

User Guide

VT2500/VT2400 Voice Gateway





WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING. DO NOT PLACE OBJECTS FILLED WITH LIQUIDS, SUCH AS VASES, ON THE UNIT.

CAUTION: TO PREVENT ELECTRIC SHOCK, THIS EQUIPMENT MAY REQUIRE A GROUNDING CONDUCTOR IN THE LINE CORD. CONNECT THE UNIT TO A GROUNDING TYPE AC WALL OUTLET USING THE POWER CORD SUPPLIED WITH THE UNIT.

CAUTION: THIS PRODUCT WAS QUALIFIED UNDER TEST CONDITIONS THAT INCLUDED THE USE OF THE SUPPLIED CABLES BETWEEN SYSTEMS COMPONENTS. TO ENSURE REGULATORY AND SAFETY COMPLIANCE, USE ONLY THE PROVIDED POWER AND INTERFACE CABLES AND INSTALL THEM PROPERLY.

CAUTION: DIFFERENT TYPES OF CORD SETS MAY BE USED FOR CONNECTIONS TO THE MAIN SUPPLY CIRCUIT. USE ONLY A MAIN LINE CORD THAT COMPLIES WITH ALL APPLICABLE PRODUCT SAFETY REQUIREMENTS OF THE COUNTRY OF USE.

CAUTION: INSTALLATION OF THIS PRODUCT MUST BE IN ACCORDANCE WITH NATIONAL WIRING CODES AND CONFORM TO LOCAL REGULATIONS.

CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL.

CAUTION: CHANGES AND MODIFICATIONS NOT EXPRESSLY APPROVED BY MOTOROLA FOR COMPLIANCE COULD VOID USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

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

- Read all of the instructions listed here and/or in the user manual before you operate this equipment. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions as described in the user documentation that comes with the product.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.
- Place this equipment in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place unit to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.
- Do not connect the plug into an extension cord, receptacle, other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this equipment on a stable surface.



- Postpone cable modem installation until there is no risk of thunderstorm or lightning activity in the area.
- *Avoid using this product during an electrical storm.* There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power surges.
- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the equipment by local lightning strikes and other electrical surges.
- Do not cover the device, or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.
- Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.
- Avoid damaging the cable modem with static by touching the coaxial cable when it is attached to the earth grounded coaxial cable TV wall outlet.
- Always first touch the coaxial cable connector on the cable modem when disconnecting or re-connecting USB or Ethernet cable from the cable modem or the user's PC.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

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 in the grounding system of the building, as close to the point of cable entry as practical.

FCC Compliance Class B Digital Device

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.

Note: 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 when the equipment is operated in an environment. 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.

Changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.



Canadian Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numérique de la class B est conforme la norme NMB-003 du Canada.

FCC Certification

This product contains a radio transmitter and accordingly has been certified as compliant with 47 CFR Part 15 of the FCC Rules for intentional radiators. Products that contain a radio transmitter are labeled with FCC ID and the FCC logo.

Important VoIP Service Information

Any services provided through this equipment:

- Are not intended to replace or be a substitute for primary line voice services or Plain Old Telephone Service (POTS)
- Are not meant to provide guaranteed 911 or E911 services or to permit access to 411 directory assistance services



The service provider, not Motorola, is responsible for the provision of VoIP telephony services through this equipment. Motorola shall not be liable for, and expressly disclaims, any direct or indirect liabilities, damages, losses, claims, demands, actions, causes of action, risks or harms arising from or related to the services provided through this equipment.

IMPORTANT: You CANNOT make any calls using this VoIP device if your broadband connection is not functioning properly or if you lose electrical power.

CAUTION: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20 cm (8 inches).

Canada - Industry Canada (IC)

The wireless radio of this device complies with RSS 210 and RSS 102 of Industry Canada.

This Class B digital device complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

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.

This device has been designed to operate with two antennae: one is a detachable dipole antenna (reverse SMA type, Tx and RX) that has a maximum gain of 3 dBi; the second is a chip antenna (RX type only) that has a maximum gain of 2 dBi. Any antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

Only use the antenna(s) provided with this product or an antenna approved by Motorola.

Regulatory, Safety, Software License, and Warranty Information Card

This product is provided with a separate *Regulatory, Safety, Software License, and Warranty Information* card. If one is not provided with this product, please ask your service provider or point-of-purchase representative, as the case may be.

- THIS PRODUCT IS IN COMPLIANCE WITH ONE OR MORE OF THE STANDARDS LISTED ON THE *REGULATORY, SAFETY, SOFTWARE LICENSE, AND WARRANTY INFORMATION* CARD. NOT ALL STANDARDS APPLY TO ALL MODELS.
- NO WARRANTIES OF ANY KIND ARE PROVIDED BY MOTOROLA WITH RESPECT TO THIS PRODUCT, EXCEPT AS STATED ON THE *REGULATORY, SAFETY, SOFTWARE LICENSE, AND WARRANTY*

**MOTOROLA**

[Overview](#) [Installation](#) [Troubleshooting](#) [Contact](#) [FAQ](#) [Specifications](#) [Glossary](#) [License](#)
[Configuration: Basic Gateway TCP/IP Wireless Print Server USB](#)

INFORMATION CARD. MOTOROLA'S WARRANTIES DO NOT APPLY TO PRODUCT THAT HAS BEEN REFURBISHED OR REISSUED BY YOUR SERVICE PROVIDER.

Copyright © 2005 by Motorola, Inc.

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

Motorola reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola to provide notification of such revision or change. Motorola provides this guide without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Motorola may make improvements or changes in the product(s) described in this manual at any time.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me, Windows NT, and Xbox are registered trademarks and Windows XP and Xbox Live are trademarks of Microsoft Corporation. Microsoft Windows screen shots are used by permission of Microsoft Corporation. Macintosh and AppleTalk are registered trademarks of Apple Computer, Inc. Iomega is a registered trademark of Iomega Corporation. Linux is a registered trademark of Linus Torvalds. Acrobat Reader is a registered trademark of Adobe Systems, Inc. Netscape and Navigator are registered trademarks of Netscape Communications Corporation. PlayStation is a registered trademark of Sony Computer Entertainment Inc. UNIX is a registered trademark of the Open Group in the United States and other countries. Wi-Fi is a registered trademark of the Wi-Fi Alliance. All other product or service names are the property of their respective owners.



