Copyright

©2012 Motorola Mobility LLC All rights reserved. MOTOROLA, and the Stylized M logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC. All other product or service names are the property of their respective owners. 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 Mobility LLC 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, 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.

©2010 Motorola Mobility LLC All rights reserved. MOTOROLA, and the Stylized M logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC. All other product or service names are the property of their respective owners. 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 Mobility LLC 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, 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.

EXCEPT AS INDICATED IN THE APPLICABLE SYSTEM PURCHASE AGREEMENT, THE SYSTEM, DOCUMENTATION AND SERVICES ARE PROVIDED “AS IS”, AS AVAILABLE, WITHOUT WARRANTY OF ANY KIND. MOTOROLA MOBILITY LLC. DOES NOT WARRANT THAT THE SYSTEM WILL MEET CUSTOMER’S REQUIREMENTS, OR THAT THEIR OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ANY ERRORS CAN OR WILL BE FIXED. MOTOROLA MOBILITY LLC. HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ORAL OR WRITTEN, WITH RESPECT TO THE SYSTEM AND SERVICES INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, INTEGRATION, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND ALL WARRANTIES ARISING FROM ANY COURSE OF DEALING OR PERFORMANCE OR USAGE OF TRADE.

EXCEPT AS INDICATED IN THE APPLICABLE SYSTEM PURCHASE AGREEMENT, MOTOROLA MOBILITY LLC. SHALL NOT BE LIABLE CONCERNING THE SYSTEM OR SUBJECT MATTER OF THIS DOCUMENTATION, REGARDLESS OF THE FORM OF ANY CLAIM OR ACTION (WHETHER IN CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE), FOR ANY (A) MATTER BEYOND ITS REASONABLE CONTROL, (B) LOSS OR INACCURACY OF DATA, LOSS OR INTERRUPTION OF USE, OR COST OF PROCURING SUBSTITUTE TECHNOLOGY, GOODS OR SERVICES, (C) INDIRECT, PUNITIVE, INCIDENTAL, RELIANCE, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, REVENUES, PROFITS OR GOODWILL, OR (D) DIRECT DAMAGES, IN THE AGGREGATE, IN EXCESS OF THE FEES PAID TO IT HEREUNDER FOR THE SYSTEM OR SERVICE GIVING RISE TO SUCH DAMAGES DURING THE 12-MONTH PERIOD PRIOR TO THE DATE THE CAUSE OF ACTION AROSE, EVEN IF COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS ARE INDEPENDENT FROM ALL OTHER PROVISIONS OF THIS AGREEMENT AND SHALL APPLY NOTWITHSTANDING THE FAILURE OF ANY REMEDY PROVIDED HEREIN.

All Motorola Mobility LLC products are furnished under a license agreement included with the product. If you are unable to locate a copy of the license agreement, please contact Motorola Mobility LLC

NOTE: THIS IS DRAFT DOCUMENTATION INTENDED FOR TESTING AND EVALUATIVE REVIEW. IT MAY CONTAIN ERRORS. IT SHOULD NOT BE CONSIDERED SUITABLE FOR USE IN A PRODUCTION ENVIRONMENT.

Motorola Mobility LLC
600 North U.S. Highway 45
Libertyville, Illinois 60048 USA
Telephone: +1 847 523 5000
Part Number
58XXXX-001-00r2 rev a
V9.1.0SKU 70

<table>
<thead>
<tr>
<th>Draft version</th>
<th>Firmware version</th>
<th>Changes this draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1</td>
<td>nbxvu9.1.0h2d2_1.1.bin</td>
<td>first draft</td>
</tr>
<tr>
<td>r1</td>
<td>include ATT 6/16 feedback; add battery door instructions</td>
<td></td>
</tr>
<tr>
<td>r2</td>
<td>nbxvu9.1.0h0d23_1.1.bin</td>
<td>add battery safety instructions; revved GUI per ERS-NVG589_1.0_UI.doc rev 13</td>
</tr>
</tbody>
</table>
Table of Contents

CHAPTER 1 Introduction ................................................. 7
  About Motorola® Documentation ................................. 7
  Documentation Conventions ...................................... 8
    General ......................................................... 8
    Internal Web Interface ....................................... 8
    Command Line Interface ...................................... 8
  Organization ..................................................... 9
  A Word About Example Screens ................................. 9

CHAPTER 2 Device Configuration ................................. 11
  Important Safety Instructions ................................. 12
  POWER SUPPLY INSTALLATION ................................. 12
  TELECOMMUNICATION INSTALLATION .......................... 12
  COAX INSTALLATION ........................................... 12
  PRODUCT VENTILATION ......................................... 12
  Motorola® Gateway Status Indicator Lights .................. 13
  Battery Installation (optional) ................................. 16
  Battery Door Installation Instructions ........................ 17
  Battery Door Removal Instructions ............................. 18
  Cradle Installation Instructions ............................... 19
  Set up the Motorola Gateway ................................. 20
  Accessing the Web Management Interface .................... 23
    Broadband Network Redirect Pages .......................... 25
    IP Diagnostics Page Redirect ................................ 26
    Offline Troubleshooting ...................................... 26
  Device Status page ............................................. 27
    Device Access Code .......................................... 27
  Tab Bar ......................................................... 31
  Help .......................................................... 31
  Links Bar ....................................................... 32
  Device List ..................................................... 32
  System Information ............................................. 34
  Access Code .................................................... 35
  Restart Device ................................................. 36
  Broadband ....................................................... 37
  Configure ....................................................... 39
  IGMP Stats ..................................................... 40
  Home Network .................................................. 41
  Configure ....................................................... 44
  HPNA Configure ............................................... 45
  Wireless ........................................................ 46
  Wireless Security .............................................. 48
  MAC Filtering ................................................... 50
### Administrator's Handbook

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Scan</td>
<td>51</td>
</tr>
<tr>
<td>Subnets &amp; DHCP</td>
<td>52</td>
</tr>
<tr>
<td>HPNA</td>
<td>54</td>
</tr>
<tr>
<td>Voice</td>
<td>56</td>
</tr>
<tr>
<td>Line Details</td>
<td>57</td>
</tr>
<tr>
<td>Call Statistics</td>
<td>58</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>62</td>
</tr>
<tr>
<td>Packet Filter</td>
<td>63</td>
</tr>
<tr>
<td>Working with Packet Filters</td>
<td>65</td>
</tr>
<tr>
<td>NAT/Gaming</td>
<td>69</td>
</tr>
<tr>
<td>Custom Services</td>
<td>71</td>
</tr>
<tr>
<td>IP Passthrough</td>
<td>75</td>
</tr>
<tr>
<td>Firewall Advanced</td>
<td>78</td>
</tr>
<tr>
<td><strong>Diagnostics</strong></td>
<td>80</td>
</tr>
<tr>
<td>Logs</td>
<td>83</td>
</tr>
<tr>
<td>Update</td>
<td>85</td>
</tr>
<tr>
<td>Resets</td>
<td>86</td>
</tr>
<tr>
<td>Event Notifications</td>
<td>87</td>
</tr>
<tr>
<td>NAT Table</td>
<td>88</td>
</tr>
<tr>
<td><strong>CHAPTER 3 Basic Troubleshooting</strong></td>
<td>89</td>
</tr>
<tr>
<td>Status Indicator Lights</td>
<td>90</td>
</tr>
<tr>
<td>LED Function Summary Matrix</td>
<td>93</td>
</tr>
<tr>
<td>Factory Reset Switch</td>
<td>96</td>
</tr>
<tr>
<td>Log Event Messages</td>
<td>97</td>
</tr>
<tr>
<td><strong>CHAPTER 4 Command Line Interface</strong></td>
<td>103</td>
</tr>
<tr>
<td>Overview</td>
<td>105</td>
</tr>
<tr>
<td>Starting and Ending a CLI Session</td>
<td>107</td>
</tr>
<tr>
<td>Logging In</td>
<td>107</td>
</tr>
<tr>
<td>Ending a CLI Session</td>
<td>107</td>
</tr>
<tr>
<td>Using the CLI Help Facility</td>
<td>107</td>
</tr>
<tr>
<td>About SHELL Commands</td>
<td>108</td>
</tr>
<tr>
<td>SHELL Prompt</td>
<td>108</td>
</tr>
<tr>
<td>SHELL Command Shortcuts</td>
<td>108</td>
</tr>
<tr>
<td>SHELL Commands</td>
<td>109</td>
</tr>
<tr>
<td>Common Commands</td>
<td>109</td>
</tr>
<tr>
<td>WAN Commands</td>
<td>116</td>
</tr>
<tr>
<td>About CONFIG Commands</td>
<td>118</td>
</tr>
<tr>
<td>CONFIG Mode Prompt</td>
<td>118</td>
</tr>
<tr>
<td>Navigating the CONFIG Hierarchy</td>
<td>118</td>
</tr>
<tr>
<td>Entering Commands in CONFIG Mode</td>
<td>118</td>
</tr>
<tr>
<td>Guidelines: CONFIG Commands</td>
<td>118</td>
</tr>
<tr>
<td>Displaying Current Gateway Settings</td>
<td>119</td>
</tr>
<tr>
<td>Step Mode: A CLI Configuration Technique</td>
<td>119</td>
</tr>
<tr>
<td>Validating Your Configuration</td>
<td>120</td>
</tr>
<tr>
<td>CONFIG Commands</td>
<td>121</td>
</tr>
<tr>
<td>Connection commands</td>
<td>121</td>
</tr>
</tbody>
</table>
CHAPTER 1 Introduction

About Motorola® Documentation

NOTE:

This guide describes the wide variety of features and functionality of the Motorola® Gateway, when used in Router mode. The Motorola® 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 family of intelligent enterprise and consumer Gateways. It consists of:

◆ Administrator’s Handbook
◆ Dedicated User Manuals
◆ 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 the Motorola’s website:
http://www.motorola.com/support
Documentation Conventions

General

This manual uses the following conventions to present information:

<table>
<thead>
<tr>
<th>Convention (Typeface)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Menu commands</td>
</tr>
<tr>
<td><strong>bold sans serif</strong></td>
<td>Web GUI page links and button names</td>
</tr>
<tr>
<td><strong>terminal</strong></td>
<td>Computer display text</td>
</tr>
<tr>
<td><strong>bold terminal</strong></td>
<td>User-entered text</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic type indicates the complete titles of manuals.</td>
</tr>
</tbody>
</table>

Internal Web Interface

<table>
<thead>
<tr>
<th>Convention (Graphics)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blue rectangle or line</td>
<td>Denotes an “excerpt” from a Web page or the visual truncation of a Web page</td>
</tr>
<tr>
<td></td>
<td>Denotes an area of emphasis on a Web page</td>
</tr>
<tr>
<td>solid rounded rectangle with an arrow</td>
<td></td>
</tr>
</tbody>
</table>

Command Line Interface

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>straight ([ ]) brackets in cmd line</td>
<td>Optional command arguments</td>
</tr>
<tr>
<td>curly ({ }) brackets, with values separated with vertical bars (</td>
<td>)</td>
</tr>
<tr>
<td><strong>bold terminal type face</strong></td>
<td>User-entered text</td>
</tr>
<tr>
<td><em>italic terminal type face</em></td>
<td>Variables for which you supply your own values</td>
</tr>
</tbody>
</table>
Organization

This guide consists of five chapters, two appendices, and an index. It is organized as follows:

◆ **Chapter 1, Introduction** — Describes the Motorola® document suite, the purpose of, the audience for, and structure of this guide. It gives a table of conventions.
◆ **Chapter 2, “Device Configuration”** — Describes how to get up and running with your Motorola® Gateway.
◆ **Chapter 3, “Basic Troubleshooting”** — Gives some simple suggestions for troubleshooting problems with your Gateway’s initial configuration.
◆ **Chapter 4, “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 5, “Technical Specifications and Safety Information”**
◆ “Appendix A Motorola® Gateway Captive Portal Implementation” — Describes the Motorola® Gateway Captive Portal Implementation
◆ “Appendix B Quality of Service (QoS) Examples” — Describes the Motorola® Gateway Quality of Service (QoS) Implementation
◆ Index

A Word About Example Screens

This manual contains many example screen illustrations. Since Motorola® 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 Device Configuration

Most users will find that the basic Quick Start configuration is all that they ever need to use. The Quick Start section may be all that you ever need to configure and use your Motorola® Gateway. For more advanced users, a rich feature set is available. The following instructions cover installation in Router Mode.

This chapter covers:

◆ “Important Safety Instructions” on page 12
◆ “Motorola® Gateway Status Indicator Lights” on page 13
◆ “Battery Installation (optional)” on page 16
◆ “Battery Door Installation Instructions” on page 17
◆ “Battery Door Removal Instructions” on page 18
◆ “Cradle Installation Instructions” on page 19
◆ “Set up the Motorola Gateway” on page 20
◆ “Accessing the Web Management Interface” on page 23
◆ “Device Status page” on page 27
◆ “Tab Bar” on page 31
◆ “Broadband” on page 37
◆ “Home Network” on page 41
◆ “Wireless” on page 46
◆ “Voice” on page 56
◆ “Firewall” on page 62
◆ “Diagnostics” on page 80
Important Safety Instructions

POWER SUPPLY INSTALLATION

Connect the power supply cord to the power jack on the Motorola® Gateway. Plug the power supply into an appropriate electrical outlet. There is no power (on / off) switch to power off the device.

**WARNING:**

The power supply must be connected to a mains outlet with a protective earth connection. Do not defeat the protective earth connection.

**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.

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.
◆ CAUTION: The external phone should be UL Listed and the connections should be made in accordance with Article 800 of the NEC.

COAX INSTALLATION

Be sure that the outside cable system is grounded, so as to provide some protection against voltage surges and built-up static charges. Article 820-20 of the NEC (Section 54, Part I of the Canadian Electrical Code) provides guidelines for proper grounding and, in particular, specifies the CATV cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

PRODUCT VENTILATION

The Motorola® 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.

**CAUTION –**

The battery used in this device may present a risk of fire or chemical burn if mis-treated. Do not disassemble, heat above manufacturer’s maximum temperature limit, or incinerate. Replace battery with Motorola P/N 586185-001-00 only. Use of another battery may present a risk of fire or explosion. Dispose of used battery promptly. Keep away from children. Do not disassemble and do not dispose of in fire.

SAVE THESE INSTRUCTIONS
Motorola® Gateway Status Indicator Lights

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

### Motorola® Gateway NVG589 status indicator lights

<table>
<thead>
<tr>
<th>LED</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>Solid Green = The device is powered.</td>
</tr>
<tr>
<td></td>
<td>Flashing Green = A Power-On Self-Test (POST) is in progress</td>
</tr>
<tr>
<td></td>
<td>Flashing Red = A POST failure (not bootable) or device malfunction occurred.</td>
</tr>
<tr>
<td></td>
<td>Orange/Amber = during firmware upgrade (see below)</td>
</tr>
<tr>
<td></td>
<td>Off = The unit has no AC power.</td>
</tr>
<tr>
<td><strong>Battery</strong></td>
<td>During the software installation, you will lose internet and phone service. The LEDs will function as follows:</td>
</tr>
<tr>
<td></td>
<td>1. As firmware is being loaded into flash, the LEDs will operate normally as described.</td>
</tr>
<tr>
<td></td>
<td>2. The installation will take a few minutes – During this phase, the Power LED will flash Orange/Amber during firmware upgrade (flash writing to memory) and all other LEDs will be off.</td>
</tr>
<tr>
<td></td>
<td>3. The Gateway will restart automatically. As the device reboots, the POWER ON LED behavior will happen.</td>
</tr>
<tr>
<td><strong>During Firmware Upgrade</strong></td>
<td>During Boot process</td>
</tr>
<tr>
<td></td>
<td>• Power LED = GREEN/FLASH</td>
</tr>
<tr>
<td></td>
<td>• All other LED = OFF</td>
</tr>
<tr>
<td></td>
<td>If the device does not boot, and fails its self test or fails to perform initial load of the boot-loader:</td>
</tr>
<tr>
<td></td>
<td>• Power LED = RED/FLASH</td>
</tr>
<tr>
<td></td>
<td>• ALL other LED = OFF</td>
</tr>
<tr>
<td></td>
<td>If the device boots and then detects a failure:</td>
</tr>
<tr>
<td></td>
<td>Power LED = GREEN/FLASH starting POST and then all LEDs will FLASH RED, including Power LED.</td>
</tr>
<tr>
<td><strong>Battery</strong></td>
<td>Solid Green = Battery in place but not being used.</td>
</tr>
<tr>
<td></td>
<td>Flashing Green = Battery charging.</td>
</tr>
<tr>
<td></td>
<td><strong>Solid Red</strong> = Battery backup mechanism has a fault.</td>
</tr>
<tr>
<td></td>
<td>Flashing Red = Battery needs to be replaced.</td>
</tr>
<tr>
<td></td>
<td><strong>Solid Amber</strong> = Battery in use.</td>
</tr>
<tr>
<td></td>
<td>Flashing Amber = Low battery.</td>
</tr>
<tr>
<td></td>
<td>Off = No battery or battery has no charge.</td>
</tr>
<tr>
<td></td>
<td>Cycle between all colors = Battery conducting self-test.</td>
</tr>
<tr>
<td>LED</td>
<td>Action</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Ethernet** | **Solid Green** = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).  
**Flickering Green** = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.  
**Off** = The device is not powered, no cable or no powered devices connected to the associated ports. |
| **Wireless** | **Solid Green** = Wi-Fi is powered.  
**Flickering Green** = Activity seen from devices connected via Wi-Fi. The flickering of the light is synchronized to actual data traffic.  
**Off** = The device is not powered or no powered devices connected to the associated ports. |
| **HomePNA** | **Solid Green** = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).  
**Flickering Green** = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.  
**Off** = The device is not powered, no cable or no powered devices connected to the associated ports. |
| **Broadband 1**, **2** | **Solid Green** = Good broadband connection (i.e., good DSL Sync or Gigabit Ethernet).  
**Flashing Green** = Attempting broadband connection (i.e., DSL attempting sync).  
**Flashing Green & Red** = If the broadband connection fails to be established for more than three consecutive minutes the LED switches to Flashing Green when attempting or waiting to establish a broadband connection alternating with a five second steady Red. This pattern continues until the broadband connection is successfully established.  
**Flashing Red** = No DSL signal on the line. This is only used when there is no signal, not during times of temporary 'no tone' during the training sequence.  
**Off** = The device is not powered.  
**Broadband 1 LED** is also the Gigabit ethernet WAN LED when that is in play (and DSL is not) |
| **Service** | **Solid Green** = IP connected (The device has a WAN IP address from DHCP or 802.1x authentication and the broadband connection is up).  
**Flashing Green** = Attempting PPP connection. Attempting IEEE 802.1X authentication or attempting to obtain DHCP information.  
**Red** = Device attempted to become IP connected and failed (no DHCP response, 802.1x authentication failed, no IP address from IPCP, etc.). The Red state times out after two minutes and the Service indicator light returns to the Off state.  
**Off** = The device is not powered or the broadband connection is not present. |
| **Phone 1, 2** | **Solid Green** = The associated VoIP line has been registered with a SIP proxy server.  
**Flashing Green** = Indicates a telephone is off-hook on the associated VoIP line.  
**Off** = VoIP not in use, line not registered or Gateway power off. |
| **USB** | **Solid Green** = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).  
**Flickering Green** = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.  
**Off** = The device is not powered, no cable or no powered devices connected to the associated ports. |
NOTE:

The NVG589 supports two VoIP lines over one RJ11 VoIP port. In order to connect two phone lines the supplied *inner/outer pair splitter adapters* must be attached to the RJ11 VoIP port in order to terminate both lines. This is a special-purpose splitter. You must only use the *inner/outer pair splitter adapters* supplied by AT&T.

<table>
<thead>
<tr>
<th>LED</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Orange/Amer when a Gigabit Ethernet device is connected to each port. Green when 10/100 Ethernet device is connected. Flash for Ethernet traffic passing.</td>
</tr>
</tbody>
</table>

**Motorola® Gateway NVG589 Rear View**
Battery Installation (optional)
The optional backup battery is located in a compartment on the bottom of the unit. Installing the battery door requires some care.

 CAUTION –

The battery used in this device may present a risk of fire or chemical burn if mistreated. Do not disassemble, heat above manufacturer’s maximum temperature limit, or incinerate. Replace battery with Motorola P/N 586185-001-00 only. Use of another battery may present a risk of fire or explosion.

Dispose of used battery promptly. Keep away from children. Do not disassemble and do not dispose of in fire.

1. Note the tab on the bottom of the battery.

2. Insert the battery into the compartment on the bottom of the unit, as shown, and press into place so that the battery contacts seat securely in the unit.

3. Then attach the compartment door. See “Battery Door Installation Instructions” on page 17.
Battery Door Installation Instructions

1. Place NVG589 Unit on a table top as shown in FIGURE (1).

2. Place battery door at an angle, as shown, and slide toward edge of unit. See FIGURE (2).

3. Rotate door in direction shown, see FIGURE (3), and snap closed.

4. Battery door installed. See FIGURE (4).
Battery Door Removal Instructions

1. Place unit on table top as shown in FIGURE (1).

2. Using both hands, pull tabs in directions shown in FIGURE (2).

3. While still pulling the tabs, pull the battery door in the direction shown. See FIGURE (3).

4. Remove battery door. See FIGURE (4).
Cradle Installation Instructions

1. Angle the NVG589 unit onto the rear of the cradle. See FIGURE (1).

2. Ensure that the NVG589 unit is latched to the rear of the cradle as shown in FIGURE (2).

3. Once the rear is latched, rotate the NVG589 unit down into the cradle and press until the snap is engaged. You should hear a “click” for positive engagement. See FIGURE (3).

4. Reverse sequence, by first pulling on the cradle, for removal.
Set up the Motorola Gateway

Refer to your Quickstart Guide for instructions on how to connect your Motorola® 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® Gateway models are supplied for any of these connections. Be sure to enable Dynamic Addressing on your PC. Perform the following:

**Microsoft Windows:**

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

a. Some Windows versions follow a path like this:

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

b. Some Windows versions follow a path like this:

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

Then go to Step 2.

Step 2. Select Obtain an IP address automatically.

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

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

Step 5. OK the settings. Restart if prompted.
c. Windows Vista and Windows 7 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 path like this:

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

b. Mac OS X follows a path like this:

Apple Menu -> System Preferences -> Network

Then go to Step 2.

Step 2. Select Built-in Ethernet

Step 3. Select Configure Using DHCP

Step 4. Close and Save, if prompted.

Proceed to "Accessing the Web Management Interface" on page 23.
Accessing the Web Management Interface

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

2. Enter **http://192.168.1.254** in the Location text box.
   
   While the Gateway is determining the Broadband network type, the following screen appears.

   ![Device Status Page](image)

   The Device Status Page appears.
3. Check to make sure the Broadband and Service LEDs are lit **GREEN** to verify that the connection to the Internet is active.

**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.
**Broadband Network Redirect Pages**

After a few minutes if the Broadband network cannot be determined, the following screen appears. Contact AT&T Customer care at the number shown for assistance.

If you click the **Continue** button, the following screen appears. Here you can manually select the Broadband network type, if you know it.
IP Diagnostics Page Redirect

In the event that your connection to the Internet fails, the Broadband LED will flash RED and you are redirected to the IP Diagnostics page. Follow the on-screen troubleshooting suggestions. For additional troubleshooting information, see “Diagnostics” on page 80 and “Basic Troubleshooting” on page 89.

When your connection is restored or the problem is resolved, the Broadband LED will turn GREEN.

Note:

For AT&T this function is enabled by default. See the CLI command "set management lan-redirect enable [ off | on ]" on page 149.

Offline Troubleshooting

If the WAN is down, the following will be displayed at the top of the page.

1. Click the “Restart” button next to each system below marked as “Down”.
2. Restart your device using the button below.
3. If this condition persists for more than 15 minutes, please contact the AT&T Help Desk at 1-800-288-2020.
Device Status page

After you have performed the basic Easy Login configuration, any time you log in to your Motorola® Gateway you will access the Motorola® Gateway Home Page.

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

Device Access Code

You may be required to provide your Device Access Code in order to access the web management configuration pages. The Device Access Code is unique to your device. It is printed on a label on the side of the Gateway.

Enter your Device Access Code and click the Continue button.
The Device Status Page appears.
The Device Status displays the following information in the center section:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadband</td>
<td>‘Waiting for DSL’ is displayed while the Gateway is training. This</td>
</tr>
<tr>
<td></td>
<td>should change to ‘Up’ within two minutes. ‘Up’ is displayed when the ADSL</td>
</tr>
<tr>
<td></td>
<td>line is synched and the session is established. ‘Down’ indicates inability</td>
</tr>
<tr>
<td></td>
<td>to establish a connection; possible line failure.</td>
</tr>
<tr>
<td>Battery</td>
<td>Status: Normal or Low Battery or Charging or Warning - No battery or</td>
</tr>
<tr>
<td></td>
<td>battery has no charge or Warning: Battery backup mechanism has a fault.</td>
</tr>
<tr>
<td>Wireless</td>
<td>Status: Your wireless signal may be ‘On’ or ‘Off’.</td>
</tr>
<tr>
<td></td>
<td>Network ID (SSID): This is the name or ID that is displayed to a client</td>
</tr>
<tr>
<td></td>
<td>scan. The default SSID for the Gateway is attxxx where xxx is the last 3</td>
</tr>
<tr>
<td></td>
<td>digits of the serial number located on the side of the Gateway.</td>
</tr>
<tr>
<td></td>
<td>Authentication Type: The type of wireless encryption security in use. May</td>
</tr>
<tr>
<td></td>
<td>be Disabled, WPA or WEP, Default Key or Manual.</td>
</tr>
<tr>
<td></td>
<td>Network Key: Wireless network encryption key in use.</td>
</tr>
<tr>
<td>Coax to STB</td>
<td>Status: Off or On.</td>
</tr>
<tr>
<td>Voice</td>
<td>Line 1: Indication of VoIP or other phone connection.</td>
</tr>
<tr>
<td></td>
<td>Line 2: Indication of VoIP or other phone connection.</td>
</tr>
</tbody>
</table>

Some fields may or may not display, depending on your particular setup.

The Diagnostics button will connect you to the Troubleshoot page. See “Diagnostics” on page 80.

### Common Tasks

- **Go to AT&T online support for troubleshooting and repair**
  
  This link will connect you to the IP Diagnostics page with help for troubleshooting and the AT&T Help Desk information. See “IP Diagnostics Page Redirect” on page 26.

- **Modify your Wireless security or settings**
  
  This link will connect you to the Wireless page. See “Wireless” on page 46.

- **Restart your device**
  
  This link will connect you to the Restart Device page. See “Restart Device” on page 36.

The right-hand frame displays some links to commonly performed tasks for easy access.
◆ **Find a computer on your home network**
   This link will connect you to the Device List page. See "Device List on page 32."

◆ **Adjust firewall settings for gaming and applications**
   This link will connect you to the NAT/Gaming page. See "NAT/Gaming on page 69."
Tab Bar

The tab bar is located at the top of every page, allowing you to move freely about the site.

The tabs reveal a succession of pages that allow you to manage or configure several features of your Gateway. Each tab is described in its own section.

Help

Help is provided in your Gateway. Help is available in the right hand frame on every page in the Web interface.

Here is an example:

The page shown here is displayed when you are on the System Information page.
Links Bar

The links bar at the top of each page allows you to configure different aspects of the features displayed on the page. For example, on the Home Summary page, the button bar is shown below:

<table>
<thead>
<tr>
<th>Status</th>
<th>Device List</th>
<th>System Information</th>
<th>Access Code</th>
<th>Restart Device</th>
<th>Battery</th>
</tr>
</thead>
</table>

Click the links below to be taken to each section.
- "Device Status page" on page 27
- "Device List" on page 32
- "System Information" on page 34
- "Access Code" on page 35
- "Restart Device" on page 36

Link: Device List

When you click the Device List link, the Device List page appears.

<table>
<thead>
<tr>
<th>Device List</th>
<th>Home Network Devices</th>
<th>Clear Device List</th>
<th>Scan for Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>IPv4 Address / Name</td>
<td>Status</td>
<td>Type</td>
</tr>
<tr>
<td>00:0f:cc:3e:64</td>
<td>192.168.1.253</td>
<td>Thu Jan 1 00:01:43:1970</td>
<td>Ethernet</td>
</tr>
<tr>
<td>00:0f:cc:3e:64</td>
<td>192.168.1.50</td>
<td>Thu Jan 1 00:01:43:1970</td>
<td>Ethernet</td>
</tr>
<tr>
<td>00:0f:cc:3e:64</td>
<td>192.168.1.143</td>
<td>Thu Jan 1 00:01:43:1970</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>

The page displays the following information:

<table>
<thead>
<tr>
<th>Home Network Devices</th>
<th>Displays the IPv4 Address, Network Name, and MAC Address of devices connected to this device on your local area network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Client device’s unique hardware address.</td>
</tr>
<tr>
<td>IPv4 Address / Name</td>
<td>Client device’s IP address or device network name.</td>
</tr>
<tr>
<td>Last Activity</td>
<td>Date and time of last traffic for this client device.</td>
</tr>
<tr>
<td>Status</td>
<td>May be off or on.</td>
</tr>
<tr>
<td>Allocation</td>
<td>Type of IP address assignment, for example, Static or DHCP.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Type of connection, for example, Ethernet or Wireless.</td>
</tr>
</tbody>
</table>
For Wireless client connections, the Device List displays the familiar bars indicating signal strength, as follows:

- Click the **Clear Device List** button to update the Home Network summary.
- Click the **Scan for Devices** button to seek out other devices that have been connected since the last Home Network summary update.
### Link: System Information

When you click the **System Information** link, the **System Information** page appears.

