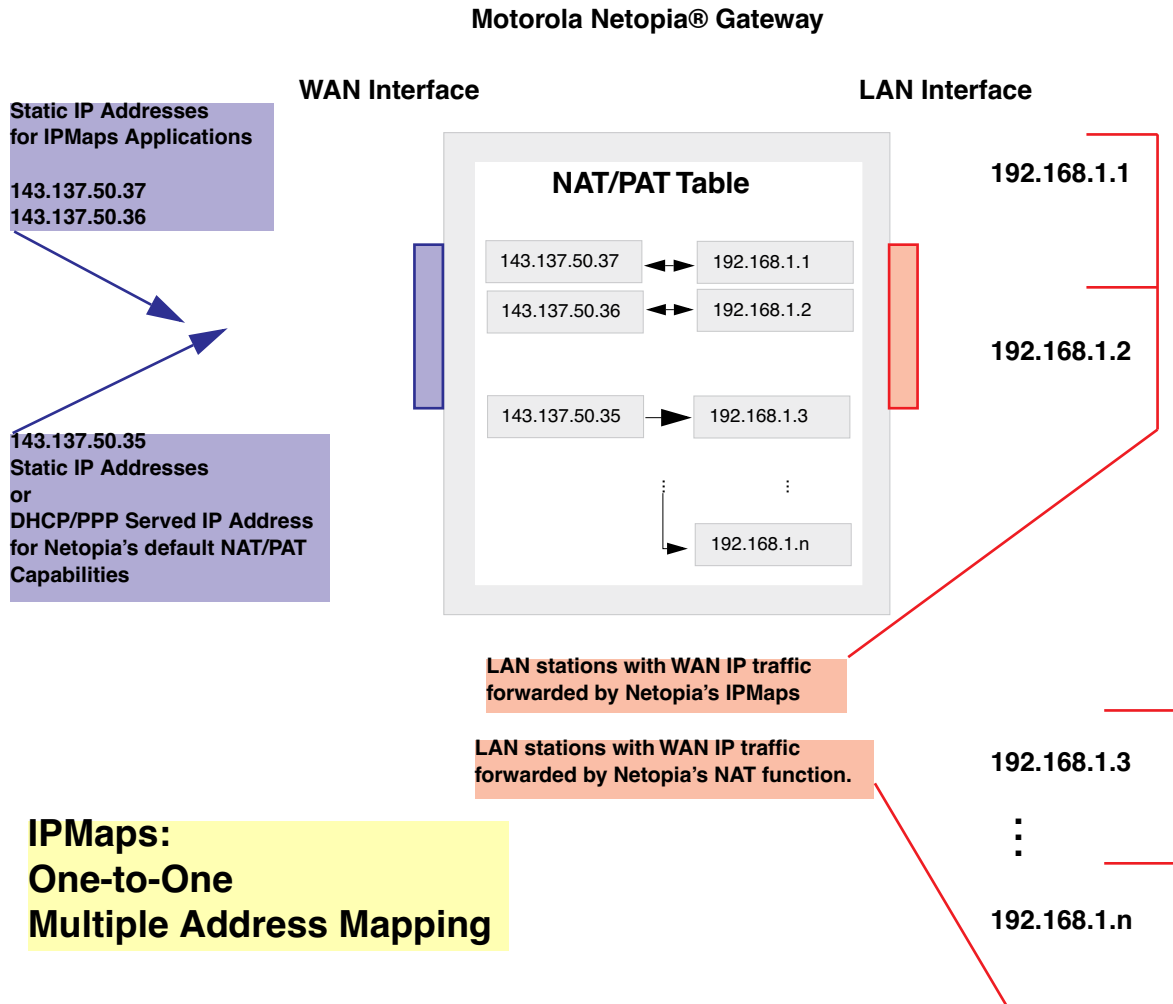
Can I use IPMaps with my PPPoE or PPPoA connection? Yes. IPMaps can be assigned to the WAN interface **provided they are on the same subnet**. Service providers will need to ensure proper routing to all IP addresses assigned to your WAN interface.

Will IPMaps allow IP addresses from different subnets to be assigned to my Gateway? IPMap will support statically assigned WAN IP addresses from the **same** subnet.

WAN IP addresses from different subnets are **not supported**.

IPMaps Block Diagram

The following diagram shows the IPMaps principle in conjunction with existing Motorola Netopia® NAT operations:



[Link: 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:

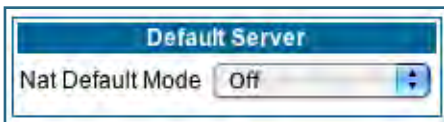
- Where you cannot anticipate what port number or packet protocol an in-bound application might use. For example, some network games select arbitrary port numbers when a connection is opened.
 - When you want all unsolicited traffic to go to a specific LAN host.
- Configure for IP Passthrough.

Configure a Default Server. This feature allows you to direct unsolicited or non-specific traffic to a designated LAN station. With NAT “On” in the Gateway, 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.

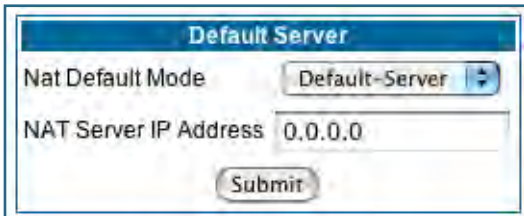
Use the following steps to setup a NAT default server to receive this information:

1. Select the [Configure](#) toolbar button, then [Advanced](#), then the [Default Server](#) link.



2. From the pull-down menu, select [Default-Server](#).

The NAT Server IP Address field appears.

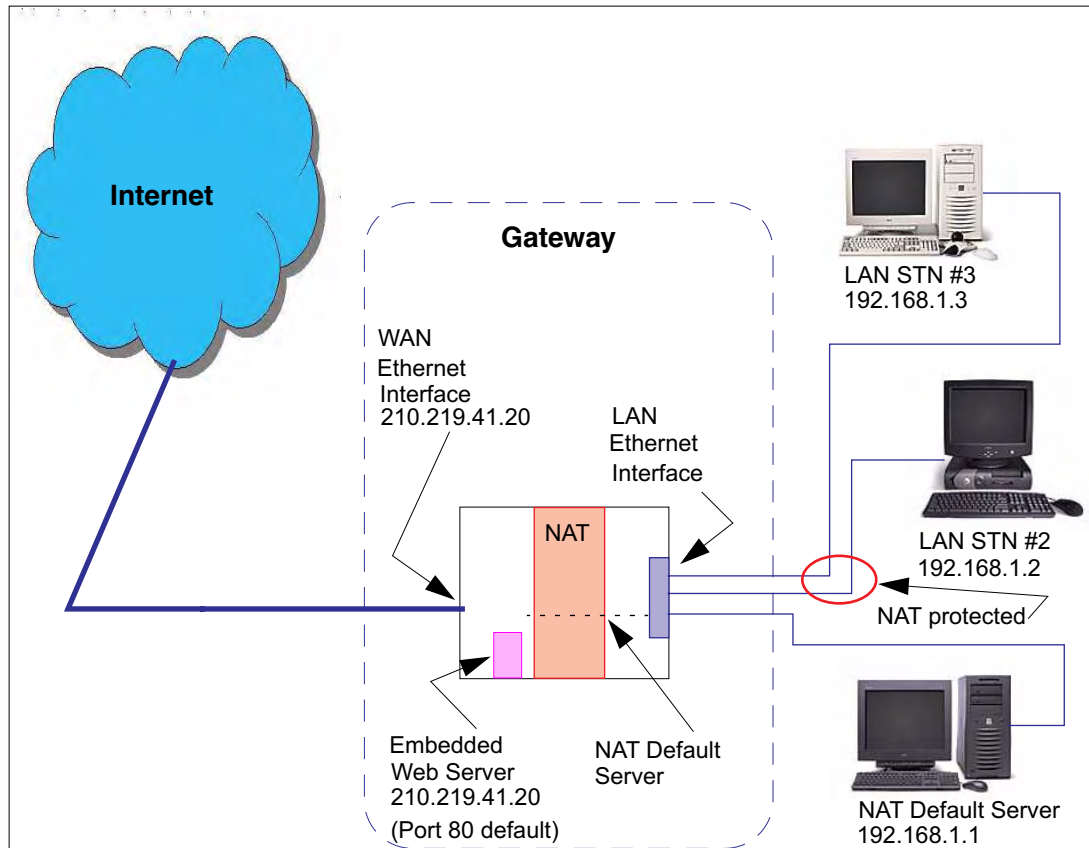


3. Determine the IP address of the LAN computer you have chosen to receive the unexpected or unknown traffic.

Enter this address in the NAT Server IP Address field.

4. Click the [Submit](#) button.
5. Click the [Alert](#) button.
6. Click the [Save and Restart](#) link to confirm.

Typical Network Diagram. A typical network using the NAT Default Server looks like this:



You can also use the LAN-side address of the Gateway, 192.168.1.x to access the web and telnet server.

NAT Combination Application. Motorola Netopia®'s NAT security feature allows you to configure a sophisticated LAN layout that uses **both** the Pinhole and Default Server capabilities.

With this topology, you configure the embedded administration ports as a first task, followed by the Pinholes and, finally, the NAT Default Server.

When using both NAT pinholes and NAT Default Server the Gateway works with the following rules (in sequence) to forward traffic from the Internet to the LAN:

1. **If the packet is a response to an existing connection created by outbound traffic from a LAN PC, forward to that station.**
2. **If not, check for a match with a pinhole configuration and, if one is found, forward the packet according to the pinhole rule.**
3. **If there's no pinhole, the packet is forwarded to the Default Server.**

IP-Passthrough. Your Gateway 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. 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 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.

- If you want to manually assign the WAN address to a LAN PC, do not check the **DHCP Enable** checkbox.
- If you check the **DHCP Enable** checkbox, the screen expands.

The **Host Hardware Address** field displays. Here you enter the MAC address of the designated IP-Passthrough computer.

- If this MAC address is not all zeroes, then it will use DHCP to set the LAN host's address to the (configured or acquired) WAN IP address.
The MAC address must be six colon-delimited or dash-delimited sets of hex digits ('0' – 'FF').
- If you leave the MAC address as zeros then the first DHCP client will be assigned the WAN address.

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.

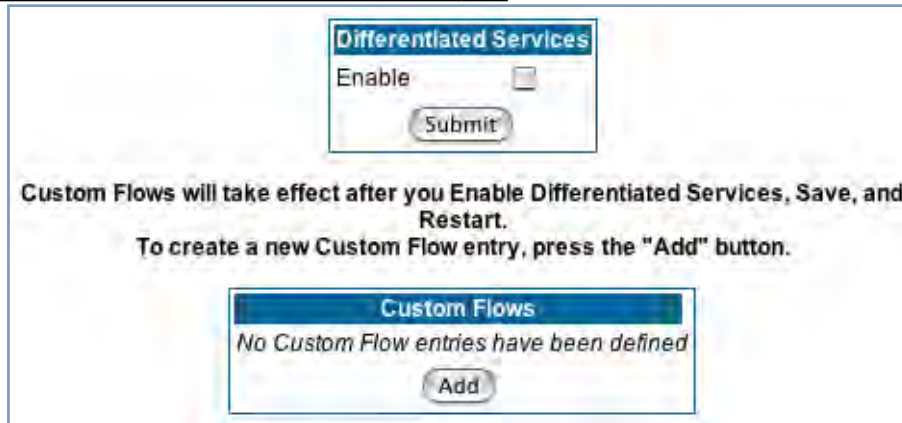
A restriction. Since both the Gateway and the passthrough host will use the same IP address, new sessions that conflict with existing sessions will be rejected by the Gateway. For example, suppose you are a teleworker using an IPSec tunnel from the Gateway *and* from the passthrough host. Both tunnels 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: Differentiated Services](#)

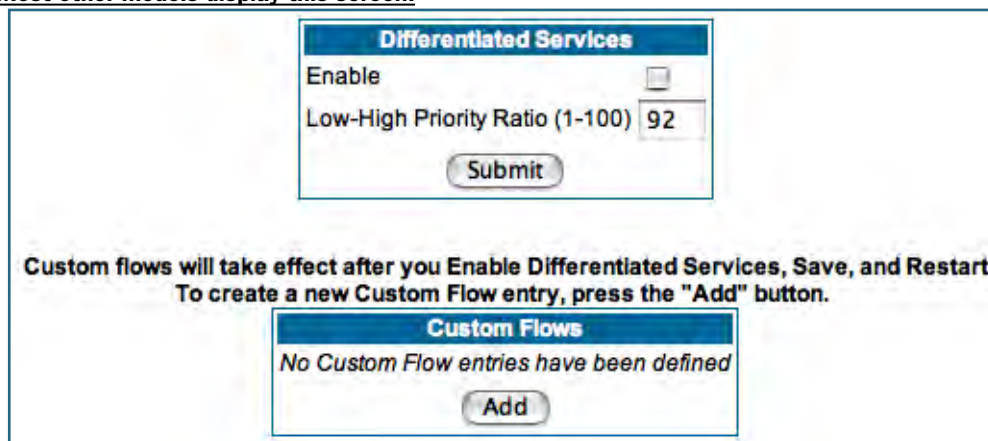
When you click the [Differentiated Services](#) link, the Differentiated Services configuration screen appears.

Differentiated Services (Diffserv) allow your Gateway to make Quality of Service (QoS) decisions about what path Internet traffic, such as Voice over IP (VoIP), should travel across your network. For example, you may want streaming video conferencing to use high quality, but more restrictive, connections, or, you might want e-mail to use less restrictive, but less reliable, connections.

VDSL and Bonded ADSL models display this screen:



Most other models display this screen:



- To enable Differentiated Services, check the **Enable** checkbox.
- (Not displayed on VDSL and Bonded ADSL models) Enter a value from 60 to 100 (percent) in the **Low-High Priority Ratio** field. The default is 92.

Differentiated Services uses the low-to-high priority queue ratio to regulate traffic flow. For example, to provide the least possible latency and highest possible throughput for high priority traffic, you could set the ratio to 100(%). This would cause the gateway to forward low priority data *only after* the high priority queue is completely empty. In practice, you should set it to something less than 100%, since the low priority traffic might have to wait too long to be passed, and consequently be subject to time-outs.