Contents

Introduction	1
Models	1
Features	1
Network Connection Types	2
Sample Wired Network for Home or Office (VT2400)	3
Sample Wireless Network for Home or Office (VT2500)	3
Sample Combination Wired and Wireless Network for Home or Office (VT2500)	4
Front Panel	5
Rear Panel	7
 Before You Begin	 8
Requirements and Prerequisites	8
Signing Up for Service	8
Existing Routers	8
Precautions	9
Document Conventions	9
Related Documentation	9
 Installation	 10
Positioning Your Router for Optimal Wireless Performance (VT2500 only)	10
Hardware Setup	11
Antenna Installation (VT2500 only)	11
Physical Placement	12
Horizontal Installation	12
Vertical Installation	13
Wall Mount Installation	13
Electrical Connection	14
 Connecting the VT2400/VT2500 to a Network	 16
Setting Up a New Network	16
Adding the VT2500/VT2400 to an Existing Network	17
Configuring the Voice Gateway to the Modem	17
Cable Modem	17
DSL Modem	17
Checking the Network Connections	18
 Basic Configuration	 19
Starting the VT2400/VT2500 Voice Gateway Setup Program	20
Changing the Default Password	22
Setting Up Minimum Security Network Options	23
Setting the Firewall Policy and Enabling the Firewall	23
Disabling the Wireless Option	25
Enabling Wireless Security for Wireless Devices	25



Gaming Configuration Guidelines	26
Configuring the Firewall for Gaming	26
Configuring Port Triggers	26
Configuring a Gaming DMZ Host	27
Help	28
Rebooting	29
Logging Out	30

Advanced Configuration 31

Using the Getting Started Wizard	32
Gateway > STATUS	33
Gateway > WAN — DHCP Client	34
Gateway > WAN — PPPoE Client	35
Gateway > WAN — Static	36
Gateway > LAN — nat config	37
Gateway > LAN — dhcp server config	38
Gateway > LAN — dhcp leases	40
Gateway > LAN — static leases	41
Gateway > PORT FORWARDING — status	43
Gateway > PORT FORWARDING — config	44
Gateway > PORT TRIGGERS - predefined	46
Gateway > PORT TRIGGERS - custom	48
Gateway > DNS	50
Gateway > LOG	51
System > CONTROL	52
System > CONFIGURATION — backup	53
System > CONFIGURATION — restore	54
System > CONFIGURATION — reset	55
System > LOG	56
Firewall > FIREWALL — basic	57
Firewall > FIREWALL — advanced	59
Firewall > CONTENT FILTER — status	61
Firewall > CONTENT FILTER — config	62
Firewall > SCHEDULES — status	64
Firewall > SCHEDULES — config	65
Firewall > LOG	67
Voice > STATUS	68
Voice > SERVICE	69
Users > USERS — status	71
Users > USERS — config	72
Users > USER GROUPS	73
Users > LOG	74
Wireless > STATUS	75
Wireless > NETWORK	76
Wireless > SECURITY — basic	77
Wireless > SECURITY — advanced	78
Wireless > STATISTICS	79



Configuring TCP/IP	80
Configuring TCP/IP in Windows 95, Windows 98, or Windows Me	80
Configuring TCP/IP in Windows 2000	83
Configuring TCP/IP in Windows XP	87
Verifying the IP Address in Windows 95, Windows 98, or Windows Me	91
Verifying the IP Address in Windows 2000 or Windows XP	92
 Setting Up Your Wireless LAN (WLAN)	 94
Encrypting Wireless LAN Transmissions	95
Configuring WPA on the VT2500	96
Configuring WEP on the VT2500	98
Restricting Wireless LAN Access	100
Configuring the Wireless Network Name on the VT2500	101
Configuring a MAC Access Control List on the VT2500	103
Configuring the Wireless Clients	104
Configuring a Wireless Client for WPA	105
Configuring a Wireless Client for WEP	105
Configuring a Wireless Client with the Network Name (ESSID)	105
Wireless Pages in the VT2500 Setup Program	106
Wireless > STATUS	107
Wireless > NETWORK	108
Wireless > SECURITY — basic	111
Wireless > SECURITY — advanced	112
Wireless > STATISTICS	114
 Troubleshooting	 116
Front-Panel Lights and Error Conditions	117
 Contact Us	 118
 Frequently Asked Questions	 119
 Specifications	 120
Wall Mounting Template	122
 Glossary	 124
 Software License	 144



Introduction

Thank you for purchasing the [VT2400/VT2500 Voice Gateway](#) for your home, home office, or small business/enterprise. The [VT2400/VT2500](#) Voice Gateway is ideal for:

- Households having multiple computers that require connection to the Internet and to each other
- Homes, small businesses, or home offices that require affordable telephone service
- Internet gamers that desire easier setup for:
 - programs such as DirectX® 7 or DirectX® 8
 - sites such as MSN Games by Zone.com or Battle.net®

The [voice gateway](#) is an adapter that allows up to two analog telephones to use digital telephony services over any broadband Internet connection using:

- a cable modem with high-speed data service from a cable television company
- a DSL (digital subscriber line) modem with high-speed data service from a telephone company

Because the [voice gateway](#) is directly connected to your broadband modem, the it can prioritize voice calls over data traffic. This helps ensure high-quality phone service. In addition, it offers rich features for enhanced telephone service, such as caller ID.

The [voice gateway](#) also provides a built-in router ([VT2400/VT2500](#)) and wireless access point ([VT2500](#) only) for a home or small office network.

Models

The [VT2400/VT2500 Voice Gateway](#) family includes these models (the VT2500 and VT2400 are covered in this manual):

- VT2000** Provides two telephone lines and connection to a router and a modem. Refer to the VT2000/VT1000 Series Voice Terminal User Guide for details.
- VT2400** Provides two telephone lines, a built-in router, and connection to a modem
- VT2500** Provides two telephone lines, a built-in wireless access point and router, and connection to a modem

You can use a [VT2400/VT2500](#) with almost any:

- Cable modem or DSL modem (broadband modem)
- Microsoft Windows®, Macintosh®, or UNIX® computer with a 10Base-T or 10/100Base-T Ethernet adapter

Features

The [VT2400/VT2500 Voice Gateway](#) provides:

- Up to two lines of robust, full-featured telephone and fax service
- Voice-over-data prioritization, which allows you to talk on the phone while using the Internet without a reduction in voice quality
- VPN pass-through support for remote access to enterprise applications



- Full network connectivity in a single unit, eliminating the cost and clutter of stand-alone routers, hubs, and wireless access points
- Portability — can plug into any broadband connection (cable or DSL)
- Plug-and-play installation
- Compact, low-profile design
- Easy Web-based configuration
- Support for rich telephone service features such as caller ID, call waiting, three-way calling, call forwarding, etc.
- Firewall and parental controls