<table>
<thead>
<tr>
<th>System Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Motorola</td>
</tr>
<tr>
<td>Model Number</td>
<td>NAVG999</td>
</tr>
<tr>
<td>Serial Number</td>
<td>15797850092</td>
</tr>
<tr>
<td>Software Version</td>
<td>9.1.010103</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:24:c8:40:c1:a2</td>
</tr>
<tr>
<td>First Use Date</td>
<td>2012/04/27 08:52:32</td>
</tr>
<tr>
<td>Time Since Last Reboot</td>
<td>00:00:37:32</td>
</tr>
<tr>
<td>Datapump Version</td>
<td>A28v44F0288_rc18_224d_rc</td>
</tr>
<tr>
<td>Legal Disclaimer</td>
<td>Licenses</td>
</tr>
</tbody>
</table>

The page displays the following information:

- **Manufacturer**: This is the manufacturer’s identifier name.
- **Model Number**: This is the manufacturer’s model number.
- **Serial Number**: This is the unique serial number of your Gateway.
- **Software Version**: This is the version number of the current embedded software in your Gateway.
- **MAC Address**: Unique hardware address of this Gateway unit.
- **First Use Date**: Date and Time when the Gateway is first used. This field changes to the current date and time after a reset to factory defaults.
- **Time Since Last Reboot**: Elapsed time since last reboot of the Gateway in days:hr:min:sec.
- **Datapump Version**: Underlying operating system software datapump version.
- **Legal Disclaimer**: Clicking the **Licenses** link displays a listing of software copyright attributions also shown here: "Copyright Acknowledgments" on page 183.
Link: Access Code

Access to your Gateway is controlled through an account named Admin. The default Admin password for your Gateway is the unique Access Code printed on the label on the side of your Gateway.

As the Admin, you can change this password to a different one of your own choosing between 8 and 20 characters long. The new password must also include two characters from any these categories: alpha, number, and special characters.

Example: “fru1tfi13s_likeabanaana”


You can always return to the original default password by clicking the Use Default Access Code button.
Link: Restart Device

When the Gateway is restarted, it will disconnect all users, initialize all its interfaces, and load the Operating System Software.

When you make configuration changes, you may be required restart for the changes to take effect.
When you click the **Broadband** tab, the **Broadband Status** page appears.

The **Broadband Status** page displays information about the Gateway’s WAN connection(s) to the Internet.

### Broadband Status

<table>
<thead>
<tr>
<th></th>
<th>Line 1</th>
<th>Line 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line State</strong></td>
<td>Down</td>
<td>Down</td>
</tr>
<tr>
<td><strong>Downstream Sync Rate (kbps)</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Upstream Sync Rate (kbps)</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Data Path</strong></td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

**Broadband Connection**
- Down

**IPv4 Address**
- 0.0.0.0

**MAC Address**
- 00:24:80:49:17:e2

**Primary DNS**
- 

**Secondary DNS**
- 

**Primary DNS Name**
- 

**Secondary DNS Name**
- 

**MTU**
- 1500

**IPv6**
- Status: Unavailable

**Global Unicast IPv6 Address**
- 

**Border Relay IPv4 Address**
- 

**IPv4 Statistics**
- Transmit Packets: 0
- Transmit Errors: 0
- Transmit Discards: 0

**IPv6 Statistics**
- Transmit Packets: 0
- Transmit Errors: 0
- Transmit Discards: 0

**Downstream and Upstream Statistics**

<table>
<thead>
<tr>
<th></th>
<th>Line 1 Downstream</th>
<th>Line 1 Upstream</th>
<th>Line 2 Downstream</th>
<th>Line 2 Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SN Margin (dB)</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Line Attenuation (dB)</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Output Power(dBm)</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Errored Seconds</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Loss of Signal</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Loss of Frame</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>FEC Errors</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>CRC Errors</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Clear Statistics**

---

**Broadband Status**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line State</strong></td>
<td>May be Up (connected) or Down (disconnected).</td>
</tr>
<tr>
<td><strong>Broadband Connection</strong></td>
<td>May be Up (connected) or Down (disconnected).</td>
</tr>
</tbody>
</table>
### Administrator’s Handbook

<table>
<thead>
<tr>
<th><strong>Downstream Sync Rate</strong></th>
<th>This is the rate at which your connection can download (receive) data on your DSL line, in kilobits per second.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upstream Sync Rate</strong></td>
<td>This is the rate at which your connection can upload (send) data on your DSL line, in kilobits per second.</td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
<td>Method of regulating the DSL signal. DMT (Discrete MultiTone) allows connections to work better when certain radio transmitters are present.</td>
</tr>
<tr>
<td><strong>Data Path</strong></td>
<td>Type of path used by the device’s processor.</td>
</tr>
<tr>
<td><strong>Broadband IPv4 Address</strong></td>
<td>The public IP address of your device, whether dynamically or statically assigned.</td>
</tr>
<tr>
<td><strong>Gateway IPv4 Address</strong></td>
<td>Your ISP’s gateway router IP address.</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>Your Gateway’s unique hardware address identifier.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>The IP Address of the Primary Domain Name Server.</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong></td>
<td>The IP Address of the backup Domain Name Server, if available.</td>
</tr>
<tr>
<td><strong>Primary DNS Name</strong></td>
<td>The name of the Primary Domain Name Server.</td>
</tr>
<tr>
<td><strong>Secondary DNS Name</strong></td>
<td>The name of the backup Domain Name Server, if available.</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Maximum Transmittable Unit before packets are broken into multiple packets.</td>
</tr>
</tbody>
</table>

### IPv6

<table>
<thead>
<tr>
<th><strong>Status</strong></th>
<th>May be <strong>Enabled</strong> or <strong>Unavailable</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Unicast IPv6 Address</strong></td>
<td>The public IPv6 address of your device, whether dynamically or statically assigned.</td>
</tr>
<tr>
<td><strong>Border Relay IPv4 Address</strong></td>
<td>The public IPv4 address of your device.</td>
</tr>
</tbody>
</table>

### IPv4 Statistics

<table>
<thead>
<tr>
<th><strong>Transmit Packets</strong></th>
<th>IPv4 packets transmitted.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transmit Errors</strong></td>
<td>Errors on IPv4 packets transmitted.</td>
</tr>
<tr>
<td><strong>Transmit Discards</strong></td>
<td>IPv4 packets dropped.</td>
</tr>
</tbody>
</table>

### IPv6 Statistics

<table>
<thead>
<tr>
<th><strong>Transmit Packets</strong></th>
<th>IPv6 packets transmitted.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transmit Errors</strong></td>
<td>Errors on IPv6 packets transmitted.</td>
</tr>
<tr>
<td><strong>Transmit Discards</strong></td>
<td>IPv6 packets dropped.</td>
</tr>
</tbody>
</table>

### Downstream and Upstream Statistics

<table>
<thead>
<tr>
<th><strong>SN Margin (db)</strong></th>
<th>Signal to noise margin, in decibels. Reflects the amount of unwanted “noise” on the DSL line.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line Attenuation</strong></td>
<td>Amount of reduction in signal strength on the DSL line, in decibels.</td>
</tr>
<tr>
<td><strong>Output Power (dBm)</strong></td>
<td>Measure of power output in decibels (dB) referenced to one milliwatt (mW).</td>
</tr>
<tr>
<td><strong>Errored Seconds</strong></td>
<td>The number of uncorrected seconds after being down for seven consecutive seconds.</td>
</tr>
<tr>
<td><strong>Loss of Signal</strong></td>
<td>The absence of any signal for any reason, such as a disconnected cable or loss of power.</td>
</tr>
<tr>
<td><strong>Loss of Frame</strong></td>
<td>A signal is detected but cannot sync with signal caused by mismatched protocols, wrong ISP connection configuration, or faulty cable.</td>
</tr>
<tr>
<td><strong>FEC Errors</strong></td>
<td>(Forwarded Error Correction errors) Count of received errored packets that were fixed successfully with out a retry.</td>
</tr>
<tr>
<td><strong>CRC Errors</strong></td>
<td>Number of times data packets have had to be resent due to errors in transmission or reception.</td>
</tr>
</tbody>
</table>
Link: Configure

When you click the Configure link, the Broadband Configure screen appears. Here you can reconfigure your type of broadband connection should it change in the future.

- **Broadband Connection Source** - dsl, ethernet, or auto (automatically detected).
- **Media** – Auto (the default self-sensing rate), 10M full- or half-duplex, 100M full- or half-duplex, or 1G full- or half-duplex.
- **MDI-X** – Auto (the default self-sensing crossover setting), Off, or On.
- The WAN connection is automatically configured. However, you can adjust the **Maximum allowable MTU** (Maximum Transmittable Unit) value, if your service provider suggests it. The default 1500 is the maximum value, but some services require other values. 1492 is common.

If you make any change here, click the **Save** button.
Link: IGMP Stats

When you click the IGMP Stats link, the IGMP Stats screen appears.

The IGMP Statistics screen reports IGMP Proxy Groups and Multicast Forwarding information. It also displays a packet counter.
When you click the **Home Network** tab, the **Home Network Status** page appears.

The **Home Network Status** page displays information about the Gateway’s local area network.

If you click the **Run Congestion Detection** button, the device will generate statistics for each of the 11 channels available, displaying:

- Channel number
- AP Count
- Congestion Score (1 - 10)

You can clear the current statistics information by clicking the **Clear Statistics** button.
Home Network Status

<table>
<thead>
<tr>
<th>Device IPv4 Address</th>
<th>The Gateway's own IP address on the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Netmask</td>
<td>The Gateway's own netmask on the network.</td>
</tr>
<tr>
<td>DHCPv4 Start Address</td>
<td>The starting IP address of the DHCP range served by the Gateway.</td>
</tr>
<tr>
<td>DHCPv4 End Address</td>
<td>The ending IP address of the DHCP range served by the Gateway.</td>
</tr>
<tr>
<td>DHCP Leases Available</td>
<td>The number of IP addresses of the DHCP range available to be served by the Gateway.</td>
</tr>
<tr>
<td>DHCP Leases Allocated</td>
<td>The number of IP addresses of the DHCP range currently being served by the Gateway.</td>
</tr>
<tr>
<td>DHCP Primary Pool</td>
<td>Source pool of the IP addresses served by the Gateway, Public or Private.</td>
</tr>
</tbody>
</table>

IPv6

<table>
<thead>
<tr>
<th>Status</th>
<th>May be Enabled or Unavailable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global IPv6 Address</td>
<td>The public IPv6 address of your device, whether dynamically or statically assigned.</td>
</tr>
<tr>
<td>Link-local IPv6 Address</td>
<td>The private IPv6 address of your device, whether dynamically or statically assigned.</td>
</tr>
<tr>
<td>Router Advertisement Prefix</td>
<td>The IPv6 prefix to include in router advertisements.</td>
</tr>
</tbody>
</table>

IPv4 Statistics

<table>
<thead>
<tr>
<th>Transmit Packets</th>
<th>IPv4 packets transmitted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Errors</td>
<td>Errors on IPv4 packets transmitted.</td>
</tr>
<tr>
<td>Transmit Discards</td>
<td>IPv4 packets dropped.</td>
</tr>
</tbody>
</table>

IPv6 Statistics

<table>
<thead>
<tr>
<th>Transmit Packets</th>
<th>IPv6 packets transmitted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Errors</td>
<td>Errors on IPv6 packets transmitted.</td>
</tr>
<tr>
<td>Transmit Discards</td>
<td>IPv6 packets dropped.</td>
</tr>
</tbody>
</table>

Wireless Status

<table>
<thead>
<tr>
<th>Wireless Radio Status</th>
<th>Indicates whether the Wi-Fi radio is Enabled or Disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name (SSID)</td>
<td>This is the name or ID that is displayed to a client scan. The default SSID for the Gateway is <strong>attxxx</strong> where <strong>xxx</strong> is the last 3 digits of the serial number located on the side of the Gateway.</td>
</tr>
<tr>
<td>Hide SSID</td>
<td>May be either On or Off. If On, your SSID will not appear in a client scan.</td>
</tr>
<tr>
<td>Wireless Security</td>
<td>The type of wireless encryption security in use. May be Disabled, WPA or WEP, Default Key or Manual.</td>
</tr>
<tr>
<td>Network Key</td>
<td>Shows the information of the security encryption key in use.</td>
</tr>
<tr>
<td>Mode</td>
<td>May be 802.11B only, 802.11G only, 802.11N, or 802.11 B/G/N.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The capacity of the wireless LAN to carry traffic in megahertz.</td>
</tr>
<tr>
<td>Current Radio Channel</td>
<td>The radio channel that your Wi-Fi network is broadcasting on.</td>
</tr>
<tr>
<td>Radio Channel Selection</td>
<td>May be set to automatic or manually selected.</td>
</tr>
<tr>
<td>MAC Address Filtering</td>
<td>May be either On or Off. If On, you can accept or block client devices from your WLAN based on their MAC address.</td>
</tr>
<tr>
<td>Power Level</td>
<td>May be adjusted up to 100%, lower if multiple wireless access points are in use, and might interfere with each other.</td>
</tr>
</tbody>
</table>
Wireless MAC Address | Shows the information of the MAC address of the wireless subsystem.
---|---

**LAN Wireless Statistics**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Bytes</td>
<td>Number of bytes transmitted on the Wi-Fi network.</td>
</tr>
<tr>
<td>Receive Bytes</td>
<td>Number of bytes received on the Wi-Fi network.</td>
</tr>
<tr>
<td>Transmit Packets</td>
<td>Number of packets transmitted on the Wi-Fi network.</td>
</tr>
<tr>
<td>Receive Packets</td>
<td>Number of packets received on the Wi-Fi network.</td>
</tr>
<tr>
<td>Transmit Error Packets</td>
<td>This is the number of errors on packets transmitted on the Wi-Fi network.</td>
</tr>
<tr>
<td>Receive Error Packets</td>
<td>This is the number of errors on packets received on the Wi-Fi network.</td>
</tr>
<tr>
<td>Transmit Discard Packets</td>
<td>This is the number of packets transmitted on the Wi-Fi network that were dropped.</td>
</tr>
<tr>
<td>Receive Discard Packets</td>
<td>This is the number of packets received on the Wi-Fi network that were dropped.</td>
</tr>
</tbody>
</table>

**LAN Ethernet Statistics**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>up or down</td>
</tr>
<tr>
<td>Transmit Speed</td>
<td>This is the maximum speed of which the port is capable.</td>
</tr>
<tr>
<td>Transmit Packets</td>
<td>This is the number of packets sent out from the port.</td>
</tr>
<tr>
<td>Transmit Bytes</td>
<td>This is the number of bytes sent out from the port.</td>
</tr>
<tr>
<td>Transmit Dropped</td>
<td>This is the number of packets sent out from the port that were dropped.</td>
</tr>
<tr>
<td>Transmit Errors</td>
<td>This is the number of errors on packets sent out from the port.</td>
</tr>
<tr>
<td>Receive Packets</td>
<td>This is the number of packets received on the port.</td>
</tr>
<tr>
<td>Receive Bytes</td>
<td>This is the number of bytes received on the port.</td>
</tr>
<tr>
<td>Receive Unicast</td>
<td>This is the number of unicast packets received on the port.</td>
</tr>
<tr>
<td>Receive Multicast</td>
<td>This is the number of multicast packets received on the port.</td>
</tr>
<tr>
<td>Receive Dropped</td>
<td>This is the number of packets received on the port that were dropped.</td>
</tr>
<tr>
<td>Receive Errors</td>
<td>This is the number of errors on packets received on the port.</td>
</tr>
</tbody>
</table>

The links at the top of the Home Network page access a series of pages to allow you to configure and monitor features of your device. The following sections give brief descriptions of these pages.
Link: Configure

When you click the Configure link, the Configure page for the Ethernet LAN appears.

For each Ethernet Port, 1 through 4, you can select:

- **Ethernet** – Auto (the default self-sensing rate), 10M full- or half-duplex, 100M full- or half-duplex, or 1G full- or half-duplex.
- **MDI-X** – Auto (the default self-sensing crossover setting), off, or on.

Click the Save button.
Link: HPNA Configure

When you click the HPNA Configure link, the HPNA Configure page for the HomePNA network appears.

Here you can turn HomePNA Networking On or Off.

If desired, you can choose the Output Jack, either the Coax jack or the Phone jack, or let the device Auto sense it automatically.

Click the Save button.
Link: Wireless

When you click the Wireless link the Wireless page appears. The Wireless page displays the status of your Wireless LAN elements.

The Wireless page’s center section contains a summary of the Wireless Access Point’s configuration settings and operational status.

<table>
<thead>
<tr>
<th>Field</th>
<th>Status and/or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Operation</td>
<td>May be either <strong>On</strong> or <strong>Off</strong>.</td>
</tr>
<tr>
<td>Network Name (SSID)</td>
<td>This is the name or ID that is displayed to a client scan. The default SSID for the Gateway is <strong>attxxx</strong> where <strong>xxx</strong> is the last 3 digits of the serial number located on the side of the gateway.</td>
</tr>
<tr>
<td>Hide SSID</td>
<td>May be either <strong>Off</strong> or <strong>On</strong>. If On, your SSID will not appear in a client scan.</td>
</tr>
<tr>
<td>Security</td>
<td>The type of wireless encryption security in use. May be <strong>OFF-No Privacy</strong>, <strong>WPA-PSK</strong> or <strong>WEP, Default Key</strong> or <strong>Manual</strong>.</td>
</tr>
<tr>
<td>WPA Version</td>
<td>If WPA is selected, may be <strong>Both</strong>, <strong>WPA-1</strong>, or <strong>WPA-2</strong>.</td>
</tr>
<tr>
<td>WEP Key Length</td>
<td>May be 10 characters for 40/64-bit, or 26 characters for 128-bit WP encryption.</td>
</tr>
<tr>
<td>Key</td>
<td>Here you can enter a manual encryption key.</td>
</tr>
<tr>
<td>Mode</td>
<td>May be 802.11B only, 802.11G only, 802.11N, or 802.11 B/G/N.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The capacity of the wireless LAN to carry traffic in megahertz, <strong>20</strong> or <strong>40</strong>.</td>
</tr>
<tr>
<td>Channel</td>
<td>The radio channel that your Wi-Fi network is broadcasting on.</td>
</tr>
<tr>
<td>Power Level</td>
<td>May be adjusted up to 100%, lower if multiple wireless access points are in use, and might interfere with each other.</td>
</tr>
<tr>
<td>Wireless Protected Setup (WPS)</td>
<td>May be either <strong>On</strong> or <strong>Off</strong>.</td>
</tr>
</tbody>
</table>

◆ The Wireless Operation function is automatically enabled by default. If you uncheck the checkbox, the Wireless Options are disabled, and the Wireless Access Point will not provide or broadcast its wireless LAN services.
Network Name (SSID) – preset to a number unique to your unit. You can either leave it as is, or change it by entering a freeform name of up to 32 characters, for example “Hercule’s Wireless LAN”. On client PCs’ software, this might also be called the Network Name. The Wireless ID is used to identify this particular wireless LAN. Depending on their operating system or client wireless card, users must either:
• select from a list of available wireless LANs that appear in a scanned list on their client
• or enter this name on their clients in order to join this wireless LAN.

Hide SSID – If enabled, this mode hides the wireless network from the scanning features of wireless client computers. Unless both the wireless clients and the Gateway share the same Network Name (SSID) in hidden mode, the Gateway’s wireless LAN will not appear as an available network when scanned for by wireless-enabled computers. Members of the hidden WLAN must log onto the Gateway’s wireless network with the identical SSID as that configured in the Gateway. 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 Hide SSID, 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.


Mode – The pull-down menu allows you to select and lock the Gateway into the wireless transmission mode you want: B/G/N, B-only, B/G, G-only, or N-only. For compatibility with clients using 802.11b (up to 11 Mbps transmission), 802.11g (up to 20+ Mbps), 802.11a (up to 54 Mbit/s using the 5 GHz band), or 802.11n (from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz), select B/G/N. To limit your wireless LAN to one mode or the other, select G-only, N-only, or B-only, or some combination that applies to your setup.

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.

Bandwidth – May only be selected if mode is some combination of 802.11n (from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz). Measure of the width of a range of frequencies, in megahertz.

Channel (1 through 11, for North America) on which the network will broadcast. This is a frequency range within the 2.4GHz band. Channel selection depends on government regulated radio frequencies that vary from region to region. Channel selection can have a significant impact on performance, depending on other wireless activity close to this Wireless Access Point. You need not select a channel at any of the computers on your wireless network. They will automatically scan available channels seeking a Gateway broadcasting on the SSID for which they are configured. The Automatic setting allows the Wireless Access Point to determine the best channel to broadcast automatically.

Power Level – Sets the wireless transmit power, scaling down the Wireless Access Point’s wireless transmit coverage by lowering its radio power output. Default is 100% power. Transmit power settings are useful in large venues with multiple wireless routers where you want to reuse channels. Since there are only three non-overlapping channels in the 802.11 spectrum, it helps to size the Wireless Access Point’s cell to match the location. This allows you to install a router to cover a small “hole” without conflicting with other routers nearby.

Wireless Protected Setup (WPS) is a not a new security protocol. It is simply an easier way to use existing protocols to provide greater security for your wireless network connections. By default, Privacy is set to Wireless Protected Access (WPA-PSK). WPS allows you to automatically generate a new strong WPA key for your Gateway and any client devices on your wireless network. Not all client wireless devices support WPS. Refer to their documentation. Enter your all digit WPS PIN and click the Submit button. Follow the instructions that came with your wireless client.
Wireless Security

By default, Wireless Security is set to **WPA-PSK** with a pre-defined **WPA-Default Key** (Wireless Protected Access Pre-Shared Key).

Other options are available from the **Security** pull-down menu:

- **WEP - Manual**: WEP Security is a Privacy option that is based on encryption between the Router and any PCs ("clients") you have with wireless cards. If you are not using WPA-PSK Privacy, you can use WEP encryption instead. For this encryption to work, both your Wireless Access Point and each client must share the same Wireless ID (SSID), and both must be using the same encryption keys. See "**WEP-Manual**" on page 48.

- **WPA-PSK**: allows you to enter your own key, the most secure option for your wireless network. The key can be between 8 and 63 characters, but for best security it should be at least 20 characters. If you select **WPA-PSK** as your privacy setting, the **WPA Version** pull-down menu allows you to select the WPA version(s) that will be required for client connections. Choices are:
  - **Both**, for maximum interoperability,
  - **WPA-1**, for backward compatibility,
  - **WPA-2**, for maximum security.
  All clients must support the version(s) selected in order to successfully connect.

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

- **OFF - No Privacy**: This mode disables privacy on your network, allowing any wireless users to connect to your wireless LAN. Use this option if you are using alternative security measures such as VPN tunnels, or if your network is for public use.

Click the **Save** button.

**WEP-Manual**

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

**WEP - Manual** allows you to enter your own encryption keys manually. This is a difficult process, but only needs to be done once. Avoid the temptation to enter all the same characters.
**Key Length:** The pull-down menu 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.

**Key:** You enter a key using hexadecimal digits. For 40/64-bit encryption, you need ten digits; 26 digits for 128-bit WEP. Hexadecimal characters are 0 – 9, and a – f.

**Examples:**
- 40 bits: 02468ACE02
- 128 bits: 0123456789ABCDEF0123456789

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

Click the click **Save** button.
Link: MAC Filtering

When you click the MAC Filtering link the MAC Filtering page appears.

MAC Filtering allows you to specify which client PCs are allowed to join the wireless LAN by unique hardware (MAC) address.

- To enable this feature, select Blacklist or Whitelist from the MAC Filtering Type menu. Blacklist means that only MAC addresses you specify will be denied access; Whitelist means that only MAC addresses you specify will be allowed access.
- You add wireless clients that you want to Whitelist or Blacklist for your wireless LAN by selecting them from the List of MACs or by entering the MAC addresses in the Manual Entry field provided.
- Click the Add button.

Your entries will be added to a list of clients that will be either authorized (Whitelisted) or disallowed (Blacklisted) depending on your selection.

- Click the Save button.

You can Add or Delete any of your entries later by returning to this page.
Your device automatically checks for the best channel to broadcast wireless services. However, in some cases it may be useful to switch to a different channel (1 through 11, for North America) on which the network will broadcast.

This is a frequency range within the 2.4Ghz band. Channel selection depends on government regulated radio frequencies that vary from region to region. Channel selection can have a significant impact on performance, depending on other wireless activity close to this device. You need not select a channel at any of the computers on your wireless network. They will automatically scan available channels seeking a wireless device broadcasting on the SSID for which they are configured.

This scan will disconnect any wireless client devices from the wireless network.

If you want to scan for a different channel on which the device will broadcast, click the Continue button.
Link: Subnets & DHCP

When you click the Subnets & DHCP link, the Subnets & DHCP page appears.

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

Private LAN Subnet
- **Device IPv4 Address**: The IP address of your Gateway as seen from the LAN
- **Subnet Mask**: Subnet mask of your LAN
- **DHCPv4 Start Address**: First IP address in the range being served to your LAN by the Gateway's DHCP server
- **DHCPv4 End Address**: Last IP address in the range being served to your LAN by the Gateway's DHCP server

Public Subnet
- **Public Subnet Enable**: If you select On from the pull-down menu, you can enable a second subnet to distribute public addresses to DHCP clients; this means that IP addresses assigned to LAN clients will be public addresses
- **Public IPv4 Address**: The IP address of your Gateway as seen from the WAN
- **Public Subnet Mask**: Public subnet mask
- **DHCPv4 Start Address**: First IP address in the range being served from a DHCP public pool.
- **DHCPv4 End Address**: Last IP address in the range being served from a DHCP public pool.
◆ **Primary DHCP Pool**: Choose the source of the DHCP pool IP address assignment by selecting either the *Private* (local to your LAN) or *Public* (assigned remotely) radio button.

**Cascaded Router**

◆ **Cascaded Router Enable**: If you have another router behind this Gateway, choose **On** from the pull-down menu.

◆ **Cascaded Router Address**: If you chose **On** from the pull-down menu, enter the IP address of the router you are using behind this Gateway in the LAN Private IP subnet range.

◆ **Network Address**: If you chose **On** from the pull-down menu, enter the Network Address that defines the range of IP addresses available to clients of the router you are using behind this Gateway.

◆ **Subnet Mask**: If you chose **On** from the pull-down menu, enter the subnet mask for the Network Address that defines the range of IP addresses available to clients of the router you are using behind this Gateway.

**DHCP**

◆ **DHCP Lease**: Specifies the default length for DHCP leases issued by the Router. Enter lease time in **dd:hh:mm:ss** (days/hours/minutes/seconds) format.

If you make any changes here, click the **Save** button, and if prompted, restart the Gateway.
Link: HPNA

When you click the HPNA link, the HPNA Network page appears.

The HPNA Network page displays information about the Gateway’s HPNA-connected devices in 15 minute intervals.

◆ If you have two or more stations, you can select the radio button and click the Set DVR button to store the MAC address of the station as the “master DVR.” If the station order subsequently changes, the radio button will appear on the correct station.
◆ You can test the performance of each station to station pair by clicking the Run extended Test button. When you click the Run extended Test button, the following page appears as a warning about this invasive test.

![Warning](image)

If you do not run the Extended Test, the station-to-station performance section is not displayed.

◆ You can generate updated statistics by clicking the Refresh button.

Furnished statistics of the current and previous intervals are displayed as follows:

◆ Station ID
◆ HPNA MAC Address
◆ HPNA Firmware (C-coax, T=TP)
◆ HPNA Version
◆ HPNA Master

<table>
<thead>
<tr>
<th>Interval Start</th>
<th>Interval Stop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Tx Pkt</td>
<td>This is the number of Transmitted Packets</td>
</tr>
<tr>
<td>Short Rx Pkt</td>
<td>This is the number of Received Packets</td>
</tr>
<tr>
<td>CRC Errors Rx</td>
<td>This is the number of Receipt errors</td>
</tr>
<tr>
<td>Dropped Tx</td>
<td>This is the number of Transmit packets dropped</td>
</tr>
<tr>
<td>Dropped Rx</td>
<td>This is the number of Receipt packets dropped</td>
</tr>
<tr>
<td>Tx Error %</td>
<td>This is the percentage of transmitted errors</td>
</tr>
<tr>
<td>Rx Error %</td>
<td>This is the percentage of receipt errors</td>
</tr>
<tr>
<td>Frames Tx</td>
<td>This is the number of frames transmitted</td>
</tr>
<tr>
<td>Frames Rx</td>
<td>This is the number of frames received</td>
</tr>
<tr>
<td>Bytes Tx</td>
<td>This is the number of bytes transmitted</td>
</tr>
<tr>
<td>Bytes Rx</td>
<td>This is the number of bytes received</td>
</tr>
<tr>
<td>Unicast Tx</td>
<td>This is the number of unicast packets transmitted</td>
</tr>
<tr>
<td>Unicast Rx</td>
<td>This is the number of unicast packets received</td>
</tr>
<tr>
<td>Multicast Tx</td>
<td>This is the number of multicast packets transmitted</td>
</tr>
<tr>
<td>Multicast Rx</td>
<td>This is the number of multicast packets received</td>
</tr>
<tr>
<td>Local Control Req</td>
<td>This is the number of requests made to the device by local control</td>
</tr>
<tr>
<td>Local Control Repl</td>
<td>This is the number of replies made by the device to local control</td>
</tr>
<tr>
<td>Remote Control Req</td>
<td>This is the number of requests made to the device by remote control</td>
</tr>
<tr>
<td>Remote Control Repl</td>
<td>This is the number of replies made by the device to remote control</td>
</tr>
</tbody>
</table>
Voice

If you click the Voice ink, the Voice page appears.

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.

◆ The Voice page displays information about your VoIP phone lines, if configured. Your Gateway supports two phones, Line 1 and Line 2.
◆ If either one or both are registered with a SIP server by your service provider or not registered, the Voice page will display their Registration Details.

The links at the top of the Voice page access a series of pages to allow you to configure and monitor features of your device. The following sections give brief descriptions of these pages.

- "Line Details" on page 57
- "Call Statistics" on page 58
Link: Line Details

When you click the Line Details link, the Line Details page appears.