Click the [Submit](#) button.

You can then define Custom Flows. If your applications do not provide Quality of Service (QoS) control, Custom Flows allows you to define streams for some protocols, port ranges, and between specific end point addresses.

- To define a custom flow, click the [Add](#) button. The Custom Flow Entry screen appears.

The screenshot shows the 'Custom Flow Entry' configuration window. It contains the following fields and values:

Name	Custom Flow 1
Protocol	TCP
Direction	Outbound
Start Port	0
End Port	0
Inside IP Address	0.0.0.0
Inside IP Netmask	0.0.0.0
Outside IP Address	0.0.0.0
Outside IP Netmask	0.0.0.0
Quality of Service (QoS)	Off

At the bottom of the form, there is a 'Submit' button and a blue link that says 'Add or Edit more Custom Flows'.

- **Name** – Enter a name in this field to label the flow.
- **Protocol** – Select the protocol from the pull-down menu: TCP (default), UDP, ICMP, or Other. “Other” is appropriate for setting up flows on protocols with non-standard port definitions. IPSEC and PPTP are common examples.
- **Numerical Protocol** – If you select “Other” protocol, this field appears for you to provide its actual protocol number, with a range of 0 – 255.
- **Direction** – Choose Outbound (default), Inbound, or Both from the pull-down menu.
- **Start Port** – For TCP or UDP protocols, you can optionally specify a range of ports. Enter the starting port here.
- **End Port** – Enter the ending port here.
- **Inside IP Address/Netmask** – For outbound flows, specify an IP address/netmask on your LAN. For inbound flows, this setting is ignored. This setting marks packets from this LAN IP host/network based on the address and netmask information. For outbound flows, the Inside IP Address/Netmask is the source address. If you enter a zero IP address (0.0.0.0), the IP address/netmask fields

will be ignored.

- **Outside IP Address/Netmask** – If you want traffic destined for and originating from a certain WAN IP address to be controlled, enter the IP address and subnet mask here. If you leave the default all-zeroes, the outside address check is ignored.

For outbound flows, the outside address is the destination IP address for traffic; for inbound packets, the outside address is the source IP address.

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.

• **Quality of Service (QoS)** – This is the Quality of Service setting for the flow, based on the TOS bit information. Select Expedite, Assure, or Off (default) from the pull-down menu. The following table outlines the TOS bit settings and behavior:

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.

[Link: DNS](#)

Your Service Provider may maintain a Domain Name server. If you have the information for the DNS servers, enter it on the DNS page. If your Gateway is configured to use DHCP to obtain its WAN IP address, the DNS information is automatically obtained from that same DHCP Server.

If your service provider hosts a Domain Name Server, you may enter the domain name and IP address associated with the server here.

If you are receiving DNS information dynamically from your service provider, the server addresses must be entered as "0.0.0.0".

DNS	
Domain Name	<input type="text"/>
Primary DNS Server Address	<input type="text" value="0.0.0.0"/>
Secondary DNS Server Address	<input type="text" value="0.0.0.0"/>
<input type="button" value="Submit"/>	

[Link: DHCP Server](#)

Your Gateway can provide network configuration information to computers on your LAN, using the Dynamic Host Configuration Protocol (DHCP).

If you already have a DHCP server on your LAN, you should turn this service off.

If you want the Gateway to provide this service, select **Server** from the [Server Mode](#) pull-down menu, then configure the range of IP addresses that you would like the Gateway to hand out to your computers.

The screenshot shows a window titled "DHCP Server". It contains the following fields and controls:

- Server Mode:** A pull-down menu set to "Server".
- Starting IP Address:** A text box containing "192.168.1.1".
- Ending IP Address:** A text box containing "192.168.1.253".
- Lease Period (d:h:m:s):** A text box containing "00:01:00:00".
- Submit:** A button at the bottom.

You can also specify the length of time the computers can use the configuration information; DHCP calls this period the lease time.

Your Service Provider may, for certain services, want to provide configuration from its DHCP servers to the computers on your LANs. In this case, the Gateway will relay the DHCP requests from your computers to a DHCP server in the Service Provider's network.

Select **Relay-agent** and enter the IP address of the Service Provider's DHCP server in the Server Address field. This address is furnished by the Service Provider.

The screenshot shows a window titled "DHCP Server". It contains the following fields and controls:

- Server Mode:** A pull-down menu set to "Relay-agent".
- Server IP Address:** A text box containing "0.0.0.0".
- Submit:** A button at the bottom.



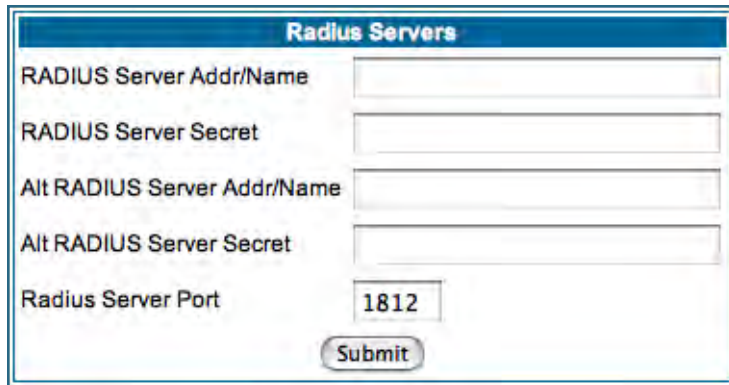
NOTE:

The relay-agent option only works when NAT is off and the Gateway is in router mode.

[Link: RADIUS Server](#)

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 click the [RADIUS](#) link, the RADIUS Servers screen appears.



- **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.
- **RADIUS Server Port:** The port on which the RADIUS server is listening, typically, the default 1812.

Click the [Submit](#) button.

You can also configure alternate RADIUS servers from the Wireless Configuration pages. See [“Use RADIUS Server” on page 65](#) for more information.

Link: [SNMP](#)

When you click the [SNMP](#) link, the SNMP configuration page appears.

Each community name below must be unique. Enter blank to delete.

Communities	
Read Community Name	public
Write Community Name	
Trap Community Name	

System Group	
System Contact	
System Location	

Notifications	
Notification Type	v1 Trap
<input type="button" value="Submit"/>	

To create a new IP Trap entry, press the "Add" button.

IP Trap Entries
No IP Trap entries have been defined
<input type="button" value="Add"/>

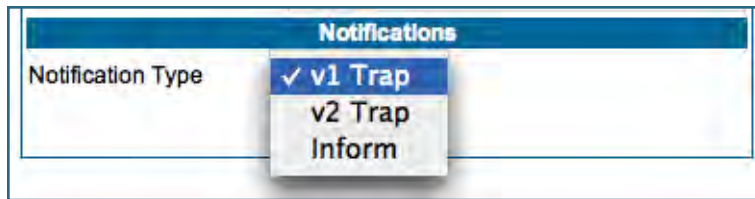
The Simple Network Management Protocol (SNMP) lets a network administrator monitor problems on a network by retrieving settings on remote network devices. The network administrator typically runs an SNMP management station program on a local host to obtain information from an SNMP agent. In this case, the Motorola Netopia® Gateway is an SNMP agent. Your Gateway supports SNMP-V1, with the exception of most sets (read-only and traps), and SNMP-V2. (For certain parts of the NPAV2TRAP.MIB – parameters under resNatParams, resDslParams, resSecParams – set is supported.)

You enter SNMP configuration information on this page. Your network administrator furnishes the SNMP parameters.



WARNING:

SNMP presents you with a security issue. The community facility of SNMP behaves somewhat like a password. The community “public” is a well-known community name. It could be used to examine the configuration of your Gateway by your service provider or an uninvited reviewer. The information can be read from the Gateway. If you are strongly concerned about security, you may leave the “public” community blank.

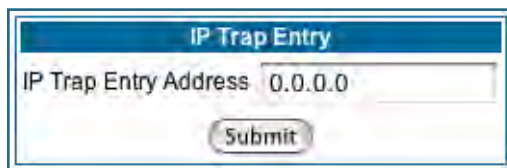


The **Notification Type** pull-down menu allows you to configure the type of SNMP notifications that will be generated:

- **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.

To send SNMP traps, you must add IP addresses for each trap receiver you want to have. Click the [Add](#) button.

The **IP Trap Entry** screen appears.



Enter an IP Trap Entry IP address. This is the destination for SNMP trap messages, the IP address of the host acting as an SNMP console.

Click the [Submit](#) button. Click the Alert icon, and in the resulting page, click the [Save and Restart](#) link.

[Link: IGMP \(Internet Group Management Protocol\)](#)

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.

See the “Advanced” option in [“LAN” on page 49](#) for more information.

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.

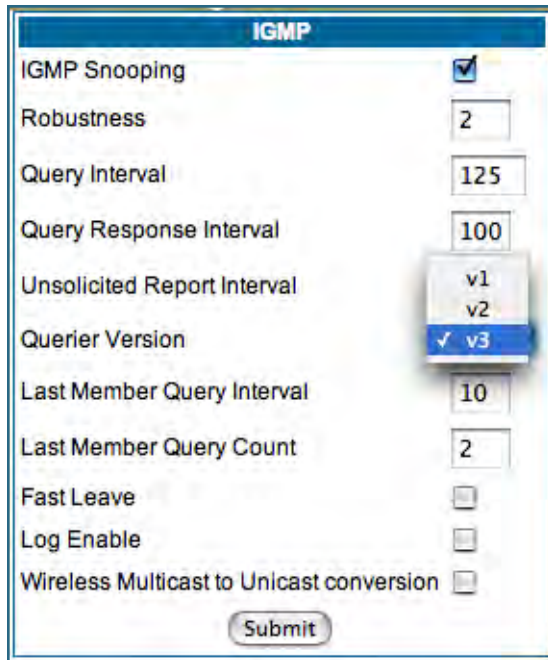
IGMP Version 3 supports:

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.

To configure IGMP options available in Motorola Netopia® Gateways, click the [IGMP](#) link.

The **IGMP** page appears.



You can set the following options:

- **IGMP Snooping** – checking this checkbox 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.

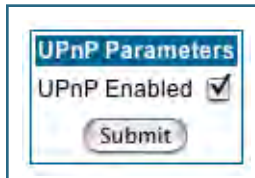
- **Querier Version** – Select a version of the IGMP Querier from the pull-down menu: **v1**, **v2**, or **v3**. The default **v3** allows for backward compatibility mode with the earlier versions, and should not need to be changed. However, for administrative purposes you may select either **v1** or **v2**.
- **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 deci-seconds).
- **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** – Checking this checkbox 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. By default, Fast Leave is set to **Off**.
- **Log Enable** – If you check this checkbox, all IGMP messages on both the LAN and the WAN will be logged.
- **Wireless Multicast to Unicast conversion** – This checkbox only appears if **IGMP Snooping** is enabled. If you check this checkbox, 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.

Click the [Submit](#) button. Click the Alert icon, and in the resulting page, click the [Save and Restart](#) link.

[Link: 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.

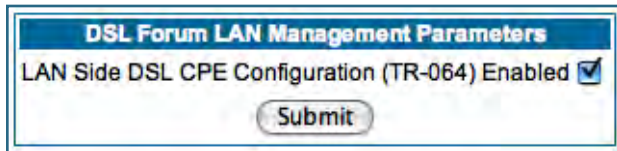
PCs using UPnP can retrieve the Gateway’s WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with a UPnP-enabled Motorola Netopia® Gateway, will not need application layer gateway support on the Motorola Netopia® Gateway to work through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

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

- Uncheck the [UPnP Enabled](#) checkbox, and click the [Submit](#) button.
- The Alert icon will appear in the upper right corner of the web page. Click the Alert icon, and when prompted, click the [Save and Restart](#) link.

Link: LAN Management

TR-064 is a LAN-side DSL Gateway configuration specification. It 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.



DSL Forum LAN Management Parameters

LAN Side DSL CPE Configuration (TR-064) Enabled

Submit

TR-064 is enabled by default. To *disable* it:

- Uncheck the **Enabled** checkbox, and click the **Submit** button.
- The Alert icon will appear in the upper right corner of the web page. Click the Alert icon, and when prompted, click the **Save and Restart** link.

Link: Ethernet Bridge

The Motorola Netopia® Gateway can be used as a bridge, rather than a router. A bridge is a device that joins two networks. As an Internet access device, a bridge connects the home computer directly to the service provider's network equipment with no intervening routing functionality, such as Network Address Translation. Your home computer becomes just another address on the service provider's network. In a DSL connection, the bridge serves simply to convey the digital data information back and forth over your telephone lines in a form that keeps it separate from your voice telephone signals.

If your service provider's network is set up to provide your Internet connectivity via bridge mode, you can set your Motorola Netopia® Gateway to be compatible.

Bridges let you join two networks, so that they appear to be part of the same physical network. As a bridge for protocols other than TCP/IP, your Gateway keeps track of as many as 512 MAC (Media Access Control) addresses, each of which uniquely identifies an individual host on a network. Your Gateway uses this bridging table to identify which hosts are accessible through which of its network interfaces. The bridging table contains the MAC address of each packet it sees, along with the interface over which it received the packet. Over time, the Gateway learns which hosts are available through its WAN port and/or its LAN port.

When configured in Bridge Mode, the Motorola Netopia® will act as a pass-through device and allow the workstations on your LAN to have public addresses directly on the internet.



NOTE:

In this mode the Motorola Netopia® is providing NO firewall protection as is afforded by NAT. Also, only the workstations that have a public address can access the internet. This can be useful if you have multiple static public IPs on the LAN.