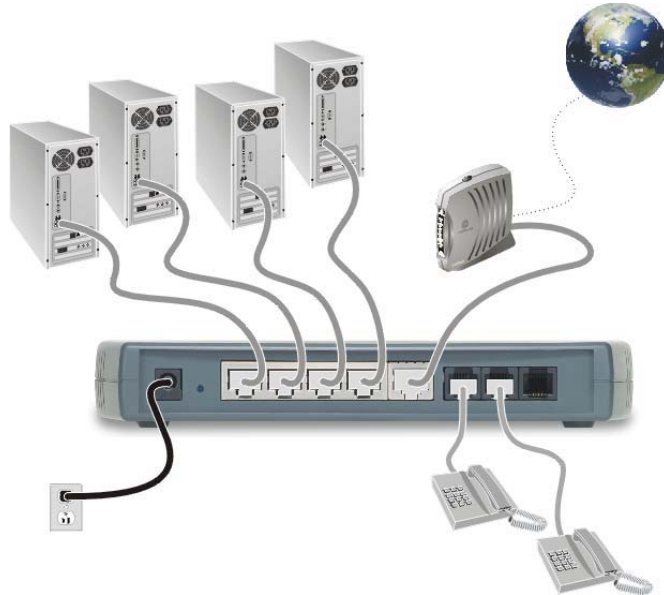
Network Connection Types

As shown in the following illustrations, the [VT2400/VT2500 Voice Gateway](#) can be set up with a wired or wireless connection, or a combination of the two:

- Ethernet (wired) local area network (LAN)
- Wireless LAN (802.11b/g, WiFi certified) ([VT2500](#) only)
- Combination Ethernet and Wireless LAN ([VT2500](#) only)

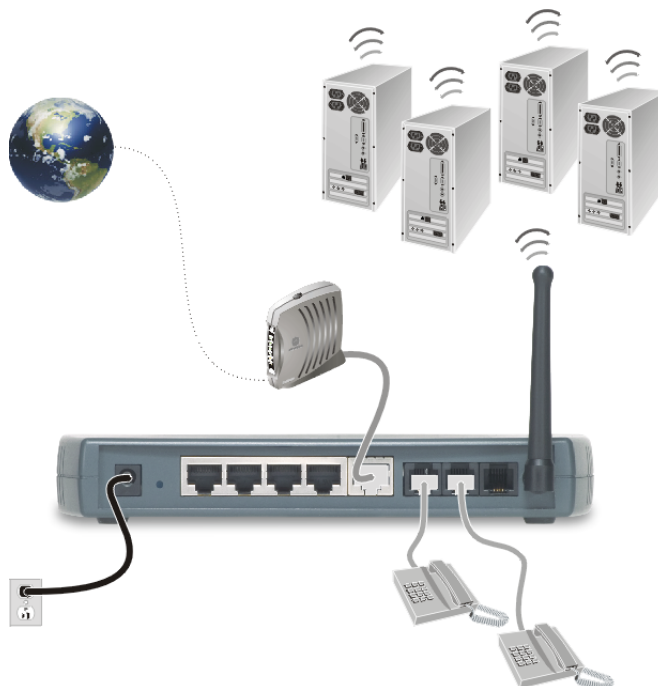
Sample Wired Network for Home or Office (VT2400)

The [VT2400](#) Voice Gateway adds advanced routing features and four Ethernet LAN ports, allowing you to connect multiple PCs without the need for a stand-alone hub or router. The [VT2400](#) also includes a firewall to help protect your network against external attacks.



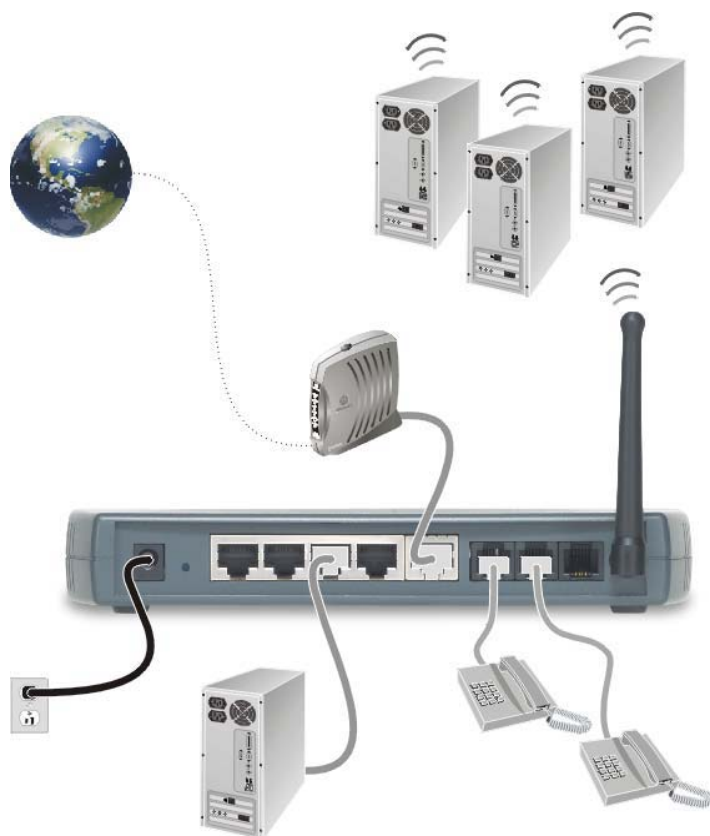
Sample Wireless Network for Home or Office (VT2500)

The [VT2500](#) Wireless Voice Gateway offers all the features of the [VT2400](#) with the added convenience of a built-in 802.11b/g wireless access point for wireless access to broadband services. It eliminates the need for stand-alone routers, hubs, and access points, providing a single platform for connecting telephones and PCs to a broadband link.



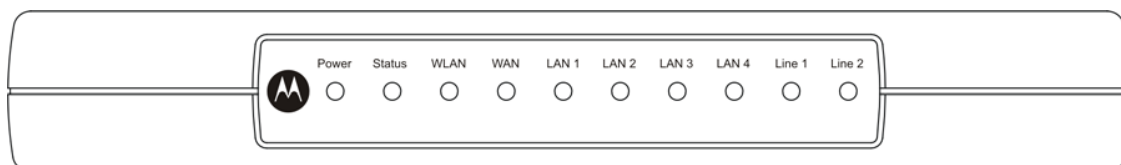
Sample Combination Wired and Wireless Network for Home or Office (VT2500)

The [VT2500](#) Wireless Voice Gateway allows you to set up a combination of wired and wireless PCs and other devices in your home or office network. Either a cable or DSL modem can be used.