◆ If your service provider has enabled your VoIP phone lines, you can register them by clicking the Register Line 1 or Register Line 2 button(s).
◆ To test if the lines are enabled, click the Ring Line 1 or Ring Line 2 button(s). If enabled and registered, the respective phone will ring until you click the Stop Ring Line 1 or Stop Ring Line 2 buttons.
◆ To clear the current state of each phone line, click the Reset Line 1 or Reset Line 2 button(s). This will disconnect any calls currently in progress as well.
◆ To update the display, click the Refresh button.
Link: Call Statistics

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

For **Line 1** and **Line 2**, the two available phone lines, the Call Statistics page displays the following information:

<table>
<thead>
<tr>
<th></th>
<th>Last Call</th>
<th>Cumulative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incoming</td>
<td>Outgoing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTP Packet Loss</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RTP Packet Loss percent-</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Total RTCP Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Inter Arrival Jitter (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Max Inter Arrival Jitter (in ms)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sum of Inter Arrival Jitter (in ms)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sum of Inter Arrival Jitter Squared (in ms)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sum of Franc Loss</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sum of Franc Loss Squared</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Max One Way Delay (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Sum of One Way Delay (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Sum of One Way Delay Squared</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Avg Round Trip Time (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Max Round Trip Time (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Sum of Round Trip Time (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>Sum of Round Trip Time Squared</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Last Call</th>
<th>Cumulative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incoming</td>
<td>Outgoing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTP Packet Loss</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RTP Packet Loss percent-</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Total RTCP Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Inter Arrival Jitter (in ms)</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Last Call/Cumulative – Incoming/Outgoing**

- **RTP Packet Loss**: Real-time Transport Protocol packets dropped
- **RTP Packet Loss percentage**: Percent of Real-time Transport Protocol packets dropped
- **Total RTCP Packets**: Total Real-time Transport Control Protocol packets
- **Average Inter Arrival Jitter**: This is calculated continuously in milliseconds as each data packet is received and averaged.
- **Max Inter Arrival Jitter**: This is the maximum value in milliseconds recorded as each data packet is received.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sum of Inter Arrival Jitter</td>
<td>This is calculated continuously in milliseconds as each data packet is received and totalled.</td>
</tr>
<tr>
<td>Sum of Inter Arrival Jitter Squared</td>
<td>This is calculated continuously in milliseconds as each data packet is received and the total is squared.</td>
</tr>
<tr>
<td>Sum of Franc Loss</td>
<td>Fraction Lost: The fraction of RTP data packets lost since the previous SR or RR packet was sent. This fraction is defined to be the number of packets lost divided by the number of packets expected. This will be calculated on every RTCP SR packet. Sum of the fraction lost is calculated with all the RTCP packets.</td>
</tr>
<tr>
<td>Sum of Franc Loss Squared</td>
<td>Fraction lost is squared with every RTCP SR or RR packet. Sum of all this will give the Sum of Franc Loss Squared.</td>
</tr>
<tr>
<td>Max One Way Delay</td>
<td>One Way Delay will be calculated in milliseconds on every RTCP SR or RR packet. This value is (systime - lsr - dslr) / 2. lsr means last SR timestamp, dslr means delay since last SR.</td>
</tr>
<tr>
<td>Sum of One Way Delay</td>
<td>The sum of all the one way delays calculated in milliseconds on every RTCP packet is displayed as Sum of One Way Delay.</td>
</tr>
<tr>
<td>Sum of One Way Delay Squared</td>
<td>One Way Delay is squared with every RTCP SR or RR packet. Sum of all this will give the Sum of One Way Delay Squared.</td>
</tr>
<tr>
<td>Avg Round Trip Time</td>
<td>Average time in milliseconds from this local source to destination address and back again for all logged calls.</td>
</tr>
<tr>
<td>Max Round Trip Time</td>
<td>Maximum amount of time in milliseconds from this local source to destination address and back again for all logged calls.</td>
</tr>
<tr>
<td>Sum of Round Trip Time</td>
<td>Sum of time in milliseconds from this local source to destination address and back again for all logged calls.</td>
</tr>
<tr>
<td>Sum of Round Trip Time Squared</td>
<td>Sum squared of time from this local source to destination address and back again for all logged calls.</td>
</tr>
</tbody>
</table>
For **Line 1** and **Line 2**, the two available phone lines, the Call Summary section displays the following information:

**Call Summary - Line 1 and Line 2**

- **Call Timestamp**: Date and Time of the current call
- **Type**: May be Incoming or Outgoing
- **Duration**: Length of time in seconds of call connection
- **Codec in Use**: Audio codec used for decoding the call packet traffic.
- **Far-End Host Information**: SIP server IP information: IP address and port number
- **Far-End Caller Information**: Caller ID information, if available

**Cumulative Since Last Reset**

- **Last Reset Timestamp**: Date and Time of the last call
- **Number of Calls**: Total number of calls for each VoIP line
- **Duration**: Time in seconds since the last call
- **Number of Incoming Calls Failed**: Number of incoming calls that fail to connect
- **Number of Outgoing Calls Failed**: Number of outgoing calls that fail to connect
The following table is the simplified version of VOIP line/hook/etc. states during different conditions.

<table>
<thead>
<tr>
<th>VOIP Line 1/2</th>
<th>Hook state</th>
<th>WAN IP</th>
<th>Reg-state</th>
<th>FXS Voltage</th>
<th>Tone</th>
<th>LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td>On/Off-hook</td>
<td>UP</td>
<td>Idle</td>
<td>OFF</td>
<td>N/A</td>
<td>off</td>
</tr>
<tr>
<td>Enabled</td>
<td>On-hook</td>
<td>UP</td>
<td>Registered</td>
<td>ON</td>
<td>N/A</td>
<td>Solid</td>
</tr>
<tr>
<td>Enabled</td>
<td>Off-hook</td>
<td>UP</td>
<td>Registered</td>
<td>ON</td>
<td>DIAL TONE</td>
<td>Blink</td>
</tr>
<tr>
<td>Enabled</td>
<td>On/off hook</td>
<td>UP</td>
<td>Failure</td>
<td>OFF</td>
<td>N/A</td>
<td>off</td>
</tr>
<tr>
<td>Enabled</td>
<td>On/off hook</td>
<td>DOWN</td>
<td>Idle</td>
<td>OFF</td>
<td>N/A</td>
<td>off</td>
</tr>
</tbody>
</table>

The following table provides the state changes during the boot-up procedure.

<table>
<thead>
<tr>
<th>VOIP Line 1/2</th>
<th>WAN Status</th>
<th>Hook State</th>
<th>Reg-state</th>
<th>FXS Voltage</th>
<th>Tone</th>
<th>LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td>Down</td>
<td>Off-hook</td>
<td>Idle</td>
<td>On-to-off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>Enabled</td>
<td>Down</td>
<td>On/Off-hook</td>
<td>Idle</td>
<td>ON</td>
<td>Congestion</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td>Up</td>
<td>Off-hook</td>
<td>Registered</td>
<td>ON</td>
<td>Congestion. Dial Tone played after the hook state is changed.</td>
<td>ON</td>
</tr>
</tbody>
</table>

Dial Tone
Firewall

When you click the **Firewall** tab, the **Firewall** Status page appears. The Firewall page displays the status of your system firewall elements.

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 system. Stateful inspection can be enabled on a WAN interface whether NAT is enabled or not.

The center section displays the following:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filter</td>
<td>May be On or Off</td>
</tr>
<tr>
<td>IP Passthrough</td>
<td>May be On or Off</td>
</tr>
<tr>
<td>NAT Default Server</td>
<td>May be On or Off</td>
</tr>
<tr>
<td>Firewall Advanced</td>
<td>May be On or Off</td>
</tr>
</tbody>
</table>

The links at the top of the Firewall page access a series of pages to allow you to configure security features of your device. The following sections give brief descriptions of these pages.

- “Packet Filter” on page 63
- “NAT/Gaming” on page 69
- “IP Passthrough” on page 75
- “Firewall Advanced” on page 78
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 Filtersets. Each Filterset can have up to eight rules configured.

**WARNING:**

Before attempting to configure filters and filtersets, please read and understand this entire section thoroughly. The Motorola Gateway incorporating NAT has advanced security features built in. Improperly adding filters and filtersets 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 filtersets can enhance network security, there are disadvantages:

- Filters are complex. Combining them in filtersets 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. Filtersets are not a substitute for password protection, effective safeguarding of passwords, and general awareness of how your network may be vulnerable.

Motorola’s packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the Gateway’s filtersets 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 filtersets, you should read the next few sections to learn more about how these powerful security tools work.
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 (where the packet was sent from)
◆ The destination IP address (where the packet is going)
◆ The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Other filter attributes
There are three other attributes to each filter:

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

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

◆ Be sure the filterset'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 filtersets is part of reaching that goal.

Each filterset 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 filterset designs.
Working with Packet Filters
To work with filters, begin by accessing the Packet Filter page.

Packet Filter
◆ Enable/Disable Packet Filters – Click this button to globally turn your filters on or off.

Packet Filter Rules
Buttons: Click either Add a ‘Drop’ Rule or Add a ‘Pass’ Rule button.
◆ Action:
  • drop: If you select drop, the specified packets will be blocked.
  • pass: If you select pass, the specified packets will be forwarded.
Enter the **Source IP Address** or **Destination IP Address** this filter will match on.

As you create new Matches, the pulldown items change. There can only be one match from each Match Type for a given rule. Match Types like Source Port, Destination Port, and TCP Flags are only available if other matches (for example, Protocol =TCP) have previously been created.

Select **Protocol**, if necessary, from the pull-down menu: **ICMP**, **TCP**, **UDP**, or **None** to specify any another IP transport protocol.

If you chose **by number**, enter the **Protocol by number** here.

If you chose **by name**, enter the **Protocol by name** here.

Enter the **Source Port** this filter will match on.

Enter the **Destination Port** this filter will match on.

If you selected **ICMP**, enter the **ICMP Type** here.

When you are finished configuring the filter, click the **Enter Match** button.

The filter is automatically saved.
## Packet Filter Rules List

Your entries are displayed as a table.

<table>
<thead>
<tr>
<th>Order</th>
<th>Action</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Drop</td>
<td>207.53.17.9</td>
<td></td>
<td>TCP</td>
<td>8080</td>
<td></td>
</tr>
</tbody>
</table>
Port Warnings:

If the packet filter or port forwarding rule involves TCP port 80 or 3389; or UDP port 47806, 43962, 69, 123, or 53; or if you attempt to add or change a match such that this occurs AND if running in VDSL/Ethernet mode, the following warning will appear.

![Warning Message]

**Warning:** The change you are attempting to make may cause AT&T U-verse TV to stop working properly.

Please select “Confirm” to continue with the change, or “Cancel” to revert the change.
When you click the **NAT/Gaming** link, the **NAT/Gaming** page appears.

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

From the **Service** pull-down menu, you can select any of a large number of predefined games and software. (See “List of Supported Games and Software” on page 73.)

In addition to choosing from these predefined services you can also select a user defined custom service. (See “Custom Services” on page 71.)

For each supported game or service, you can view the protocols and port ranges used by the game or service by clicking the **Service Details** button. For example:

Select a hosting device from the **Needed by Device** pull-down menu.

1. Once you choose a software service or game, click **Add**.
2. Select a PC to host the software from the Select Host Device pull-down menu and click **Save**.
Each time you enable a software service or game your entry will be added to the list of Service names displayed on the NAT Configuration page.

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

To configure a Custom Service, click the Add/Edit Services button. The Custom Services page appears.

Enter the following information:

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

Once you define a Custom Service it becomes available in the Application Hosting Entry Service menu as one of the services to select.

Click the Add button.
Each time you enable a custom service your entry will be added to the list of Service names displayed on the Custom Services page.

Changes are saved immediately.

To remove this Service, click the Delete button.

To edit this Service, click the Edit button.

Note:

You cannot edit a Custom Service if the Service is active; it must be inactive before it can be edited.
<table>
<thead>
<tr>
<th>List of Supported Games and Software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AIM Talk</strong></td>
</tr>
<tr>
<td><strong>Age of Empires, v.1.0</strong></td>
</tr>
<tr>
<td><strong>Age of Wonders</strong></td>
</tr>
<tr>
<td><strong>Asheron's Call</strong></td>
</tr>
<tr>
<td><strong>Battlefield 1942</strong></td>
</tr>
<tr>
<td><strong>BitTornado</strong></td>
</tr>
<tr>
<td><strong>Blazing Angels Online</strong></td>
</tr>
<tr>
<td><strong>Buddy Phone</strong></td>
</tr>
<tr>
<td><strong>Call of Duty</strong></td>
</tr>
<tr>
<td><strong>Close Combat for Windows 1.0</strong></td>
</tr>
<tr>
<td><strong>Combat Flight Sim: WWII Europe Series, v 1.0</strong></td>
</tr>
<tr>
<td><strong>Dark Reign</strong></td>
</tr>
<tr>
<td><strong>Delta Force Black Hawk Down</strong></td>
</tr>
<tr>
<td><strong>DirecTV STB 1</strong></td>
</tr>
<tr>
<td><strong>Doom 3</strong></td>
</tr>
<tr>
<td><strong>Empire Earth</strong></td>
</tr>
<tr>
<td><strong>F-22, Lightning 3</strong></td>
</tr>
<tr>
<td><strong>Fighter Ace II</strong></td>
</tr>
<tr>
<td><strong>H.323 compliant (Netmeeting, CUSeeME)</strong></td>
</tr>
<tr>
<td><strong>Half Life</strong></td>
</tr>
<tr>
<td><strong>Half Life Steam</strong></td>
</tr>
<tr>
<td><strong>Hellbender for Windows, v 1.0</strong></td>
</tr>
<tr>
<td><strong>Hotline Server</strong></td>
</tr>
<tr>
<td><strong>IMAP Client</strong></td>
</tr>
<tr>
<td><strong>Internet Phone</strong></td>
</tr>
<tr>
<td><strong>Kazaa</strong></td>
</tr>
<tr>
<td><strong>Lord of the Rings Online</strong></td>
</tr>
<tr>
<td><strong>MSN Messenger</strong></td>
</tr>
<tr>
<td><strong>Medal of Honor Allied Assault</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Midtown Madness, v 1.0</td>
</tr>
<tr>
<td>Motocross Madness 2, v 2.0</td>
</tr>
<tr>
<td>Need for Speed 3, Hot Pursuit</td>
</tr>
<tr>
<td>Operation FlashPoint</td>
</tr>
<tr>
<td>PPTP</td>
</tr>
<tr>
<td>Quake 3</td>
</tr>
<tr>
<td>RealAudio</td>
</tr>
<tr>
<td>Rogue Spear</td>
</tr>
<tr>
<td>SSH server</td>
</tr>
<tr>
<td>Soldier of Fortune</td>
</tr>
<tr>
<td>Starfleet Command</td>
</tr>
<tr>
<td>Telnet</td>
</tr>
<tr>
<td>Total Annihilation</td>
</tr>
<tr>
<td>Urban Assault, v 1.0</td>
</tr>
<tr>
<td>Warrock</td>
</tr>
<tr>
<td>Wolfenstein Enemy Territory</td>
</tr>
<tr>
<td>XBox 360 Media Center</td>
</tr>
<tr>
<td>Yahoo Messenger Phone</td>
</tr>
<tr>
<td>eMule</td>
</tr>
<tr>
<td>mlIRC Auth-IdentD</td>
</tr>
<tr>
<td>pcAnywhere (incoming)</td>
</tr>
</tbody>
</table>
Link: IP Passthrough

When you click the IP Passthrough link, the IP Passthrough page appears.

The IP Passthrough feature allows a single PC on the LAN to have the Motorola 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 PC’s MAC address. This dynamic subnet configuration is based on the local and remote WAN address and subnet mask.

- The two **DHCP** modes assign the WAN IP information needed to the client automatically.
  - You can select the MAC address of the PC you want to be the IP Passthrough client with **fixed** mode, or,
  - with “first-come-first-served” – **dynamic** – the first client to renew its address will be assigned the WAN IP.
- **Manual** mode is like statically configuring your PC. With Manual mode, you configure the **TCP/IP Properties** of the LAN client PC you want to be the IP Passthrough client. You then manually enter the WAN IP address, Gateway Address, etc. that matches the WAN IP address information of your Motorola Gateway. This mode works the same as the DHCP modes. Unsolicited WAN traffic will get passed to this client. The client is still able to access the Motorola Gateway and other LAN clients on the 192.168.1.x network, etc.
- **The Passthrough DHCP Lease** – By default, 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. You may alter this setting.
- Click **Save**. Changes take effect immediately.

**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 Router and from the passthrough host. Both tunnels go to the same remote endpoint, such as the VPN access concentrator at your employer’s office. In this case, the first one to start the IPSec traffic will be allowed; the second one – since, from the WAN, it’s indistinguishable – will fail.
NAT 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, specified by your entry in the Internal Address field.

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

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

◆ Click Save. Changes take effect immediately.
Link: Firewall Advanced

When you click the Firewall Advanced link the Firewall Advanced screen appears.

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.

DoS Protection – Denial-of-Service attacks are common on the Internet, and can render an individual PC or a whole network practically unusable by consuming all its resources. Your Gateway includes default settings to block the most common types of DoS attacks. For special requirements or circumstances, a variety of additional blocking characteristics is offered. See the following table.

<table>
<thead>
<tr>
<th>Menu item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop packets with invalid source or destination IP address</td>
<td>Whether packets with invalid source or destination IP address(es) are to be dropped</td>
</tr>
<tr>
<td>Protect against port scan</td>
<td>Whether to detect and drop port scans.</td>
</tr>
<tr>
<td>Drop packets with unknown ether types</td>
<td>Whether packets with unknown ether types are to be dropped</td>
</tr>
<tr>
<td>Drop packets with invalid TCP flags</td>
<td>Whether packets with invalid TCP flag settings (NULL, FIN, Xmas, etc.) should be dropped</td>
</tr>
<tr>
<td>Drop incoming ICMP Echo requests</td>
<td>Whether all ICMP echo requests are to be dropped; On or Off.</td>
</tr>
<tr>
<td>Menu item</td>
<td>Function</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Flood Limit</td>
<td>Whether packet flooding should be detected and offending packets be dropped; On or Off.</td>
</tr>
<tr>
<td>Flood rate limit</td>
<td>Specifies the number limit of packets per second before dropping the remainder.</td>
</tr>
<tr>
<td>Flood burst limit</td>
<td>Specifies the number limit of packets in a single burst before dropping the remainder.</td>
</tr>
<tr>
<td>Flood limit ICMP enable</td>
<td>Whether ICMP traffic packet flooding should be detected and offending packets be dropped; On or Off.</td>
</tr>
<tr>
<td>Flood limit UDP enable</td>
<td>Whether UDP traffic packet flooding should be detected and offending packets be dropped; On or Off.</td>
</tr>
<tr>
<td>Flood limit UDP Pass multicast</td>
<td>Allows exclusion of UDP multicast traffic. On by default.</td>
</tr>
<tr>
<td>Flood limit TCP enable</td>
<td>Allows exclusion of TCP traffic. Off by default.</td>
</tr>
<tr>
<td>Flood limit TCP SYN-cookie</td>
<td>Allows TCP SYN cookies flooding to be excluded. (Additional)</td>
</tr>
<tr>
<td>Neighbor Discovery Attack protec-</td>
<td>Prevents downstream traffic from an upstream device that sends excessive traffic but receives no replies; On or Off.</td>
</tr>
<tr>
<td>tion</td>
<td>Reflexive ACL</td>
</tr>
<tr>
<td></td>
<td>When IPv6 is enabled, Reflexive Access Control Lists can deny inbound IPv6 traffic unless this traffic results from returning outgoing packets (except as configured through firewall rules).</td>
</tr>
</tbody>
</table>

If you make any changes here, click the Save button.
Diagnostics

When you click the Diagnostics tab, the Troubleshoot page appears.

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

You can run all the tests in order by clicking the Run Full Diagnostics button.

The device will automatically test a number of components to determine any problems. You can see detailed results of the tests by clicking the Details buttons for each item.
Here is an example of the Ethernet Details screen.

Test Internet Access

These tests send a PING from the modem to either the LAN or WAN to verify connectivity. A PING could be either an IP address (163.176.4.32) or Domain Name (www.motorola.com). You enter a web address URL or an IP address in the respective field.

Click the Ping, Trace, NSLookup, or Detect Missing Filter button.

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

- **Ping** - tests the “reachability” of a particular network destination by sending an ICMP echo request and waiting for a reply.
- **Traceroute** - displays the path to a destination by showing the number of hops and the router addresses of these hops.
- **NSLookup** - converts a domain name to its IP address and vice versa.
- **Detect Missing Filter** - if you click the Detect Missing Filter button, a warning message appears at the top since the detection takes up to 2 minutes. When completed the Progress area might look like following.

To use the Ping capability, type a destination address (domain name or IP address) in the text box and click the Ping, Trace, or Lookup button. The results are displayed in the Progress Window.

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

Each test generates one of the following result codes:

<table>
<thead>
<tr>
<th>Result</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>* PASS:</td>
<td>The test was successful.</td>
</tr>
<tr>
<td>* FAIL:</td>
<td>The test was unsuccessful.</td>
</tr>
</tbody>
</table>
Below are some specific tests:

<table>
<thead>
<tr>
<th>Result</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>* SKIPPED:</td>
<td>The test was skipped because a test on which it depended failed.</td>
</tr>
<tr>
<td>* PENDING:</td>
<td>The test timed out without producing a result. Try running the test again.</td>
</tr>
<tr>
<td>* WARNING:</td>
<td>The test was unsuccessful. The Service Provider equipment your Modem connects to may not support this test.</td>
</tr>
</tbody>
</table>

Below are some specific tests:

### Action

#### From the Check Connection page:
- Ping the internet default gateway IP address
  - DSL is down, DSL settings are incorrect; Gateway's IP address or subnet mask are wrong; gateway router is down.
- Ping an internet site by IP address
  - Site is down.
- Ping an internet site by name
  - Servers are down; site is down.

#### From a LAN PC:
- Ping the Modem's LAN IP address
  - IP address and subnet mask of PC are not on the same scheme as the Modem; cabling or other connectivity issue.
- Ping an internet site by IP address
  - PC's subnet mask may be incorrect, site is down.
- Ping an internet site by name
  - DNS is not properly configured on the PC, site is down.
When you click **Logs**, the Logs page appears.

The current status of the device is displayed for all logs: **System**, **Firewall**, or **VoIP**. Choose the log you want to display from the pull-down menu.

- You can clear all log entries by clicking the **Clear Log** button.
- You can save logs to a text (.TXT) file by clicking the **Save to File** button. This will download the file to your browser’s default download location on your hard drive. The file can be opened with your favorite text editor.

---

**Note:**

Some browsers, such as Internet Explorer for Windows XP, require that you specify the Motorola device’s URL as a “Trusted site” in “Internet Options: Security”. This is necessary to allow the “download” of the log text file to the PC.
The following is an example log portion saved as a .TXT file:

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Proto</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2012-05-06T12:04:58-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>2</td>
<td>P0000-00-000000-000000</td>
<td>192.168.1.105</td>
<td>192.168.1.254</td>
<td>TCP</td>
<td>Downstream direction</td>
</tr>
<tr>
<td>3</td>
<td>P0000-00-000000-000000</td>
<td>192.168.1.105</td>
<td>192.168.1.254</td>
<td>TCP</td>
<td>Downstream direction</td>
</tr>
<tr>
<td>4</td>
<td>P0000-00-000000-000000</td>
<td>192.168.1.105</td>
<td>192.168.1.254</td>
<td>TCP</td>
<td>Downstream direction</td>
</tr>
<tr>
<td>5</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>192.168.1.43</td>
<td>192.168.1.254</td>
<td>TCP</td>
<td>Downstream direction</td>
</tr>
<tr>
<td>6</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>7</td>
<td>2012-03-05T12:24:07-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>8</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>9</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>10</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>11</td>
<td>P0000-00-000000-000000</td>
<td>192.168.1.255</td>
<td>192.168.1.255</td>
<td>UDP</td>
<td>Generic Discards</td>
</tr>
<tr>
<td>12</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>13</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>14</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>15</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>16</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>17</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>18</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>19</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>20</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>21</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>22</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>23</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>24</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>25</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>26</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>27</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>28</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>29</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>30</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>31</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>32</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>33</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>34</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>35</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
<tr>
<td>36</td>
<td>2012-05-06T12:33:00-05:00</td>
<td>10.8.50.176</td>
<td>10.8.205.145</td>
<td>ICMP</td>
<td>Echo Request</td>
</tr>
</tbody>
</table>

The last message was repeated 14 times.

The last message was repeated 13 times.

The last message was repeated 12 times.

The last message was repeated 13 times.

The last message was repeated 14 times.

The last message was repeated 13 times.
Link: Update

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

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

To update your software from a file on your PC, you must first download the software from your Service Provider's Support Site to your PC's hard drive.

- **Browse** your computer for the operating system file you downloaded and select the file.
- **Click the Update button.**
  - The LEDs will operate normally as described in "**Status Indicator Lights**" on page 90.
  - The installation may take a few minutes and the web page will indicate a 3-part countdown before returning you to the Home page; wait for it to complete. During the software installation, you will lose Internet and phone service. The LEDs will function as follows:
    - During this phase, the **Power LED** will flash **Orange/Amber** during firmware upgrade (flash writing to memory) and all other LEDs will be off.
  - The Gateway will restart automatically.
    - As the device reboots, the POWER ON LED behavior will happen.
  - Your new operating system will then be running.
Link: Resets

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

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

It might also be useful to reset your connection to the Internet without deleting all of your configuration settings.

◆ Click the **Reset IP** to refresh your Internet WAN IP address. LAN-side users will be briefly disconnected from the Internet, but will otherwise be unaffected.

◆ Click the **Reset Connection** button to disconnect and reconnect all of your connections, including your VoIP phones.

◆ Click the **Reset Device** button to reset the Gateway back to its original factory default settings.

◆ Click the **Restart** button to reboot the device. Previous configuration settings are still retained.

**Resets**

Resetting IP will refresh the broadband IP address.

[Reset IP]

Resetting your connection will re-establish your broadband connection.

[Reset Connection]

Restarting your device will disconnect all users and restart all device subsystems, retaining existing configuration settings.

[Restart]

**WARNING:** Resetting your device to factory default settings will permanently delete all configuration changes since the system was installed.

[Reset Device...]

**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.
When you click **Event Notifications**, the **Event Notifications** page appears.

![Event Notifications](image)

- If you check the **Broadband Status Notification** checkbox, the device will alert users on your network if the connection to the Internet should fail. In that event, troubleshooting suggestions will display.
- If you check the **Missing Filter Notification** checkbox, the device will alert users on your network if hardware line filters are either missing or improperly installed. In that event, troubleshooting suggestions will display.
Link: NAT Table

When you click the **NAT Table** link, the **NAT Table** page appears.

The **NAT Table** page displays the network address translation sessions in use by the Gateway. You can use the pull-down menu to limit the displayed sessions to selected IP addresses.