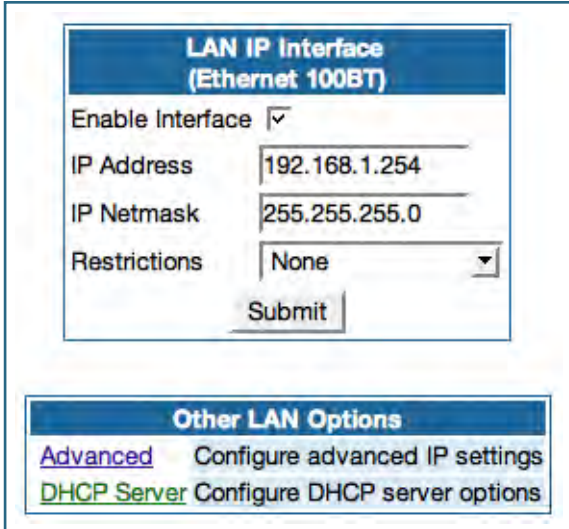
Bridging per WAN is supported in conjunction with VLANs – individual WANs can be bridged to the LAN only if the WANs are part of a VLAN. (See [“VLAN” on page 107](#) for more information.) The capability to bridge individual VLANs is supported only if the underlying encapsulation is RFC1483-Bridged (ether-Ilc).

Configuring for Bridge Mode

1. Browse into the Motorola Netopia® Gateway's web interface.
2. Click on the [Configure](#) button in the upper Menu bar.
3. Click on the [LAN](#) link.

The LAN page appears.

4. In the box titled LAN IP Interface (Ethernet 100BT):



LAN IP Interface (Ethernet 100BT)

Enable Interface

IP Address

IP Netmask

Restrictions

Submit

Other LAN Options

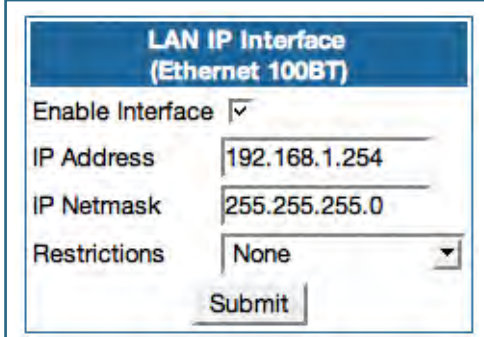
[Advanced](#) Configure advanced IP settings

[DHCP Server](#) Configure DHCP server options

Make note of the Ethernet IP Address and subnet mask. You can use this address to access the router in the future.

5. Click on the [Advanced](#) link in the left-hand links toolbar.
6. Under the heading of Services, click on the [Ethernet Bridge](#) link.

The Ethernet Bridge page appears.



LAN IP Interface (Ethernet 100BT)

Enable Interface

IP Address

IP Netmask

Restrictions

Submit

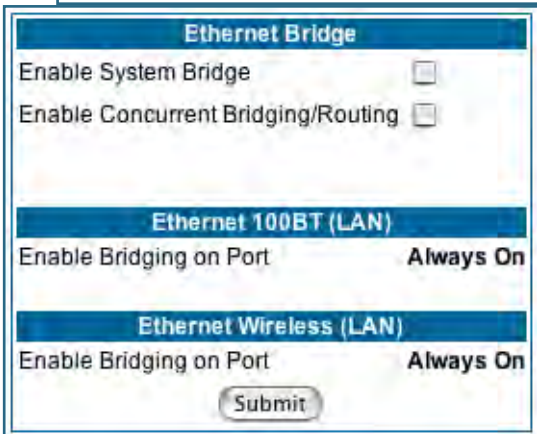
The appearance of this page varies, depending on your Gateway's interfaces.

7. **If available:**
 - a. Check the **Enable Bridging on Port** selection. (This may be Always On.)
 - b. Click [Submit](#).
8. **If you want the Gateway to do both bridging and routing, check the [Enable Concurrent Bridging/Routing](#) checkbox.**

When this mode is enabled, the Gateway will appear to be a router, but also bridge traffic from the LAN if it has a valid LAN-side address.

9. Check the [Enable System Bridge](#) checkbox.

The window shrinks.



Ethernet Bridge

Enable System Bridge

Enable Concurrent Bridging/Routing

Ethernet 100BT (LAN)

Enable Bridging on Port **Always On**

Ethernet Wireless (LAN)

Enable Bridging on Port **Always On**

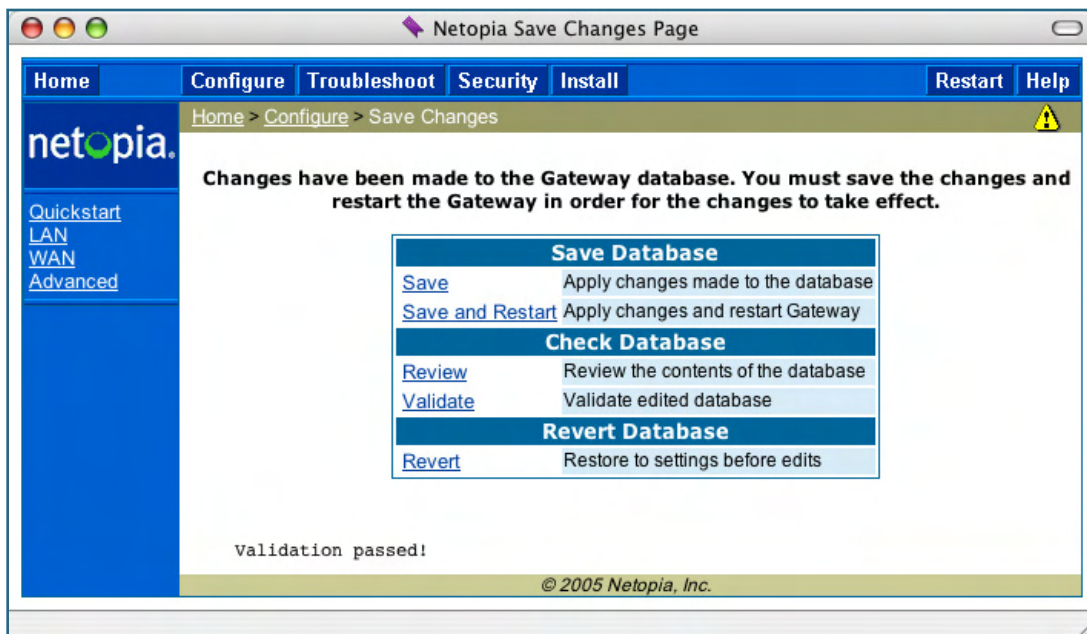
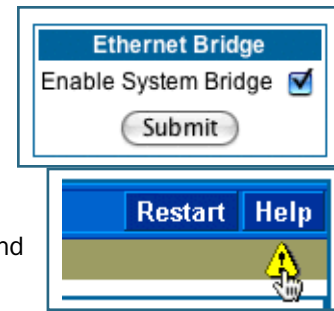
Submit

- b. Click [Submit](#).

At this point you should be ready to do the final save on the configuration changes you have made.

The yellow **Alert** symbol will appear beneath the Help button on the right-hand end of the menu bar.

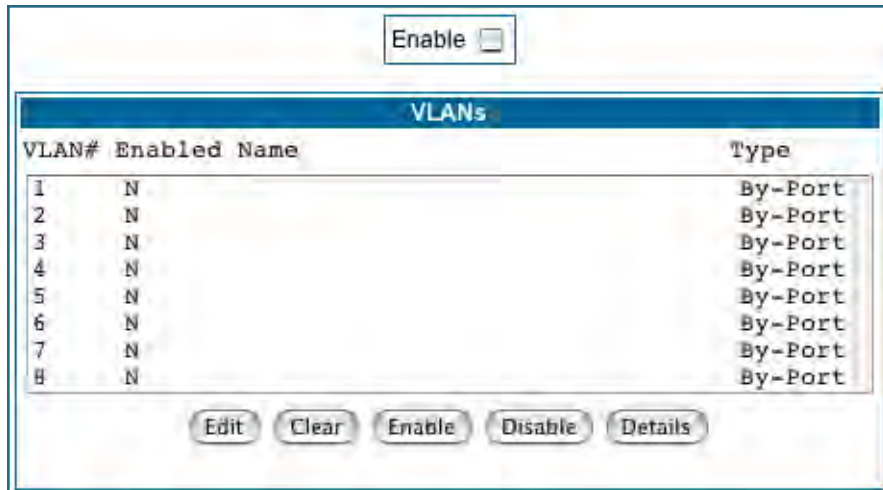
10. **Click on the Alert symbol and you will see whether your changes have been validated.**
11. **If you are satisfied with the changes you have made, click [Save and Restart](#) in the Save Database box to Apply changes and restart Gateway.**



You have now configured your Motorola Netopia® Gateway for bridging, and it will bridge all traffic across the WAN. You will need to make configurations to your machines on your LAN. These settings must be made in accordance with your ISP. If you ever need to get back into the Motorola Netopia® Gateway again for management reasons, you will need to manually configure your machine to be in the same subnet as the Ethernet interface of the Motorola Netopia®, since DHCP server is not operational in bridge mode.

Link: VLAN

When you click the [VLAN](#) link the **VLANs** page appears.



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:

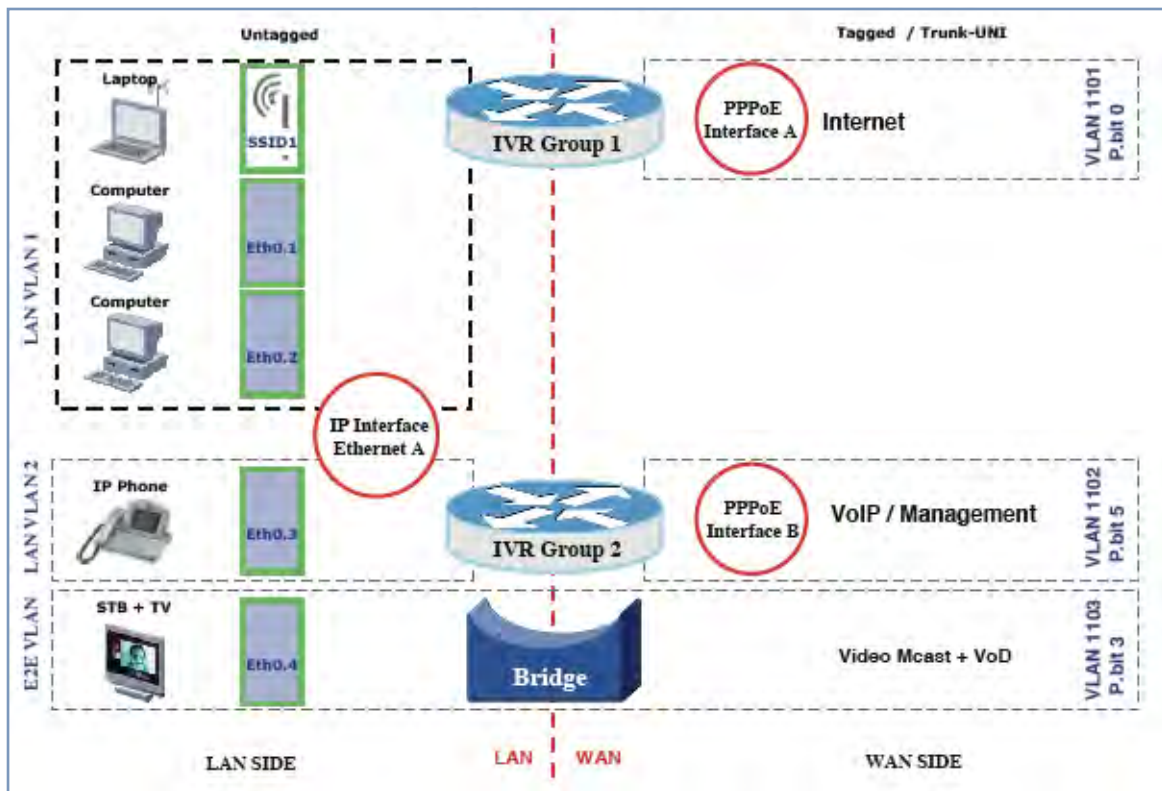
- If traffic needs to be bridged between LAN and WAN you can create a single VLAN that encompasses the WAN port and LAN ports.
- If traffic needs to be routed then you must define four elements:
 - LAN-side VLANs
 - WAN-side VLANs
 - Associate IP Interfaces to VLANs
 - Inter-VLAN Routing Groups: configuration 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.

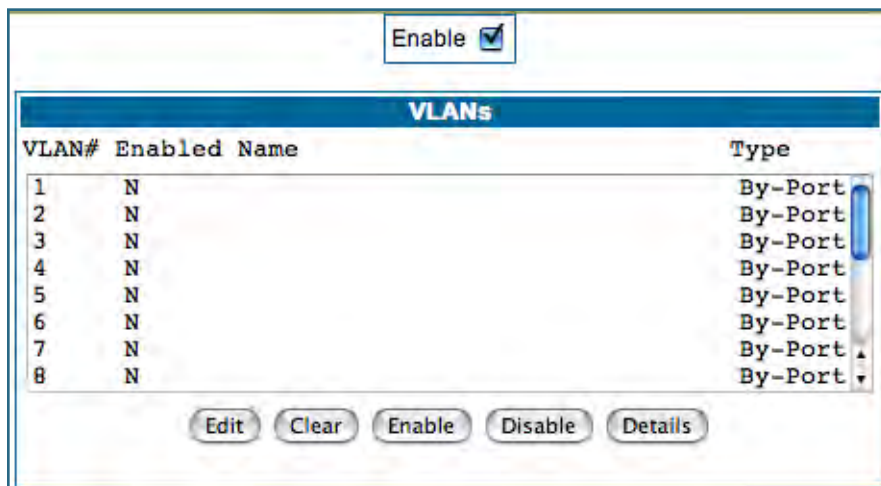
- Example: to route between a VCC and all the LAN ports, which effectively is similar to the default configuration without any VLANs:
Create a VLAN named "VccWan" consisting of vcc1, ip-vcc1, routing-group 1
Create a VLAN named "Lan" consisting of eth0.1, eth0.2, eth0.3, eth0.4, ssid1, ssid2, ssid3, 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.



To create a VLAN select a list item from the main VLAN page and click the [Edit](#) button.

The **VLAN Entry** page appears.