Front Panel

The front panel of your [VT2400/VT2500](#) provides the following LEDs:



Indicator	VT2500/VT2400 Function
Power	Solid green if voice gateway is plugged in and operating normally
Status	Series of blinks indicates various voice gateway events (see next table)
WLAN (VT2500 only)	Green indicates activity on the wireless LAN
WAN	Indicates activity on the WAN (Internet) and link speed *
LAN 1	The devices on a single LAN port or LAN 1 are connected and operational *
LAN 2	The devices on LAN 2 are connected and operational *
LAN 3	The devices on LAN 3 are connected and operational *
LAN 4	The devices on LAN 4 are connected and operational *
Line 1	Series of blinks indicates status of Line 1 (see next table)
Line 2	Series of blinks indicates status of Line 2 (see next table)

* Connection speed is indicated as follows: Green if 100Base-T; Amber if 10Base-T



As a troubleshooting aid, the STATUS, LINE 1, and LINE 2 indicators blink as follows during start-up and image upgrades:

LED Activity	Status LED	Line 1 or Line 2 LED ^a
None	N/A	Service is not present on the line
One blink	Performing its initial boot sequence	The line is off the hook
Two blinks	Obtaining its network IP address	N/A
Three blinks	Downloading its configuration profile from your VoIP provider	N/A
Continuous	Downloading a firmware upgrade initiated by your VoIP provider	Attempting to reregister with your VoIP provider after interruption in service (PSTN failover - see next table)
Solid	N/A	Successfully registered with your VoIP provider

a. Line 2 is optional

The WAN port has a dual color LED to indicate network traffic and connection speed:

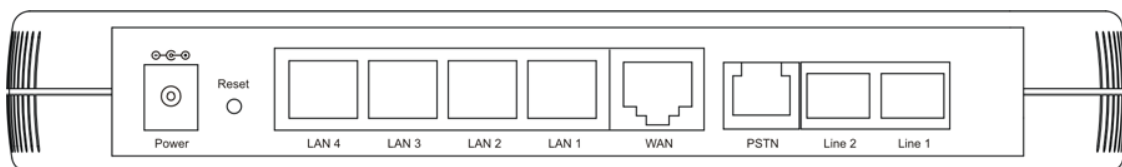
LED Activity	WAN LED
Solid green	If there is a 100Base-T connection without activity
Solid amber	If there is a 10Base-T connection without activity
Blinking amber	If there is a 10Base-T connection with activity

Caution!

Never unplug your Motorola voice terminal while its light is blinking continuously. Instead, allow the image upgrade to finish. If you unplug the Motorola voice terminal during an image upgrade, it may become inoperable.

Rear Panel

The rear panel provides the following connectors:



:

Item	Type	Connects To
POWER	12 V	An adapter that you plug into an AC power outlet
LAN	RJ-45	Ethernet connectors for up to four computers/devices
WAN	RJ-45	Ethernet connector to your broadband modem, switch, or hub ("WAN" or "wide area network" refers here to the Internet)
LINE 1	RJ-11	Telephone line one
LINE 2	RJ-11	Telephone line two
PSTN failover	RJ-11?	Supports a live phone line from the public switched telephone network, or "land phone" connected to plain old telephone service. If there is a power failure, phones connected to the voice terminal will still work, but calls will be routed to the PSTN connection instead of the VoIP broadband connection.
Reset button	?	Reboots the voice terminal if your VoIP service provider has enabled it.

Before You Begin

Before you begin installation, check that you received the following items with your [VT2400/VT2500](#):

Item		Description
AC adapter and line cord		Connects the VT2400/VT2500 to an AC electrical outlet
Ethernet cable		Connects the WAN port on the VT2400/VT2500 to a broadband modem (cable or DSL) Connects the LAN ports on the VT2400/VT2500 to a computer or other networked device
Vertical mounting stand		Provides vertical mounting on a flat surface for space economy

Requirements and Prerequisites

In addition to the [VT2400/VT2500 Voice Gateway](#), you also need:

- An established Internet connection using a DSL or cable modem (refer to the instructions that came with your modem)
- Activated voice service from your VoIP provider (see ["Signing Up for Service"](#) on page 8)
- One or two touch-tone telephones
- Computers with these minimum requirements:
 - Pentium-class processor or faster
 - 16 MB of memory
 - 10 MB of hard disk space available
 - Windows® 98, Windows® 98 SE, Windows® Me®, Windows® NT, Windows® XP or other Web-enabled PC
 - An Ethernet cable for each computer to be wired to the network (one is provided with the voice gateway). A wireless adapter installed in each computer to be wireless on the network (refer to the instructions that came with your wireless adapter)
- Optional:
 - You may need additional 10/100Base-T category 3 or better straight-through Ethernet cables with RJ-45 terminators to connect additional Ethernet devices (PCs).
 - Plugging the power adapter into a surge protector is also recommended.

Signing Up for Service

To activate voice service, you must provide the MAC address printed on the bar code label marked **MTA MAC ID** on the bottom of the [VT2400/VT2500](#) to your VoIP provider.

Existing Routers

If you have an existing router or wireless access point, you should print out the router or wireless access point configuration screens so that configuring the VT is made easier. Keep the printed copies for reference later.

Precautions

Caution!



Contact your VoIP provider before connecting your [VT2400/VT2500](#) to your existing telephone wiring. Connect each LINE port to a telephone *only*; never to a traditional telephone service.

Postpone installation until there is no risk of thunderstorm or lightning activity in the area.

To prevent overheating the [VT2400/VT2500](#), do not block the ventilation holes on the top and sides of the unit.

Do not open the [VT2400/VT2500](#). *Refer all service to your VoIP provider.*

Wipe the [VT2400/VT2500](#) with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

Any services provided through this equipment:

- Are not intended to replace or be a substitute for primary line voice services or Plain Old Telephone Service (POTS)
- Are not meant to provide guaranteed 911 or E911 services or to permit access to 411 directory assistance services

The service provider, not Motorola, is responsible for the provision of VoIP telephony services through this equipment. Motorola shall not be liable for, and expressly disclaims, any direct or indirect liabilities, damages, losses, claims, demands, actions, causes of action, risks or harms arising from or related to the services provided through this equipment.

IMPORTANT: You *cannot* make any calls using this VoIP device if your broadband connection is not functioning properly or if you lose electrical power.