To refresh all the sessions displayed, click the **Reset** button.
CHAPTER 3  Basic Troubleshooting

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

Before troubleshooting, make sure you have

◆ read the User Manual;
◆ plugged in all the necessary cables; and
◆ set your PC’s TCP/IP controls to obtain an IP address automatically.
Status Indicator Lights

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

Motorola® Gateway NVG589 status indicator lights

<table>
<thead>
<tr>
<th>LED</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>Solid Green = The device is powered.</td>
</tr>
<tr>
<td></td>
<td>Flashing Green = A Power-On Self-Test (POST) is in progress</td>
</tr>
<tr>
<td></td>
<td>Flashing Red = A POST failure (not bootable) or device malfunction occurred.</td>
</tr>
<tr>
<td></td>
<td>Orange/Amber = during firmware upgrade (see below)</td>
</tr>
<tr>
<td></td>
<td>Off = The unit has no AC power.</td>
</tr>
<tr>
<td><em>During Firmware Upgrade</em></td>
<td>During the software installation, you will lose internet and phone service. The LEDs will function as follows:</td>
</tr>
<tr>
<td></td>
<td>1. As firmware is being loaded into flash, the LEDs will operate normally as described.</td>
</tr>
<tr>
<td></td>
<td>2. The installation will take a few minutes –</td>
</tr>
<tr>
<td></td>
<td>During this phase, the Power LED will flash Orange/Amber during firmware upgrade (flash writing to memory) and all other LEDs will be off.</td>
</tr>
<tr>
<td></td>
<td>3. The Gateway will restart automatically.</td>
</tr>
<tr>
<td></td>
<td>As the device reboots, the POWER ON LED behavior will happen.</td>
</tr>
<tr>
<td><strong>Battery</strong></td>
<td>Solid Green = Battery in place but not being used.</td>
</tr>
<tr>
<td></td>
<td>Flashing Green = Battery charging.</td>
</tr>
<tr>
<td></td>
<td>Solid Red = Battery backup mechanism has a fault.</td>
</tr>
<tr>
<td></td>
<td>Flashing Red = Battery needs to be replaced.</td>
</tr>
<tr>
<td></td>
<td>Solid Amber = Battery in use.</td>
</tr>
<tr>
<td></td>
<td>Flashing Amber = Low battery.</td>
</tr>
<tr>
<td></td>
<td>Off = No battery or battery has no charge.</td>
</tr>
<tr>
<td></td>
<td>Cycle between all colors = Battery conducting self-test.</td>
</tr>
<tr>
<td>LED</td>
<td>Action</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Operation:</strong></td>
<td><strong>Power Action</strong></td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
<td><strong>Solid Green</strong> = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).&lt;br&gt;<strong>Flickering Green</strong> = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.&lt;br&gt;<strong>Off</strong> = The device is not powered, no cable or no powered devices connected to the associated ports.</td>
</tr>
<tr>
<td><strong>Wireless</strong></td>
<td><strong>Solid Green</strong> = Wi-Fi is powered.&lt;br&gt;<strong>Flickering Green</strong> = Activity seen from devices connected via Wi-Fi. The flickering of the light is synchronized to actual data traffic.&lt;br&gt;<strong>Off</strong> = The device is not powered or no powered devices connected to the associated ports.</td>
</tr>
<tr>
<td><strong>HomePNA</strong></td>
<td><strong>Solid Green</strong> = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).&lt;br&gt;<strong>Flickering Green</strong> = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.&lt;br&gt;<strong>Off</strong> = The device is not powered, no cable or no powered devices connected to the associated ports.</td>
</tr>
<tr>
<td><strong>Broadband 1</strong>, <strong>2</strong></td>
<td><strong>Solid Green</strong> = Good broadband connection (i.e., good DSL Sync or Gigabit Ethernet ).&lt;br&gt;<strong>Flashing Green</strong> = Attempting broadband connection (i.e., DSL attempting sync).&lt;br&gt;<strong>Flashing Green &amp; Red</strong> = If the broadband connection fails to be established for more than three consecutive minutes the LED switches to <strong>Flashing Green</strong> when attempting or waiting to establish a broadband connection alternating with a five second steady <strong>Red</strong>. This pattern continues until the broadband connection is successfully established.&lt;br&gt;<strong>Flashing Red</strong> = No DSL signal on the line. This is only used when there is no signal, not during times of temporary ‘no tone’ during the training sequence.&lt;br&gt;<strong>Off</strong> = The device is not powered.&lt;br&gt;<strong>Broadband 1 LED</strong> is also the Gigabit ethernet WAN LED when that is in play (and DSL is not).</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td><strong>Solid Green</strong> = IP connected (The device has a WAN IP address from DHCP or 802.1x authentication and the broadband connection is up).&lt;br&gt;<strong>Flashing Green</strong> = Attempting PPP connection. Attempting IEEE 802.1X authentication or attempting to obtain DHCP information.&lt;br&gt;<strong>Red</strong> = Device attempted to become IP connected and failed (no DHCP response, 802.1x authentication failed, no IP address from IPCP, etc.). The Red state times out after two minutes and the Service indicator light returns to the Off state.&lt;br&gt;<strong>Off</strong> = The device is not powered or the broadband connection is not present.</td>
</tr>
<tr>
<td><strong>Phone 1, 2</strong></td>
<td><strong>Solid Green</strong> = The associated VoIP line has been registered with a SIP proxy server.&lt;br&gt;<strong>Flashing Green</strong> = Indicates a telephone is off-hook on the associated VoIP line.&lt;br&gt;<strong>Off</strong> = VoIP not in use, line not registered or Gateway power off.</td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td><strong>Solid Green</strong> = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).&lt;br&gt;<strong>Flickering Green</strong> = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.&lt;br&gt;<strong>Off</strong> = The device is not powered, no cable or no powered devices connected to the associated ports.</td>
</tr>
</tbody>
</table>
NOTE:

The NVG589 supports two VoIP lines over one RJ11 VoIP port. In order to connect two phone lines the supplied **inner/outer pair splitter adapters** must be attached to the RJ11 VoIP port in order to terminate both lines. This is a special-purpose splitter. You must only use the **inner/outer pair splitter adapters** supplied by AT&T.
# LED Function Summary Matrix

<table>
<thead>
<tr>
<th>Function</th>
<th>Solid Green</th>
<th>Flashing Green</th>
<th>Flashing Red</th>
<th>Off</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>The device is powered.</td>
<td>A Power-On Self-Test (POST) is in progress</td>
<td>A POST failure (not bootable) or device malfunction occurred.</td>
<td>The unit has no AC power.</td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
<td>Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).</td>
<td>Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.</td>
<td>The device is not powered, no cable or no powered devices connected to the associated ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Wireless</strong></td>
<td>Wi-Fi is powered.</td>
<td>Activity seen from devices connected via Wi-Fi. The flickering of the light is synchronized to actual data traffic.</td>
<td>The device is not powered or no powered devices connected to the associated ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Phone 1, 2</strong></td>
<td>The associated VoIP line has been registered with a SIP proxy server.</td>
<td>Indicates a telephone is off-hook on the associated VoIP line.</td>
<td>VoIP not in use, line not registered or Gateway power off.</td>
<td></td>
</tr>
<tr>
<td><strong>WPS</strong></td>
<td>Indicates when WPS is broadcasting.</td>
<td></td>
<td>not in use, not broadcasting.</td>
<td></td>
</tr>
<tr>
<td>Broadband</td>
<td>Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solid Green = Good broadband connection (i.e., good DSL Sync).</td>
<td>Solid Green = IP connected (The device has a WAN IP address from DHCP or 802.1x authentication and the broadband connection is up).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flashing Green = Attempting broadband connection (i.e., DSL attempting sync).</td>
<td>Flashing Green = Attempting PPP connection. Attempting IEEE 802.1X authentication or attempting to obtain DHCP information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flashing Green &amp; Red = If the broadband connection fails to be established for more than three consecutive minutes the LED switches to Flashing Green when attempting or waiting to establish a broadband connection alternating with a five second steady Red. This pattern continues until the broadband connection is successfully established.</td>
<td>Red = Device attempted to become IP connected and failed (no DHCP response, 802.1x authentication failed, no IP address from IPCP, etc.). The Red state times out after two minutes and the Service indicator light returns to the Off state.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flashing Red = No DSL signal on the line. This is only used when there is no signal, not during times of temporary 'no tone' during the training sequence.</td>
<td>Off = The device is not powered.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Off = The device is not powered.</td>
<td>Off = The device is not powered or the broadband connection is not present.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If a status indicator light does not look correct, look for these possible problems:

<table>
<thead>
<tr>
<th>If LED is not Lit</th>
<th>Possible problems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the power adapter is plugged into the DSL Modem properly.</td>
<td></td>
</tr>
<tr>
<td>◆ Try a known good wall outlet.</td>
<td></td>
</tr>
<tr>
<td>◆ If a power strip is used, make sure it is switched on.</td>
<td></td>
</tr>
<tr>
<td><strong>Broadband</strong></td>
<td></td>
</tr>
<tr>
<td>◆ Make sure that any telephone has a microfilter installed.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure that you are using the correct cable. The DSL cable is the thinner standard telephone cable and labeled “Data Cable.”</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the DSL cable is plugged into the correct wall jack.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the DSL cable is plugged into the DSL port on the DSL Modem.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the DSL line has been activated at the central office DSLAM.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the DSL Modem is not plugged into a micro filter.</td>
<td></td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the you are using the yellow Ethernet cable, not the DSL cable. The Ethernet cable is thicker than the standard telephone cable.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the Ethernet cable is securely plugged into the Ethernet jack on the PC.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the Ethernet cable is securely plugged into the Ethernet port on the DSL Modem.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure you have Ethernet drivers installed on the PC.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the PC’s TCP/IP Properties for the Ethernet Network Control Panel is set to obtain an IP address via DHCP.</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the PC has obtained an address in the 192.168.1.x range. (You may have changed the subnet addressing.)</td>
<td></td>
</tr>
<tr>
<td>◆ Make sure the PC is configured to access the Internet over a LAN.</td>
<td></td>
</tr>
<tr>
<td>◆ Disable any installed network devices (Ethernet, HomePNA, wireless) that are not being used to connect to the DSL Modem.</td>
<td></td>
</tr>
</tbody>
</table>
Factory Reset Switch

Lose your Access Code? This section shows how to reset the Motorola® Gateway so that you can access the configuration screens once again.

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

If you don’t have an Access Code, the only way to access the Motorola® Gateway is the following:

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

![Factory Reset Switch](image)

   Factory Reset Switch: Push to clear all settings

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

   - If you press the factory reset button for **less than ten (10) seconds**, the device will be rebooted.
     The indicator lights on the device will respond immediately and start blinking red within one (1) second of the reset button being pressed.
     This will occur independent of the fact that the button is still being pressed or has been released. The indicator lights will flash for a minimum of five seconds, even if the reset button is released prior to five seconds after it has been depressed. If the reset button is held for more than 5 seconds, then it will continue to flash until released or until 10 seconds (see below).

   - If you press the factory reset button for a **longer period of time**, the device will be reset to the factory default shipped settings.
     If the button is held for ten seconds, the Power indicator continues to flash, for an additional 5 seconds and then the indicator lights will return to their normal operating mode, independent of whether or not the reset button is still depressed.
## 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.

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.
Access-related Log Messages

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.

13. dropped - reassembly time-out: 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.

Firewall Log Messages Detail (AT&T requirement #841)

<table>
<thead>
<tr>
<th>Reason Enumeration (C)</th>
<th>Log Text Representation</th>
<th>Why the packet was logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM_LOGDROP_CAT_DIR</td>
<td>DIRECTION</td>
<td>Direction (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_DIR_UP</td>
<td>DIRECTION-UP</td>
<td>Upstream direction</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_DIR_DOWN</td>
<td>DIRECTION-DOWN</td>
<td>Downstream direction</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ETH</td>
<td>ETH</td>
<td>Ethernet Header (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ETH_SRC_ADDR</td>
<td>ETH-SRC</td>
<td>Ethernet Source MAC Address</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ETH_DST_ADDR</td>
<td>ETH-DST</td>
<td>Ethernet Destination MAC Address</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ETH_PROT</td>
<td>ETH-PROTOCOL</td>
<td>Ethernet Protocol</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ETH_VLAN</td>
<td>ETH-VLAN</td>
<td>Ethernet VLAN ID (where applicable)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_IP</td>
<td>IP</td>
<td>IP Header (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_IP_SRC</td>
<td>IP-SRC</td>
<td>IP Source Address</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_IP_DST</td>
<td>IP-DST</td>
<td>IP Destination Address</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_IP_PROT</td>
<td>IP-PROTOCOL</td>
<td>IP Protocol</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_IP_SPOOF</td>
<td>IP-SPOOF</td>
<td>IP Address is spoofed (could not have been sent by a device legitimately with the address in the source address field)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_IP_IILL</td>
<td>IP-ILLEGAL</td>
<td>IP Address is illegal (either src or dest)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_TCP</td>
<td>TCP</td>
<td>TCP Header (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_TCP_SRC_PORT</td>
<td>TCP-SRC-PORT</td>
<td>TCP Source Port</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_TCP_DST_PORT</td>
<td>TCP-DST-PORT</td>
<td>TCP Destination Port</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_TCP_FLAGS</td>
<td>TCP-FLAGS</td>
<td>TCP Flags field</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_UDP</td>
<td>UDP</td>
<td>UDP Header (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_UDP_SRC_PORT</td>
<td>UDP-SRC-PORT</td>
<td>UDP Source Port</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_UDP_DST_PORT</td>
<td>UDP-DST-PORT</td>
<td>UDP Destination Port</td>
</tr>
</tbody>
</table>
### Firewall Log Messages Detail (AT&T requirement #841)

<table>
<thead>
<tr>
<th>Reason Enumeration (C)</th>
<th>Log Text Representation</th>
<th>Why the packet was logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM_LOGDROP_CAT_ICMP</td>
<td>ICMP</td>
<td>ICMP Packet (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ICMP_TYPE</td>
<td>ICMP-TYPE</td>
<td>ICMP Type Field</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ICMP_CODE</td>
<td>ICMP-CODE</td>
<td>ICMP Code Field</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_ICMP6</td>
<td>ICMPv6</td>
<td>ICMPv6 (generic)</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_POLICY</td>
<td>POLICY</td>
<td>Policy (generic). This currently includes filterset rules, restricted hosts, IPv6 Profiles.</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_POLICY_INPUT</td>
<td>POLICY-INPUT-GEN-DISCARD</td>
<td>Packets destined for the CPE that are generically discarded (we specify the packets we want; the rest are discarded.)</td>
</tr>
</tbody>
</table>
| NM_LOGDROP_CAT_POLICY_WAN_MGMT | POLICY-WAN-MGMT-ACCESS | 1) Trying to access CPE service from WAN side using LAN-side port  
2) Trying to access CPE service from LAN side using WAN-side IP address  
3) Trying to access CPE service from WAN side using IPv6 |
| NM_LOGDROP_CAT_POLICY_ICMP_ECHO | POLICY-ICMP-ECHO | ICMP Echo Request discarded (more specific than NM_LOGDROP_CAT_ICMP_TYPE) |
| NM_LOGDROP_CAT_POLICY_UWC_RESTRICT | POLICY-UWC-RESTRICT | Packets dropped because of "Universal Wi-Fi Configuration" restrictions (currently unused) |
| NM_LOGDROP_CAT_POLICY_RESTRICTED_HOST | POLICY-RESTRICTED-HOST | Packets dropped because of "Restricted Host" feature (either content or time restrictions) (currently unused) |
| NM_LOGDROP_CAT_POLICY_WAN_DNS_QUERY | POLICY-WAN-SIDE-DNS_QUERY | DNS query packets received on a WAN interface |
| NM_LOGDROP_CAT_POLICY_WAN_DHCP_TOSRVR | POLICY-WAN-SIDE-DHCP-TO-SRVR | DHCP DISCOVER/REQUEST received on a WAN interface |
| NM_LOGDROP_CAT_POLICY_AH | POLICY-IPV6-AH | IPv6 Packets with AH header (if so configured) |
| NM_LOGDROP_CAT_POLICY_ESP | POLICY-IPV6-ESP | IPv6 Packets with ESP header (if so configured) |
| NM_LOGDROP_CAT_POLICY_DEP_HEADER | POLICY-DEPRECATED-HEADER | IPv6 Packets with deprecated header (currently this only includes routing extension header type 0) |
| NM_LOGDROP_CAT_POLICY_CAPT_PORTAL | POLICY-CAPTIVE-PORTAL | [IPv6] Packets dropped because captive portal is enabled. |
| NM_LOGDROP_CAT_FLOW | FLOW | Packets rejected as a result of analysis of multiple related packets (generic) |
## Firewall Log Messages Detail (AT&T requirement #841)

<table>
<thead>
<tr>
<th>Reason Enumeration (C)</th>
<th>Log Text Representation</th>
<th>Why the packet was logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM_LOGDROP_CAT_FLOW_FLOOD</td>
<td>FLOOD</td>
<td>Packets rejected because of flood-limiting</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_FLOW_PORTSCAN</td>
<td>PORTSCAN</td>
<td>Packets rejected because of Port-scan detection</td>
</tr>
<tr>
<td>NM_LOGDROP_CAT_FLOW_DOS_OTHER</td>
<td>OTHER-DoS</td>
<td>Packets rejected because of other DoS detection. Currently this includes downstream flows that don't generate upstream responses - specifically addressing IPv6 Neighbor Discovery DoS attacks.</td>
</tr>
</tbody>
</table>
CHAPTER 4  Command Line Interface

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

This chapter covers the following topics:
- “Overview” on page 105
- “Starting and Ending a CLI Session” on page 107
- “Using the CLI Help Facility” on page 107
- “About SHELL Commands” on page 108
- “SHELL Commands” on page 109
- “About CONFIG Commands” on page 118
- “CONFIG Commands” on page 121
- “Debug Commands” on page 171
CONFIG Commands

“Connection commands” on page 121
“Filterset commands” on page 124
“Queue commands” on page 128
“IP Gateway commands” on page 130
“IPv6 Commands” on page 130
“IP DNS commands” on page 138
“IP IGMP commands” on page 139
“NTP commands” on page 141
“Application Layer Gateway (ALG) commands” on page 142
“Dynamic DNS Commands” on page 142
“Link commands” on page 143
“Management commands” on page 146
“Remote access commands” on page 148
“Physical interfaces commands” on page 150
“PPPoE relay commands” on page 156
“NAT Pinhole commands” on page 157
“Security Stateful Packet Inspection (SPI) commands” on page 157
“VoIP commands” on page 159
“System commands” on page 167
Overview

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

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

<table>
<thead>
<tr>
<th>Command Verbs</th>
<th>Status and/or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Delete configuration list data</td>
</tr>
<tr>
<td>help</td>
<td>Help command option</td>
</tr>
<tr>
<td>save</td>
<td>Save configuration data</td>
</tr>
<tr>
<td>script</td>
<td>Print configuration data</td>
</tr>
<tr>
<td>set</td>
<td>Set configuration data</td>
</tr>
<tr>
<td>validate</td>
<td>Validate configuration settings</td>
</tr>
<tr>
<td>view</td>
<td>View configuration data</td>
</tr>
</tbody>
</table>

### Keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conn</td>
<td>Connection options</td>
</tr>
<tr>
<td>ip</td>
<td>TCP/IP protocol options</td>
</tr>
<tr>
<td>dns</td>
<td>Domain Name System options</td>
</tr>
<tr>
<td>igmp</td>
<td>IGMP configuration options</td>
</tr>
<tr>
<td>ntp</td>
<td>Network Time Protocol options</td>
</tr>
<tr>
<td>gateway</td>
<td>Gateway options</td>
</tr>
<tr>
<td>link</td>
<td>WAN link options</td>
</tr>
<tr>
<td>mgmt</td>
<td>System management options</td>
</tr>
<tr>
<td>phy</td>
<td>Physical interface options</td>
</tr>
<tr>
<td>dsl</td>
<td>DSL configuration options</td>
</tr>
<tr>
<td>enet</td>
<td>Ethernet options</td>
</tr>
<tr>
<td>pinhole</td>
<td>Pinhole options</td>
</tr>
<tr>
<td>system</td>
<td>Gateway’s system options</td>
</tr>
<tr>
<td>log</td>
<td>System activity logging options</td>
</tr>
</tbody>
</table>

### Command Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>Go to top level of configuration mode</td>
</tr>
<tr>
<td>quit</td>
<td>Exit from configuration mode; return to shell mode</td>
</tr>
<tr>
<td>exit</td>
<td>Exit from configuration mode; return to shell mode</td>
</tr>
</tbody>
</table>
Starting and Ending a CLI Session

Open a telnet connection from a workstation on your network.

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

```
telnet <ip_address>
```

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

Logging In

The command line interface log-in process emulates the log-in process for a UNIX host. To logon, enter the username and your password.

Entering the administrator password lets you display and update all Motorola Gateway settings.

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

Ending a CLI Session

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

Using the CLI Help Facility

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

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

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

◆ Monitor its performance
◆ Display and reset Gateway statistics
◆ Issue administrative commands to restart Motorola Gateway functions

SHELL Prompt

When you are in SHELL mode, the CLI prompt is the name of the Motorola Gateway followed by a right angle bracket (>). For example, if you open a CLI connection to the Motorola Gateway named "Motorola-3000/9437188," you would see Motorola-3000/9437188> as your CLI prompt.

SHELL Command Shortcuts

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

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

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

Common Commands

**arp nnn.nnn.nnn.nnn**

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

**clear [ yes ]**

Clears the configuration settings in a Motorola Gateway. You are prompted to confirm the clear command by entering **yes**.

**clear_certificate**

Removes an SSL certificate that has been installed.

**configure**

Puts the command line interface into Configure mode, which lets you configure your Motorola Gateway with Config commands. Config commands are described starting on page 121.

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

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

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

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

You can also download an SSL certificate file from a trusted Certification Authority (CA), on platforms that support SSL, as follows:

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

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

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

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

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

Adds the message in the `message_string` argument to the Motorola Gateway diagnostic log.

**loglevel [ level]**

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

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

Use the following values for the `level` argument:

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

**netstat -i**

Displays the IP interfaces for your Motorola Gateway.

**netstat -r**

Displays the IP routes stored in your Motorola Gateway.

**nslookup [ hostname | ip_address ]**

Performs a domain name system lookup for a specified host.

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

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

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

- The `hostname` argument is the name of the device you want to ping; for example, `ping ftp.motorola.com`.
- The `ip_address` argument is the IP address, in dotted decimal notation, of the device you want to locate. If a host using the specified name or IP address is active, it returns one or more ICMP Echo replies, confirming that it is accessible from your network.
- The `-s size` argument lets you specify the size of the ICMP packet.
- The `-c count` argument lets you specify the number of ICMP packets generated for the ping request. Values greater than 250 are truncated to 250.
You can use the **ping** command to determine whether a hostname or IP address is already in use on your network. You cannot use the **ping** command to ping the Motorola Gateway’s own IP address.

### quit

Exits the Motorola Gateway command line interface.

### reset arp

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

### reset crash

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

### reset dhcp server

Clears the DHCP lease table in the Motorola Gateway.

### reset enet [ all ]

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

### reset firewall-log

Rewinds the firewall log to the first entry.

### reset ipmap

Clears the IPMap table (NAT).

### reset log

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

### reset wan

This function resets WAN interface statistics.

### reset wepkeys

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

### restart [ seconds ]

Restarts your Motorola Gateway. If you include the optional **seconds** argument, your Motorola Gateway will restart when the specified number of seconds have elapsed. You must enter the complete **restart** command to initiate a restart.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show all-info</td>
<td>Displays all settings currently configured in the Motorola Gateway.</td>
</tr>
<tr>
<td>show bridge interfaces</td>
<td>Displays bridge interfaces maintained by the Motorola Gateway.</td>
</tr>
<tr>
<td>show bridge table</td>
<td>Displays the bridging table maintained by the Motorola Gateway.</td>
</tr>
<tr>
<td>show config</td>
<td>Dumps the Motorola Gateway’s configuration script just as the <code>script</code> command does in config mode.</td>
</tr>
<tr>
<td>show crash</td>
<td>Displays the most recent crash information, if any, for your Motorola Gateway.</td>
</tr>
<tr>
<td>show daylight-savings</td>
<td>Displays the auto-daylight savings time settings information.</td>
</tr>
<tr>
<td>show dhcp agent</td>
<td>Displays DHCP relay-agent leases.</td>
</tr>
<tr>
<td>show dhcp server leases</td>
<td>Displays the DHCP leases stored in RAM by your Motorola Gateway.</td>
</tr>
<tr>
<td>show dhcp client</td>
<td>Displays the DHCP clients stored in RAM by your Motorola Gateway.</td>
</tr>
<tr>
<td>show diffserv</td>
<td>Displays the Differentiated Services and QoS values configured in the Motorola Gateway.</td>
</tr>
<tr>
<td>show dsl [ all ]</td>
<td>Displays DSL port statistics, such as upstream and downstream connection rates and noise levels.</td>
</tr>
<tr>
<td>show dslf device-association</td>
<td>Displays LAN devices that conform with the TR111 Gateway requirement. It displays - IP Address, Manufacture OUI and Serial number.</td>
</tr>
<tr>
<td>show enet [ all ]</td>
<td>Displays Ethernet interface statistics maintained by the Motorola Gateway. Supports display of individual LAN switch port statistics as well as WAN Ethernet statistics (where applicable).</td>
</tr>
</tbody>
</table>
Example:

Ethernet driver full statistics - 10/100 Ethernet

Port Status: Link up
Type: 100BASET Duplex: Full

General:
- Transmit OK: 434
- Receive OK: 267
- Tx Errors: 0
- Rx Errors: 0

Receiver:
- Incompl Packet Errors: 0
- No RBD’s For Packet: 0
- Carrier Sense Lost: 0
- Deferred Replen: 0

Transmitter:
- TX Retries: 0
- Single Collisions: 0
- No Buf For Packet: 0

Upper Layers:
- Rx No Handler: 0
- Rx No Message: 0
- Rx Octets: 30773
- Rx Unicast Pkts: 267
- Rx multicast Pkts: 0
- Tx Discards: 0
- Tx Octets: 31692

10/100 Ethernet phy.enet.port

Port Status: Link up
Duplex: Full-duplex active
Speed: 100BASE-T
- Transmit OK: 434
- Transmit unicastpkts: NA
- Receive OK: 267
- Receive unicastpkts: 267

**show group-mgmt**

Displays the IGMP Snooping Table. See "IP IGMP commands" on page 139 for detailed explanation.

**show ip arp**

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

**show ip igmp**

Displays the contents of the IGMP Group Address table and the IGMP Report table maintained by your Motorola Gateway.
**show ip interfaces**
Displays the IP interfaces for your Motorola Gateway.

**show ip firewall**
Displays firewall statistics.

**show ip lan-discovery**
Displays the LAN Host Discovery Table of hosts on the wired or wireless LAN, and whether or not they are currently online.

**show ip routes**
Displays the IP routes stored in your Motorola Gateway.

**show ipmap**
Displays IPMap table (NAT).

**6rd-check 6rd_ip_v6_conn_name**
Sends out 6rd loopback packets to the 6rd BG. Verifies 6rd connectivity to the 6rd BG.

**show ipv6 interfaces**
Display IPv6 interfaces.

**show ipv6 routes**
Display IPv6 route table.

**show ipv6 neighbors**
Display IPv6 neighbor table.

**show ipv6 dhcp server leases**
Display DHCPv6 server lease table.

**show ipv6 statistics**
Display IPv6 statistics information.

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

**show firewall-log**
Displays blocks of information from the Motorola Gateway firewall log.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show memory [ all ]</td>
<td>Displays memory usage information for your Motorola Gateway. If you include the optional <strong>all</strong> argument, your Motorola Gateway will display a more detailed set of memory statistics.</td>
</tr>
<tr>
<td>show ptm</td>
<td>Displays statistics information for each PTM session.</td>
</tr>
<tr>
<td>show post-results</td>
<td>Displays POST results.</td>
</tr>
<tr>
<td>show pppoe</td>
<td>Displays status information for each PPPoE socket, such as the socket state, service names, and host ID values.</td>
</tr>
<tr>
<td>show rootcert [ all</td>
<td>supplicant</td>
</tr>
<tr>
<td>show rtsp</td>
<td>Displays RTSP ALG session activity data.</td>
</tr>
<tr>
<td>show status</td>
<td>Displays the current status of a Motorola Gateway, the device’s hardware and software revision levels, a summary of errors encountered, and the length of time the Motorola Gateway has been running since it was last restarted. Identical to the <strong>status</strong> command.</td>
</tr>
<tr>
<td>show summary</td>
<td>Displays a summary of WAN, LAN, and Gateway information.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays detail of VLAN status and statistics.</td>
</tr>
<tr>
<td>show wireless [ all ]</td>
<td>Shows wireless status and statistics.</td>
</tr>
<tr>
<td>show wireless clients [ MAC_address ]</td>
<td>Displays details on connected clients, or more details on a particular client if the MAC address is added as an argument.</td>
</tr>
</tbody>
</table>
show voip
Displays VoIP call statistics.

show voiplog
Displays VoIP event logs.

telnet [ hostname | ip_address ] [ port ]
Lets you open a telnet connection to the specified host through your Motorola Gateway.
◆ The hostname argument is the name of the device to which you want to connect; for example, telnet ftp.Motorola.com.
◆ The ip_address argument is the IP address, in dotted decimal notation, of the device to which you want to connect.
◆ The port argument is the number of the port over which you want to open a telnet session.

traceroute ( ip_address | hostname )
Traces the routing path to an IP destination.

upload [ server_address ][ filename ] [ confirm ]
Copies the current configuration settings of the Gateway to a TFTP (Trivial File Transfer Protocol) server. The TFTP server must be accessible on your Ethernet network. The server_address argument identifies the IP address of the TFTP server on which you want to store the Motorola Gateway settings. The filename argument identifies the path and name of the configuration file on the TFTP server. If you include the optional confirm keyword, you will not be prompted to confirm whether or not you want to perform the operation.

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

who
Displays the names of the current shell and PPP users.

WAN Commands
atmping vccn [ segment | end-to-end ]
Lets you check the ATM connection reachability and network connectivity. This command sends five Operations, Administration, and Maintenance (OAM) loopback calls to the specified vpi/vci destination. There is a five second total timeout interval.
Use the segment argument to ping a neighbor switch.
Use the end-to-end argument to ping a remote end node.

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

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

**reset dsl**

Resets any open DSL connection.

**reset ppp vccn**

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

**show atm [all]**

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

**show ppp {{ stats | lcp | ipcp }}**

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

**start ppp vccn**

Opens a PPP link on the specified virtual circuit.
About CONFIG Commands

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

CONFIG Mode Prompt

When you are in CONFIG mode, the CLI prompt consists of the name of the Motorola Gateway followed by your current `node` in the hierarchy and two right angle brackets (>>). For example, when you enter CONFIG mode (by typing `config` at the SHELL prompt), the `Motorola-3000/9437188 (top))>>` prompt reminds you that you are at the top of the CONFIG hierarchy. If you move to the `ip` node in the CONFIG hierarchy (by typing `ip` at the CONFIG prompt), the prompt changes to `Motorola-3000/9437188 (ip)>>` to identify your current location.

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

Navigating the CONFIG Hierarchy

- **Moving from CONFIG to SHELL** — You can navigate from anywhere in the CONFIG hierarchy back to the SHELL level by entering `quit` at the CONFIG prompt and pressing Return.
  
  `Motorola-3000/9437188 (top))>> quit`
  
  `Motorola-3000/9437188 >`

- **Moving from top to a subnode** — You can navigate from the top node to a subnode by entering the node name (or the significant letters of the node name) at the CONFIG prompt and pressing RETURN. For example, you move to the IP subnode by entering `ip` and pressing RETURN.
  
  `Motorola-3000/9437188 (top))>> ip`
  
  `Motorola-3000/9437188 (ip)>>`

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

- **Jumping down several nodes at once** — You can jump down several levels in the CONFIG hierarchy by entering the complete path to a node.

- **Moving up one node** — You can move up through the CONFIG hierarchy one node at a time by entering the `up` command.

- **Jumping to the top node** — You can jump to the top level from anywhere in the CONFIG hierarchy by entering the `top` command.

- **Moving from one subnode to another** — You can move from one subnode to another by entering a partial path that identifies how far back to climb.

- **Moving from any subnode to any other subnode** — You can move from any subnode to any other subnode by entering a partial path that starts with a top-level CONFIG command.

- **Scrolling backward and forward through recent commands** — You can use the Up and Down arrow keys to scroll backward and forward through recent commands you have entered. When the command you want appears, press Enter to execute it.

Entering Commands in CONFIG Mode

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

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

For example:

set ip ethernet A 192.31.222.57

Guidelines: CONFIG Commands

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

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

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

Displaying Current Gateway Settings

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

Step Mode: A CLI Configuration Technique

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

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

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

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

```
Motorola-3000/9437188 (top)>> set system
...
  system
  name ("Motorola-3000/9437188"): Mycroft
  Diagnostic Level (High): medium
Stepping mode ended.
```

**Validating Your Configuration**

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

```
Motorola-3000/9437188 (top)>> validate
  Error: Subnet mask is incorrect
  Global Validation did not pass inspection!
```

You can use the `validate` command to verify your configuration settings at any time. Your Motorola Gateway automatically validates your configuration any time you save a modified configuration.
### CONFIG Commands

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

#### Connection commands

**conn**s are used to create connections, for example, a WAN or LAN **conn**. There may be more than one of each depending on your model. **names** correspond to the system object IDs (OIDs) but you can name them yourself.

**set conn name name link-oid value**

Sets the connection named **name** to point to an associated link specified by the **link-oid** value.

**set conn name name type [ static | dhcpc | ppp ]**

Specifies whether the **type** of the connection named **name** is static, dhcpc, or ppp.

**set conn name name side [ lan | wan ]**

Specifies whether this **conn** is LAN- or WAN-side. A **conn** can be either **lan** or **wan**.

**set conn name name lan-type [ private | public | public-delegated ]**

Specifies whether this **conn**’s LAN is private, public, or public-delegated. The default is **private**, the usual type of local network.

**set conn name name dhcp-server-enable [ on | off ]**

Turns the DHCP server for this connection **on** or **off**. The DHCP server can be enabled per connection. The default is **on**.

**set conn name name mcast-forwarding [ off | on ]**

Turns IP IGMP multicast forwarding for this connection **off** or **on**. The default is **off**.