VLAN Entry: 1

Enable

VLAN Name

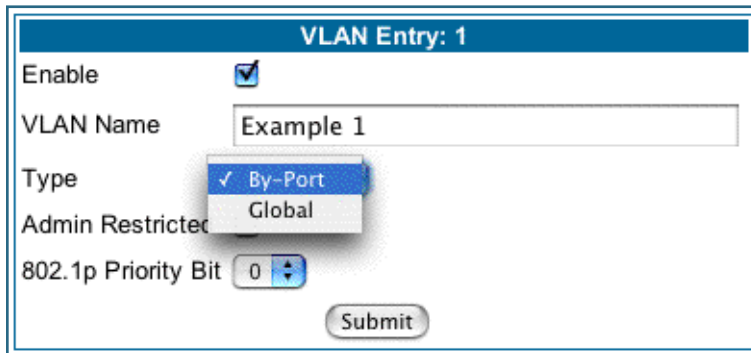
Type **By-Port**

Admin Restricted

802.1p Priority Bit

Submit

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



VLAN Entry: 1

Enable

VLAN Name

Type **By-Port**
Global

Admin Restricted

802.1p Priority Bit

Submit

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:** indicates 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** indicates 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.)

- **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 **VLAN Port Configuration** screen appears.

Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	<input type="checkbox"/>				
eth0.2	<input type="checkbox"/>				
eth0.3	<input type="checkbox"/>				
eth0.4	<input type="checkbox"/>				
ssid1	<input type="checkbox"/>				
usb	<input type="checkbox"/>				
vcc1	<input type="checkbox"/>				
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 **Enable Multiple Wireless IDs** on [page 59](#))
- 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.

Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1
eth0.2	<input type="checkbox"/>				
eth0.3	<input type="checkbox"/>				
eth0.4	<input type="checkbox"/>				
ssid1	<input type="checkbox"/>				
ssid2	<input type="checkbox"/>				
ssid3	<input type="checkbox"/>				
usb	<input type="checkbox"/>				
vcc1	<input type="checkbox"/>				

IP interfaces: none

Submit

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. See [“Differentiated Services” on page 92](#) for more information.

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 271](#). See also [“Differentiated Services” on page 92](#) for more information.

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 if it is to be routed; otherwise leave the default. 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

usb

vcc1

IP interfaces: none

Submit

- 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.


Port Configuration for VLAN: 1

Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
eth0.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
eth0.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
eth0.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
ssid1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
ssid2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
ssid3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
vcc1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

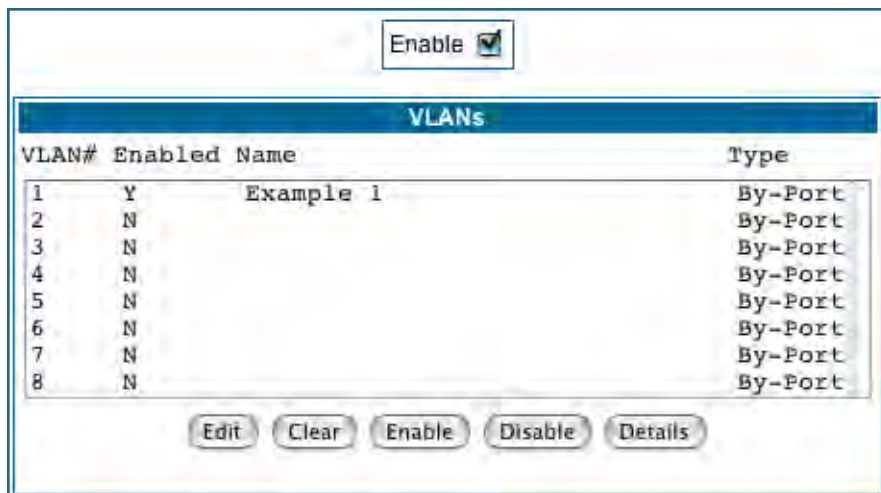
IP interfaces


Inter-VLAN-Group Enable

Group-1	<input checked="" type="checkbox"/>
Group-2	<input type="checkbox"/>
Group-3	<input type="checkbox"/>
Group-4	<input type="checkbox"/>
Group-5	<input type="checkbox"/>
Group-6	<input type="checkbox"/>
Group-7	<input type="checkbox"/>
Group-8	<input type="checkbox"/>

- Click the [Submit](#) button.
- When you are finished, click the Alert icon  in the upper right-hand corner of the screen, and in the resulting screen, click the [Save](#) link.
- If you want to create more VLANs, click the [Advanced](#) link (in the left-hand toolbar) and then the [VLAN](#) link in the resulting page, and 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.



- When you are finished, click the Alert icon  in the upper right-hand corner of the screen, and in the resulting screen, click the [Save and Restart](#) link.

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.

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

Admin Restricted

Off

802.1p Priority Bit (VLAN#: 1)

0

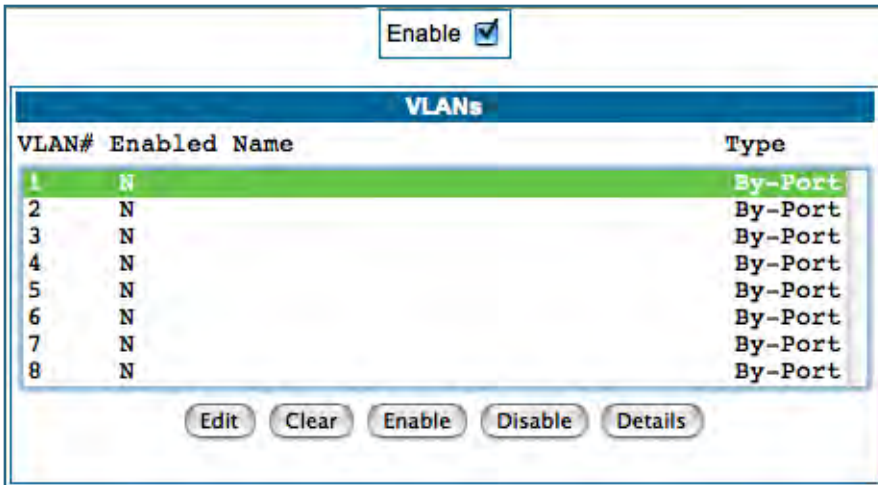
Portname	Enable	Tag	Priority	Promote	802.1p Priority Bit
eth0.1	On	Off	On	On	0
eth0.2	On	Off	Off	Off	0
eth0.3	Off				
eth0.4	Off				
ssid1	On	Off	Off	Off	0
ssid2	Off				
ssid3	Off				
vcc1	Off				
IP interfaces	ip-eth-a				
Inter-VLAN-Group	Enable				
Group-1	On				
Group-2	Off				
Group-3	Off				
Group-4	Off				
Group-5	Off				
Group-6	Off				
Group-7	Off				
Group-8	Off				

Example

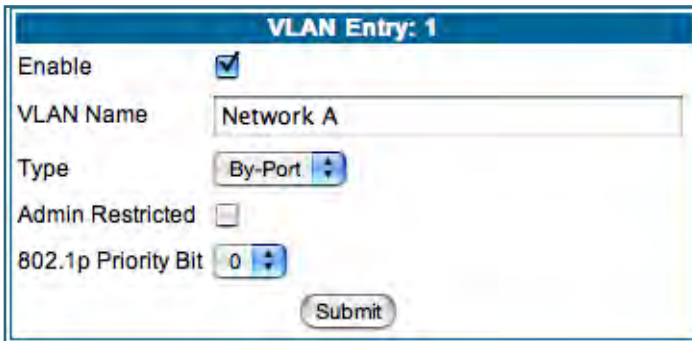
The following is a simple example of how you might configure some VLANs:

You want to configure a 3347NWG-VGx Gateway with two SSIDs (see [“Multiple SSIDs” on page 59](#) 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.



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



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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
eth0.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
eth0.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
eth0.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
ssid1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
ssid2	<input type="checkbox"/>			
ssid3	<input type="checkbox"/>			
vcc1	<input type="checkbox"/>			
IP interfaces	ip-eth-a			
Inter-VLAN-Group	Enable			
Group-1	<input checked="" type="checkbox"/>			
Group-2	<input type="checkbox"/>			
Group-3	<input type="checkbox"/>			
Group-4	<input type="checkbox"/>			
Group-5	<input type="checkbox"/>			
Group-6	<input type="checkbox"/>			
Group-7	<input type="checkbox"/>			
Group-8	<input type="checkbox"/>			

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 Entry: 2	
Enable	<input checked="" type="checkbox"/>
VLAN Name	Network B
Type	By-Port
Admin Restricted	<input checked="" type="checkbox"/>
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**.

Portname	Enable	Tag	Priority	Promote	802.1p	Priority Bit
eth0.1	<input type="checkbox"/>					
eth0.2	<input type="checkbox"/>					
eth0.3	<input type="checkbox"/>					
eth0.4	<input type="checkbox"/>					
ssid1	<input type="checkbox"/>					
ssid2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			0
ssid3	<input type="checkbox"/>					
vcc1	<input type="checkbox"/>					

IP interfaces: ip-eth-a

Inter-VLAN-Group: Group-2

Submit

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 Entry: 3

Enable:

VLAN Name: WAN VLAN

Type: By-Port

Admin Restricted:

802.1p Priority Bit: 0

Submit

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

Port Configuration for VLAN: 3				
Portname	Enable	Tag	Priority	Promote 802.1p Priority Bit
eth0.1	<input type="checkbox"/>			
eth0.2	<input type="checkbox"/>			
eth0.3	<input type="checkbox"/>			
eth0.4	<input type="checkbox"/>			
ssid1	<input type="checkbox"/>			
ssid2	<input type="checkbox"/>			
ssid3	<input type="checkbox"/>			
vcc1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
IP interfaces	ip-vcc1			
Inter-VLAN-Group	Enable			
Group-1	<input checked="" type="checkbox"/>			
Group-2	<input checked="" type="checkbox"/>			
Group-3	<input type="checkbox"/>			
Group-4	<input type="checkbox"/>			
Group-5	<input type="checkbox"/>			
Group-6	<input type="checkbox"/>			
Group-7	<input type="checkbox"/>			
Group-8	<input type="checkbox"/>			

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.

11. **Once you have finished with the configuration of the VLANs, click the Alert icon in the upper right hand corner.**

This will validate that the settings are legal for your network.

12. **Click the [Save and Restart](#) link.**

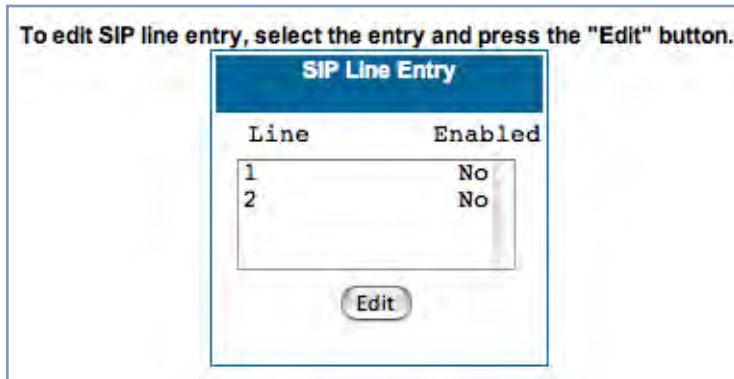
This will restart the Motorola Netopia® Gateway and retain the VLAN configuration.

[Link: VoIP](#)

(supported models only)

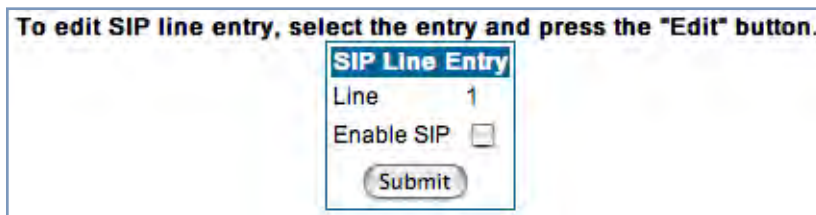
Voice-over-IP (VoIP) refers to the ability to make voice telephone calls over the Internet. This differs from traditional phone calls that use the Public Switched Telephone Network (PSTN). VoIP calls use an Internet protocol, Session Initiation Protocol (SIP), to transmit sound over a network or the 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.

When you click the [VoIP](#) link, the **SIP Line Entry** page appears.



To enable a VoIP line, select one of the lines from the SIP Line Entry menu that corresponds to the port on the Gateway to which your phone is connected.

Click the [Edit](#) button. In the resulting screen, check the **Enable SIP** checkbox.



The screen expands to display the features that you can enable for that line.

To edit SIP line entry, select the entry and press the "Edit" button.

SIP Line Entry	
Line	1
Enable SIP	<input checked="" type="checkbox"/>
Transport Type	UDP
Registration Interval (in secs)	<input type="text" value="3600"/>
Registrar Server	<input type="text"/>
Registrar Port	<input type="text" value="5060"/>
Proxy Server	<input type="text"/>
Proxy Port	<input type="text" value="5060"/>
Outbound Proxy Server	<input type="text"/>
Outbound Proxy Port	<input type="text" value="5060"/>
User Display Name	<input type="text"/>
SIP User Name	<input type="text"/>
SIP User Password	<input type="password"/>
Auth User ID	<input type="text"/>
Call Features	
DTMF Mode	<input type="text" value="Info"/>
Enable End of Dial Marker	<input type="checkbox"/>
Enable Call Forwarding Unconditionally	<input type="checkbox"/>
Enable Call Forwarding On Busy	<input type="checkbox"/>
Enable Call Forwarding On No Answer	<input type="checkbox"/>
Enable Waiting	<input type="checkbox"/>
Enable Conferencing	<input type="checkbox"/>
Subscribe for Do Not Disturb	<input type="checkbox"/>
Subscribe for MWI	<input type="checkbox"/>
<input type="button" value="Submit"/>	

SIP Line Entry

Registration Interval (in secs)	Length of time the VoIP registration will be valid before it will be renewed. Default is 1 hour.
Registrar Server	Registration Server name or IP address.
Registrar Port	Registration Server port. Default is 5060.
Proxy Server	Proxy server name or IP address.