Document Conventions

Before you begin using the [VT2400/VT2500](#), become familiar with the style conventions used in this manual:

Bold type	Indicates text that you must type exactly as it appears, fields you are instructed to select on a graphical user interface (GUI), or a default value
SMALL CAPS	Denotes silk screening on the equipment, typically representing front- and rear-panel controls and input/output (I/O) connections, and LEDs
<i>Italic type</i>	Denotes a displayed variable, a variable that you must type, or is used for emphasis
KEY + KEY	Key combinations indicating that you hold down the first key and then press the second key
KEY, KEY	Key combinations indicating that you press the first key, release it, and then press the second key
Courier font	Indicates text displayed on a graphical user interface (GUI), such as system messages

Related Documentation

The [VT2400/VT2500 Series Voice Gateway Quick Start Guide](#) provides instructions for end users to quickly set up and configure the [voice gateway](#).

Installation

Follow the steps and guidelines in this section to physically set up and position the [VT2400/VT2500](#) voice gateway on a flat surface or mount it on the wall.

Positioning Your Router for Optimal Wireless Performance ([VT2500 only](#))

Your voice gateway has an embedded wireless router that uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 Wireless Fidelity (Wi-Fi). This standard is subdivided into distinct categories of speed and the frequency spectrum used, designated by the lowercase letter after the standard.

For example, the router supports both the 'b' and 'g' specifications. The 802.11b specification transmits data rates up to 11 Mbps while the 802.11g specification transmits data rates up to 54 Mbps. These are theoretical standards so performance may vary. The radio waves radiate in a donut-shaped pattern. The waves travel through walls and floors, but transmission power and distance are affected. The theoretical distance limit is 1,000 feet (305 meters), but actual throughput and distance varies.

Both standards operate in the 2.4 GHz range, meaning other electrical appliances also might interfere with the router – televisions, radios, microwave ovens, or 2.4 GHz cordless telephones. Therefore, positioning the [voice gateway](#) where it encounters the least interference helps maintain a better connection.

The following table lists the expected wireless range of the router. This table is only a guide and coverage varies due to local conditions.

Data Rate	Open Area	Closed Area
54 Mbps	Up to 100 ft (30m)	Up to 60 ft (18 m)
11 Mbps	Up to 900 feet (275 m)	Up to 160 feet (49 m)
5.5 Mbps	Up to 1300 feet (396 m)	Up to 200 feet (61 m)
2 or 1 Mbps	Up to 1500 feet (457 m)	Up to 300 feet (91 m)

To achieve the best wireless performance, review these guidelines before deciding where to place the [voice gateway](#):

- Placing the [voice gateway](#) in the center of your network is the best location because the antenna sends out the signal in all directions.
- Placing the [voice gateway](#) in a higher location, such as on top of a cabinet, helps disperse the signal cleanly, especially to receiving locations on upper stories.
- If possible, position the [voice gateway](#) so there is direct line of sight between the unit and your other home network devices.
- Avoid placing the [voice gateway](#) next to large solid objects like computer cases, monitors, walls, fireplaces, etc. This helps the signal penetrate more cleanly.
- Other wireless devices such as televisions, radios, microwaves, and 2.4 GHz cordless telephones can interfere with the signal. Keep these devices away from the [voice gateway](#).
- Mirrors, especially silver-coated, can reduce transmission performance.

Hardware Setup

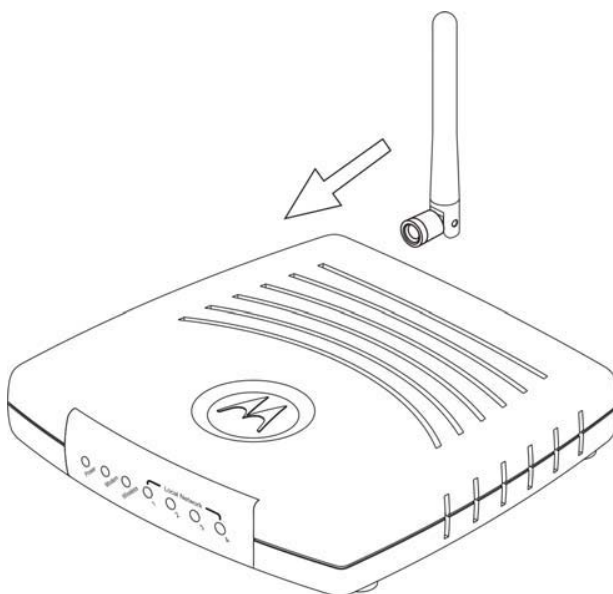
Hardware setup includes:

- antenna installation (*VT2500 only*)
- physical placement - horizontal, vertical, or mounted on the wall
- electrical connection - connecting the power cord

Antenna Installation (*VT2500 only*)

When shipped, the antenna for the router is not connected to the [voice gateway](#). To attach the antenna to the [voice gateway](#):

- 1 Locate the antenna port on the back of the [voice gateway](#) (the threaded knob).
- 2 Screw the antenna connector clockwise onto the threaded knob until firmly seated. Do not over-tighten.

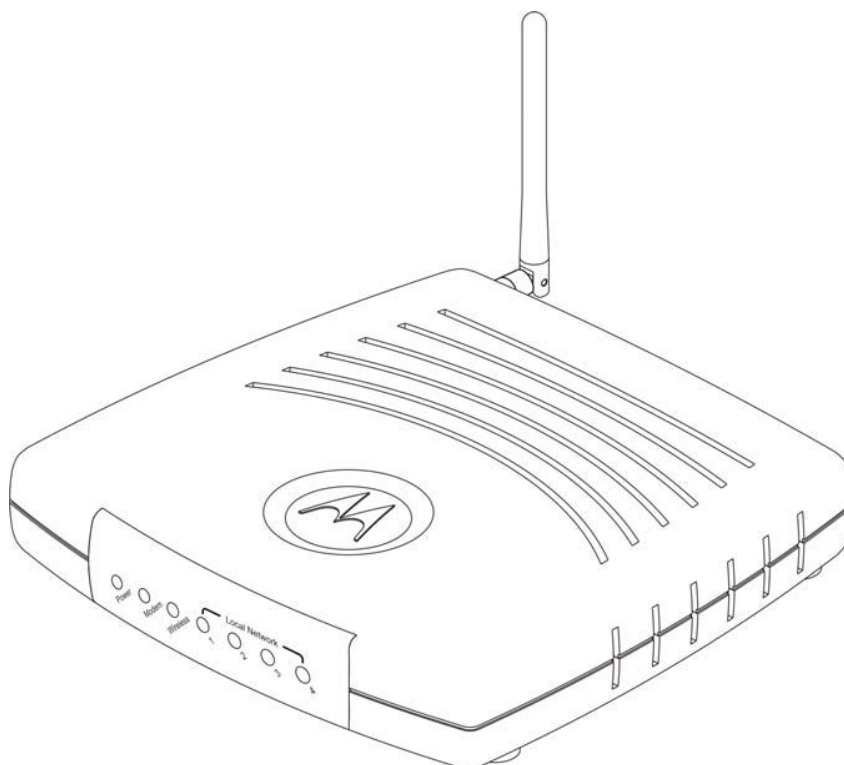


Physical Placement

For desktop use, the [voice gateway](#) can be installed either horizontally or vertically. It can also be mounted on a wall.