**set conn name name rip-send [ off | v1 | v2 | v1-compat | v2-md5 ]**

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

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

**set conn name name rip-receive [ off | v1 | v2 | v1-compat | v2-md5 ]**

Specifies whether the device should use Routing Information Protocol (RIP) broadcasts to update its routing tables with information received from other Gateways on the other side of the connection. If you specify **v2-md5**, you must also specify a rip-receive-key. Keys are ASCII strings with a maximum of 31 characters, and must match the other Gateway(s) keys for proper operation of MD5 support. The default is **off**.
set conn name name icmp-echo-drop [ off | on ]

If set to on, drops echo-requests received on the particular interface. The default is off.

set conn name name icmp-err-suppress [ off | on ]

An additional option to suppress ICMP error messages on WAN IP interfaces. The default is off.

set conn name name static ipaddr ipaddr

Specifies a static IP address when the connection type has been set to static. The default is 192.168.1.254.

Note:

You must also set the gateway address OR turn it off, otherwise the settings cannot be saved. See "IP Gateway commands" on page 130.

Example:

```
set conn name name icmp-echo-drop [ off | on ]
set conn name name icmp-err-suppress [ off | on ]
set conn name name static ipaddr ipaddr
```

```bash
NOS/128600225634272/conf
Config Mode v1.3
NOS/128600225634272 (top)>> conn
NOS/128600225634272 (conn)>> set
conn
(conn) node list ...
"LAN"
"WAN"
Select (name) node to modify from list, or enter new (name) to create.
conn name (?):
name "LAN"
link-oid ("LAN") [ LAN | WAN | PPPoE | ]:
type (static) [ static | dhcp | ppp ]:
side (lan) [ lan | wan ]:
lan-type (private) [ private | public | public-delegated ]:
mcast-forwarding (off) [ off | on ]:
rip-send (off) [ off | v1 | v2 | v1-compat | v2-md5 ]:
rip-receive (off) [ off | v1 | v2 | v1-compat | v2-md5 ]:
fs-egress ("" [ Security | QoSUpstream | WanEgress ] :
fs-ingress ("" [ Security | QoSUpstream | WanEgress ] :
static
ipaddr ("192.168.1.254"):
netmask ("255.255.255.0"):
dhcp-server-enable (on) [ off | on ]:
dhcp-server
start-addr ("192.168.1.64"):
end-addr ("192.168.1.253"):
lease-time (01:00:00:00):
subnet-order (1) [ 1 - 8 ]:
gen-option
(gen-option) node list ...
Select (name) node to modify from list, or enter new (name) to create.
```
gen-option name (?):
  option-group
(option-group) node list ...
Select (name) node to modify from list,
or enter new (name) to create.
  option-group name (?):
  filterset
(filterset) node list ...
Select (name) node to modify from list,
or enter new (name) to create.
  filterset name (?):
name "WAN"
  link-oid ("WAN") [ LAN | WAN | PPPoE | ]:
  type (dhcpc) [ static | dhcpc | ppp ]; static
  side (wan) [ lan | wan ]:
  mcast-forwarding (off) [ off | on ]:
  nat-enable (on) [ off | on ]:
  rip-receive (off) [ off | v1 | v2 | v1-compat | v2-md5 ]:
  icmp-echo-drop (on) [ off | on ]:
  icmp-err-suppress (off) [ off | on ]:
  fs-egress ("WanEgress") [ Security | QosUpstream | WanEgress | ]:
  fs-ingress ("" ) [ Security | QosUpstream | WanEgress | ]:
static
  ipaddr ("": 10.3.53.100
  netmask ("255.255.255.0":
NOS/128600225634272 (conn)>> set ip gateway address 10.3.53.1
NOS/128600225634272 (conn)>> save

If you do not want the gateway use this command to turn it off:
  set ip gateway enable off

__set conn name name static netmask netmask__

Specifies a static netmask when the connection type has been set to static. The default is 255.255.255.0.

__set conn name name dhcp-server start-addr ipaddr__

If dhcp-server-enable is set to on, specifies the first address in the DHCP address range. The Motorola Gateway can reserve a sequence of up to 253 IP addresses within a subnet, beginning with the specified address for dynamic assignment. The default is 192.168.1.64

__set conn name name dhcp-server end-addr ipaddr__

If dhcp-server-enable is set to on, specifies the last address in the DHCP address range. The default is 192.168.1.253

__set conn name name dhcp-server lease-time seconds__

If dhcp-server-enable is set to on, specifies the default length for DHCP leases issued by the Motorola Gateway. Lease time is in seconds. Default is 3600.
set conn name name dhcp-server subnet-order [1... 8]

If dhcp-server-enable is set to on, specifies the order in which to address the first of 8 possible subnets. Ordinarily, this is the first one, the default 1.

set conn name name nat-enable [ on | off ]

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

set conn name name dhcp-client discover-time seconds

The DHCP client parameters appear when the connection type has been set to dhcpc. discover-time is in seconds; the default is 30.

set conn name name dhcp-client dns-enable [ on | off ]

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

set conn name name dhcp-client dns-override [ off | on ]

This allows you to enable or disable overriding default DNS behavior. The default is off.

set conn name name dhcp-client vendor-class string

The vendor-class default information varies by model and components. This is information that identifies the unit.

set conn name name fs-egress filterset_name

Attaches a user filterset to a conn which is applied to transmitted packets. See "Filterset commands" on page 124.

set conn name name fs-ingress filterset_name

Attaches a user filterset to a conn which is applied to received packets. See "Filterset commands" on page 124.

Filterset commands

Filtersets provide packet filtering and QoS configuration. Packets are identified by characteristics that allow QoS and forwarding decisions to be made. These characteristics can be at the MAC layer, IP layer, TCP | UDP | ICMP layer(s), or (in applicable circumstances) 802.1q/p (VLAN-tagging) layer.

Your Gateway is capable of adding and stripping 802.1Q tags to and from frames before transmission on its LAN interfaces. See also "Link commands" on page 143 for more information.

A maximum of 8 filtersets are supported. Each filterset can have up to 8 rules configured. A maximum 8 egress queues are supported. Each queue can have up to 8 entries.

A filterset rule identifies packet attributes to match with its match parameters. It acts on these packets using its default action parameters.
set filterset name filterset_name rule number order number

Determines order of execution of filterset rules (1 before 2, etc). If order is unspecified, the value of order is set to 1 more than the last order in the filterset. If order is set to an already existing order value, order values of other rules are incremented automatically.

set filterset name filterset_name rule number match-eth-proto number

Matches ethernet protocol field to the supplied value.

set filterset name filterset_name rule number match-eth-length number

Matches ethernet length field to the supplied value.

set filterset name filterset_name rule number match-eth-p-bits number

Matches VLAN priority bits.

set filterset name filterset_name rule number match-eth-vid number

Matches VLAN id number.

set filterset name filterset_name rule number match-eth-src-mac-addr mac_address

Matches supplied source MAC address field.

set filterset name filterset_name rule number match-eth-dst-mac-addr mac_address

Matches supplied destination MAC address field.

set filterset name filterset_name rule number match-src-ip-addr ip_address_range

Matches supplied value with packet's source ip address field.

set filterset name filterset_name rule number match-dst-ip-addr ip_address_range

Matches supplied value with packet's destination ip address field.

set filterset name filterset_name rule number match-protocol protocol_string

Matches supplied value with packet's protocol field.

set filterset name filterset_name rule number match-tos [ number | descriptive_value ]

Matches tos field from numeric value 0-255; or one of the following descriptive values:

- Minimize-Delay (0x10)
- Maximize-Throughput (0x08)
- Maximize-Reliability (0x04)
- Minimize-Cost (0x02)
- Normal-Service (0x00)
set filterset name filterset_name rule number
match-dscp [ number | diffserv_class_string ]

Matches diffserv class with supplied numerical value, which can be in decimal (ex: 32) or in Hex (ex: 0x20);

Or match the supplied diffserv class. This value may be any of the BE, EF, AFxx or CSx classes. A full list is:

{ "CS0", 0x00 } 
{ "CS1", 0x08 } 
{ "CS2", 0x10 } 
{ "CS3", 0x18 } 
{ "CS4", 0x20 } 
{ "CS5", 0x28 } 
{ "CS6", 0x30 } 
{ "CS7", 0x38 } 
{ "BE", 0x00 } 
{ "AF11", 0x0A } 
{ "AF12", 0x0C } 
{ "AF13", 0x0E } 
{ "AF21", 0x12 } 
{ "AF22", 0x14 } 
{ "AF23", 0x16 } 
{ "AF31", 0x1A } 
{ "AF32", 0x1C } 
{ "AF33", 0x1E } 
{ "AF41", 0x22 } 
{ "AF42", 0x24 } 
{ "AF43", 0x26 } 
{ "EF", 0x2E }

set filterset name filterset_name rule number match-src-port number [ number ]

Matches TCP|UDP source port field or port range.

set filterset name filterset_name rule number match-dst-port number [ number ]

Matches TCP|UDP destination port field or port range.

set filterset name filterset_name rule number match-tcp-flags tcp_flag_string

Matches TCP flags in a packet. The flag string is comma-delimited.

set filterset name filterset_name rule number match-packet-length number [ number ]

Matches packet length against value or range.

set filterset name filterset_name rule number action forward [ pass | drop | reject ]

Executes the named filterset's default action: pass, drop, or reject.

set filterset name filterset_name rule number
match-qos-marker-enable [ off | on ]

Turns the function of tagging the packet according to the queue marker name on or off. Default is off.
set filterset name filterset_name rule number
   action set-qos-marker qos_marker_string
Tags the packet according to the queue marker name. See "Queue commands" on page 128.

set filterset name filterset_name rule number action set-tos number
Sets the packet tos field to the supplied value.

set filterset name filterset_name rule number
   action set-dscp [ number | diffserv_class_string ]
Sets the dscp field to the supplied value.

set filterset name filterset_name rule number action set-eth-p-bits number
Sets vlan priority bits to the supplied value.

set filterset filterset_name rule number action do-filterset name
Executes the supplied filterset.

Default actions
If a packet passes through all of a filter's rules without a match, then the filterset's default-actions come into play. These behave the same way that rule actions behave.

set filterset name filterset_name default-action set-qos-marker qos_marker_string
Tags the packet according to the queue marker name.

set filterset name filterset_name default-action set-tos number
Sets the packet tos field to the supplied value.

set filterset name filterset_name default-action set-dscp [ number | diffserv_class_string ]
Sets the dscp field to the supplied value.

set filterset name filterset_name default-action set-eth-p-bits number
Sets vlan priority bits to the supplied value.

set filterset name filterset_name default-action do-filterset name
Executes the supplied filterset.

set filterset name filterset_name default-action forward [ pass | drop | reject ]
Executes the named filterset's default action: pass, drop, or reject.
Queue commands

Queue configuration typically requires a classification component to set a QoS marker to a packet and a queueing component to schedule the marked packets to the link. This is accomplished using filtersets ("Filterset commands" on page 124).

The basic queue's size and “length” are controls for how many packets and total bytes can be enqueued before it is considered to be full. Once it is full, any attempts to enqueue another packet will result in a “tail-drop.”

Both constraints are simultaneously used, such that it is full when either packet count OR byte count exceeds the limit. This allows flexibility in obtaining a balance, where a large number of small packets, but only a small number of large packets can be enqueued.

If there are no tail-drops – that is, the queue is not blocked from sending and doesn't over-fill and dump packets – then these queue size/bytes parameters do not affect anything. Their only function is to adjust the threshold at which the queue is considered full, which dictates when tail drops will occur. So if there are no tail-drops, then increasing the queue length will have no effect. Increasing the queue length has no effect unless there are tail-drops.

The maximum size/bytes of a queue balances how much burstiness can be buffered versus having a queue that is simply too long.

Burstiness smoothing requires queueing up the buffers. For example, if the upstream line rate is 1mbps, but the traffic source sends 100mbps bursts for 10ms every second (which coincidentally averages 1mbps) then the router will have to buffer enough (about a full second worth of traffic) so that the burst of traffic doesn't get tail-dropped when it arrives and is enqueued at the same time in the same burst.

On the other hand, it is undesirable to buffer too much data in the queue(s) since the packets may be stale by the time they are sent. It may be desirable to drop the traffic sufficiently that there are queueing disciplines such as Random Early Discard (red) that don't drop from the tail of the queue. Instead, red drops packets towards the front of the queue, so that the congestion is noticed more quickly in order for the sender to scale back bandwidth usage to avoid drops.

the following types of queue “building blocks” are supported:

◆ basic queue
◆ ingress queue
◆ priority queue
◆ wfq (weighted fair queue)

Basic queues have three different packet dropping options

◆ byte|packet fifo (bpfifo)
◆ random early discard (red)
◆ stochastic fairness queuing (sfq)

---

**set queue name** queue_name type [ basic | ingress | priority | wfq ]

Sets the type of queue.

**set queue name** queue_name options [ off | red | sfq ]

Sets the queue packet dropping options.

**set queue name** queue_name size [ 1... 64 ]

Sets the maximum number of packets that can be enqueued.
set queue name queue_name bytes [ 2048... 131072 ]
Sets the maximum total number of bytes that can be enqueued.

set queue name queue_name perturb [ 0... 100 ]
Sets the interval in seconds for queue algorithm perturbation when queue option is sfq.

set queue name queue_name police-rate [ 0... 100000000 ]
Sets the rate in milliseconds that is used for policing traffic when the queue type is ingress.

set queue name queue_name police-burst [ 0... 100000000 ]
Sets the burst rate in milliseconds that is used for policing traffic when the queue type is ingress.

set queue name queue_name bw-sharing [ on | off ]
Enables or disables bandwidth sharing, when the queue type is either priority or wfq.

set queue name queue_name bps-mode [ bps | relative ]
Sets the mode of the weighted fair queue. bps indicates that weights are defined as “bits-per-second”. relative indicates that weights are defined as a proportion of the sum of the weights of all inputs to the wfq.

set queue name queue_name entry number input queue_name
Sets the input to a priority or weighted fair queue.

set queue name queue_name entry number marker queue_marker
Sets the marker with which packets must be marked to be directed to this queue entry’s input queue when the type is priority or wfq.

set queue name queue_name entry number priority [ 0... 255 ]
Sets the priority level of this queue. A lower value indicates a higher priority. All entries of equal priority will be subject to a round robin algorithm.

◆ for (strict) priority queue, the higher priority gets link resource first.
◆ for wfq queue, each entry gets reserved bandwidth according to its weight. If different priority is given, any excess bandwidth is offered to higher priority entry first; otherwise any excess bandwidth is distributed to the weights ratio.

set queue name queue_name entry number weight [ 0... 100 ]
Sets the weight level of this weighted fair queue. Weight units are dependent on bps-mode setting.

◆ If bps-mode is set to bps, then setting the weight to 0 will allocate the remaining available bandwidth to the queue entry.
◆ If no priority specified, excess bandwidth will be distributed proportionately to the weight ratio.

set queue name queue_name entry number peak [ 0... 100,000,000 ]
Sets the peak level of this weighted fair queue. The peak parameter is a number of 0 through 100,000,000 in bits/second. It must be at least 50,000 for best effect. It is the peak data rate allowed on the queue entry, and usually
supports bandwidth sharing, that is, if other queues are not busy and there is spare bandwidth, then a busy queue is allowed to go up to the peak rate.

**set queue name queue_name default-entry queue_name**

Indicates the input queue which is used if there is no match between the packet queue marker and the configured markers in any of the queue’s inputs when the queue type is priority or wfq.

**IP Gateway commands**

**set ip gateway enable [ on | off ]**

Specifies the conn of the gateway. Normally, this would be the WAN connection. Specifies whether the Motorola Gateway should send packets to a default Gateway if it does not know how to reach the destination host.

**set ip gateway conn-oid value**

Sets the default Gateway to point to an associated link specified by the conn-oid value.

**set ip gateway address ip_address**

Specifies the IP address of a host on a local or remote network in standard dotted-quad format.

**IPv6 Commands**

**set ip6 enable [ on | off ]**

Enables/disables IPv6 globally. The default is off. When enabled, the following default configuration is created:

```bash
set ip6 enable on
set ip6 conn name "WANv6" enable on
set ip6 conn name "WANv6" type rd
set ip6 conn name "WANv6" mtu 1472
set ip6 conn name "WANv6" side wan
set ip6 conn name "WANv6" mcast-forwarding off
set ip6 conn name "WANv6" icmp-echo-drop on
set ip6 conn name "WANv6" traffic-class-clear on
set ip6 conn name "WANv6" 6rd-tunnel type cpe
set ip6 conn name "WANv6" 6rd-tunnel ipv4-conn "WAN"
set ip6 conn name "WANv6" 6rd-tunnel use-dhcp-values off
set ip6 conn name "WANv6" 6rd-tunnel prefix ":::"
set ip6 conn name "WANv6" 6rd-tunnel prefix-length 1
set ip6 conn name "WANv6" 6rd-tunnel ipv4-common-bits 0
set ip6 conn name "WANv6" 6rd-tunnel relay-ipv4-addr "0.0.0.0"
set ip6 conn name "WANv6" 6rd-tunnel ipv4-tx-tos-mode off
set ip6 conn name "WANv6" 6rd-tunnel force-tx-to-br on
set ip6 conn name "WANv6" 6rd-tunnel anti-spoof-enable on
set ip6 conn name "WANv6" 6rd-tunnel tx-df-bit-set on
set ip6 conn name "LANv6" enable off
set ip6 gateway enable on
set ip6 gateway conn "WANv6"
set ip6 gateway address ":::"
set ip6 dhcp-server enable on
```
set ip6 dhcp-server information-only off
set ip6 dhcp-server preference 255
set ip6 dhcp-server authoritative on
set ip6 dhcp-server rapid-commit on
set ip6 dhcp-server unicast off
set ip6 dhcp-server leasequery off
set ip6 dhcp-server pd-enable on
set ip6 dhcp-server default-lease-time 2592000
set ip6 dhcp-server preferred-lifetime 604800
set ip6 dhcp-server T1 302400
set ip6 dhcp-server T2 483840
set ip6 dhcp-server info-refresh-time 86400
set ip6 dns primary-address ""
set ip6 dns secondary-address ""

Default IPv6 security configuration values:

set security spi ip6 src-mcast-drop off
set security spi ip6 invalid-mcast-scope-drop on
set security spi ip6 forbidden-addr-drop on
set security spi ip6 deprecated-ext-hdr-drop on
set security spi ip6 src-addr-from-lan-unassigned-drop on
set security spi ip6 lan-assigned-src-addr-from-wan-drop on
set security spi ip6 ula-drop on
set security spi ip6 ignore-dns-from-wan on
set security spi ip6 ignore-dhcp-from-wan on
set security spi ip6 esp-hdr-drop on
set security spi ip6 ah-hdr-drop on
set security spi ip6 allow-inbound off
set security spi ip4 invalid-addr-drop on
set security spi ip4 private-addr-drop off
set security spi flood-limit enable off
set security ip6 firewall-level low
set security ip6 enable on

ip6 gateway conn

set ip6 gateway enable [ on | off ]

Enables or disables IPv6 default gateway.

set ip6 gateway conn value

Sets the default Gateway to point to an associated link specified by the conn-oid value. Normally, this would be the WAN connection.

set ip6 gateway address ipv6_address

Specifies the IPv6 address of a host on a local or remote network in standard IPv6 format.

ip6 conn

set ip6 conn name name enable [ on | off ]

Enables/disables the IPv6 connection named name.
set ip6 conn name name type [ static | autoconf | rd | dp | aiccu ]
Type of connection. See below for connection types.

set ip6 conn name name mtu octets
Specified MTU of connection.

set ip6 conn name name side [ lan | wan ]
Specified whether the connection is LAN side or WAN side.

set ip6 conn name name mcast-fwding [ off | on ]
Turns IPv6 multicast forwarding for this connection off or on. The default is off. (not yet implemented)

set ip6 conn name name old-prefix-purge-timer
The time in seconds for which old, invalid prefixes are advertised with a lifetime of zero. The intent is to “flush out”
global prefixes on attached IPv6 hosts which suddenly become invalid.

Static Connections

ip6 conn (type = static): Statically configured IPv6 connection.

set ip6 conn name name static link-oid link_name
Sets the connection named name to point to an associated link specified by the link-oid link_name.

set ip6 conn name name static ipaddr ipv6_address
Specifies a static IPv6 address.

set ip6 conn name name static prefix-length value
Specifies the prefix length of the connection’s static IPv6 address. Default is 64.

6rd Connections

ip6 conn (type = rd, side = wan). This WAN connection type is a 6rd tunnel over an IPv4 conn in accordance
with RFC 5569.

set ip6 conn name name 6rd-tunnel type [ cpe | gateway ]
The 6rd connection can operate in “cpe” or “gateway” mode as configured by the type parameter. “cpe” mode is
used when operating as a CPE; “gateway” mode is used when operating as a “6rd relay” as per RFC 5569.

set ip6 conn name name 6rd-tunnel ipv4-conn-oid ipv4_name
Sets the 6rd connection named name to tunnel over an associated IPv4 connection named ipv4_name.
set ip6 conn name name 6rd-tunnel use-dhcp-values [ off | on ]

If this parameter is on, 6rd-provisioned parameters are obtained via the underlying DHCPv4 client associated with IPv4 connection named ipv4-name. See “draft-ietf-softwire-ipv6-6rd-10” for DHCP format description.

ip6 conn (type = rd, 6rd-tunnel use-dhcp-values = off).

set ip6 conn name name 6rd-tunnel prefix IPv6_address

6rd domain prefix.

set ip6 conn name name 6rd-tunnel prefix-length value [ 1 - 63 ]

6rd domain prefix length.

set ip6 conn name name 6rd-tunnel ipv4-common-bits value [ 0 - 31 ]

The number of bits common to all IPv4 addresses within the 6rd domain. The top-most bits of the IPv4 address will be “subtracted” from the 6rd address. If the whole 32-bit IPv4 address is contained in the 6rd IPv6 address, this value is set to zero. Default is 0, meaning all 42 bits of the IPv4 address are embedded in the 6rd prefix.

set ip6 conn name name 6rd-tunnel relay-ipv4-addr IPv4_address

The IPv4 anycast address of the 6rd border gateway.

set ip6 conn name name 6rd-tunnel ipv4-tx-tos-mode [ off | use-ipv6 ]

off means the TOS field in the IPv4 header is set to zero for transmitted 6rd packets. use-ipv6 means the the TOS field in the IPv4 header is set to the DS field of the 6rd-encapsulated IPv6 packet.

set ip6 conn name name 6rd-tunnel ipv4-tx-to-br [ off | on ]

off means each packet set to a destination IPv6 address within the originating 6rd domain is sent directly to the 6rd endpoint. on means that all packets are transmitted to the 6rd border gateway.

AICCU (SixXS tunnel broker) Connections

ip6 conn (type = aiccu, side = wan). This connection type enables an IPv6 connection to the IPv6 internet over an IPv4/NAT/UDP tunnel to a tunnel endpoint administered by tunnel broker SIXXS (www.sixxs.net).

You set up an account with SIXXS, and subsequently get assigned a tunnel and a subnet (usually a /48 subnet).

set ip6 conn name name aiccu username username

SIXXS username.

set ip6 conn name name aiccu password password

SIXXS password.
Delegated Prefix Connections

**ip6 conn (type = dp, side = lan).** A conn of type "delegated prefix" obtains its global prefix information from one or more prefix from another IPv6 conn (typically a WAN conn), if available. In order for a "dp" connection to become fully operational, its underlying link must be up AND the IPv6 connection which delegates the prefix must have created one or more prefixes from which to draw the "dp" connection's global prefix.

```
set ip6 conn name name dp link-oid link_name
```

```
set ip6 conn name name dp conn-oid ipv6_conn_name
```
Sets the dp connection named name to obtain its prefix from IPv6 connection named `ipv6_conn_name`.

```
set ip6 conn name name dp subnet-length value [ 0 - 16 ]
```
The length of the subnet portion of the delegated prefix. Default is 0.

```
set ip6 conn name name dp subnet-id value [ 0 - 65535 ]
```
If a subnet length is specified, the value that would occupy the of the subnet portion of the conn's IPv6 prefix. Default is 0.

```
set ip6 conn name name dp stay-up [ off | on ]
```
If the delegated prefix parameter `stay-up` is set to `on`, the global prefix assigned from the conn delegating the prefix remains active in the event that the conn delegating the prefix goes down, and the prefix becomes invalid. This enables local LAN-side hosts to continue to use the global prefix uninterrupted. If parameter `stay-up` is set to `off`, the connection's delegated prefix becomes invalid when the connection named `ipv6-conn-name` delegating the prefix goes down.

Router Advertisement and DHCPv6 Server

**ip6 conn (side = lan).** Router Advertisements and the DHCPv6 server are available on LAN-side conns as the means to provide clients with stateful or stateless IPv6 prefixes and addresses, as well as addition client parameters such as MTU size and IPv6-addressable DNS servers.

```
set ip6 conn name name radv enable [ off | on ]
```
on means radv is enabled for this conn.

```
set ip6 conn name name radv min-rtr-adv-interval seconds [ 3 - 1350 ]
```
The minimum time allowed between sending unsolicited multicast router advertisements from the link, in seconds.

```
set ip6 conn name name radv max-rtr-adv-interval seconds [ 4 - 1800 ]
```
The maximum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds.

```
set ip6 conn name name dhcp-server enable [ off | on ]
```
on means the DHCPv6 server is enabled for this conn.
set ip6 conn name name dhcp-server addr-count value [ 0 - 256 ]

The number of IPv6 addresses available to serve to DHCPv6 stateful clients. If the `addr-count` parameter is set to zero, the DHCPv6 server operates in “stateless” mode.

set ip6 conn name name dhcp-server start-addr-offset value [ 0 - 65536 ]

If the `addr-count` parameter is greater than zero, the start address is an offset from the base address of the prefix which is assigned to the LAN conn.

set ip6 conn name name dhcp-server lease-time seconds [ 180 - 8553600 ]

DHCPv6 lease time.

set ip6 conn name name dhcp-server dns-server optional IPv6 address

IPv6 address of advertised DNS server (optional).

**IPv6 DHCP Server**

set ip6 dhcp-server enable [ on | off ]

Globally enables or disables DHCPv6 servers on all IPv6 LAN conns. The default is on.

set ip6 dhcp-server information-only [ off | on ]

When set to on DHCPv6 servers on all IPv6 LAN conns operate in stateless “information-only” mode. The default is off.

set ip6 dhcp-server preference 255

Sets the preference option, as defined in RFC1315, sec. 22.8. The preference option in the server’s Advertise message may assist a DHCPv6 client in selecting from more than one server on the LAN.

set ip6 dhcp-server authoritative [ on | off ]

If a client requests an IP address on a given network segment that the server knows is not valid for that segment, and `authoritative` is set to on, the server will respond with a DHCPNAK message, causing the client to forget its IP address and try to get a new one. If `authoritative` is set to off, the server will ignore the client’s request. The default is on.

set ip6 dhcp-server rapid-commit [ on | off ]


set ip6 dhcp-server unicast [ off | on ]


set ip6 dhcp-server leasequery [ off | on ]

Enables or disables DHCPv6 Leasequery option per rfc5007. (http://tools.ietf.org/rfc/rfc5007.txt) The default is off.
set ip6 dhcp-server pd-enable [ on | off ]

Enables or disables prefix delegation globally on all DHCPv6 servers on all IPv6 LAN cons, overriding individual DHCPv6 server settings. The default is on.

set ip6 dhcp-server default-lease-time seconds

Sets the global DHCPv6 lease time setting in seconds. The default is 2592000 (30 days).

set ip6 dhcp-server preferred-lifetime seconds

Sets the global DHCPv6 preferred lifetime of prefixes in seconds, per RFC 3633. (http://www.ietf.org/rfc/rfc3633.txt) The default is 604800 (7 days).

set ip6 dhcp-server T1 seconds
set ip6 dhcp-server T2 seconds

Sets global DHCPv6 T1, T2 values, per RFC 3315 for local NA addresses:

| T1 | The time at which the client contacts the server from which the addresses in the IA_NA were obtained to extend the lifetimes of the addresses assigned to the IA_NA; T1 is a time duration relative to the current time expressed in units of seconds. Defaults to 302400 (3.5 days). |
| T2 | The time at which the client contacts any available server to extend the lifetimes of the addresses assigned to the IA_NA; T2 is a time duration relative to the current time expressed in units of seconds. Defaults to 483840 (5.6 days). |

and also per global DHCPv6 T1, T2 values, per RFC 3633 for PD prefixes:

| T1 | The time at which the requesting router should contact the delegating router from which the prefixes in the IA_PD were obtained to extend the lifetimes of the prefixes delegated to the IA_PD; T1 is a time duration relative to the current time expressed in units of seconds. |
| T2 | The time at which the requesting router should contact any available delegating router to extend the lifetimes of the prefixes assigned to the IA_PD; T2 is a time duration relative to the current time expressed in units of seconds. |

set ip6 dhcp-server info-refresh-time seconds

In seconds, per rfc 4242: The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6 in stateless mode. (http://tools.ietf.org/html/rfc4242) The default is 86400 (24 hours).

Static Routes

ip6 static-route.

set ip6 static-route name conn-oid ipv6_conn_name

Route is directed to IPv6 connection named ipv6_conn_name.

set ip6 static-route name nexthop IPv6_address

Next-hop IPv6 address for forwarding. Can be a global or link-local address.
set ip6 static-route *name prefix* *IPv6_prefix*
IPv6 prefix.

set ip6 static-route *name prefix-length* *value* [ 1 - 64 ]
IPv6 prefix-length.

set ip6 static-route *name metric* *value* [ 0 - 255 ]
metric assigned to route.
IP DNS commands

set ip dns domain-name domain_name

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

set ip dns primary-address ip_address

Specifies the IP address of the primary DNS name server.

set ip dns secondary-address ip_address

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

set ip dns proxy-enable [ on | off ]

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

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 Gateways use a protocol for forwarding multicasting: Internet Group Management Protocol (IGMP).

Motorola Gateways support IGMP Version 1, Version 2, or Version 3.

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

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

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

IGMP Version 3 supports:

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

These features require no user configuration on the Gateway.

You can set the following options:

◆ IGMP Snooping – enables the Motorola 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 Gateway waits to receive a response to a General Query message. The default query response interval is 10 seconds and must be less than the query interval.

◆ Unsolicited Report Interval – the amount of time in seconds between repetitions of a particular computer’s initial report of membership in a group. The default unsolicited report interval is 10 seconds.