SIP Line Entry


Proxy Port	Proxy server port, if required. Default is 5060.
Outbound Proxy Server	Outbound Proxy server name or IP address, if required.
Outbound Proxy Port	Outbound Proxy server port, if required. Default is 5060.
User Display Name	Name of this phone's user to be displayed on the Home page. Example: "Jacob Q. Smith"
SIP User Name	Registration user ID. Example: "jqsmith"
SIP User Password	Registration user password.
Auth User ID	The authorization ID that authenticates the user to SIP for the specified phone. Most SIP Servers expect this to be the User Name itself but some may use Auth User ID .

Call Features Settings


DTMF Mode	Choose the Dual Tone Multi-Frequency Mode: <ul style="list-style-type: none"> • 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.
Enable End of Dial Marker	If you check this checkbox, the Gateway will generate an "end of dial" (#) signal that indicates that the dialed number is complete.
Enable Call Forwarding Unconditionally	If you check this checkbox, all calls will be forwarded to a specified number. The Unconditional Call Forwarding Number field will appear for you to enter the number, if enabled.
Enable Call Forwarding On Busy	If you check this checkbox, calls will be forwarded to a specified number if the line is busy. The On Busy Call Forwarding Number field will appear for you to enter the number, if enabled.
Enable Call Forwarding On No Answer	If you check this checkbox, calls will be forwarded to a specified number if there is no answer. The On No Answer Call Forwarding Number field will appear for you to enter the number, if enabled.
Enable Waiting	If you check this checkbox, call waiting is enabled.
Enable Conferencing	If you check this checkbox, 3-party teleconferencing is enabled.
Subscribe for Do Not Disturb	If you check this checkbox, the Gateway will reject VoIP calls without ringing the phone.
Subscribe for MWI	If you check this checkbox, Message Waiting Indicator is enabled when new voice mail is received.

When you are finished entering the required information, click the [Submit](#) button.

To configure the second voice port, return to the **SIP Line Entry** screen by clicking the [VoIP](#) link in the Breadcrumb Trail.

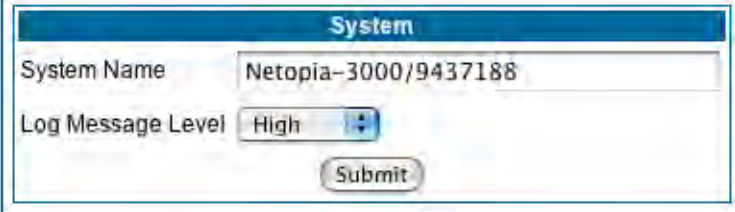
When you are finished, click the Alert icon  in the upper right corner of the page, and in the resulting page, click the [Save and Restart](#) link.

The **Home** page for a VoIP-enabled Gateway with both phone lines registered is shown below.

Home		Configure	Troubleshoot	Security	Install	Restart	Help
							
Configure Troubleshoot Security Install Basic Mode							
General Information							
Hardware	Netopia Model 2247-41-10NA ADSL2 WIAD						
Serial Number	9437188						
Software Version	7.7.4	BreakWater Firewall	ClearSailing				
Product ID	1225						
Date & Time	Fri Jun 1 10:07:20 2007	Safe Harbour	On				
WAN							
Status	Up	Data Rate (Kbps)	Downstream: 8000 Upstream: 800				
Local Address	0.0.0.0	Peer Address	0.0.0.0				
Connection Type	Always On						
NAT	On	WAN Users	Unlimited				
LAN							
IP Address	192.168.1.254						
Netmask	255.255.255.0						
DHCP Server	On	Ethernet Status	Up				
		DHCP Leases	0 out of 253 leases in use				
VoIP							
Line 1 Registration	Registered	Line 2 Registration	Registered				
Line 1 Account	4004	Line 2 Account	4005				
© 2007 Netopia, Inc.							

Link: System

The **System Name** defaults to your Gateway's factory identifier combined with its serial number. Some cable-oriented Service Providers use the System Name as an important identification and support parameter.



The screenshot shows a web form titled "System". It contains two main input fields: "System Name" with the value "Netopia-3000/9437188" and "Log Message Level" with a dropdown menu set to "High". A "Submit" button is located at the bottom right of the form.

The System Name can be 1 – 255 characters long; it can include embedded spaces and special characters.

The **Log Message Level** alters the severity at which messages are collected in the Gateway's system log. Do not alter this field unless instructed by your Support representative.

Link: Syslog Parameters

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the Gateway's WAN Event History. Syslog sends log-messages to a host that you specify.

To enable syslog logging, click on the [Syslog Parameters](#) link.



The screenshot shows a small form titled "Syslog Parameters". It contains a checkbox labeled "Syslog" which is currently unchecked, and a "Submit" button below it.

Check the **Syslog** checkbox.

The screen expands.



The expanded screenshot shows the "Syslog Parameters" form with the following fields and options:

- Syslog**: A checkbox that is checked.
- Syslog Host Name/IP Address**: A text input field.
- Facility**: A pull-down menu currently set to "local0".
- Log Violations**: An unchecked checkbox.
- Log Access Attempts**: An unchecked checkbox.
- Log Accepted Packets**: An unchecked checkbox.
- Submit**: A button at the bottom.

- **Syslog**: Enable syslog logging in the system.
- **Syslog Host Name/IP Address**: Enter the name or the IP Address of the host that should receive syslog messages.
- **Facility**: From the pull-down menu, select the Syslog facility to be used by the router when generating syslog messages. Options are *local0* through *local7*.
- **Log Violations**: If you check this checkbox, the Gateway will generate messages whenever a packet is discarded because it violates the router's security policy.
- **Log Access Attempts**: If you check this checkbox, the Gateway will generate messages whenever a packet attempts to access the router or tries to pass through the router. This option is disabled by default.
- **Log Accepted Packets**: If you check this checkbox, the Gateway will generate messages whenever a packet accesses the router or passes through the router. This option is disabled by default.



NOTE:

Syslog needs to be enabled to comply with logging requirements mentioned in The Modular Firewall Certification Criteria - Baseline Module - version 4.1 (specified by ICSA Labs).

For more information, please go to the following URL:

<http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/baseline.pdf>

Log Event Messages

Administration Related Log Messages

- | | |
|---|--|
| 1. administrative access attempted: | This log-message is generated whenever the user attempts to access the router's management interface. |
| 2. administrative access authenticated and allowed: | This log-message is generated whenever the user attempts to access the router's management interface and is successfully authenticated and allowed access to the management interface. |
| 3. administrative access allowed: | If for some reason, a customer does not want password protection for the management interface, this log-message is generated whenever any user attempts to access the router's management interface and is allowed access to the management interface. |
| 4. administrative access denied - invalid user name: | This log-message is generated whenever the user tries to access the router's management interface and authentication fails due to incorrect user-name. |
| 5. administrative access denied - invalid password: | This log-message is generated whenever the user tries to access the router's management interface and authentication fails due to incorrect password. |
| 6. administrative access denied - telnet access not allowed: | This log-message is generated whenever the user tries to access the router's Telnet management interface from a Public interface and is not permitted since Remote Management is disabled. |
| 7. administrative access denied - web access not allowed: | This log-message is generated whenever the user tries to access the router's HTTP management interface from a Public interface and is not permitted since Remote Management is disabled. |

System Log Messages

- | | |
|--|--|
| 1. Received NTP Date and Time: | This log-message is generated whenever NTP receives Date and time from the server. |
| 2. EN: IP up: | This log-message is generated whenever Ethernet WAN comes up. |
| 3. WAN: Ethernet WAN1 activated at 100000 Kbps: | This log-message is generated when the Ethernet WAN Link is up. |
| 4. Device Restarted: | This log-message is generated when the router has been restarted. |

DSL Log Messages (most common):

- | | |
|---|--|
| 1. WAN: Data link activated at <Rate> Kbps (rx/tx) | This log message is generated when the DSL link comes up. |
| 2. WAN: Data link deactivated | This log message is generated when the DSL link goes down. |
| 3. RFC1483 up | This log message is generated when RFC1483 link comes up. |
| 4. RFC1483-<WAN-instance>: IP down | This log message is generated when RFC1483 link goes down. |

DSL Log Messages (most common):

- | | |
|---|---|
| 5. PPP: Channel <ID> up Dialout Profile name: <Profile Name> | This log message is generated when a PPP channel comes up. |
| 6. PPP-<WAN Instance> down: <Reason> | This log message is generated when a PPP channel goes down. The reason for the channel going down is displayed as well. |

Access-related Log Messages

- | | |
|---|--|
| 1. permitted: | This log-message is generated whenever a packet is allowed to traverse router-interfaces or allowed to access the router itself. |
| 2. attempt: | This log-message is generated whenever a packet attempts to traverse router-interfaces or attempts to access the router itself. |
| 3. dropped - violation of security policy: | This log-message is generated whenever a packet, traversing the router or destined to the router itself, is dropped by the firewall because it violates the expected conditions. |
| 4. dropped - invalid checksum: | This log-message is generated whenever a packet, traversing the router or destined to the router itself, is dropped because of invalid IP checksum. |
| 5. dropped - invalid data length: | This log-message is generated whenever a packet, traversing the router or destined to the router itself, is dropped because the IP length is greater than the received packet length or if the length is too small for an IP packet. |
| 6. dropped - fragmented packet: | This log-message is generated whenever a packet, traversing the router, is dropped because it is fragmented, stateful inspection is turned ON on the packet's transmit or receive interface, and deny-fragment option is enabled. |
| 7. dropped - cannot fragment: | This log-message is generated whenever a packet traversing the router is dropped because the packet cannot be sent without fragmentation, but the do not fragment bit is set. |
| 8. dropped - no route found: | This log-message is generated whenever a packet, traversing the router or destined to the router itself, is dropped because no route is found to forward the packet. |
| 9. dropped - invalid IP version: | This log-message is generated whenever a packet, traversing the router or destined to the router itself, is dropped because the IP version is not 4. |
| 10. dropped - possible land attack: | This log-message is generated whenever a packet, traversing the router or destined to the router itself, is dropped because the packet is TCP/UDP packet and source IP Address and source port equals the destination IP Address and destination port. |
| 11. TCP SYN flood detected: | This log-message is generated whenever a SYN packet destined to the router's management interface is dropped because the number of SYN-sent and SYN-receives exceeds one half the number of allowable connections in the router. |
| 12. Telnet receive DoS attack - packets dropped: | This log-message is generated whenever TCP packets destined to the router's telnet management interface are dropped due to overwhelming receive data. |

Access-related Log Messages

13. dropped - reassembly timeout:

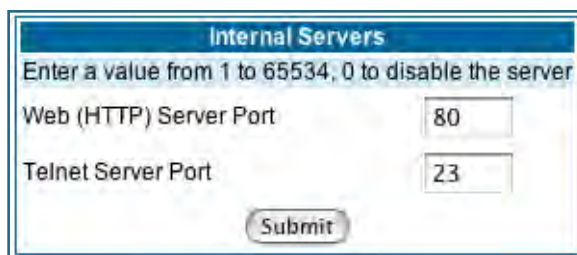
This log-message is generated whenever packets, traversing the router or destined to the router itself, are dropped because of reassembly timeout.

14. dropped - illegal size:

This log-message is generated whenever packets, traversing the router or destined to the router itself, are dropped during reassembly because of illegal packet size in a fragment.

Link: Internal Servers

Your Gateway ships with an embedded Web server and support for a Telnet session, to allow ease of use for configuration and maintenance. The default ports of **80** for HTTP and **23** for Telnet may be reassigned. This is necessary if a pinhole is created to support applications using port 80 or 23. [See "Pinholes" on page 82.](#) for more information on Pinhole configuration.



Internal Servers	
Enter a value from 1 to 65534, 0 to disable the server	
Web (HTTP) Server Port	80
Telnet Server Port	23
<input type="button" value="Submit"/>	

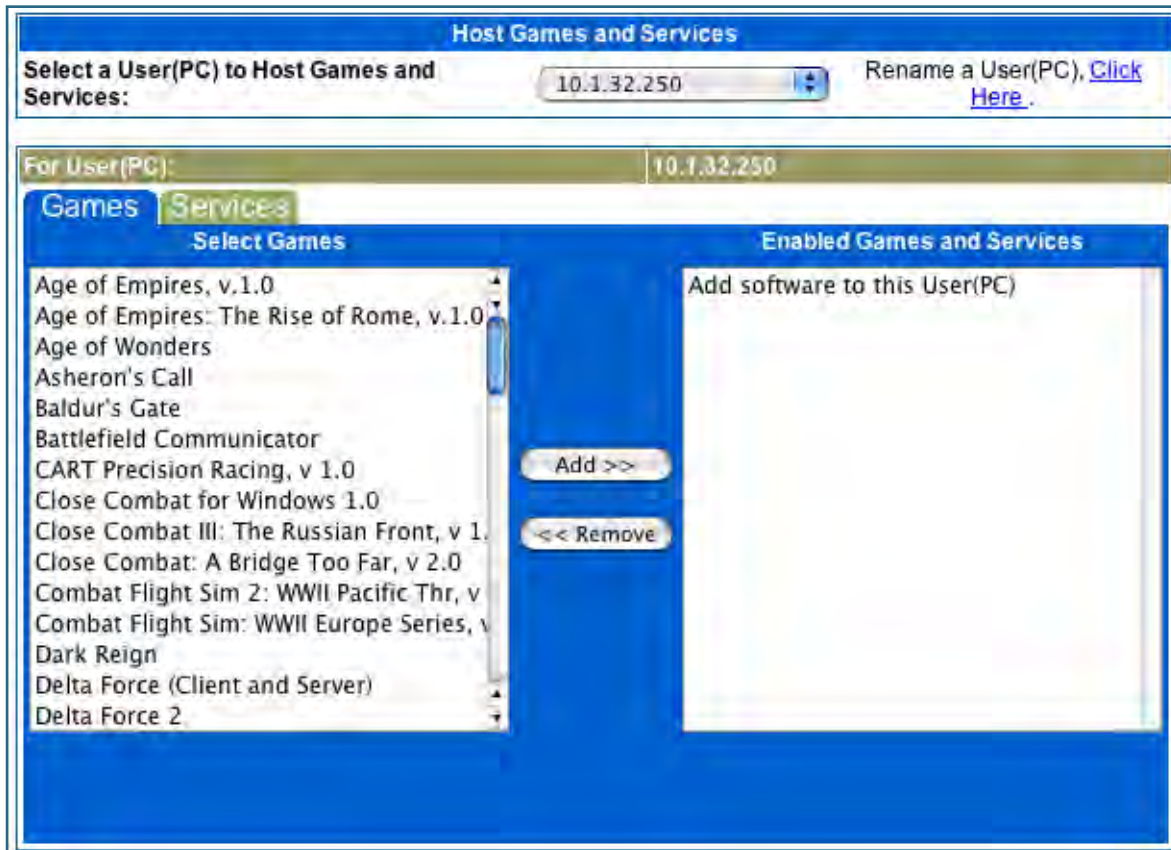
Web (HTTP) Server Port: To reassign the port number used to access the Motorola Netopia® embedded Web server, change this value to a value greater than 1024. When you next access the embedded Motorola Netopia® Web server, append the IP address with <port number>, (e.g. Point your browser to **http://210.219.41.20:8080**).