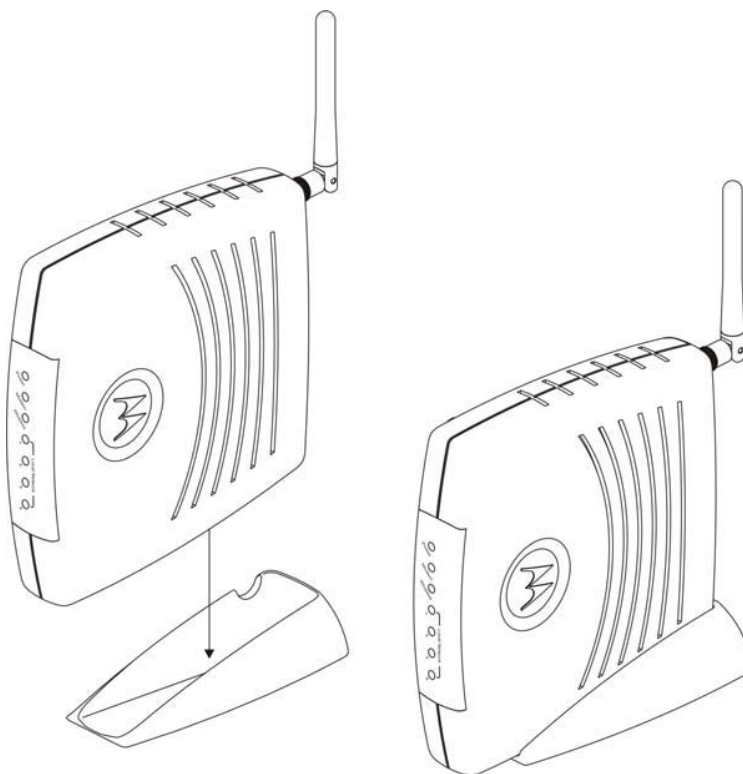
Horizontal Installation

- 1 Place the [voice gateway](#) in the desired location as shown in the figure below.
- 2 Follow the installation procedures for connecting and configuring the [voice gateway](#) to a network.



Vertical Installation

- 1 Insert the router into the supplied base stand. Ensure that the antenna's location is on top. The [voice gateway](#)'s foot slides snugly into a notch in the base stand to keep it stable.
- 2 Follow the installation procedures for connecting and configuring the [voice gateway](#) to a network.



Wall Mount Installation

If you mount the VT2400/VT2500 on the wall, you must:

- Position the VT2400/VT2500 as specified by the local or national codes governing residential or business communications services.
- Follow all local standards for installing a network interface router/network interface device (NIU/NID).

If possible, mount the [VT2400/VT2500](#) to concrete, masonry, a wooden stud, or other solid wall material. Use anchors when necessary, such as when you must mount the [voice gateway](#) on drywall.

To mount the [VT2400/VT2500](#) on the wall:

- 1 Print the Wall Mounting Template diagram in the [Specifications](#) section of this manual.

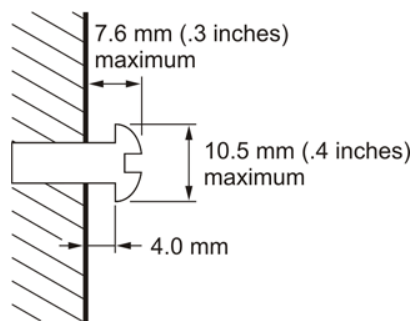
The illustration shows the two keyholes with the plus sign that indicates the center where the screws must be located (7.047 inches apart). The drawing provides the exact dimensions required to mount the [VT2400/VT2500](#) on a wall.

- 2 To print the Wall Mounting Template, click the **Print** icon or choose **Print** from the File menu.
- 3 In the *Pages* field, enter the page number in this manual on which the Wall Mounting Template appears.
- 4 Click **OK**.
- 5 Measure the printed template with a ruler to ensure that it is the same size as the template drawing indicates (7.047 inches).
- 6 Use a center punch to mark the center of the holes on the wall.
- 7 On the wall, locate the marks for the mounting holes you just made.

Warning!

Before drilling holes, check the structure for potential damage to water, gas, or electric lines.

- 8 Drill the holes to a depth of at least 3.8 cm (1½ inches).
- 9 If necessary, seat an anchor in each hole. Use M5 x 38 mm (#10-16 x 11/2 inch) screws with a flat underside and maximum screw head diameter of 10.5 mm to mount the [voice gateway](#).
- 10 Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown:
 - –There must be 4.0 mm (.16 inches) between the wall and the underside of the screw head.
 - –The maximum distance from the wall to the top of the screw head is 7.6 mm (.3 in).



- 11 Remove the two plastic feet (nearest to the LED panel) from the bottom of the router to uncover the keyholes.
- 12 Place the [voice gateway](#) so the keyholes are above the mounting screws.
- 13 Slide the [voice gateway](#) down until it stops against the top of the keyhole opening.
- 14 Follow the installation procedures for connecting and configuring the [voice gateway](#).

Electrical Connection

Your [voice gateway](#) does not have an On/Off power switch and therefore is only powered on by plugging in the power adapter.



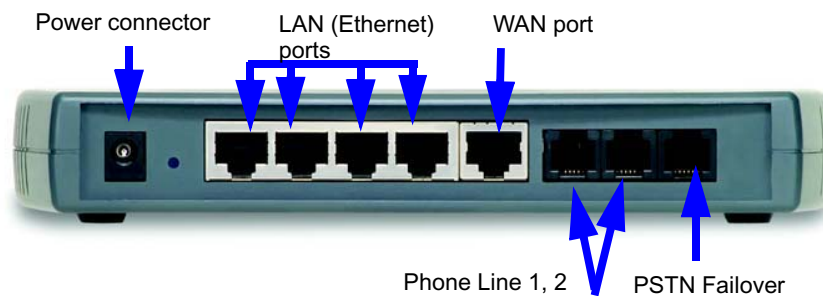
To power
supply

- 1 Connect the power adapter to the [voice gateway](#) **Power** port, found on the back of the unit.
- 2 Plug the power adapter into a grounded and surge-protected power outlet. The Power LED on the front panel lights green when connected properly.

Connecting the VT2400/VT2500 to a Network

If you are setting up a wireless network only, the computers in the following diagrams will not use Ethernet cables to connect them.