◆ Querier Version – select a version of the IGMP Querier: version 1, version 2, or version 3. If you know you will be communicating with other hosts that are limited to v1 or v2, for backward compatibility, select accordingly; otherwise, allow the default v3.

NOTE:

IGMP Querier version is relevant only if the Gateway is configured for IGMP forwarding. If any IGMP v1 routers are present on the subnet, the querier must use IGMP v1. The use of IGMP v1 must be administratively configured, since there is no reliable way of dynamically determining whether IGMP v1 routers are present on a network. IGMP forwarding is enabled per IP Profile and WAN Connec-
◆ **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** – set to off by default, fast leave enables a non-standard expedited leave mechanism. The querier keeps track of which client is requesting which channel by IP address. When a leave message is received, the querier can check its internal table to see if there are any more clients on this group. If there are none, it immediately sends an IGMP leave message to the upstream querier.

◆ **Log Enable** – If set to on, all IGMP messages on both the LAN and the WAN will be logged.

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

```plaintext
set ip igmp querier-version [ 1 | 2 | 3 ]
```
Sets the IGMP querier version: version 1, version 2, or version 3. If you know you will be communicating with other hosts that are limited to v1, for backward compatibility, select 1; otherwise, allow the default 3.

```plaintext
set ip igmp robustness value
```
Sets IGMP robustness range: from 2 – 255. The default is 2.

```plaintext
set ip igmp query-interval value
```
Sets the query-interval range: from 10 seconds – 600 seconds, The default is 125 seconds.

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

```plaintext
set ip igmp unsolicited-report-interval value
```
Sets the unsolicited report interval: the amount of time in seconds between repetitions of a particular computer’s initial report of membership in a group. The default is 10 seconds.

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

```plaintext
set ip igmp max-group-memberships value
```
Sets the maximum number of IGMP group memberships. Default is 20.

```plaintext
set ip igmp fwd-admin-groups [ off | on ]
```
Turns Admin group forwarding off or on. Default is off.
set ip igmp last-member-interval value

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

set ip igmp last-member-count value

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

set ip igmp default-fwd-allow [ on | off ]

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

set ip igmp snooping-entry-time seconds

The snooping-entry-time is the amount of time an entry will remain in the snooping table (in seconds) after being added. An entry is added when a “JOIN” is seen from a multicast client. Any new joins (triggered by upstream queries) will reset the timeout back to seconds. If no additional joins are seen, the entry will expire after seconds. Default is 130.

set ip igmp snooping-unreg-mode [ block | flood ]

The snooping-unreg-mode can be set to block or flood. This indicates what should happen to unregistered multicast traffic – traffic that hasn't been subscribed to by any clients. If set to flood, the traffic will be sent to all LAN ports. If set to block, the traffic will not be sent to any LAN ports; it will be dropped. Default is block.

NTP commands

set ip ntp enable [ on | off ]

Enables or disables acquiring the time of day from an NTP (Network Time Protocol) server.

set ip ntp server-address server_address

set ip ntp alt-server-address alt_server_address

Specify the NTP server(s) to use for time updates. The NTP server-address and alt-server-address can be entered as DNS names as well as IP addresses.

set ip ntp update-period minutes

update-period specifies how often, in minutes, the Gateway should update the clock. Default is 1440.
**Application Layer Gateway (ALG) commands**

These commands allow you to enable or disable the router's support for a variety of Application Layer Gateways (ALGs). An application layer gateway (ALG) is a NAT component that helps certain application sessions to pass cleanly through NAT. Each ALG has a slightly different function based on the particular application's protocol-specific requirements.

An internal client first establishes a connection with the ALG. The ALG determines if the connection should be allowed or not and then establishes a connection with the destination computer. All communications go through two connections — client to ALG and ALG to destination. The ALG monitors all traffic against its rules before deciding whether or not to forward it. The ALG is the only address seen by the public Internet so the internal network is concealed. In some situations, it may be desirable to disable some of the ALGs.

- **set ip alg esp-enable [ on | off ]**
  
  Turns the ESP (Encapsulated Security Payload) ALG for file transfers on or off. Default is on.

- **set ip alg esp-setup-timeout value**
  
  Specifies the timeout value for the ESP ALG setup. Default is 180.

- **set ip alg esp-stream-timeout value**
  
  Specifies the timeout value for the ESP ALG streaming. Default is 300.

- **set ip alg ftp-enable [ on | off ]**
  
  Turns the FTP (File Transfer Protocol) ALG for file transfers on or off. Default is on.

- **set ip alg h323-enable [ on | off ]**
  
  Turns the H323 ALG for audio, video, and data communications across IP-based networks on or off. Default is on.

- **set ip alg pptp-enable [ on | off ]**
  
  Turns the PPTP (Point-to-Point Transfer Protocol) ALG for authentication on or off. Default is on.

- **set ip alg sip-enable [ on | off ]**
  
  Turns the SIP (Session Initiation Protocol) ALG for voice communication initiation on or off. Default is on.

- **set ip alg tftp-enable [ on | off ]**
  
  Turns the TFTP (Trivial File Transfer Protocol) ALG for simple file transfers and firmware updates on or off. Default is on.

**Dynamic DNS Commands**

- **set ip dynamic-dns enable [ off | on ]**

  Enables or disables Dynamic DNS. Dynamic DNS support allows you to use the free services of www.dyndns.org. Dynamic DNS automatically directs any public Internet request for your computer's name to your current dynamically-assigned IP address. This allows you to get to the IP address assigned to your Gateway, even though your actual IP address may change as a result of a PPPoE connection to the Internet.
set ip dynamic-dns service-type [ dyndns ]
set ip dynamic-dns username myusername
set ip dynamic-dns password mypassword
set ip dynamic-dns hostname myhostname
set ip dynamic-dns retries [ 1 - 64 ]

Enables or disables dynamic DNS services. The default is off. If you specify dyndns.org, you must supply your hostname, username for the service, and password. Number of retries defaults to 5.

Default server settings

Set ip wan-allocation mode [ normal | defaultserver ]

Sets the WAN mode to direct your Gateway to forward all externally initiated IP traffic (TCP and UDP protocols only) to a default host on the LAN, otherwise this feature is disabled. Default is normal.

Link commands

Links represent physical connections. Currently, port-based VLAN support is provided at this level. Your Gateway is capable of adding and stripping 802.1Q tags to and from frames before transmission on its LAN interfaces. See also “Filterset commands” on page 124 and “Queue commands” on page 128 for more information.

set link name name type [ ethernet | ppp ]

Specifies whether the type of the link named name is ethernet or ppp.

set link name name mtu-override [ 0 - 1500 ]

Specifies whether the Maximum Transmission Unit value should be set to other than the standard 1500. A setting of 0 (zero) turns off override.

set link name name igmp-snooping [ off | on ]

Turns igmp-snooping off or on on the link named name.

set link name name port-vlan ports [ lan-1...4 | hpna | ssid-1...4 | ptm | vc-1 | vc-2 ]

Specifies a port-based VLAN on the selected ports on the link named name.

set link name name port-vlan priority [ 0 - 7 ]

Specifies the 802.1p priority bit. If you set this to a value greater than 0, all packets of this VLAN with unmarked priority bits (pbits) will be re-marked to this priority.

set link name name tagged-vlan name integer ports [ lan-1...4 | hpna | ssid-1...4 | ptm | vc-1 | vc-2 ]

Specifies a tagged VLAN on the selected port on the link named name. Default is ptm.

set link name name tagged-vlan name integer vid vlan_id

Specifies a VLAN ID (vid) on the selected link named name. Default is 0.
**set link name** *name* tagged-vlan *name* integer priority [0 - 7]

Specifies the 802.1p priority bit. If you set this to a value greater than 0, all packets of this VLAN with unmarked priority bits (pbits) will be re-marked to this priority.

**set link name** *name* supplicant type [none | eap-tls]

Specifies whether the EAP TLS supplicant is enabled on the link named *name*. Default is eap-tls.

**set link name** *name* supplicant priority [0 - 7]

Sets the supplicant priority on the link named *name* when supplicant type is eap-tls. Default is 0.

**set link name** *name* ppp sub-link *link_name*

Specifies a name *link_name* for this secondary link when one is required.

**set link name** *name* ppp auth-type [on | off]

Enables or disables PPP login authorization.

**set link name** *name* ppp username *uname*

Specifies a username *uname* for authentication on the specified link when ppp auth-type is set to on.

**set link name** *name* ppp password *pwd*

Specifies a password *pwd* for authentication on the specified link when ppp auth-type is set to on.

**set link name** *name* ppp magic-number [on | off]

Enables or disables LCP magic number negotiation.

**set link name** *name* ppp protocol-compression [off | on]

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

**set link name** *name* ppp max-failures integer

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

**set link name** *name* ppp max-configures integer

Specifies the maximum number of unacknowledged configuration requests that your Gateway will send. The integer argument can be any number between 1 and 20.

**set link name** *name* ppp max-terminates integer

Specifies the maximum number of unacknowledged termination requests that your Gateway will send before terminating the PPP link. The integer argument can be any number between 1 and 10.
**set link name** *name* **ppp restart-timer** *integer*

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

**set link name** *name* **ppp connection-type** [ **instant-on** | **always-on** ]

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

**set link name** *name* **ppp echo-request** [ **on** | **off** ]

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.

**set link name** *name* **ppp echo-failures** *integer*

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

**set link name** *name* **ppp echo-interval** *integer*

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

**set link name** *name* **ppp mru** *integer*

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

**set link name** *name* **pppoe service-name** *name*

Specifies an ISP name or a class or quality of service. The Service Name tells the access concentrator which network service the Motorola Gateway is trying to reach.

---

**NOTE:**

This is an expert-mode setting that will rarely be used. The setting should be left on, unless you are an expert user who knows you do not want the Gateway to acquire any nameserver addresses from this PPP connection.

---

Controls whether the Gateway accepts nameserver addresses from the peer.

- The default is on, which means the Gateway expects to get nameserver addresses when the PPP link comes up. This especially applies when the primary WAN connection is PPP.
- However, there are some unusual situations where the PPP connection is not the primary WAN, for example when the connection is used only for management. In that situation it may be desirable to not pick up more nameserver addresses. You can do that by setting the parameter to off.
set link name name pppoe ac-name name

Specifies this particular Access Concentrator unit from all others. Some access provider networks may have multiple PPPoE servers, and having the Motorola Gateway indicate an AC Name specifies to which one the Motorola Gateway is trying to connect.

Management commands
All management related items are grouped in this section.

set management account administrator username username

Specifies the username for the administrative user – the default is admin.

set management account user username username

Specifies the username for the non-administrative user – the default is user.

set management cwmp enable [ off | on ]

Turns cwmp (TR-069 CPE WAN Management Protocol) on or off. TR-069 allows a remote Auto-Config Server (ACS) to provision and manage the Motorola Gateway. TR-069 protects sensitive data on the Gateway by not advertising its presence, and by password protection.

set management cwmp acs-url acs_url:port_number

set management cwmp acs-username acs_username

set management cwmp acs-password acs_password

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

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

http://some_url.com:port_number

or

http://123.45.678.910:port_number

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

https://some_url.com:port_number

or

https://123.45.678.910:port_number

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

set management lanmgmt enable [ off | on ]

Turns TR-064 LAN side management services on or off. The default is off.
**set management shell idle-timeout [ 1...120 ]**

Specifies a timeout period of inactivity for telnet access to the Gateway, after which a user must re-login to the Gateway. Default is 15 minutes for telnet.

**set management shell ssh-port [ 1 - 65534 ]**

Specifies the port number for secure shell (SSH) communication with the Motorola Gateway. Defaults to port 0 (off).

**set management shell telnet-port [ 1 - 65534 ]**

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

**set management upnp enable [ off | on ]**

Turns Universal Plug-and-Play (UPnP) on or off.

**set management web http-port [ 1 - 65534 ]**

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

**set management web https-port [ 1 - 65534 ]**

Sets the secure web access port for secure management of the Motorola Gateway. Default is port 443.

**set management web https-cert-cn string**

Specifies a certificate from a trusted certificate authority to identify the secure web access.

**set management web idle-timeout [ 1...120 ]**

Specifies a timeout period of inactivity for HTTP access to the Gateway, after which a user must re-login to the Gateway. Default is 5 minutes for HTTP.

**NOTE:**

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

**set management web isp-help-desk phone_number_string**

Specifies the ISP Help Desk phone number as it appears in the web UI. For AT&T, the default is: 1-800-288-2020.
Remote access commands

**set management remote-access http-port [ 1 - 65534 ]**
Sets the web access port for remote access management of the Gateway. Default is port 51003.

**set management remote-access http-idle-timeout [ 1...120 ]**
Specifies a timeout period of inactivity for remote HTTP access to the Gateway, after which a user must re-login to the Gateway. Default is 20 minutes for HTTP.

**set management remote-access http-total-timeout [ 1...120 ]**
Specifies a total timeout period of inactivity for remote HTTP access to the Gateway, after which a user must re-login to the Gateway. Default is 20 minutes for HTTP.

**set management remote-access http-max-clients number**
Specifies the maximum number of client sessions for remote web access management. Defaults to 1 (one).

**set management remote-access https-port [ 1 - 65534 ]**
Sets the secure web access port for remote access management of the Gateway. Default is port 51443.

**set management remote-access https-idle-timeout [ 1...120 ]**
Specifies a timeout period of inactivity for secure remote HTTPS access to the Gateway, after which a user must re-login to the Gateway. Default is 20 minutes for HTTPS.

**set management remote-access https-total-timeout [ 1...120 ]**
Specifies a total timeout period of inactivity for secure remote HTTPS access to the Gateway, after which a user must re-login to the Gateway. Default is 20 minutes for HTTPS.

**set management remote-access https-max-clients number**
Specifies the maximum number of client sessions for secure remote web access management. Defaults to 1 (one).

**set management remote-access telnet-port [ 1 - 65534 ]**
Specifies the port number for remote access telnet (CLI) communication with the Motorola Gateway. Because port numbers in the range 0-1024 are used by other protocols, you should use numbers in the range 1025-65534 when assigning new port numbers to the Motorola Gateway telnet configuration interface. A setting of 0 (zero) will turn the server off. Defaults to port 0.

**set management remote-access telnet-idle-timeout [ 1...120 ]**
Specifies a timeout period of inactivity for remote telnet access to the Gateway, after which a user must re-login to the Gateway. Default is 5 minutes for telnet.

**set management remote-access telnet-total-timeout [ 1...120 ]**
Specifies a total timeout period of inactivity for remote telnet access to the Gateway, after which a user must re-login to the Gateway. Default is 20 minutes for telnet.
set management remote-access telnet-max-clients \textit{number}

Specifies the maximum number of client sessions for remote telnet access management. Defaults to 4.

set management remote-access ssh-port [ 1 - 65534 ]

Specifies the port number for secure shell (SSH) communication with the Motorola Gateway. Defaults to port 22.

set management remote-access ssh-idle-timeout [ 1...120 ]

Specifies a timeout period of inactivity for remote secure shell (SSH) access to the Gateway, after which a user must re-login to the Gateway. Default is 5 minutes for SSH.

set management remote-access ssh-total-timeout [ 1...120 ]

Specifies a total timeout period of inactivity for remote secure shell (SSH) access to the Gateway, after which a user must re-login to the Gateway. Default is 20 minutes for SSH.

set management remote-access ssh-max-clients \textit{number}

Specifies the maximum number of client sessions for remote secure shell (SSH) access management. Defaults to 4.

set management lan-redirect enable [ off | on ]

If set to \texttt{on}, if a WAN failure condition is detected, the LAN client's browser is redirected to a web page of failure and help text information. The redirect will only occur once, as the web UI maintains a state variable to determine whether the redirect has occurred; to continually redirect would block the user from reconfiguring the router.

set management lan-redirect missing-filter-notify [ on | off ]

If set to \texttt{on}, if a missing filter on the line is detected, the LAN client's browser is redirected to a web page of failure and help text information. The redirect will only occur once, as the web UI maintains a state variable to determine whether the redirect has occurred; to continually redirect would block the user from reconfiguring the router.

set management lan-access wan-cpe-mgmt-block [ off | web | all ]

Blocks management of the device from the LAN via the web or all interface(s).

\textbf{TR-064}

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

set management lanmgmt enable [ off | on ]

Turns TR-064 LAN side management services on or off. The default is \texttt{off}. 
Physical interfaces commands

**DSL interfaces**

**set physical dsl enable [ off | on ]**

Turns the physical DSL interface off or on. Default is on.

**set physical dsl dsl-mode [ auto | single | bonded ]**

Sets the mode for the DSL connection, whether a single line or bonded. If the default auto is set, the device will try both single and bonded, attempting to detect and lock on the mode in use.

**set physical dsl loopback [ off | on ]**

Turns the DSL loopback mode off or on. Default is off.

**set physical dsl annexm [ off | on ]**

Turns optional DSL Annex M off or on. Default is off. If enabled, data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream depending on the distance from the DSLAM to the customer’s premises.

**set physical dsl modulation auto [ off | on ]**

Turns automatic DSL modulation off or on. Default is off.

**set physical dsl modulation vdsl2 [ off | on ]**

Turns vdsl2 DSL modulation off or on. Default is on.

**set physical dsl modulation adsl2 [ off | on ]**

Turns adsl2 DSL modulation off or on. Default is on.

**set physical dsl modulation adsl2+ [ off | on ]**

Turns adsl2+ DSL modulation off or on. Default is on.

**set physical dsl modulation annex-l [ off | on ]**

Turns annex-l DSL modulation off or on. Default is off.

**set physical dsl modulation annex-m [ off | on ]**

Turns annex-m DSL modulation off or on. Default is off.

**set physical dsl profile-8a [ on | off ]**

Enables or disables VDSL2 profile 8a governing upstream and downstream bandwidth. Default is on.

**set physical dsl profile-8b [ on | off ]**

Enables or disables VDSL2 profile 8b governing upstream and downstream bandwidth. Default is on.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set physical dsl profile-8c [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl profile-8d [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl profile-12a [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl profile-12b [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl profile-17a [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl profile-30a [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl bit-swap [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl trellis [ on</td>
<td>off ]</td>
</tr>
<tr>
<td>set physical dsl vectoring-enable [ off</td>
<td>on ]</td>
</tr>
<tr>
<td>set physical dsl vectoring-timeout-ms milliseconds</td>
<td>Specifies a timeout interval in milliseconds. Default is 5000. If vectoring-enable is set to on,</td>
</tr>
<tr>
<td>set physical dsl nlnm-threshold [ 0 - 480 ]</td>
<td>Specifies the New Low Noise Model (NLMN) value between 0 and 480. Default is 60.</td>
</tr>
<tr>
<td>set physical dsl transport [ atm</td>
<td>ptm</td>
</tr>
<tr>
<td>set physical dsl atm vcc 1 enable [ off</td>
<td>on ]</td>
</tr>
</tbody>
</table>
set physical dsl atm vcc 1 aal-type [ aal5 | aal0pkt | aal0cell ]
Sets the ATM Adaptation Layer type (aal-type): AAL5, AAL0-packet, or AAL0-cell. Default is aal5.

set physical dsl atm vcc 1 datapath [ phy0fast | phy0interleaved ]
Sets the ATM datapath, Fast Path or Interleaved. Default is phy0fast.

set physical dsl atm vcc 1 encap-type [ llcsnap-eth | llcsnap-rtip | llcencaps-ppp | vcmux-eth | vcmux-ipoa | vcmux-pppooa ]
 Specifies the data link encapsulation type. Default is llcsnap-eth.

set physical dsl atm vcc 1 vpi [ 0 - 255 ]
Sets the Virtual Path Identifier (vpi) for the circuit. Default is 0.

set physical dsl atm vcc 1 vci [ 32 - 65535 ]
Sets the Virtual Channel Identifier (vci) for the circuit. Default is 35.

set physical dsl atm vcc 2 enable [ off | on ]
Turns atm on or off on vcc 2. Default is on.

set physical dsl atm vcc 2 aal-type [ aal5 | aal0pkt | aal0cell ]
Sets the ATM Adaptation Layer type (aal-type): AAL5, AAL0-packet, or AAL0-cell. Default is aal5.

set physical dsl atm vcc 2 datapath [ phy0fast | phy0interleaved ]
Sets the ATM datapath, Fast Path or Interleaved. Default is phy0fast.

set physical dsl atm vcc 2 encap-type [ llcsnap-eth | llcsnap-rtip | llcencaps-ppp | vcmux-eth | vcmux-ipoa | vcmux-pppooa ]
Specifies the data link encapsulation type. Default is llcsnap-eth.

set physical dsl atm vcc 2 vpi [ 0 - 255 ]
Sets the Virtual Path Identifier (vpi) for the circuit. Default is 8.

set physical dsl atm vcc 2 vci [ 32 - 65535 ]
Sets the Virtual Channel Identifier (vci) for the circuit. Default is 35.

set physical dsl atm vcc vcc_num tx-queue queue_name
Attaches the egress queue template to the atm vc when the queue type is egress.

set physical dsl atm vcc vcc_num rx-queue queue_name
Attaches the ingress queue to the atm vc when the queue type is ingress.
set physical dsl ptm datapath [phy0fast | phy0interleaved]

Sets the ATM datapath, Fast Path or Interleaved. Default is phy0fast.

set physical dsl ptm priority [low | high]

Sets the Packet Transfer Mode (ptm) priority. Default is low.

set physical dsl ptm tx-queue queue_name

Attaches the egress queue template to the ptm interface when the queue type is egress.

set physical dsl ptm rx-queue queue_name

Attaches the ingress queue to the ptm interface when the queue type is ingress.

set physical dsl atm vcc 1 auto-vpi-vci [on | off]

Turns Automatic VPI/VCI Detection on or off. If you leave the default on, the device will try a series of VPI/VCI pairs that are commonly used by service providers. When one pair succeeds, the device will use this one for future connections.

set physical dsl atm vcc 1 vpi-vci-list vpi_vci_pairs

Specifies the series of VPI/VCI pairs that the device will use to attempt a connection. The default set ("0/35 8/35 0/43 0/51 0/59 8/43 8/51 8/59") may changed.

set physical dsl atm vcc 1 qos enable [off | on]

Turns QoS off or on on the virtual circuit. Default is off.

set physical dsl power-save enable [off | on]

Turns power saving mode off or on. Default is off.

Ethernet interfaces

set physical enet [1 - 4] mac-addr-override mac_addr

You can override your Gateway's Ethernet MAC address with any necessary setting. Some ISPs require your account to be identified by the MAC address, among other things. Enter your 12-character Ethernet MAC override address as instructed by your service provider, for example: 12 34 AB CD 19 64

set physical enet [1 - 4] port media [auto | 100-fd | 100-hd | 10-fd | 10-hd]

Sets the Ethernet port's media flow control: Automatic, 100 Mbps Full-Duplex, 100 Mbps Half-Duplex, 10 Mbps Full-Duplex, or 10 Mbps Half-Duplex. Default is auto.

set physical enet [1 - 4] port mdix [auto | on | off]

Sets the Ethernet port's crossover detection. Default is off.

set physical enet [1 - 4] tx-queue queue_name

Attaches the egress queue template to the ethernet interface when the queue type is egress.
**set physical enet [ 1 - 4 ] rx-queue queue_name**

Attaches the ingress queue to the ethernet interface when the queue type is ingress.

**set physical enet [ 1 - 4 ] port power-save enable ""**

Turns power saving mode off or on.

**set physical ensw max-age seconds**

Sets the maximum delay on the Ethernet switch in seconds. Default is 300 (5 minutes).

**set physical ensw qos-mode [ off | p-bit ]**

Sets QoS up on Ethernet switch, classified by priority-bit mapping. Default is off. When p-bit is selected, packets will be mapped from their priority (even if untagged) to one of four queues per-port in the Ethernet switch.

See “Quality of Service (QoS) Examples” on page 207 for more information.

**Note**

This only applies to packets sent from the host CPU to a switch port; it does not apply to port-to-port traffic.

**set physical ensw p-bit-map pbit-to-4queue-map**

Sets the mapping from the 8 priority-bits to the four queues in the Ethernet switch. The lowest priority queue is “1”, and the highest priority queue is “4”.

**Example:** Mapping is “1 1 2 2 3 3 4 4”, where priority bit values 0 and 1 would map to queue 1, and values 2 and 3 would map to queue 2, etc.

**Wireless interfaces**

**set physical wireless enable [ on | off ]**

Enables or disables the wireless capability for supported Wi-Fi Gateways. Default is on.

**set physical wireless standard [ bg | b-only | g-only | bgn | n-only | an | a-only ]**

Sets and locks the Gateway into the wireless transmission mode you want: bg, b-only, g-only, bgn, n-only, an, or a-only. For compatibility with clients using 802.11b (up to 11 Mbps transmission), 802.11g (up to 20+ Mbps), 802.11a (up to 54 Mbit/s using the 5 GHz band), or 802.11n (from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz), select B/G/N. To limit your wireless LAN to one mode or the other, select G-only, N-only, A-only, or B-only, or some combination that applies to your setup. Default is bgn.

**set physical wireless auto-channel [ off | on ]**

Turns auto-channel detection on or off.

**set physical wireless bandwidth [ narrow | wide ]**

Specifies whether the Wi-Fi channel is narrow or wide band. Default is narrow in compliance with FCC requirements.
**set physical wireless default-channel [ 1... 11 ]**

(1 through 11, for North America) on which the network will broadcast. This is a frequency range within the 2.4Ghz band. Channel selection depends on government regulated radio frequencies that vary from region to region. The widest range available is from 1 to 14. Europe, France, Spain and Japan differ. Channel selection can have a significant impact on performance, depending on other wireless activity close to this Router. Channel selection is not necessary at the client computers; the clients will scan the available channels seeking access points using the same SSID as the client. Defaults to 6.

**set physical wireless power [ 1 - 100 ]**

Sets some value lower than 100 percent transmit power if your Gateway is located close to other Wi-Fi Gateways and causes interference. Defaults to 100 (percent).

**set physical wireless mul2uni [ off | on ]**

Turns wireless “many-to-one” packet scheduling off or on. Default is off.

**set physical wireless ssid 1 enable [ on | off ]**

Enables or disables the first (default) Wi-Fi SSID.

**set physical wireless ssid 1 name name**

Specifies a name for the first Wi-Fi SSID. Defaults to a unique value per router of the form “ATTxxx”.

**set physical wireless ssid 1 access-type [ none | allow | deny ]**

Specifies the type of address list for defining MAC address filtering. If set to allow, only hosts with the specified addresses will be permitted to join the WLAN of the specified SSID. If set to deny, any hosts except those with the specified addresses will be permitted to join the specified SSID. Default is none.

**set physical wireless ssid 1 access-list mac_address**

Specifies the MAC address of devices controlled by MAC address filtering.

**set physical wireless ssid 1 hidden [ off | on ]**

Enables or disables “closed system mode” for the specified SSID. If set to on, the specified SSID will not appear on client scans. Clients must log into the SSID with the exact SSID name and credentials specified for that SSID.

**set physical wireless ssid 1 isolate [ off | on ]**

If set to on, blocks wireless clients from communicating with other wireless clients on the LAN side of the Gateway. Defaults to off.

**set physical wireless ssid 1 security [ none | wep | wpa ]**

Sets the wireless privacy type: none, wep, or wpa-psk. Default is none.

**set physical wireless ssid 2 enable [ off | on ]**

Enables or disables the second available SSID.
set physical wireless ssid 3 enable [ off | on ]

Enables or disables the third available SSID.

set physical wireless ssid 4 enable [ off | on ]

Enables or disables the fourth available SSID.

set physical wireless wps [ on | off ]

Enables or disables Wi-Fi Protected Setup (WPS) for simplified security configuration with Wi-Fi clients that support it.

set physical wireless wmm enable [ off | on ]

Enables or disables Wi-Fi Multimedia settings for multimedia queueing characteristics.

set physical wireless wmm power-save [ off | on ]

Turns power saving mode off or on for wireless multimedia when wmm enable is on. Default is on.

set physical wireless power-save enable [ off | on ]

Turns power saving mode off or on for all wireless services. Default is off.

**PPPoE relay commands**

set pppoe-relay enable [ on | off ]

Allows the Gateway to forward PPPoE packets. Default is on.

set pppoe-relay max-sessions [ 0... 4 ]

Specifies the maximum number of PPPoE relay sessions. Default is 4.
NAT Pinhole commands

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

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

The following list identifies protocol type and port number for common TCP/IP protocols:
- FTP (TCP 21)
- telnet (TCP 23)
- SMTP (TCP 25)
- TFTP (UDP 69)

**set pinhole name name protocol [ tcp | udp ]**

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

**set pinhole name name ext-port-range [ 0 - 49151 ]**

Specifies the first and last port number in the range being translated.

**set pinhole name name int-addr ipaddr**

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

**set pinhole name name int-start-port [ 0 - 65535 ]**

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

Security Stateful Packet Inspection (SPI) commands

**set security firewall-level [ low | high | off ]**

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.

The high setting is recommended, but for special circumstances, a low level of firewall protection is available. You can also turn all firewall protection off. Defaults to low.

**set security spi ip4 invalid-addr-drop [ on | off ]**

Enables or disables whether Broadband packets with invalid source or destination addresses should be dropped. Default is on.