Telnet Server Port: To reassign the port number used to access your Motorola Netopia® embedded Telnet server, change this value to a value greater than 1024. When you next access the Motorola Netopia® embedded Telnet server, append the IP address with <port number>, (e.g. **telnet 210.219.41.20 2323**).

You can also use the LAN-side address of the Gateway, 192.168.1.x:8100 to access the web server and 192.168.1.x:2323 to access the telnet server. The value of 0 for an internal server port will disable that server. You can disable Telnet or Web, but not both. If you disabled both ports, you would not be able to reconfigure the unit without pressing the reset button.

[Link: Software Hosting](#)

Software Hosting allows you to host internet applications when NAT is enabled. **User(PC)** specifies the machine on which the selected software is hosted. You can host different games and software on different PCs.



To select the games or software that you want to host for a specific PC, highlight the name(s) in the box on the left side of the screen. Click the [Add](#) button to select the software that will be hosted.

To remove a game or software from the hosted list, highlight the game or software you want to remove and click the [Remove](#) button.

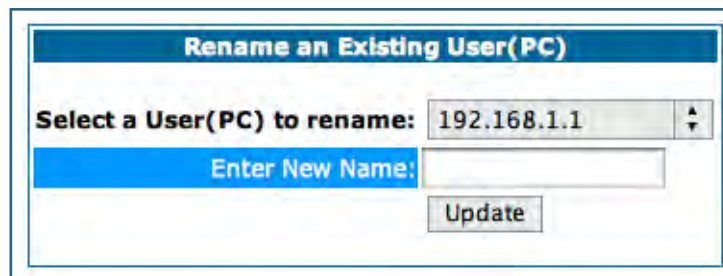
List of Supported Games and Software

Age of Empires, v.1.0	Age of Empires: The Rise of Rome, v.1.0	Age of Wonders
Asheron's Call	Baldur's Gate	Battlefield Communicator
Buddy Phone	Calista IP Phone	CART Precision Racing, v 1.0
Citrix Metaframe/ICA Client	Close Combat for Windows 1.0	Close Combat: A Bridge Too Far, v 2.0
Close Combat III: The Russian Front, v 1.0	Combat Flight Sim: WWII Europe Series, v 1.0	Combat Flight Sim 2: WWII Pacific Thr, v 1.0
Dark Reign	Delta Force (Client and Server)	Delta Force 2
Diablo II Server	Dialpad	DNS Server
Dune 2000	eDonkey 2000	eMule
F-16, Mig 29	F-22, Lightning 3	Fighter Ace II
FTP	GNUtella	H.323 compliant (Netmeeting, CUSeeME)
Half Life	Hellbender for Windows, v 1.0	Heretic II
Hexen II	Hotline Server	HTTP
HTTPS	ICQ 2001b	ICQ Old
IMAP Client	IMAP Client v.3	Internet Phone
IPSec	IPSec IKE	Jedi Knight II: Jedi Outcast
Kali	KazaA	LimeWire
Links LS 2000	Mech Warrior 3	Mech Warrior 4: Vengeance
Medal of Honor Allied Assault	Microsoft Flight Simulator 98	Microsoft Flight Simulator 2000
Microsoft Golf 1998 Edition, v 1.0	Microsoft Golf 1999 Edition	Microsoft Golf 2001 Edition
Midtown Madness, v 1.0	Monster Truck Madness, v 1.0	Monster Truck Madness 2, v 2.0
Motocross Madness 2, v 2.0	Motocross Madness, v 1.0	MSN Game Zone
MSN Game Zone (DX7 an 8 Play)	Need for Speed 3, Hot Pursuit	Need for Speed, Porsche
Net2Phone	NNTP	Operation FlashPoint
Outlaws	pcAnywhere (incoming)	POP-3
PPTP	Quake II	Quake III
Rainbow Six	RealAudio	Return to Castle Wolfenstein

Roger Wilco	Rogue Spear	ShoutCast Server
SMTP	SNMP	SSH server
StarCraft	Starfleet Command	StarLancer, v 1.0
Telnet	TFTP	Tiberian Sun: Command and Conquer
Timbuktu	Total Annihilation	Ultima Online
Unreal Tournament Server	Urban Assault, v 1.0	VNC, Virtual Network Computing
Westwood Online, Command and Conquer	Win2000 Terminal Server	XBox Live Games
Yahoo Messenger Chat	Yahoo Messenger Phone	ZNES

Rename a User(PC)

If a PC on your LAN has no assigned host name, you can assign one by clicking the [Rename a User\(PC\)](#) link.



To rename a server, select the server from the pull-down menu. Then type a new name in the text box below the pull-down menu. Click the [Update](#) button to save the new name.



NOTE:

The new name given to a server is only known to Software Hosting. It is not used as an identifier in other network functions, such as DNS or DHCP.

[Link: Backup](#)

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.



The screenshot shows the 'Backup Options' section of a web interface. At the top, there is a blue header with the text 'Backup Options'. Below this, the 'Backup' field is a pull-down menu currently showing 'disabled'. Underneath, there is another blue header for 'Backup IP Gateway'. Below that, the 'Enable Backup Gateway' checkbox is unchecked. At the bottom of this section is a 'Submit' button.

When you click the [Backup](#) link, the **Backup Options** page appears.



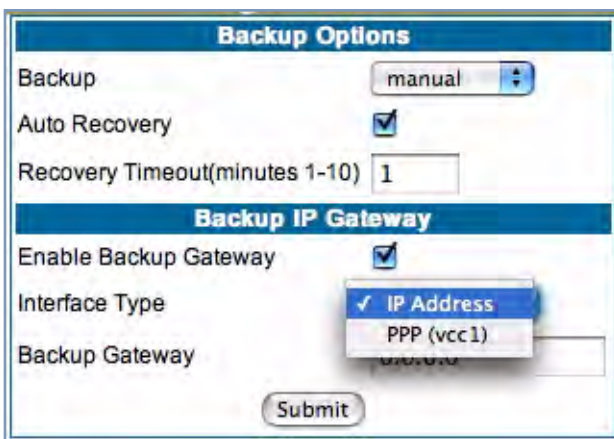
This screenshot is similar to the previous one, but the 'Backup' pull-down menu is open, showing three options: 'disabled' (with a checkmark), 'manual', and 'automatic'. The 'Enable Backup Gateway' checkbox remains unchecked, and the 'Submit' button is still visible at the bottom.

Select either **manual** or **automatic** from the pull-down menu.

- If you choose **manual**, you will have to switch manually to your alternate gateway in the event of a connection failure.
- For fail-over purposes, choose **automatic**.

Manual options

If you choose manual, you can also choose Auto Recovery. If you chose **Auto Recovery**, enter the number of minutes that the system should wait before it assumes that a connection has been re-established. This allows you to be sure that the primary WAN connection is well re-established before the Gateway switches back to it from the backup mode. Minimum value is one minute.



The screenshot shows the 'Backup Options' page with 'manual' selected in the 'Backup' dropdown. The 'Auto Recovery' checkbox is checked, and the 'Recovery Timeout (minutes 1-10)' is set to '1'. Below this is the 'Backup IP Gateway' section, where the 'Enable Backup Gateway' checkbox is checked. The 'Interface Type' dropdown is open, showing 'IP Address' selected and 'PPP (vcc1)' as an alternative. The 'Backup Gateway' field is empty. A 'Submit' button is at the bottom.

- Check the **Enable Backup Gateway** checkbox.
- From the pull-down menu, select the **Interface Type** to which you want to direct the backup connection. If you have defined multiple VCCs, you can choose a secondary one. Otherwise, to backup to an IP device on the LAN, choose **IP Address**.

The screen expands to allow you to enter an IP address of your **Backup Gateway**.

Click the [Submit](#) button; click the Alert icon, and in the resulting page, click the [Save and Restart](#) link.

Once Backup is configured, a new field appears in the Home Page.

BACKUP	
Current Port	Primary
Current State	up
<input type="button" value="Force Backup"/>	

If your DSL WAN link fails, you can switch to your Backup Gateway by clicking the [Force Backup](#) button.

Automatic options

If you select automatic as your Backup option, the screen expands to allow you to enter additional information.

Backup Options	
Backup	automatic
Failure Timeout(minutes 1-10)	1
Ping Host 1	address
Address	0.0.0.0
Ping Host 2	address
Address	0.0.0.0
Auto Recovery	<input checked="" type="checkbox"/>
Recovery Timeout(minutes 1-10)	1
Backup IP Gateway	
Enable Backup Gateway	<input checked="" type="checkbox"/>
Interface Type	IP Address
Backup Gateway	0.0.0.0
<input type="button" value="Submit"/>	

- **Failure Timeout (minutes 1-10)** – Enter the number of minutes you want the system to wait before the backup port becomes enabled in the event of primary line failure. This allows you to be sure the WAN connection is not merely briefly interrupted before the gateway switches to backup mode.

- **Ping Host 1 and Ping Host 2** – Select **address** or **name** from the pull-down menu enter IP address(es) or resolvable DNS name(s) that the Gateway will ping.

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.



Note:

For best results, enter an IP address and not a host name. If a host name is used it may not be resolvable, and may keep the interface down.

- While the Gateway is in backup mode, it will continue to ping both hosts via the primary interface. If either host responds to a ping and the **Auto Recovery** checkbox is checked, the Gateway will revert to the primary interface.
- If you chose Auto Recovery, select **Recovery Timeout (minutes 1-10)**. Enter the number of minutes you want 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.
- Check the **Enable Backup Gateway** checkbox

-
- From the pull-down menu, select the **Interface Type** to which you want to direct the backup connection. If you have defined multiple VCCs, you can choose a secondary one. Otherwise, to backup to an IP device on the LAN, choose **IP Address**.

The screen expands to allow you to enter an IP address of your **Backup Gateway**.

Click the [Submit](#) button; click the Alert icon, and in the resulting page, click the [Save and Restart](#) link.

Once Backup is configured, a new field appears in the Home Page.



For automatic mode, it should not be necessary to switch to Backup manually. However, you can force a switch to your Backup Gateway by clicking the [Force Backup](#) button.

[Link: Ethernet MAC Override](#)

(Only available on models with Ethernet WAN interfaces, such as the 338X-series or VDSL Gateways.)

Your Gateway comes with its own MAC (Media Access Control) address, also called the *Hardware Address*, a 12 character number unique for each LAN-connected device.

Your Service Provider, particularly cable service providers, may instruct you to override the default MAC address.



Ethernet MAC Address Override

Enable Override

MAC Address - - - - -

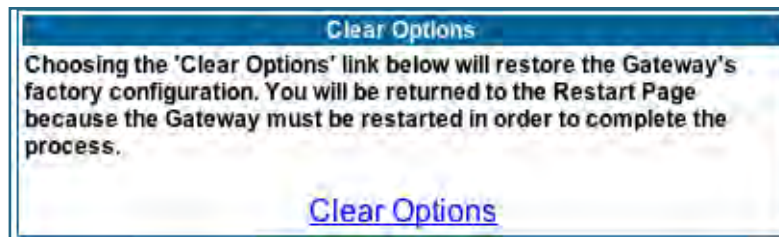
If so, check the **Enable Override** checkbox, and enter the new MAC address in the field provided.

[Link: Clear Options](#)

To restore the factory configuration of the Gateway, choose **Clear Options**. You may want to upload your configuration to a file before performing this function. You can do this using the **upload** command via the command-line interface. See the **upload** command on [page 238](#).

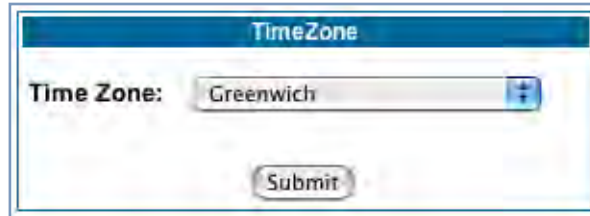
Clear Options does not clear feature keys or affect the software image.

You must restart the Gateway for **Clear Options** to take effect.



Link: Time Zone

When you click the [Time Zone](#) link, the **Time Zone** page appears.

A screenshot of a web form titled "TimeZone". The form contains a label "Time Zone:" followed by a pull-down menu currently displaying "Greenwich". To the right of the menu is a small blue icon with a plus sign. Below the menu is a "Submit" button.

You can set your local time zone by selecting the number of hours your time zone is distant from Greenwich Mean Time (GMT +12 – -12) from the pull-down menu. This allows you to set the time zone for access controls and in general.

Security

Button: Security

The Security features are available by clicking on the Security toolbar button. Some items of this category do not appear when you log on as **User**.

Feature	Description
Passwords	Allows changing the Admin or User passwords that control access to the Gateway.
Firewall	Provides access to firewall settings if the firewall feature has been purchased.
IPSec	Provides access to configuration parameters for IPSec functionality.
Stateful Inspection	Provides access to stateful inspection settings.
Packet Filter	Provides access to packet filter settings.
Security Log	Provides specific information about security-related events.