If you have an existing modem, follow the procedure in [“Adding the VT2500/VT2400 to an Existing Network”](#). If you are setting up a network for the first time (adding devices to a single PC setup), see [“Setting Up a New Network”](#) and then go to [“Configuring the Voice Gateway to the Modem”](#) on page 17.



Setting Up a New Network

Follow these instructions if you have a single PC connected directly to the modem, or no Internet connection until now.

- 1 Be sure the modem and the PCs are turned off and the [VT2400/VT2500](#) is unplugged.
- 2 If you only have a single PC connected, disconnect the Ethernet cable from the PC to the modem (on the modem end only) and connect it to a **LAN** port on the [VT2400/VT2500](#).
- 3 Connect up to three additional PCs using Ethernet cables to the [VT2400/VT2500](#). Connect one end of each Ethernet cable to a PC and the other end to a **LAN** port on the [VT2400/VT2500](#).
- 4 Connect one end of an Ethernet cable (RJ-45) to the modem, and connect the other end to the **WAN** port on the [VT2400/VT2500](#).
- 5 Connect up to two existing land phone lines (after you disconnect them from the wall jacks) and connect them to the **LINE 1** and **LINE 2** ports on the [VT2400/VT2500](#).

Adding the VT2500/VT2400 to an Existing Network

You may have a combination of wired and wireless devices on your existing network. Follow these steps to connect only those PCs to be wired. These instructions will also help you modify an existing network that uses a separate router or wireless access point.

To connect PCs using an Ethernet cable:

- 1 Be sure the existing modem, router, and PCs are turned off and the [VT2400/VT2500](#) is unplugged.
- 2 Disconnect the Ethernet cable (RJ-45) that connects the modem to the router (on the router/WAP end only) and then connect it to the **WAN** port on the [VT2400/VT2500](#).
- 3 Disconnect the Ethernet cables that connect the PCs to the router (on the router/WAP end only) and connect them to the LAN ports on the [VT2400/VT2500](#).
- 4 Connect up to two existing land phone lines (after you disconnect them from the wall jacks) and connect them to the **LINE 1** and **LINE 2** ports on the [VT2400/VT2500](#).

Configuring the Voice Gateway to the Modem

Most high-speed Internet connections use a cable modem or a DSL modem. The cable modem is connected to your cable television company coax cable. The DSL modem is connected to a telephone company phone line. Determine which modem you are using and gather the information on the worksheet below. You will use this information in the next section, Basic Configuration, before you check the voice gateway's connection to your VoIP provider.

Cable Modem

If you have a cable modem, you will need to contact your cable Internet provider for all of the information in the Cable Modem column on the worksheet. Or, you can refer to the cable modem configuration pages that you printed out before setting up the network, as recommended in [Section X](#).

DSL Modem

If you have a DSL modem, you will need to contact your telephone Internet provider for all of the information in the DSL Modem column on the worksheet. Or, you can refer to the DSL modem configuration pages that you printed out before setting up the network, as recommended in [Section X](#).



After you fill in the worksheet, perform the steps that follow the worksheet.

Modem Worksheet

	Cable Modem (cable company)	DSL Modem (phone company)
Service Name	_____	_____
Your User Name	_____	_____
Your Password	_____	_____
DHCP	Is the IP address obtained dynamically?	PPPoE
Yes	No need to fill in the rest of this section of the work sheet. Proceed to DNS Server IP Addresses.	N/A
No	What are the values for the Static IP Address, Subnet Mask, and Default Gateway:	N/A
Static IP Address	_____	N/A
Subnet Mask	_____	N/A
WAN Default Gateway	_____	N/A
	What are the DNS server IP addresses? (Sometimes DHCP does not assign them dynamically, so be sure to ask your cable provider, even if you answered Yes to DHCP above.) PPPoE requires DNS Server IP Addresses as well.	
DNS Server IP Addresses: (up to 3)	1) _____ 2) _____ 3) _____	1) _____ 2) _____ 3) _____

Checking the Network Connections

- 1 Turn on the DSL or cable modem, following the instructions provided with the modem. Wait about two minutes for it to start up.
- 2 Plug the AC power adapter to the **POWER** connector on the [VT2400/VT2500](#) and the other end to an electrical outlet. *This turns on the [VT2400/VT2500](#) Voice Gateway. You do not need to unplug it when it is not in use.*

Wait about two minutes for the [VT2400/VT2500](#) to start up. The Power light performs a series of blinks, as described in ["Front Panel"](#) on page 5.
- 3 After the Power light on the [VT2400/VT2500](#) is solid green, turn on your computer. If the Internet connection does not work as it did before you installed the [VT2400/VT2500](#), refer to ["Troubleshooting"](#) on page 116.
- 4 Before you can verify that the phone is working, you need to complete several basic configuration procedures. Proceed to ["Basic Configuration"](#) on page 19.

Basic Configuration

This section provides initial procedures required for configuring the network attached to the [voice gateway](#). These include:

- [Starting the VT2400/VT2500 Voice Gateway Setup Program](#)
- [Changing the Default Password](#)
- [Setting Up Minimum Security Network Options](#), such as selecting the firewall policy, enabling the firewall, disabling the wireless option (if you are setting up a wired network only), or enabling wireless security (if setting up a LAN with one or more wireless clients)
- [Gaming Configuration Guidelines](#)
- [Help](#)
- [Rebooting](#)
- [Logging Out](#)

For more advanced configuration information, see [“Advanced Configuration”](#) on page 31.

For normal operation, you do not need to change most default settings.

Caution!



To prevent unauthorized configuration, change the default password *immediately* when you first configure the [VT2400/VT2500](#). See [“Changing the Default Password”](#).

Firewalls are not foolproof. Choose the most secure firewall policy you can. See [“Setting Up Minimum Security Network Options”](#).

If you are using a wired LAN only and have no wireless clients, be sure you disable the wireless interface by turning off [Enable Wireless Interface](#) on the [Wireless > NETWORK](#).

For a wireless LAN only, be sure you follow the instructions in [“Setting Up Your Wireless LAN \(WLAN\)”](#).

Starting the VT2400/VT2500 Voice Gateway Setup Program

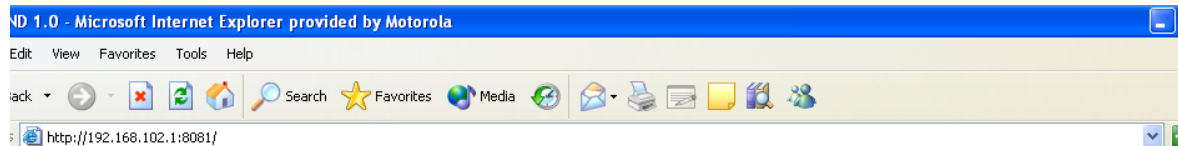
On a computer wired to the [VT2400/VT2500](#), open a Web browser.