**set security spi ip4 private-addr-drop [ on | off ]**

Enables or disables whether Broadband packets with private source or destination addresses should be dropped. Default is off.
set security spi unknown-ethertypes-drop [ on | off ]

Enables or disables whether packets with unknown ether types are to be dropped. Default is on.

set security spi portscan-protect [ on | off ]

Enables or disables whether to detect and drop port scans. Default is on.

set security spi invalid-tcp-flags-drop [ on | off ]

Enables or disables whether packets with invalid TCP flag settings (NULL, FIN, Xmas, etc.) are to be dropped. Default is on.

set security spi ip4 invalid-addr-drop [ on | off ]

Broad sets of addresses exist that should not be used as one or both of source or destination addresses. These include the following:

<table>
<thead>
<tr>
<th>IP address/mask</th>
<th>Source or destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>source</td>
</tr>
<tr>
<td>192.168.0.0.0/16</td>
<td>source</td>
</tr>
<tr>
<td>169.254.0.0/16</td>
<td>source</td>
</tr>
<tr>
<td>172.16.0.0/12</td>
<td>source</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>Source / destination</td>
</tr>
<tr>
<td>224.0.0.0/5</td>
<td>Source / destination</td>
</tr>
<tr>
<td>0.0.0.0/8</td>
<td>Source / destination</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>destination</td>
</tr>
</tbody>
</table>

The default is on.

set security spi ip4 private-addr-drop [ off | on ]

Drops packets sourced or destined for private IPv4 addresses. The default is off.

set security spi flood-limit enable [ on | off ]

Enables or disables whether packet flooding should be detected and offending packets be dropped. Default is on.

set security spi flood-limit limit pps_value

Sets a maximum Packets Per Second (PPS) value for packet flood criterion. Defaults to 4.

set security spi flood-limit burst-limit max_value

Sets a maximum value in a packet-burst for packet flood criterion. Defaults to 8.

set security spi flood-limit icmp enable [ on | off ]

Enables or disables whether ICMP packet flooding should be detected and offending packets be dropped. Defaults to on.
set security spi flood-limit udp enable [ off | on ]

Enables or disables whether UDP packet flooding should be detected and offending packets be dropped. Defaults to off.

set security spi flood-limit tcp enable [ off | on ]

Enables or disables whether TCP packet flooding should be detected and offending packets be dropped. Defaults to off.

set security spi flood-limit tcp syn-cookie [ on | off ]

Allows TCP SYN cookies flooding to be excluded. Defaults to on.

**Reflexive ACL**

set security spi ip6 allow-inbound [ on | off ]

Turns reflexive ACL on or off for IPv6.

Reflexive Access Control Lists (ACL) provide that layer 4 Session information is used to make decisions about what packets to route. Reflexive ACL reduces exposure to spoofing and denial-of-service attacks, because desired inbound packet flows are usually in response to outbound traffic.

Motorola 9.x DSL Gateways use the relevant session information about whether the packet flow was initiated from the LAN side (upstream) or WAN side (downstream). If the parameter security.spi.ip6.allow-inbound is set to off, then sessions which are initiated from the WAN side are disallowed. Upstream sessions are never precluded because of reflexive ACL. (Of course there may be other reasons that particular packets are dropped.)

For IPv4, NAT is generally enabled, so reflexive ACL is usually not an issue.

**VoIP commands**

(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 Gateway models have one or more voice ports for connecting telephone handsets. These models support VoIP. If your Gateway is a VoIP model, you can configure the VoIP features.

set voip phone n sip-option [ off | on ]

Turns SIP on or off for the phone specified by n, usually 1 or 2, depending on your Gateway's number of physical voice ports. Default is off.

set voip phone n sip-proxy-server [ server_name | ip_address ]

Specifies the SIP proxy server for the specified phone by fully qualified server name or IP address.

set voip phone n sip-proxy-server-port [ 1 - 65535 ]

Specifies the SIP proxy server port number for the specified phone. Default is 5060.

set voip phone n sip-proxy-server-transport [ udp | tcp ]

Specifies the SIP proxy server transport protocol for the specified phone. Default is UDP.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`set voip phone n sip-registrar-server [ server_name</td>
<td>ip_address ]`&lt;br&gt;Specifies the SIP registration server for the specified phone by fully qualified server name or IP address.</td>
</tr>
<tr>
<td><code>set voip phone n sip-registrar-server-port [ 1 - 65535 ]</code>&lt;br&gt;Specifies the SIP registration server port number for the specified phone. Default is 5060.</td>
<td></td>
</tr>
<tr>
<td>`set voip phone n sip-registrar-server-transport [ udp</td>
<td>tcp ]`&lt;br&gt;Specifies the SIP registration server transport protocol for the specified phone. Default is UDP.</td>
</tr>
<tr>
<td><code>set voip phone n sip-expires-time [ 5 - 65535 ]</code>&lt;br&gt;Specifies the SIP registration server time-out duration from 0 – 65535 seconds for the specified phone. Default is 3600 (1 hour).</td>
<td></td>
</tr>
<tr>
<td>`set voip phone n sip-outproxy-server [ server_name</td>
<td>ip_address ]`&lt;br&gt;Specifies the SIP outbound proxy server for the specified phone by fully qualified server name or IP address.</td>
</tr>
<tr>
<td><code>set voip phone n sip-outproxy-server-port [ 1 - 65535 ]</code>&lt;br&gt;Specifies the SIP outbound proxy server port for the specified phone. Default is 5060.</td>
<td></td>
</tr>
<tr>
<td><code>set voip phone n sip-user-display-name name</code>&lt;br&gt;Specifies the user name that is displayed on the web UI Home page, or other caller-id displays for the specified phone.</td>
<td></td>
</tr>
<tr>
<td><code>set voip phone n sip-user-name username</code>&lt;br&gt;Specifies the user name that authenticates the user to SIP for the specified phone.</td>
<td></td>
</tr>
<tr>
<td><code>set voip phone n sip-user-password password</code>&lt;br&gt;Specifies the password that authenticates the user to SIP for the specified phone.</td>
<td></td>
</tr>
<tr>
<td><code>set voip phone n auth-id string</code>&lt;br&gt;Specifies the authorization ID that authenticates the user to SIP for the specified phone. Most SIP Servers expect this to be the username itself but some may use auth-id.</td>
<td></td>
</tr>
<tr>
<td><code>set voip phone n sip-user-port [ 1 - 65535 ]</code>&lt;br&gt;Specifies the SIP user port for the specified phone, Default is 5060.</td>
<td></td>
</tr>
<tr>
<td>`set voip phone n codec G711U priority [ 1</td>
<td>2</td>
</tr>
<tr>
<td>`set voip phone n codec G711A priority [ 1</td>
<td>2</td>
</tr>
</tbody>
</table>
**set voip phone** \( n \) **codec** G729 priority [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | none ]

Assigns a priority to the *G729 annex A* codec, the common analog voice compression implementation used in North America.

**set voip phone** \( n \) **codec** G726_16 priority [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | none ]

Assigns a priority to the *G726-16* codec, a common audio media type implementation at 16 kbit/s.

**set voip phone** \( n \) **codec** G726_24 priority [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | none ]

Assigns a priority to the *G726-24* codec, a common audio media type implementation at 24 kbit/s.

**set voip phone** \( n \) **codec** G726_32 priority [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | none ]

Assigns a priority to the *G726-32* codec, a common audio media type implementation at 32 kbit/s.

**set voip phone** \( n \) **codec** G726_40 priority [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | none ]

Assigns a priority to the *G726-40* codec, a common audio media type implementation at 40 kbit/s.

**Advanced settings**

**set voip phone** \( n \) **sip-advanced-setting** sip-dtmf-mode [ inband | rfc2833 | info ]

`sip-dtmf-mode` — sets the Dual Tone Multi-Frequency Mode:
- **inband**: sends the DTMF digits as a normal inband tone.
- **rfc2833**: (default) sends the DTMF digits as an event as part of the RTP packet header information.
- **info**: sends the DTMF digits in the SIP INFO message.

**set voip phone** \( n \) **sip-advanced-setting** sip-hk-flash-mode [ cpe | info ]

Sets the behavior of the flash hook mode for the specified phone line. Default is info.

**set voip phone** \( n \) **sip-advanced-setting** sip-session-refresher [ local | remote | auto ]

Sets the method for refreshing the SIP session. Default is auto.

**set voip phone** \( n \) **sip-advanced-setting** sip-dynamic-payload [ 96 - 110 ]

Specifies a default dynamic payload value for a named telephony event. Default is 101.

**set voip phone** \( n \) **sip-advanced-setting** sip-digit-map string

Specifies rules used to recognize a number dialed by the user and to ensure this number matches the dial plan defined by the ITSP.

**set voip phone** \( n \) **sip-advanced-setting** sip-compact-header [ off | on ]

Forces all headers in the message to use compact format when set to on. Sends the SIP messages with Compact Headers, reducing the size of the SIP messages.
**set voip phone** n sip-advanced-setting sip-q-value [0 - 10]

This is used to prioritize the SIP account based on the value.

**set voip phone** n sip-advanced-setting sip-qos-tos-value [0 - 255]

Specifies the SIP Diff-Serv Type of Service (ToS) values for Quality of Service (QoS) assignment. Default is 136.

**set voip phone** n sip-advanced-setting sip-qos-p-bit-value [0 - 7]

Sets a QoS P-bit value for the SIP session. Default is 6.

**set voip phone** n sip-advanced-setting sip-qos-marker-value value

Sets a QoS marker on the SIP session packets on the specified phone line.

**set voip phone** n sip-advanced-setting rtp-qos-tos-value [0 - 255]

Specifies the RTP Diff-Serv Type of Service (ToS) values for Quality of Service (QoS) assignment. Default is 184.

**set voip phone** n sip-advanced-setting rtp-qos-p-bit-value [0 - 7]

Sets a QoS P-bit value for the RTP session. Default is 6.

**set voip phone** n sip-advanced-setting rtp-qos-marker-value value

Sets a QoS marker on the RTP session packets on the specified phone line.

**set voip phone** n sip-advanced-setting fax-redundancy-level [0 - 1]

Specifies the level of fax redundancy for t38 fax data rate management.

**set voip phone** n sip-advanced-setting sip-init-de-register [off | on]

Turns SIP de-registration on or off. Default is off.

**set voip phone** n sip-advanced-setting sip-known-ip-list string

Specifies a known IP address list of SIP servers for the SIP session.

**Advanced telephony settings**

The telephony features include advanced settings for fine tuning phone behavior. The following codecs and associated value defaults are supported:

<table>
<thead>
<tr>
<th></th>
<th>Codec G711U</th>
<th>Codec G711A</th>
<th>Codec G729</th>
<th>Codec G726_16</th>
</tr>
</thead>
<tbody>
<tr>
<td>packetization-time</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>jitter-max-reorder-delay</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>jitter-max-accept-late-seq-num</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>jitter-initial-delay</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>jitter-exe-frame-del-mode</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
</tbody>
</table>
Syntax is as follows:

```
set voip advanced-telephony-setting codec codec packetization-time value

set voip advanced-telephony-setting codec codec jitter-max-reorder-delay value

set voip advanced-telephony-setting codec codec jitter-max-accept-late-seq-num value

set voip advanced-telephony-setting codec codec jitter-initial-delay value

set voip advanced-telephony-setting codec codec jitter-exe-frame-del-mode [ off | on ]

set voip advanced-telephony-setting codec codec jitter-max-transit-delay value

set voip advanced-telephony-setting codec codec jitter-peak-transit-delay value

set voip advanced-telephony-setting codec codec jitter-delay-buff-inc value
```
set voip advanced-telephony-setting codec codec
    jitter-transit-delay-threshold value

set voip advanced-telephony-setting fxs-port-setting-for-fxo
    [ none | fxs1 | fxs2 | both | emgncy ]
Sets a port to be used for the FXS (Foreign eXchange Subscriber interface) port to the FXO (Foreign eXchange Office interface -- the phone) port. Default is none.

set voip advanced-telephony-setting rtp-port-range-start value
set voip advanced-telephony-setting rtp-port-range-end value
Sets the start and end port values for the RTP port range. Although no ports are specified for the RTP protocol, the RTP data is to be carried on an even UDP port number. The defaults in use for the Motorola Gateway are 8024 and 8036, respectively.

set voip advanced-telephony-setting rtcp-option [ off | on ]
Turns Real-Time Transport Control Protocol on or off. RTCP supports and controls RTP media streams, but does not itself deliver media streams. Default is off.

set voip advanced-telephony-setting t38-option [ off | on ]
Turns T.38 fax capability on or off. Default is off.

set voip advanced-telephony-setting sip-session-timer-value seconds
Sets a timer in seconds for SIP sessions to periodically verify that an established session is still active. Default is 2280.

set voip advanced-telephony-setting sip-t1-timer-value milliseconds
Sets a SIP T1 timer value, an estimate of the round trip time, in milliseconds from 100 – 5000. Default is 500.

set voip advanced-telephony-setting sip-dynamic-line-selection [ off | on ]
Turns dynamic (next available) line selection off or on. Default is off.

set voip RegionSpecificSettings Region-Code region_code
Specifies the set of standards in use for the geographical region. Example: "USA_DEFAULT".

set voip RegionSpecificSettings fxs-hook-flash-min-time seconds
Specifies the minimum Foreign Exchange Station (FXS) hookflash time in seconds. Default is 280.

set voip RegionSpecificSettings fxs-hook-flash-max-time seconds
Specifies the maximum Foreign Exchange Station (FXS) hookflash time in seconds. Default is 1100.

set voip RegionSpecificSettings fxs-debounce-onoff-hook-delay seconds
Specifies the on/off-hook debounce time delay for removing the ripple signal, in seconds. Default is 100.
set voip RegionSpecificSettings fxs-debounce-off-on-hook-delay seconds

Specifies the off/on-hook debounce time delay for removing the ripple signal, in seconds. Default is 300.

---

Call feature settings

set voip phone n call-feature call-forwarding-all-option [ off | on ]

call-forwarding-all-option – turns unconditional call forwarding on or off.

set voip phone n call-feature call-forwarding-on-busy-option [ off | on ]

call-forwarding-on-busy-option – turns call forwarding when line is busy on or off. Default is off.

set voip phone n call-feature call-forwarding-on-no-answer-option [ off | on ]

call-forwarding-on-no-answer-option – turns call forwarding when there is no answer on or off.

set voip phone n call-feature call-waiting-option [ off | on ]

call-waiting-option – enables or disables call waiting.

set voip phone n call-feature call-conferencing-option [ off | on ]

call-conferencing-option – enables or disables 3-way call conferencing.

set voip phone n call-feature do-not-disturb-option [ off | on ]

do-not-disturb-option – enables or disables option to prevent the phone from ringing.

set voip phone n call-feature subscribe-mwi-option [ off | on ]

subscribe-mwi-option – if set to on, the Message Waiting Indicator is enabled when new voice mail is received.

set voip phone n call-feature anonymous-call-block-option [ off | on ]

anonymous-call-block-option – if set to on, blocks calls from unidentified sources, such as those with caller-ID blocking.

set voip phone n call-feature call-transfer-option [ off | on ]

call-transfer-option – if set to on, permits call transfer to another phone.

---

DSP settings

set voip phone n dsp-settings echo-option [ echo-off | echo-on | echo-on-nlp | echo-on-cng-nlp ]

echo-option – specifies under what conditions the system invokes or disables echo cancellation. Default is echo-on-cng-nlp (Comfort Noise Generation with non-linear processor).

set voip phone n dsp-settings echo-start-attenuation [ 0 - 65535 ]

echo-start-attenuation – specifies the minimum attenuation level at which to invoke echo cancellation. Default is 8192.
set voip phone \( n \) dsp-settings echo-max-attenuation [ 0 - 65535 ]

`echo-max-attenuation` – specifies the maximum attenuation level at which to invoke echo cancellation. Default is 16384.

set voip phone \( n \) dsp-settings echo-tail-length [ 0 - 65535 ]

`echo-tail-length` – specifies the duration of an echo tail required to invoke cancellation. Default is 0.

set voip phone \( n \) dsp-settings vad-option [ off | on ]

When `vad-option` is set to on – enables Voice Activity Detection/Comfort Noise Generation. When speech is not present, the CNG algorithm generates a noise signal at the level sent from the transmit side.
**System commands**

**set system name name**

Specifies the name of your Motorola Gateway. Each Motorola Gateway is assigned a name as part of its factory initialization. The default name for a Motorola Gateway consists of the word “Motorola-7000/XXX” where “XXX” is the serial number of the device; for example, Motorola-7000/9437188. A system name can be 1 – 255 characters long. Once you have assigned a name to your Motorola Gateway, you can enter that name in the Address text field of your browser to open a connection to your Motorola Gateway.

![NOTE:

Some broadband cable-oriented Service Providers use the **System Name** as an important identification and support parameter. If your Gateway is part of this type of network, **do NOT** alter the System Name unless specifically instructed by your Service Provider.

**set system time-zone [ UTC | HST10 | AKST9AKDT | YST8 | PST8PDT | MST7MDT | MST7 | CST6CDT | CST6 | EST5EDT | AST4ADT | NST3:30NDT ]**

time-zone of 0 is Coordinated Universal Time (UTC); options are -12 through 12 (+/- 1 hour increments from UTC time).

**set system auto-daylight-savings [ on | off ]**

Time zones honoring Daylight Saving Time may be automatically designated.

**set system firewall-log enable [ on | off ]**

Turns firewall logging on or off. The firewall log tracks attempted violations of the firewall rules. Default is on.

**set system firewall-log persist [ on | off ]**

When set to on, causes the log information to be kept in flash memory. Default is off.

**set system firewall-log file-size [ 4096... 65536 ]**

Specifies a size for the firewall logs. The most recent entries are posted to the beginning of the log. When the log becomes full, the oldest entries are dropped. The default is 16384.

**set system firewall-log file-count [ 2... 8 ]**

Specifies the number of possible log files. The default is 4.

**set system fastpath software-enable [ on | off ]**

Enables or disables the fastpath accelerator processor. Fastpath works on only TCP and UDP. Default is on.

**set system fastpath hardware-enable [ off | on ]**

Enables or disables the fastpath accelerator processor. Default is off.

**set system fastpath mcast-mode 3**

Sets the mode for multicast on the fastpath accelerator processor.
set system scheduler enable [ off | on ]

Turns the system scheduler feature on or off. The default is off.

set system scheduler enable-time hr:min

Specifies a time at which to turn the system on. Default is midnight (00:00). enable-time must be supplied in 24 hour military time, colon separated, for example "05:21".

set system scheduler disable-time hr:min

Specifies a time at which to turn the system off. Default is 5 o’clock (05:00). disable-time must be supplied in 24 hour military time, colon separated, for example "21:44".

set system calendar-update enable [ on | off ]

Turns the calendar update feature on or off. The device will periodically poll the update server for new operating system software. The default is on.

set system calendar-update interval [ monthly | biweekly ]

Specifies how often the device should poll the update server, monthly or biweekly. The default is monthly.

set system calendar-update protocol [ http | https | tftp ]

Specifies the protocol for accessing the update server. The default is http.

set system calendar-update server server_address

Specifies the address of the update server by name or IP address. The default is "cpems.bellsouth.net".

set system calendar-update username string

Specifies the username for the update server. The default is "anonymous".

set system calendar-update password string

Specifies the password for the update server. The default is "guest".

set system calendar-update fwverfile filename

Specifies the firmware version filename to the update server. For the AT&T NVG589 the file is "netopiaNVG589_64.txt".

set system calendar-update day day_of_month

Specifies the numerical day of the month for the update server to be polled, for example, "21".

set system calendar-update time hr:min_AMPM

Specifies the time of day for the update server to be polled, in the form HOUR:MINUTEAM/PM. Example: "06:00AM"
set system supplicant enable [ on | off ]

Turns on the 802.1x supplicant functionality. You must set the corresponding "type" field in the WAN link to activate it:

```
NOS/142253966608 (top)>> set link name WAN supplicant
  supplicant
    type (none) [ none | eap-tls ]:
    priority (0) [ 0 - 7 ]:
```

Default is on.

set system supplicant dest-broadcast [ off | on ]

Mostly useful for debugging. If this is set to on, the destination MAC address FF:FF:FF:FF:FF:FF is used when the supplicant sends 802.1x packets. If this is off, the EAPOL-specific destination address of 01:80:C2:00:00:03 is used. Default is off.

set system supplicant eap-tls-identity string

Sets the identity sent by the supplicant in response to an Identity request from an 802.1x authenticator.

set system supplicant server-cert-check [ on | off ]

If set to on, examines the certificate chain sent by an 802.1x authenticator for validation, and ensures that the root cert of this chain is accepted by the CPE (i.e. in its trust list). Default is on.

set system voice-check enable [ off | on ]

When this is set to on, and a voice call is in progress when a software update is scheduled, the software update is deferred for the voice-check interval until the call is completed, that is, the call state becomes “idle.” If set to off, and a voice call is in progress when an update is scheduled, the call is torn down. The default is on.

set system voice-check interval [ 60 - 86400 ]

This specifies the interval in seconds for the device to wait before attempting a software update, when a software update is scheduled but a voice call is in progress, when voice-check enable is set to on. The default is 300 (5 minutes).

set system voice-check max-time [ 300 - 604800 ]

This specifies the maximum time in seconds for the device to continue to attempt a scheduled software update if a voice call is in progress and voice-check enable is set to on. The default is 3600 (1 hour).

set system log buffer-size [ 4096... 65536 ]

Specifies a size for the system log. The most recent entries are posted to the beginning of the log. When the log becomes full, the oldest entries are dropped. The default is 16384.

set system log level [ low | medium | high | alerts | failures ]

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

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

When you are in SHELL mode, the DEBUG prompt is the name of the Motorola Gateway/DEBUG followed by a right angle bracket (>). For example, if you open a CLI connection to the Motorola Gateway named “Motorola-3000/9437188,” then type “debug” you would see Motorola-3000/9437188/DEBUG> as your prompt.

Debug level is available for field debugging purposes. There is no service and quality level guarantee from Motorola. This level is intended for SEs or Telsos lab people, not for normal operation at home for end users.

Disclaimer & Warning Text

The following is displayed when entering Debug level from normal Config level.

“Warning: Accessing these commands may impact the normal operation of this device. Exit now if you entered by mistake.”

Commands

console

Make this session the console.

mirror <src-port> <dst-port>

To mirror one port’s traffic to another. Causes traffic transmitted or received on <src-port> to be mirrored on <dst-port>. Ports must support Ethernet (IPoA and PPPoA ATM ports are not supported).

mirror off

Turns off port mirroring.

show fastpath

Displays entries in fastpath.

show cpu

Displays CPU Usage as a percentage and CPU Load Averages over 1, 5 and 15 minute periods.
CHAPTER 5 Technical Specifications and Safety Information

Description

Dimensions:  
10 in H x 7.25 in L x 1.63 in W (25.4 cm H x 18.4 cm L x 4.1 cm W)  
1.28 lbs (.58 kg) (without integrated battery)  
1.77 lbs (.80 kg) (with integrated battery)

Communications interfaces: The Motorola® Gateways have a 4-port 10/100/1000Base-T Ethernet switch for your LAN connections, an FXS port for VoIP connections, a HomePNA 3.1 coax port, a USB 2.0 network port, and a 400 mW wireless radio for Wi-Fi connections.

WAN interfaces: Bonded VDSL2/single line VDSL2/bonded ADSL2+/single line ADSL, RJ-14; One-port 10/100/1000 Ethernet, RJ-45

Power Supply  
- 115VAC 36W/12VDC@3A (2phone,5REN, RINGING)

Environment

Operating temperature: 0 °C to 42 °C (32 °F to 107 °F); 8% to 95% (Non Condensing) Relative Humidity

Storage temperature: –20 °C to 85 °C (–4 °F to 185 °F)

Relative storage humidity: 20 to 80% noncondensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via CLI or web upload.

Routing: IPv4, IPv6/6rd; DHCP server/relay; DNS Proxy, Dynamic DNS Support; Multiple subnet support

WAN support: PPPoA, DHCP, static IP address; ADSL, ADSL2/2+, ADSL2 Reach Extended protocol (ITU G.992.3 annex L)

Security: Stateful Packet Inspection Firewall; Virtual DMZ/IP pass-through; Denial of Service (DoS) protection; VPN Pass-through (PPTP, L2TP, IPSec)

Wi-Fi Security. WEP (64-bit, 128-bit, 256-bit) encryption 802.1x, WPA, WPA-PSK, 802.11i/WPA2, WPA2-PSK EAP-TLS, EAP-TTLS, EAP-SIM MAC Address filtering
Management/configuration methods: HTTP (Web server), telnet command line interface

Diagnostics: Ping, event logging, routing table displays, statistics counters, web-based management, traceroute, nslookup, and diagnostic commands.

Agency approvals

North America
Safety Approvals:
- United States – UL 60950, Third Edition
- Canada – CSA: CAN/CSA-C22.2 No. 60950-00

EMC:
- United States – FCC Part 15 Class B
- Canada – ICES-003

Telecom:
- United States – 47 CFR Part 68
- Canada – CS-03

Integrated Battery:
- Hazardous Materials Regulations and Procedures CFR Title 49, Section 173,
- Subsection 185
- UL60950/CAN/CSA-C22.2 No. 60950—Recognized component (U.S. and Canada)
- UL 2054—Recognized component (U.S. and Canada)
- UN Manual of test and Criteria, sect. 38.3, CE, IEC62133
- California Code of Regulation Title 20
Manufacturer’s Declaration of Conformance

Warnings:

This is a Class B product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

United States. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Service requirements. In the event of equipment malfunction, if under warranty we will exchange a product deemed defective. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.

Technical Support for Hardware Products
1-877-466-8646
http://www.motorola.com/support

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This Class B digital apparatus meets all requirements of the Canadian Interference -Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Declaration for Canadian users

NOTICE: The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Department does not guarantee the equipment will operate to the user’s satisfaction.
Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company’s inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

**Caution**

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.
Important Safety Instructions

Caution
DO NOT USE BEFORE READING THE INSTRUCTIONS: Do not connect the Ethernet ports to a carrier or carriage service provider’s telecommunications network or facility unless: a) you have the written consent of the network or facility manager, or b) the connection is in accordance with a connection permit or connection rules.

Connection of the Ethernet ports may cause a hazard or damage to the telecommunication network or facility, or persons, with consequential liability for substantial compensation.

Caution
- The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply near the product for easy access.
- For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.0A.

Telecommunication installation cautions
- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
47 CFR Part 68 Information

FCC Requirements

1. The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.

2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.

3. The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.

4. If the telephone company requests information on what equipment is connected to their lines, inform them of:
   a. The telephone number to which this unit is connected.
   b. The ringer equivalence number. [0.XB]
   c. The USOC jack required. [RJ11C]
   d. The FCC Registration Number. [XXXUSA-XXXX-XX-E]

   Items (b) and (d) are indicated on the label. The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN’s of all devices on any one line should not exceed five (5.0). If too many devices are attached, they may not ring properly.

FCC Statements

a) This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

b) List all applicable certification jack Universal Service Order Codes (“USOC”) for the equipment: RJ11.

c) A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

d) The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2002, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

e) If this equipment, the Motorola® Gateway, causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn’t practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

f) The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

g) If trouble is experienced with this equipment, the Motorola® Gateway, for warranty information, please contact:
   Technical Support for Hardware Products
   1-877-466-8646
   http://www.motorola.com/support

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

h) This equipment not intended to be repaired by the end user. In case of any problems, please refer to the troubleshooting section of the Product User Manual before calling Motorola Technical Support.

i) Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
j) If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this Motorola® Series Gateway does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or qualified installer.

RF Exposure Statement:

NOTE: Installation of the wireless models must maintain at least 20 cm between the wireless Gateway and any body part of the user to be in compliance with FCC RF exposure guidelines.

Electrical Safety Advisory

Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources. This has been identified as a major nationwide problem. Therefore it is advised that this equipment be connected to AC power through the use of a surge arrestor or similar protection device.
Caring for the Environment by Recycling

When you see this symbol on a Motorola product, do not dispose of the product with residential or commercial waste.

Recycling your Motorola Equipment

Please do not dispose of this product with your residential or commercial waste. Some countries or regions, such as the European Union, have set up systems to collect and recycle electrical and electronic waste items. Contact your local authorities for information about practices established for your region.

If collection systems are not available, call Motorola Customer Service for assistance.

Please visit www.motorola.com/recycle for instructions on recycling.
Uw Motorola-materiaal recycleren.
Gooi dit product niet bij het huishoudelijk afval het of bedrijfsafval. In sommige landen of regio's zoals de Europese Unie, zijn er bepaalde systemen om elektrische of elektronische afvalproducten in te zamen en te recycleren. Neem contact op met de plaatselijke overheid voor informatie over de geldende regels in uw regio. Indien er geen systemen bestaan, neemt u contact op met de klantendienst van Motorola.

Recykling posiadanego sprzętu Motorola
Produktu nie należy wyrzucać do komunalnych pojemników na śmieci. W niektórych krajach i regionach, np. w Unii Europejskiej, istnieją systemy zbierania i recyklingu sprzętu elektrycznego i elektronicznego. Informacje o utylizacji tego rodzaju odpadów należy uzyskać od władz lokalnych. Jeśli w danym regionie nie istnieją systemy zbierania odpadów elektrycznych i elektronicznych, informacje o utylizacji należy uzyskać od biura obsługi klienta firmy Motorola (Motorola Customer Service).

Reciclagem do seu equipamento Motorola
Não descarte este produto junto com o lixo residencial ou comercial. Alguns países ou regiões, tais como a União Européia, criaram sistemas para coletar e reciclar produtos eletrônicos. Para obter informações sobre as práticas estabelecidas para sua região, entre em contato com as autoridades locais. Se não houver sistemas de coleta disponíveis, entre em contato com o Serviço ao Cliente da Motorola para obter assistência.

Återvinning av din Motorola-utrustning

リサイクルによる環境保護
モトローラ製品にこの記号が表示されている場合、製品を家庭または商用廃棄物として処分しないでください。欧州連合などの国または地域にとっては、電気的・電子的廃棄物を収集およびリサイクルするシステムがあります。お住まいの地域で決められている方法についての情報は、地方自治体にお問い合わせください。收集システムがない場合、モトローラ・カスタマーサービスまでお問い合わせください。

재활용으로 환경 보호하기
Motorola 제품에 이 표시가 있는 경우, 가정 또는 상업 폐기물과 함께 버리지 마십시오. 유럽 유니온과 같은 일부 국가 또는 지역에서는 재활용 및 전기 전자 폐기물 환경을 수집하는 시스템이 구축되어 있습니다. 해당 지역에 구축되어 있는 푸른색의 환경 정보는 지역 과활달로에 연락하십시오. 수집 시스템이 존재하지 않는 경우, 도움을 받기 위해 Motorola 고객서비스부로 연락하십시오.