[Link: Passwords](#)

Access to your Gateway may be controlled through two optional user accounts, **Admin** and **User**. When you first power up your Gateway, you create a password for the **Admin** account. The User account does not exist by default. As the Admin, a password for the User account can be entered or existing passwords changed.

Create and Change Passwords. You can establish different levels of access security to protect your Motorola Netopia® Gateway settings from unauthorized display or modification.

- **Admin** level privileges let you display and modify **all** settings in the Motorola Netopia® Gateway (Read/Write mode). The Admin level password is created when you first access your Gateway.
- **User** level privileges let you display (but **not** change) settings of the Motorola Netopia® Gateway. (Read Only mode)

To prevent anyone from observing the password you enter, characters in the old and new password fields are not displayed as you type them.

To display the Passwords window, click the [Security](#) toolbar button on the Home page.

The screenshot shows two windows from the Motorola Netopia Gateway interface. The top window is titled "About Passwords" and contains the following text: "Access to your Gateway is controlled through two user accounts, Admin and User." Below this, it lists "Admin: Full access to the Gateway" and "User: Not allowed to configure any parameters, install keys/software, or restart the Gateway". At the bottom of this window, it says "Use the fields below to change or create passwords." The bottom window is titled "Passwords" and contains a form with the following fields: "Username" (a pull-down menu currently showing "admin (Admin account)"), "Old Password" (a text field with a note "(Leave blank if no old password)"), "New Password" (a text field), and "Confirm Password" (a text field). Below the form, it states "Password changes are automatically saved, and take effect immediately." and there is a "Submit" button.

Use the following procedure to change existing passwords or add the User password for your Motorola Netopia® Gateway:

1. **Select the account type from the [Username](#) pull-down list.**
Choose from **Admin** or **User**.
2. **If you assigned a password to the Motorola Netopia® Gateway previously, enter your current password in the [Old Password](#) field.**
3. **Enter your new password in the [New Password](#) field.**

Motorola Netopia®'s rules for a Password are:

-
- It can have up to eight alphanumeric characters.
 - It is case-sensitive.
4. **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.
 5. **When you are finished, click the [Submit](#) button to store your modified configuration in the Motorola Netopia® unit's memory.**
Password changes are automatically saved, and take effect immediately.

[Link: Firewall](#)

Use a Motorola Netopia® Firewall

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.

Configuring for a BreakWater Setting

Use these steps to establish a firewall setting:

1. **Ensure that you have enabled the BreakWater basic firewall with the appropriate feature key.**
See [See "Use Motorola Netopia® Software Feature Keys" on page 187.](#) for reference.
NOTE: The firewall is now keyed on by default on the 2200-Series Gateways.
2. **Click the [Security](#) toolbar button.**
3. **Click [Firewall](#).**

BreakWater Firewall

ClearSailing Removes the traffic restrictions imposed by SilentRunning and LANdlocked. Protection against unwanted inbound traffic is controlled by NAT settings.
Note: The ClearSailing firewall setting is necessary to enable pinholes, IPMaps and a NAT default server.

SilentRunning Using this level of firewall protection allows secure transmission of outbound traffic, but disables any attempt for inbound traffic to identify the Gateway. This is the Internet equivalent of having an unlisted number.
Note: The SilentRunning firewall setting disables pinholes, IPMaps and a NAT default server.

LANdLocked This option turns off all inbound and outbound traffic (including pinholes and IPMaps), isolating the LAN and disabling all WAN traffic.

BreakWater Option ClearSailing SilentRunning LANdLocked

BreakWater changes are automatically saved, and take effect immediately.

4. Click on the radio button to select the protection level you want. Click [Submit](#).

Changing the BreakWater setting does **not** require a restart to take effect. This makes it easy to change the setting “on the fly,” as your needs change.

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
- HTTP
- FTP
- SNMP
- telnet
- 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:

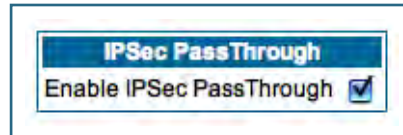
The Gateway's WAN DHCP client port in SilentRunning mode is **enabled**. This feature allows end users to continue using DHCP-served IP addresses from their Service Providers, while having no identifiable presence on the Internet.

[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.



You can disable it if your LAN-side VPN client includes its own NAT interoperability option.

Uncheck the [Enable IPSec Passthrough](#) checkbox.

- **SafeHarbour VPN IPSec** is a keyed feature that you must purchase. (See "Install Key" on page 187.) It enables Gateway-terminated VPN support.

SafeHarbour IPSec VPN

SafeHarbour 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.

If you have purchased the SafeHarbour IPSec feature key, the IPSec configuration screen offers additional options.

Two separate mechanisms for IPSec tunnel support are provided by your Gateway:

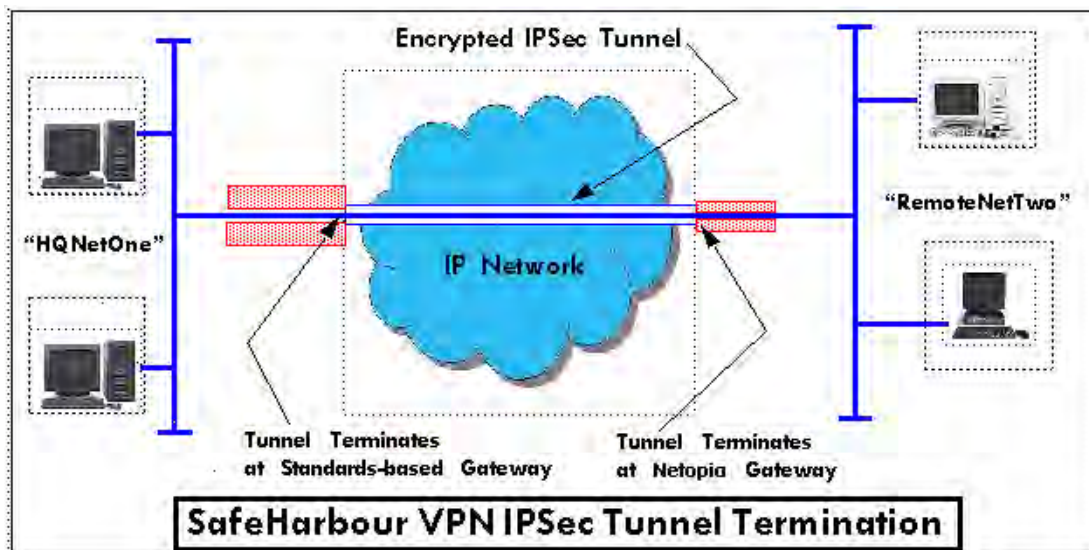
- IPSec PassThrough supports VPN clients running on LAN-connected computers. Disable this checkbox if your LAN-side VPN client includes its own NAT interoperability solution.
- SafeHarbour is a keyed feature that enables Gateway-terminated VPN support.

IPSec PassThrough
Enable IPSec PassThrough

SafeHarbour IPSec
Enable SafeHarbour IPSec

SafeHarbour IPSec Tunnel Entry						
On	Name	Peer External IP Address	Encryption Protocol	Authentication Protocol	Key Management	
<input checked="" type="checkbox"/>		0.0.0.0	ESP	ESP	IKE	<input type="button" value="Add"/>

A typical SafeHarbour configuration is shown below:



Configuring a SafeHarbour VPN

Use the following procedure to configure your SafeHarbour tunnel.

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

The tables “[Parameter Descriptions](#)” on [page 151](#) 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 149](#).**

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 149](#)) 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. **Be sure that you have SafeHarbour VPN enabled.**

SafeHarbour is a keyed feature. See [“Install Key” on page 187.](#) for information concerning installing Motorola Netopia® Software Feature Keys.

4. **Check the [Enable SafeHarbour IPSec](#) checkbox.**

Checking this box will automatically display the **SafeHarbour IPSec Tunnel Entry** parameters.

Enter the initial group of tunnel parameters. Refer to your **Setup Worksheet** and the **“Parameter Descriptions” on page 151** as required.

5. **Enter the tunnel [Name](#).**

This parameter does not have to match the peer/remote VPN device.

6. **Enter the [Peer External IP Address](#).**

7. **Select the [Encryption Protocol](#) from the pull-down menu.**

8. **Select the [Authentication Protocol](#) from the pull-down menu.**

9. **Click [Add](#).**

The Tunnel Details page appears.

Tunnel Details	
Name	my_tunnel
Peer Internal Network	0.0.0.0
Peer Internal Netmask	255.255.255.0
NAT Enable	<input checked="" type="checkbox"/>
PAT Address	0.0.0.0
Negotiation Method	Aggressive
Local ID type	IP Address
Local ID Address	0.0.0.0
Remote ID Type	IP Address
Remote ID Address	0.0.0.0
Pre-Shared Key Type	ASCII
Pre-Shared Key	netopia1
DH Group	1
PFS Enable	<input type="checkbox"/>
SA Encrypt Type	DES
SA Hash Type	MD5
Invalid SPI Recovery	<input type="checkbox"/>
Soft MBytes	1000
Soft Seconds	82800
Hard MBytes	1200
Hard Seconds	86400
IPSec MTU	1500
Xauth Enable	<input type="checkbox"/>
<input type="button" value="Update"/> <input type="button" value="Delete"/>	

10. **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 149.](#))

11. **Click [Update](#).**

The **Alert** button appears.

12. **Click the [Alert](#) button.**

13. **Click [Save and Restart](#).**

Your SafeHarbour IPSec VPN tunnel is fully configured.

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. <u>The tunnel name does not need to match the peer gateway.</u>
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. <u>The tunnel name does not need to match the peer gateway.</u>
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.
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).

Table 3: IPSec Tunnel Details page parameters

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.
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 Motorola 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. <u>This parameter does not need to match the peer gateway.</u>
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. <u>This parameter does not need to match the peer gateway.</u>
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. <u>This parameter does not need to match the peer gateway.</u>
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 <u>This parameter does not need to match the peer gateway.</u>

Table 3: IPSec Tunnel Details page parameters

IPSec MTU	<p>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.</p> <p>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 <i>can't fragment</i> 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.</p>
Xauth Enable	<p>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.</p>
Xauth Username/ Password	<p>Xauth authentication credentials.</p>

Link: Stateful Inspection

All computer operating systems are vulnerable to attack from outside sources, typically at the operating system or Internet Protocol (IP) layers. Stateful Inspection firewalls intercept and analyze incoming data packets to determine whether they should be admitted to your private LAN, based on multiple criteria, or blocked. Stateful inspection improves security by tracking data packets over a period of time, examining incoming and outgoing packets. Outgoing packets that request specific types of incoming packets are tracked; only those incoming packets constituting a proper response are allowed through the 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. Stateful Inspection parameters are active on a WAN interface only if enabled on your Gateway. Stateful inspection can be enabled on a WAN interface whether NAT is enabled or not.

Stateful Inspection Firewall installation procedure



NOTE:

Installing Stateful Inspection Firewall is mandatory to comply with Required Services Security Policy - Residential Category module - Version 4.1 (specified by ICSA Labs)

For more information please go to the following URL:

<http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/baseline.pdf>

1. Access the router through the web interface from the private LAN.

DHCP server is enabled on the LAN by default.

2. The Gateway's Stateful Inspection feature must be enabled in order to prevent TCP, UDP and ICMP packets destined for the router or the private hosts.

This can be done by navigating to **Expert Mode** -> **Security** -> **Stateful Inspection**.

No-activity Time-outs
Enter a value from 30 to 65535 (seconds)

UDP no-activity time-out: 180

TCP no-activity time-out: 14400

DoS Detect:

Submit

Exposed Addresses
[Exposed addresses](#) Configure Exposed Addresses (Active only if NAT is disabled)

Stateful Inspection Options
[PPP over Ethernet vcc1](#) Configure stateful inspection options for this interface

- **UDP no-activity time-out:** The time in seconds after which a UDP session will be terminated, if there is no traffic on the session.
- **TCP no-activity time-out:** The time in seconds after which an TCP session will be terminated, if there is no traffic on the session.

- **DoS Detect:** If you check this checkbox, the Gateway will monitor packets for Denial of Service attacks.
- **Exposed Addresses:** The hosts specified in Exposed Addresses will be allowed to receive inbound traffic even if there is no corresponding outbound traffic. This is active only if NAT is disabled on a WAN interface.
- **Stateful Inspection Options:** Enable and configure stateful inspection on a WAN interface.

Exposed Addresses

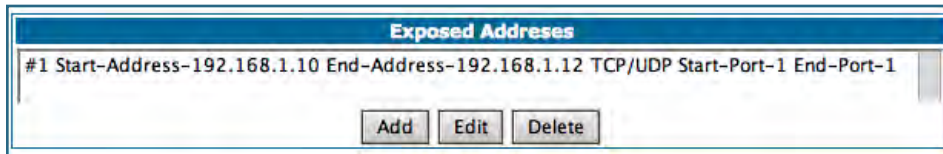
You can specify the IP addresses you want to expose by clicking the [Exposed addresses](#) link.

Add, Edit, or delete exposed addresses options are active only if NAT is disabled on a WAN interface. The hosts specified in exposed addresses will be allowed to receive inbound traffic even if there is no corresponding outbound traffic.

- **Start Address:** Start IP Address of the exposed host range.
- **End Address:** End IP Address of the exposed host range
- **Protocol:** Select the Protocol of the traffic to be allowed to the host range from the pull-down menu. Options are Any, TCP, UDP, or TCP/UDP.

- **Start Port:** Start port of the range to be allowed to the host range. The acceptable range is from 1 - 65535
- **End Port:** Protocol of the traffic to be allowed to the host range. The acceptable range is from 1 - 65535

You can add more exposed addresses by clicking the [Add more Exposed Addresses](#) link. A list of previously configured exposed addresses appears.