Motorola 기기 재활용
이 제품을 가정용 또는 사업용 폐기물과 함께 버리지 마십시오. 유럽 유니온과 같은 일부 국가 또는 지역에서는 재활용 및 전기 전자 폐기물 환경을 수집하는 시스템이 구축되어 있습니다. 해당 지역에 구축되어 있는 푸른색의 환경 정보는 지역 과활달로에 연락하십시오. 수집 시스템이 존재하지 않는 경우, 도움을 받기 위해 Motorola 고객서비스부로 연락하십시오.
重复利用，保护环境
如果 Motorola
产品上具有这个标识，请勿将产品
丢弃到家庭或商业垃圾中。

Motorola 设备的重复利用
请勿将本产品丢弃到家庭或商业垃圾中。某些国家或地区，
例如欧盟，
已经建立起回收和重复利用电气与电子废弃物的体系。请与当地相
关机构联系，获取有关所在地区相关规定的信息。如果当地尚未建
立回收体系，请致电 Motorola 客户服务以寻求帮助。

注意环保问题
在您看到产品上有 Motorola 的标志
时，勿以家用或商用的废弃物方
式处理。

Motorola 设备的回收
请勿将本产品丢弃到家庭或商业垃圾中。某些国家或地区，如欧盟，
已对废弃的电器和电子产品制定回收以及再利用体制。请与您所在
地的管理机构咨询相关规定。
若您所在的地区尚未设置回收机制，请致电 Motorola 客户服务咨询相关
事宜。

Please visit http://www.motorola.com/recycle for instructions on recycling.
Copyright Acknowledgments

Because Motorola has included certain software source code in this product, Motorola includes the following text required by the respective copyright holders:

Open Source Software Information
For instructions on how to obtain a copy of any source code being made publicly available by Motorola related to software used in this Motorola product you may send your request in writing to:
Motorola, Inc.
OSS Management
2450 Walsh Avenue
Santa Clara, CA 95051
USA
The Motorola website opensource.motorola.com also contains information regarding Motorolaís use of open source. Motorola has created the opensource.motorola.com to serve as a portal for interaction with the software community-at-large.
This document contains additional information regarding licenses, acknowledgments and required copyright notices for open source packages used in this Motorola product.

aiccu 2007.01.15
The SixXS License - http://www.sixxs.net/
Copyright (C) SixXS <info@sixxs.net>
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 SixXS nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior permission.

THIS SOFTWARE IS PROVIDED BY SIXXS 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 SIXXS 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.

dhcp (dhcp-isc) 4.1.1-P1
Copyright © 2004-2011 by Internet Systems Consortium, Inc. ("ISC")
Copyright © 1995-2003 by Internet Software Consortium
Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

DropBear 0.52
Copyright (c) 2002-2006 Matt Johnston Portions
Copyright (c) 2004 Mihnea Stoenesescu All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than “ssh” or “Secure Shell”."

Copyright (c) 2000 Andre Lucas. All rights reserved.
Portions copyright (c) 1998 Todd C. Miller
Portions copyright (c) 1996 Jason Downs
Portions copyright (c) 1996 Theo de Raadt

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 "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 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.

Copyright 1997-2003 Simon Tatham.
copyright Robert de Bath, Joris van Rantwijk, Delian Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Portions Delchev, Justin Bradford, and CORE SDI S.A.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Encryption
Aaron D. Gifford License
Copyright (c) 2000-2001, Aaron D. Gifford
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 copyright holder nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTOR(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 AUTHOR OR CONTRIBUTOR(S) 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.
RSA Data Security License
Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.
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. 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.

expat 1.95.7
Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
and Clark Cooper
Copyright (c) 2001, 2002 Expat maintainers.
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:
The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.
The SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GNU General Public License 2.0 (GPL)
This Motorola product contains the following open source software packages licensed under the terms of the
GPL 2.0 license:
* Linux 2.6.30
* Arptables 0.0.3-4
* bridge-utils 1.2
* busybox 1.18.3
* dnsmasq 2.45
* ez-ipupdate 3.0.11b7
* haserl 0.9.26
* inld
* iproute2
* iptables 1.4.0
* ntpclient 2003_194
* pppd 2.4.4
* rp-pppoe 3.10
* samba 3.0.25a
* udev 136
* vconfig 1.6
* wget 1.10.2
* zebra 0.94

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble
The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation’s software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

    c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is
void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under
this License will not have their licenses terminated so long as such
parties remain in full compliance.

5. You are not required to accept this License, since you have not
signed it. However, nothing else grants you permission to modify or
distribute the Program or its derivative works. These actions are
protected by law if you do not accept this License. Therefore, by
modifying or distributing the Program (or any work based on
the Program), you indicate your acceptance of this License to do so, and
all its terms and conditions for copying, distributing or modifying
the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License 2.1 (LGPL)

This Motorola product contains the following open source software packages licensed under the terms of the LGPL 2.1 license:

* uClibc 0.9.29

Version 2.1, February 1999
Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but you should consider it less advantageous than the ordinary General Public License.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that you have. This means that you must make sure that each recipient, in addition to all of the others, can receive the entire source code of the library in the same form as you received it. You must make the sameétractions with all your users.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library." The former contains code derived from the library, whereas the latter must be combined with the library in order to run.
0. This License Agreement applies to any software library or other program which contains a notice placed by
the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General
Public License (also called “this License”). Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with
application programs (which use some of those functions and data) to form executable programs.

The “Library”, below, refers to any such software library or work which has been distributed under these terms. A
“work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a
work containing the Library or a portion of it, either verbatim or with modifications and/or translated
straightforwardly into another language. (Hereinafter, translation is included without limitation in the term
“modification”.

“Source code” for a work means the preferred form of the work for making modifications to it. For a library,
complete source code means all the source code for all modules it contains, plus any associated interface
definition files, for example header files, minus the scripts used to control compilation and installation of the
Library, and the scripts needed to re-create the object files or data files should the original source code not
be available. The “user” of a work means either you or a third party authorized by you to distribute to the
public the work under the terms of this License. A “modified version” of the work means either the original
version, as you received it, or any changes you or others have made under this License. To “distribute” a
work means to pass it to a third party.

Activities other than copying, distribution and modification are not covered by this License; they are outside its
scope. The act of running a program using the Library is not restricted, and output from such a program is
covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool
for writing it). Whether that is true depends on what the Library does and what the program that uses the Library
does.

1. You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any
medium, provided that you conspicuously and appropriately provide on each copy an appropriate copyright
notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of
any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty
protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the
Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you
also meet all of these conditions:

   a) The modified work must itself be a software library.

   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date
      of any change.

   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this
      License.

   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application
      program that uses the facility, other than as an argument passed when the facility is invoked, then you must
      make a good faith effort to ensure that, in the event an application does not supply such function or table, the
      facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined
   independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table
   used by this function must be optional: if the application does not supply it, the square root function must still
   compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived
from the Library, and can be reasonably considered independent and separate works in themselves, then this
License, and its terms, do not apply to those sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole
must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus
to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather,
the intent is to exercise the right to control the distribution of derivative or collective works based on the
Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on
the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this
License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given
copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the
ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of
the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.)

Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public
License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or
executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete
corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2
above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent
access to copy the source code from the same place satisfies the requirement to distribute the source code, even
though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by
being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a
derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the
Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is
therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for
the work may be a derivative work of the Library even though the source code is not. Whether this is true is
especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold
for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros
and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of
whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will
still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the
terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the location to find the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library included in the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

* b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

* c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. In that case, from the perspective of Section 6 of this License, you cannot distribute such a combined library, unless the license restrictions of this License do not permit linking those proprietary libraries with the Library.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.
* 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.
* The name of the author may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS 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 COPYRIGHT OWNER 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
INTERUPTION) 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.

muhttp 1.1.3
Copyright (c) 2005 Robbert Haarman

Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL 0.9.8k
OpenSSL SSLeay License
LICENSE ISSUES
The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in
the documentation and/or other materials provided with the
distribution.
3. All advertising materials mentioning features or use of this
software must display the following acknowledgment:
   "This product includes software developed by the OpenSSL Project
   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names ‘OpenSSL Toolkit’ and ‘OpenSSL Project’ must not be used to
   endorse or promote products derived from this software without
   prior written permission. For written permission, please contact
   openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL"
   nor may “OpenSSL” appear in their names without prior written
   permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following
   acknowledgment:
   "This product includes software developed by the OpenSSL Project
   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.
This package is an SSL implementation written
by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.
This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution, be it the RC4, RSA,
Ihash, 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 rouines 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 publically 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.]

pcre 5.0
PCRE is a library of functions to support regular expressions whose syntax
and semantics are as close as possible to those of the Perl 5 language.
Release 5 of PCRE is distributed under the terms of the "BSD" licence, as
specified below. The documentation for PCRE, supplied in the "doc"
directory, is distributed under the same terms as the software itself.
Written by: Philip Hazel <ph10@cam.ac.uk>
University of Cambridge Computing Service,
Copyright (c) 1997-2004 University of Cambridge
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.
* 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.
* Neither the name of the University of Cambridge 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 COPYRIGHT HOLDERS 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 COPYRIGHT OWNER 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.

PPPD Composite Licenses
Copyright (c) 1984-2000 Carnegie Mellon University. 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. The name “Carnegie Mellon University” must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact:
   Office of Technology Transfer
   Carnegie Mellon University
   5000 Forbes Avenue
   Pittsburgh, PA 15213-3890
   (412) 268-4387, fax: (412) 268-7395
   tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).”

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

------------------------------------------------------------------------------

Copyright (c) 1999-2004 Paul Mackerras. 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. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

3. Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by Paul Mackerras <paulus@samba.org>.”

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING
OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

----------------------------------------------------------------------------------------------------------------------------------------
Author: Arvin Schnell <arvin@suse.de> . (No copyright, but listed the author for attribution.)

----------------------------------------------------------------------------------------------------------------------------------------
Copyright (C) 2002 Roaring Penguin Software Inc.

This plugin may be distributed according to the terms of the GNU General Public License, version 2 or (at your option) any later version.
Copyright (C) 2002 Roaring Penguin Software Inc.

Copyright (C) 1996, Matjaz Godec <gody@elgo.si>
Copyright (C) 1996, Lars Fenneberg <l5y050@public.uni-hamburg.de>
Copyright (C) 1997, Miguel A.L. Paraz <map@phil.net>

Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>
Copyright (C) 2002 Roaring Penguin Software Inc.
MPPE support is by Ralf Hofmann, <ralf.hofmann@elvido.net>, with modification from Frank Cusack, <frank@google.com>.

This plugin may be distributed according to the terms of the GNU General Public License, version 2 or (at your option) any later version.

----------------------------------------------------------------------------------------------------------------------------------------
Author: Ben McKeegan ben@netservers.co.uk

Copyright (C) 2002 Netservers

This plugin may be distributed according to the terms of the GNU General Public License, version 2 or (at your option) any later version.
See the respective source files to find out which copyrights apply.

----------------------------------------------------------------------------------------------------------------------------------------
Copyright (C) 2002 Roaring Penguin Software Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Roaring Penguin Software Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Roaring Penguin Software Inc.
Roaring Penguin Software Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

----------------------------------------------------------------------------------------------------------------------------------------
Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.
Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

----------------------------------------------------------------------------------------------------------------------------------------
Copyright 1992 Livingston Enterprises, Inc.

Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566
Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.
Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.
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.

Copyright (c) 1989 Regents of the University of California.
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 the University of California, Berkeley. 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.

Van Jacobson (van@helios.ee.lbl.gov), Dec 31, 1989:
- Initial distribution.

Modified June 1993 by Paul Mackerras, paulus@cs.anu.edu.au,
so that the entire packet being decompressed doesn’t have
to be in contiguous memory (just the compressed header).

--------------------

Copyright 1995-2000 EPFL-LRC/ICA, and are licensed under the GNU Lesser
General Public License.
Written 1995-2000 by Werner Almesberger, EPFL-LRC/ICA */

Copyright 2000 Mitchell Blank Jr.
Based in part on work from Jens Axboe and Paul Mackerras.
Updated to ppp-2.4.1 by Bernhard Kaindl

Updated to ppp-2.4.2 by David Woodhouse 2004.
- disconnect method added
- remove_options() abuse removed.

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version
2 of the License, or (at your option) any later version.

--------------------

Copyright (C) 1995 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:
1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software
in a product, an acknowledgment in the product documentation would be
appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly
Mark Adler
gzip@prep.ai.mit.edu madler@alumni.caltech.edu

--------------------

Copyright (C) 2003 Andrew Bartlet <abartlet@samba.org>
Copyright 1999 Paul Mackerras, Alan Curry.
Copyright (C) 2002 Roaring Penguin Software Inc.
Copyright (C) 1996, Matjaz Godec <gody@elgo.si>
Copyright (C) 1996, Lars Fenneberg <ln5y050@public.uni-hamburg.de>
Copyright (C) 1997, Miguel A.L. Paraz <map@phil.net>
Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>
Copyright (C) 2002 Roaring Penguin Software Inc.
Copyright (C) 2003, Sean E. Millichamp <sean at bruenor dot org>
4. Redistributions of any form whatsoever must retain the following acknowledgment:
   "This product includes software developed by Tommi Komulainen <Tommi.Komulainen@iki.fi>.

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY
SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN
AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING
OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Original version, based on RFC2023
Copyright (c) 1995, 1996, 1997 Francis.Dupont@inria.fr, INRIA Rocquencourt,
Alain.Durand@imag.fr, IMAG,
Jean-Luc.Richier@imag.fr, IMAG-LSR.
Copyright (c) 1998, 1999 Francis.Dupont@inria.fr, GIE DYADE,
Alain.Durand@imag.fr, IMAG,
Jean-Luc.Richier@imag.fr, IMAG-LSR.

Ce travail a été fait au sein du GIE DYADE (Groupement d'Intérêt Économique ayant pour membres BULL S.A. et l'INRIA).

Ce logiciel informatique est disponible aux conditions usuelles dans la recherche, c'est-à-dire qu'il peut être utilisé, copié, modifié, distribué à l'unique condition que ce texte soit conservé afin que l'origine de ce logiciel soit reconnue.

Le nom de l'Institut National de Recherche en Informatique et en Automatique (INRIA), de l'IMAG, ou d'une personne morale ou physique ayant participé à l'élaboration de ce logiciel ne peut être utilisé sans son accord préalable explicite.

Ce logiciel est fourni tel quel sans aucune garantie, support ou responsabilité d'aucune sorte.

Ce logiciel est dérivé de sources d'origine "University of California at Berkeley" et "Digital Equipment Corporation" couvertes par des copyrights.

L'Institut d'Informatique et de Mathématiques Appliquées de Grenoble (IMAG) est une fédération d'unités mixtes de recherche du CNRS, de l'Institut National Polytechnique de Grenoble et de l'Université Joseph Fourier regroupant sept laboratoires dont le laboratoire Logiciels, Systèmes, Réseaux (LSR).

This work has been done in the context of GIE DYADE (joint R&D venture between BULL S.A. and INRIA).

This software is available with usual "research" terms with the aim of retain credits of the software.

Permission to use, copy, modify and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies,
and the name of INRIA, IMAG, or any contributor not be used in advertising or publicity pertaining to this material without the prior explicit permission. The software is provided "as is" without any warranties, support or liabilities of any kind.

This software is derived from source code from "University of California at Berkeley" and "Digital Equipment Corporation" protected by copyrights.

Grenoble's Institute of Computer Science and Applied Mathematics (IMAG) is a federation of seven research units funded by the CNRS, National Polytechnic Institute of Grenoble and University Joseph Fourier.
The research unit in Software, Systems, Networks (LSR) is member of IMAG.

------------------------------------------------------------------------------
Copyright (c) 1995 Eric Rosenquist. 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. The name(s) of the authors of this software must not be used to
   endorse or promote products derived from this software without
   prior written permission.

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY
SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----------------------------------------------------------------------
Copyright (C) Andrew Tridgell 1999-2004
Copyright (C) Anton Blanchard 2001
Copyright (C) Paul `Rusty' Russell 2000
Copyright (C) Jeremy Allison 2000-2003

** NOTE! The following LGPL license applies to the tdb library. This does NOT imply that all of Samba is released under the LGPL.
This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

radvd 1.5
radvd license
The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:
0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
1. All terms of all other applicable copyrights and licenses must be followed.
2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software must display the following acknowledgement with the name(s) of the authors as specified in the copyright notice(s) substituted where indicated:

   This product includes software developed by the authors which are mentioned at the start of the source files and other contributors.
5. Neither the name(s) of the author(s) 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 ITS AUTHORS 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 AUTHORS 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.

sglib 1.0.3
License Conditions: You can use a verbatim copy (including this copyright notice) of sglib freely in any project, commercial or not. You can also use derivative forms freely under terms of Open Source Software license or under terms of GNU Public License. If you need to use a derivative form in a commercial project, or you need sglib under any other license conditions, contact the author.

zlib 1.2.3
Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler
This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:
1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.
Appendix A  Motorola® Gateway Captive Portal Implementation

This section contains information about the Motorola Gateway Captive Portal Support.

**Overview**

Motorola follows the 2Wire RPC specification for implementation of Captive Portal.

The Captive Portal feature redirects all TCP traffic destined to port 80 and redirects it to a Captive Portal URL. A White-IP address list can be configured to avoid the captive portal redirect. All HTTP traffic destined to the IP addresses within this white IP address list will not be redirected to the Captive Portal. Any Changes to the Captive Portal parameters will take place immediately and do not require a reboot.

- PortalURL can be a maximum of 512 characters long.
- A maximum of 500 White IP Addresses are supported. WhiteIPAddresses list takes a comma-separated string, which can be Individual IP addresses or a range of IP addresses. For a range of IP Addresses, subnet mask is required.
- The following formats of IP address are accepted:
  - Individual IP address - 144.130.120.62 or 144.130.120.62/32
  - Range of 64 IP addresses - 144.130.120.64/26
- White IP Address list gets rewritten on any changes.
- Clearing the Captive Portal URL disables Captive Portal. Turning OFF the enable parameter can also disable captive Portal functionality.
- Captive Portal is **disabled by default and enabled via TR-069**
- White List can be a combination of FQDN (Fully Qualified Domain Names) and white IP Address/cidr.
- FQDNs will be resolved to IP addresses on BOOT and whenever a new list is pushed.
- For NVG589, Captive Portal implementation only redirects port 80 traffic. Traffic to port 443 is allowed.
- DNS Traffic will not be blocked
Captive Portal RPC

RPC supported per 2Wire requirements that will set Captive Portal Parameters.

```xml
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
    xmlns:tns="urn:dslforum-org:cwmp-1-0"
    targetNamespace="urn:dslforum-org:cwmp-1-0"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified">
  <xs:import namespace="http://schemas.xmlsoap.org/soap/envelope/"
      schemaLocation="soapenv.xsd"/>
  <xs:import namespace="http://schemas.xmlsoap.org/soap/encoding/"
      schemaLocation="soapenc.xsd"/>
  <xs:complexType name="CaptivePortalParamStruct">
    <xs:sequence>
      <xs:element name="Enable" type="soapenc:boolean">
        <xs:annotation>
          <xs:documentation> If true, the Captive Portal is enabled. </xs:annotation>
        </xs:documentation>
      </xs:element>
      <xs:element name="RedirectURL">
        <xs:annotation>
          <xs:documentation> the URL to be redirected to. </xs:annotation>
        </xs:documentation>
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:maxLength value="512"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="WhiteList" type="tns:WhiteList">
        <xs:annotation>
          <xs:documentation> a list of sites and IP address to be escaped by the Captive Portal. </xs:annotation>
        </xs:documentation>
      </xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="X_00D09E_GetCaptivePortalParams">
    <xs:annotation>
      <xs:documentation> X_00D09E_GetCaptivePortalParams message is to get the Captive Portal parameters on a CPE. </xs:annotation>
    </xs:documentation>
  </xs:element>
</xs:schema>
```

**X_00D09E_GetCaptivePortalParams RPC:**

<!-- X_00D09E_GetCaptivePortalParams -->

```xml
<xs:element name="X_00D09E_GetCaptivePortalParams">
  <xs:annotation>
    <xs:documentation> X_00D09E_GetCaptivePortalParams message is to get the Captive Portal parameters on a CPE. </xs:documentation>
  </xs:annotation>
</xs:element>
```
X_00D09E_GetCaptivePortalParams RPC:

<!-- X_00D09E_GetCaptivePortalParamsResponse -->
<xs:element name="X_00D09E_GetCaptivePortalParamsResponse">
  <xs:annotation>
    <xs:documentation>X_00D09E_GetCaptivePortalParamsResponse response message for X_00D09E_GetCaptivePortalParams request.</xs:documentation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="CaptivePortalParamStruct" type="tns:CaptivePortalParamStruct"/>
      </xs:sequence>
    </xs:complexType>
  </xs:annotation>
</xs:element>

X_00D09E_SetCaptivePortalParams RPC:

<!-- X_00D09E_SetCaptivePortalParams -->
<xs:element name="X_00D09E_SetCaptivePortalParams">
  <xs:annotation>
    <xs:documentation>X_00D09E_SetCaptivePortalParams message to set the Captive Portal parameters on a CPE.</xs:documentation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="CaptivePortalParamStruct" type="tns:CaptivePortalParamStruct"/>
      </xs:sequence>
    </xs:complexType>
  </xs:annotation>
</xs:element>

<!-- X_00D09E_SetCaptivePortalParamsResponse -->
<xs:element name="X_00D09E_SetCaptivePortalParamsResponse">
  <xs:annotation>
    <xs:documentation>X_00D09E_SetCaptivePortalParamsResponse response message is a response for X_00D09E_SetCaptivePortalParams request.</xs:documentation>
    <xs:complexType/>
  </xs:annotation>
</xs:element>
This section contains information about the Motorola Gateway QoS implementation.

**Overview**

When packets arrive on a high speed interface and are forwarded to a low speed interface, there is contention for bandwidth. This is the use case for QoS: to make effective use of bandwidth.

The basic steps for Quality of Service are to match and identify packets as belonging to a class of traffic, and to give each class of traffic a certain behavior such as priority queuing or bandwidth shaping across critical networking bottlenecks.

Packets forwarded through the system are classified using sets of filter rules to match various criteria, for example p-bit, DSCP, IP address, port, etc. The matching rule can set the classification, which is the name of the queue that is to be used.

*Figure 1. Illustration of upstream congestion, all traffic is consistently delayed.*

*Figure 2. Illustration of classification and transmit queue in a simple high/low priority scheme. Low priority may transmit only when high priority is completely empty.*
After the packet has been classified, it can be put in the proper queue. Queues are assigned to interfaces and can be constructed of several queue components to deliver the desired behavior. The components of an interface queue are these building blocks:

- **basic queues**: a 1 input 1 output packet list with a length of 64 packets by default. Packets will tail-drop when enqueued to a full basic queue.
- **priority queue**: 2 or more input, 1 output. Schedules the packets from the various inputs strictly according to input's priority.
- **weighted fair queue**: 1 or more input, 1 output. Schedules the packets according to bandwidth constraints

Packets are enqueued to basic queues, and only to basic queues. Basic queues are output to priority queues and weighted fair queues, which act as “plumbing” elements that alter the dequeuing order and rate, respectively. Priority queues and weighted fair queues can contain one another.
Weighted fair queues are used to constrain bandwidth. For example, consider a weighted fair queue with three basic queues as inputs, EF, AF and BE:

\[
\text{WFQ}
\]

\[
\begin{align*}
\text{Input 1: } & \text{ EF} \\
\text{Input 2: } & \text{ AF} \\
\text{Input 3: } & \text{ BE}
\end{align*}
\]

Each input entry is configured with a weight value, which is the rate at which to limit the traffic. This weight can be either absolute (bps) or a relative percentage of the interface's data-rate. This allows dedicating a split amount of bandwidth to each queue. A special value for the weight parameter is zero, which will use the remainder of unclaimed bandwidth.

There is an option to enable bandwidth sharing, so that unused bandwidth in idle queues can be shared to other queues. When the traffic resumes in the previously idle queue, the previously shared-out bandwidth is taken back.

When bandwidth sharing is enabled, a secondary rate configuration appears on each input entry, the peak parameter. This is a hard limit on the amount of bandwidth that the particular input entry can use. This rate will not be exceeded, even if there is an excess pool of idle bandwidth that could otherwise be shared.

**Upstream QoS: Priority and shaping**

The Gateway uses the DSL sync rate to determine traffic shaping requirements for WAN traffic. In this case there are 6 basic queues, and a hierarchy of both priority queue and weighted fair queue with bandwidth sharing and dual rate shaping. First the packets are classified via the filterset, to set the QoS-marker with the name of the desired basic queues. The queues are shown here, with packets traveling from left to right. Each basic queue feeds into a WFQ entry, and is shaped between the minimum bandwidth defined by “weight”, and the maximum rate defined by “peak”. If there is sufficient bandwidth, the WFQ entry shapes at the peak rate. If there is no spare bandwidth available for sharing, then the queue is shaped at the “weight” rate. The weight rate is defined either as a bps value, or as a percentage of line-rate that is determined once the upstream WAN data-rate is acquired. This “weight” value behaves as a Committed Information Rate (CIR), and the “peak” value behaves as a Peak Information Rate (PIR.)

![Figure 6. Illustration of default queues used for AT&T](image-url)
Packet Rx > Filterset Rules:
Match Rule 1? Set QoS marker = EF
Match Rule 2? Set QoS marker = AF1
Match Rule 3? Set QoS marker = BE

EF  CIR/PIR -> wfg_hi  -> PQ1 \ AF4 CIR/PIR \ > PQ output to interface Tx
AF3 CIR/PIR \ / AF2 CIR/PIR  \ wfg_lo > PQ2 /
AF1 CIR/PIR / BE  CIR/PIR /

Downstream QoS: Ethernet Switch

The simplest way of handling downstream QoS (from WAN to LAN) is to use the per-port queues that are present in the Ethernet switch. This achieves the greatest efficiency since the queues are handled in the switch hardware, and should be used when a strict priority queue with 4 priorities is sufficient.

The traffic is classified by priority-bit value. This can be the value retained from WAN ingress (assuming WAN is tagged,) or it can be a value that is set via a filter rule, which allows for advanced classification criteria to be used. Even though the LAN interface might not be tagged, there is still an internal priority field which is used to convey this information to the switch.

Downstream QoS: Egress queues

The secondary method of downstream QoS is to assign egress queues to the LAN port configuration. This is less efficient, however it allows more advanced queue scheduling algorithms to be used. Packets are classified by QoS markers set by filter rules.

This method is typically not recommended for deployment configuration as this mechanism can consume a large amount of CPU processing bandwidth.
# Index

## Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>!! command</td>
<td>108</td>
</tr>
</tbody>
</table>

## A

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Code</td>
<td>35</td>
</tr>
<tr>
<td>Address resolution table</td>
<td>113</td>
</tr>
<tr>
<td>Administrator password</td>
<td>107</td>
</tr>
<tr>
<td>Arguments, CLI</td>
<td>118</td>
</tr>
<tr>
<td>ARP Command</td>
<td>109, 116</td>
</tr>
</tbody>
</table>

## B

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic queues</td>
<td>208</td>
</tr>
<tr>
<td>Broadband Network Redirect</td>
<td>25</td>
</tr>
<tr>
<td>Broadband Status</td>
<td>37</td>
</tr>
<tr>
<td>Broadband Status Notification</td>
<td>87</td>
</tr>
</tbody>
</table>

## C

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Statistics</td>
<td>58</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>203</td>
</tr>
<tr>
<td>CLI</td>
<td>103</td>
</tr>
<tr>
<td>!! command</td>
<td>108</td>
</tr>
<tr>
<td>Arguments</td>
<td>118</td>
</tr>
<tr>
<td>Command shortcuts</td>
<td>108</td>
</tr>
<tr>
<td>Command truncation</td>
<td>118</td>
</tr>
<tr>
<td>Configuration mode</td>
<td>118</td>
</tr>
<tr>
<td>Keywords</td>
<td>118</td>
</tr>
<tr>
<td>Navigating</td>
<td>118</td>
</tr>
<tr>
<td>Prompt</td>
<td>108, 118</td>
</tr>
<tr>
<td>Restart command</td>
<td>108</td>
</tr>
<tr>
<td>SHELL mode</td>
<td>108</td>
</tr>
<tr>
<td>View command</td>
<td>119</td>
</tr>
</tbody>
</table>

## D

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Server</td>
<td>77</td>
</tr>
<tr>
<td>designing a new filter set</td>
<td>64</td>
</tr>
<tr>
<td>Detect Missing Filter</td>
<td>81</td>
</tr>
<tr>
<td>Device Access Code</td>
<td>27</td>
</tr>
<tr>
<td>Device List</td>
<td>32</td>
</tr>
<tr>
<td>DHCP lease table</td>
<td>111</td>
</tr>
<tr>
<td>Diagnostic log</td>
<td>111, 114</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>80</td>
</tr>
<tr>
<td>Documentation conventions</td>
<td>8</td>
</tr>
<tr>
<td>Downstream QoS</td>
<td>210</td>
</tr>
</tbody>
</table>

## E

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet statistics</td>
<td>111</td>
</tr>
<tr>
<td>Event Notifications</td>
<td>87</td>
</tr>
</tbody>
</table>

## F

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter parts</td>
<td>64</td>
</tr>
<tr>
<td>parts of</td>
<td>64</td>
</tr>
<tr>
<td>filter sets disadvantages</td>
<td>63</td>
</tr>
<tr>
<td>using</td>
<td>65</td>
</tr>
<tr>
<td>filters using</td>
<td>64, 65</td>
</tr>
<tr>
<td>firewall</td>
<td>114</td>
</tr>
<tr>
<td>Firewall Advanced</td>
<td>78</td>
</tr>
<tr>
<td>Firewall Status</td>
<td>62</td>
</tr>
</tbody>
</table>

## H

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>31</td>
</tr>
<tr>
<td>Home Network</td>
<td>41</td>
</tr>
<tr>
<td>HPNA</td>
<td>54</td>
</tr>
<tr>
<td>HPNA Configure</td>
<td>45</td>
</tr>
</tbody>
</table>

## I

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Echo</td>
<td>110</td>
</tr>
<tr>
<td>IGMP</td>
<td>139</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>139</td>
</tr>
<tr>
<td>IGMP Stats</td>
<td>40</td>
</tr>
<tr>
<td>IP DNS commands</td>
<td>138</td>
</tr>
<tr>
<td>IP Gateway commands</td>
<td>130</td>
</tr>
<tr>
<td>IP IGMP commands</td>
<td>139</td>
</tr>
<tr>
<td>IP interfaces</td>
<td>114</td>
</tr>
<tr>
<td>IP Passthrough</td>
<td>75</td>
</tr>
<tr>
<td>IP routes</td>
<td>114</td>
</tr>
<tr>
<td>IPMap table</td>
<td>114</td>
</tr>
</tbody>
</table>
Motorola Mobility DSL Gateways

Motorola Mobility LLC
600 North U.S. Highway 45
Libertyville, Illinois 60048 USA
Telephone: +1 847 523 5000

July 13, 2012