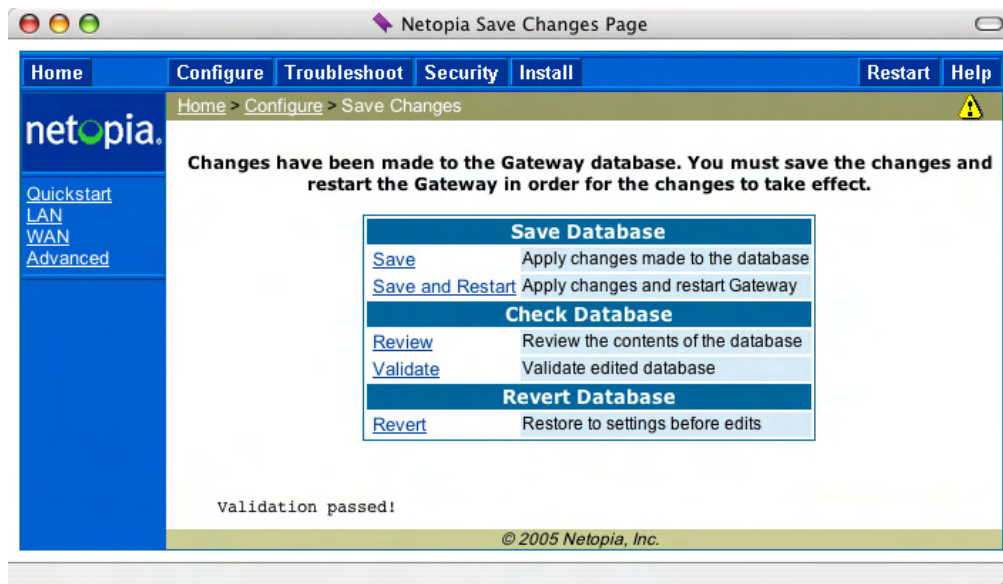


Click the [Add](#) button to add a new range of exposed addresses.

You can edit a previously configured range by clicking the [Edit](#) button, or delete the entry entirely by clicking the [Delete](#) button.

All configuration changes will trigger the Alert Icon.  Click on the Alert icon.

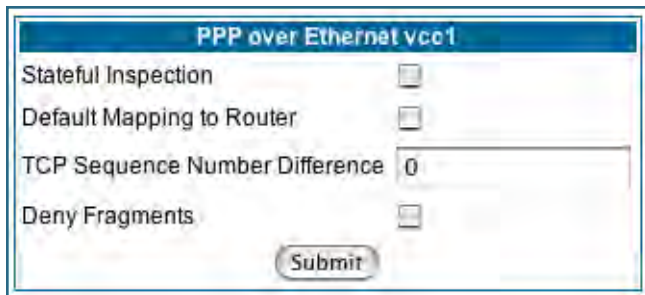
This allows you to validate the configuration and reboot the Gateway.



Click the [Save and Restart](#) link. You will be asked to confirm your choice, and the Gateway will reboot with the new configuration.

Stateful Inspection Options

Stateful Inspection Parameters are active on a WAN interface only if you enable them on your Gateway.



- **Stateful Inspection:** To enable stateful inspection on this WAN interface, check the checkbox.
- **Default Mapping to Router:** This is disabled by default. This option will allow the router to respond to traffic received on this interface, for example, ICMP Echo requests.



NOTE:

If Stateful Inspection is enabled on a WAN interface **Default Mapping to Router** must be enabled to allow inbound VPN terminations to the router.

- **TCP Sequence Number Difference:** Enter a value in this field. This value represents the maximum sequence number difference allowed between subsequent TCP packets. If this number is exceeded, the packet is dropped. The acceptable range is 0 – 65535. A value of 0 (zero) disables this check.
- **Deny Fragments:** To enable this option, which causes the router to discard fragmented packets on this interface, check the checkbox.

Open Ports in Default Stateful Inspection Installation

Port	Protocol	Description	LAN (Private) Interface	WAN (Public) Interface
23	TCP	telnet	Yes	No
53	UDP	DNS	Yes	No
67	UDP	Bootps	Yes	No
68	UDP	Bootpc	Yes	No
80	TCP	HTTP	Yes	No
137	UDP	Netbios-ns	Yes	No
138	UDP	Netbios-dgm	Yes	No
161	UDP	SNMP	Yes	No
500	UDP	ISAKMP	Yes	No
520	UDP	Router	Yes	No

Firewall Tutorial

General firewall terms



Note:

Breakwater Basic Firewall (see [“BreakWater Basic Firewall” on page 142](#)) does not make use of the packet filter support and can be used in addition to filtersets

Filter rule: A filter set is comprised of individual filter rules.

Filter set: A grouping of individual filter rules.

Firewall: A component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the network.

Packet: Unit of communication on the Internet.

Packet filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports.

Port: A number that defines a particular type of service.

Basic IP packet components

All IP packets contain the same basic header information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP data stream (the User Data from above) to make filtering decisions.

Basic protocol types

TCP: Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.

UDP: User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not retransmit the data. RFC 768 is the specification for UDP.

There are many more ports defined in the Assigned Addresses RFC. The table that follows shows some of these port assignments.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP		
80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

- “What is not explicitly allowed is denied.”

and

- “What is not explicitly denied is allowed.”

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and in the future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is forwarded through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not forward through the remainder of the filter rules.

For example, if you had the following filter set...

- Allow WWW access;
- Allow FTP access;
- Allow SMTP access;
- Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would forward through the first rule (WWW), go through the second rule (FTP), and match this rule; the packet is allowed through.

If you had this filter set for example....

- Allow WWW access;

- Allow FTP access;
- Deny FTP access;
- Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would forward through the first filter rule (WWW), match the second rule (FTP), and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Implied rules

With a given set of filter rules, there is an Implied rule that may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied rule is NO.
N+N+N=Y	If all filter rules are NO, the implied rule is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied rule is NO.

Example filter set page

This is an example of the Motorola Netopia® filter set page:

Filter Set: Filter

Input Rules:

#	Fwd	Src IP Address	Src Mask	Dst IP Address	Dst Mask	Prot	Src Port	Dst Port
1	No	199.211.211.17	0.0.0.0	0.0.0.0	0.0.0.0	TCP	=23	NC
2	No	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	TCP	NC	=6000
3	Yes	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	ICMP		
4	Yes	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	TCP	NC	=1023
5	Yes	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	UDP	NC	=1023

Output Rules:
No Output Filter Rules have been defined.

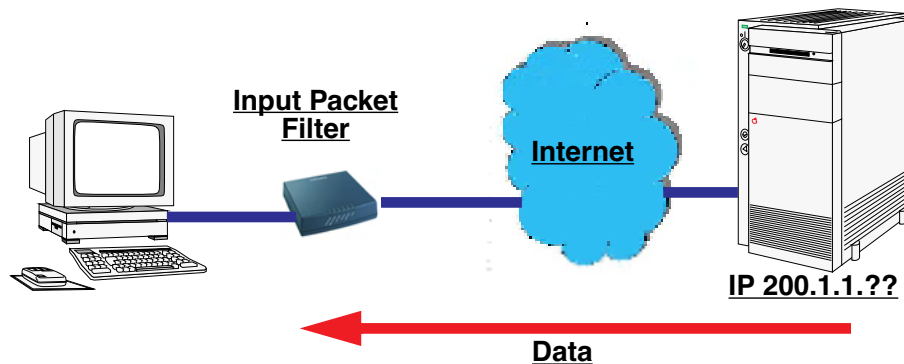
Filter basics

In the source or destination IP address fields, the IP address that is entered must be the network address of the subnet. A host address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

Netopia Embedded Software Version 7.7.4 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No Compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined
Less Than or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined

Example network



Example filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field in Netopia Embedded Software Version 7.7.4. This will *not* forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

This incoming IP packet has a source IP address that does not match the network address in the Source IP Address field in Netopia Embedded Software Version 7.7.4. This rule *will* forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

This rule does *not* match and this packet will be forwarded.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104.

This rule *does* match and this packet will *not* be forwarded.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96.

This rule *does* match and this packet will *not* be forwarded. This rule masks off a *single* IP address.

[Link: Packet Filter](#)

When you click the [Packet Filter](#) link the **Filter Sets** screen appears.



Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security. The Packet Filter engine allows creation of a maximum of eight Filter Sets. Each Filter Set can consist of many rules. There can be a maximum of 32 filter rules in the system.



WARNING:

Before attempting to configure filters and filter sets, please read and understand this entire section thoroughly. Motorola Netopia® Gateways incorporating NAT have advanced security features built in. Improperly adding filters and filter sets increases the possibility of loss of communication with the Gateway and the Internet. Never attempt to configure filters unless you are local to the Gateway.

Although using filter sets can enhance network security, there are disadvantages:

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints in addition to NAT.
- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, and general awareness of how your network may be vulnerable.

Netopia Embedded Software Version 7.7.4's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the Gateway's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called *firewalling* your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can be either an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

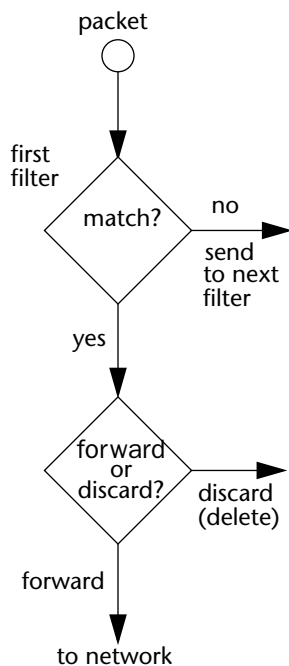
A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.

A filter inspects data packets like a customs inspector scrutinizing packages.



Filter priority



Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.

If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can forward or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither forward nor discard the packet (because it cannot match any criteria), the second filter has a chance to forward or reject it, and so on. Because of this hierarchical structure,

each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

- Forwards the packet to the local or remote network
- Blocks (discards) the packet
- Ignores the packet

A filter forwards or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

A filtering rule

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

“Block all Telnet attempts that originate from the remote host 199.211.211.17.”

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter in Netopia Embedded Software Version 7.7.4:

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address and subnet mask (where the packet was sent from)
- The destination IP address and subnet mask (where the packet is going)
- The TOS bit setting of the packet. Certain types of IP packets, such as voice or multimedia packets, are sensitive to delays introduced by the network. A delay-sensitive packet is identified by a special low-latency setting called the TOS bit. It is important for such packets to be received rapidly or the quality of service degrades.
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Filter Input Rule Entry #1	
Forward	<input checked="" type="checkbox"/>
Source IP	199.211.211.17
Source Mask	255.255.255.255
Destination IP	0.0.0.0
Destination Mask	0.0.0.0
TOS	0
TOS Mask	0
Protocol	TCP
Source Port Compare:	Equal to
Source Port:	23
Destination Port Compare:	No compare
<input type="button" value="Submit"/>	
Add or Edit more Filter Rules	

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The following tables show a few common services and their associated port numbers:

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	TFTP	69
World Wide Web	80	who	513
SNMP	161		

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

- **No Compare:** No comparison of the port number specified in the filter with the packet's port number.
- **Not Equal To:** For the filter to match, the packet's port number cannot equal the port number specified in the filter.
- **Less Than:** For the filter to match, the packet's port number must be less than the port number specified in the filter.
- **Less Than or Equal:** For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.
- **Equal:** For the filter to match, the packet's port number must equal the port number specified in the filter.
- **Greater Than:** For the filter to match, the packet's port number must be greater than the port number specified in the filter.
- **Greater Than or Equal:** For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

Other filter attributes

There are three other attributes to each filter:

- The filter's order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to forward packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:

Filter Set: Filter								
Input Rules:								
#	Fwd	Src IP Address	Src Mask	Dst IP Address	Dst Mask	Prot	Src Port	Dst Port
1	No	199.211.211.17	0.0.0.0	0.0.0.0	0.0.0.0	TCP	=23	NC
2	No	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	TCP	NC	=6000
3	Yes	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	ICMP		
4	Yes	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	TCP	NC	=1023
5	Yes	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	UDP	NC	=1023

Output Rules:
No Output Filter Rules have been defined.

The table's columns correspond to each filter's attributes:

- **#:** The filter's priority in the set. Filter number 1, with the highest priority, is first in the table.
- **Fwd:** Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there's a match.
- **Src-IP:** The packet source IP address to match.
- **Src-Mask:** The packet source subnet mask to match.
- **Dst-IP:** The packet destination IP address to match.
- **Dst-Mask:** The packet destination IP address to match.
- **Protocol:** The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if those protocols are used.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

- **Src Port:** The source port to match. This is the port on the sending host that originated the packet.
- **Dst Port:** The destination port to match. This is the port on the receiving host for which the packet is intended.
- **NC:** Indicates No Compare, where specified.

Filtering example #1

Returning to our filtering rule example from above (see [page 165](#)), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

- The rule you want to implement as a filter is:

"Block all Telnet attempts that originate from the remote host 199.211.211.17."

- The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Destination IP address could have been anything. The mask for Source IP address must be 255.255.255.255 since an exact match is desired.
 - Source IP Address = 199.211.211.17
 - Source IP address mask = 255.255.255.255
 - Destination IP Address = 0.0.0.0
 - Destination IP address mask = 0.0.0.0
- Using the tables on [page 166](#), find the destination port and protocol numbers (the *local* Telnet port):
 - Protocol = TCP (or 6)
 - Destination Port = 23
- The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:
 - Forward = unchecked

This four-step process is how we produced the following filter from the original rule:

Filter Input Rule Entry #1	
Forward	<input type="checkbox"/>
Source IP	199.211.211.17
Source Mask	255.255.255.255
Destination IP	0.0.0.0
Destination Mask	0.0.0.0
TOS	0
TOS Mask	0
Protocol	TCP
Source Port Compare:	Equal to
Source Port:	23
Destination Port Compare:	No compare
<input type="button" value="Submit"/>	
Add or Edit more Filter Rules	

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:



This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.



Note:

The protocol attribute for this filter is *Any* by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought must go into designing a new filter set. You should consider the following guidelines:

- Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.
- Be sure each individual filter's purpose is clear.
- Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.
- Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:
 - Forwarded if all the filters are configured to discard (*not* forward)
 - Discarded if all the filters are configured to forward
 - Discarded if the set contains a combination of forward and discard filters

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

Each filter set you design will be based on one of the following approaches:

- That which is not expressly prohibited is permitted.
- That which is not expressly permitted is prohibited.

It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.