Caution:



Run the voice gateway configuration setup program only from a PC attached to the voice gateway with an Ethernet cable. Do not use a wireless device to configure the network.

- 1 On a computer wired to the [VT2400/VT2500](#), open a Web browser, such as Internet Explorer or Netscape.
- 2 In the Address or Location field, type **http://192.168.102.1** or **http://192.168.0.1** and press ENTER to display the Log In window:



Voice Terminal

VT2500


MOTOROLA

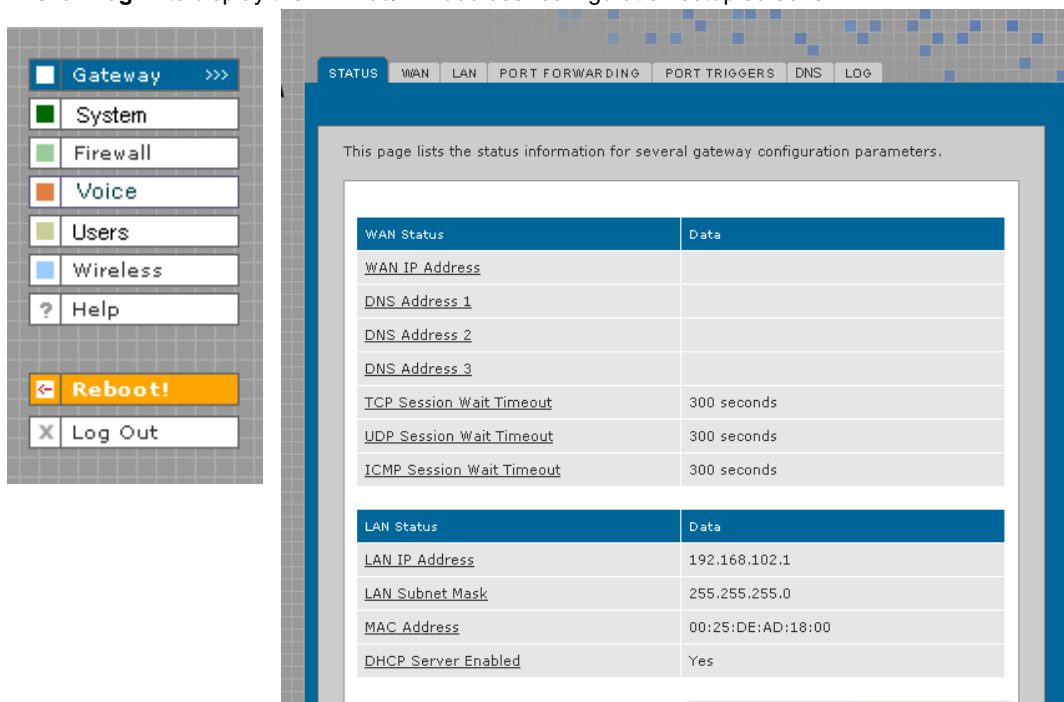
User ID:

Password:

Login

- 3 In the User ID field, type the **user name**. The default is **admin** (this field is case sensitive).
- 4 In the Password field, type the **password**. The default is **motorola** (this field is case sensitive).

- 5 Click **Log In** to display the [VT2400/VT2500](#) user configuration setup screens:



If you have difficulty starting the [VT2400/VT2500](#) setup program, see [“Troubleshooting”](#) for information.

*After you edit the field and click **Apply** for some settings, you are required to reboot the [VT2400/VT2500](#) for the changes to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.*

Changing the Default Password

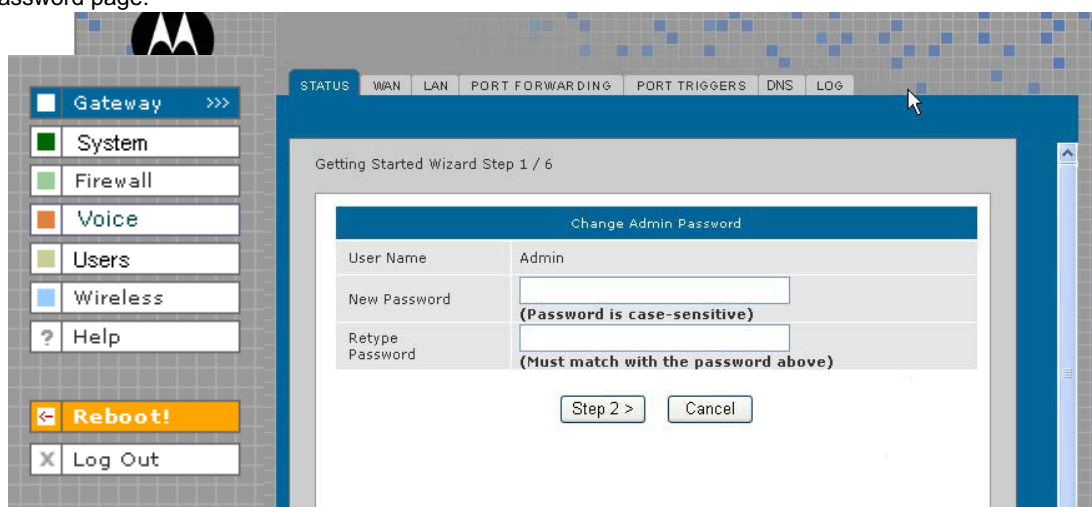
Caution!



To prevent unauthorized configuration, change the default password *immediately* when you first configure the [VT2400/VT2500 Voice Gateway](#).

To change the default password after you log in:

- 1 On the Gateway > STATUS page, click **Launch Getting Started Wizard** to display the Change Admin Password page:



- 2 In the **Old Password** field, type the old **password**. The default password is **motorola** (this field is case sensitive).
- 3 In the **New Password** field, type the new **password**.
- 4 In the **Retype Password** field, type the new **password** again.
- 5 Click **Apply** to make your changes.

Setting Up Minimum Security Network Options

For basic operation of your network, these tasks must be completed:

- Selecting the firewall policy and enabling the firewall
- Disabling the wireless option (if you are setting up a wired network only); or
- Enabling wireless security (if setting up a LAN with one or more wireless devices)

Setting the Firewall Policy and Enabling the Firewall

The [VT2400/VT2500](#) firewall protects your LAN from attacks and other intrusions from the Internet. This section describes using the Policy > POLICY — config page to choose one of the *predefined firewall policies* provided with the [voice gateway](#).

Caution!



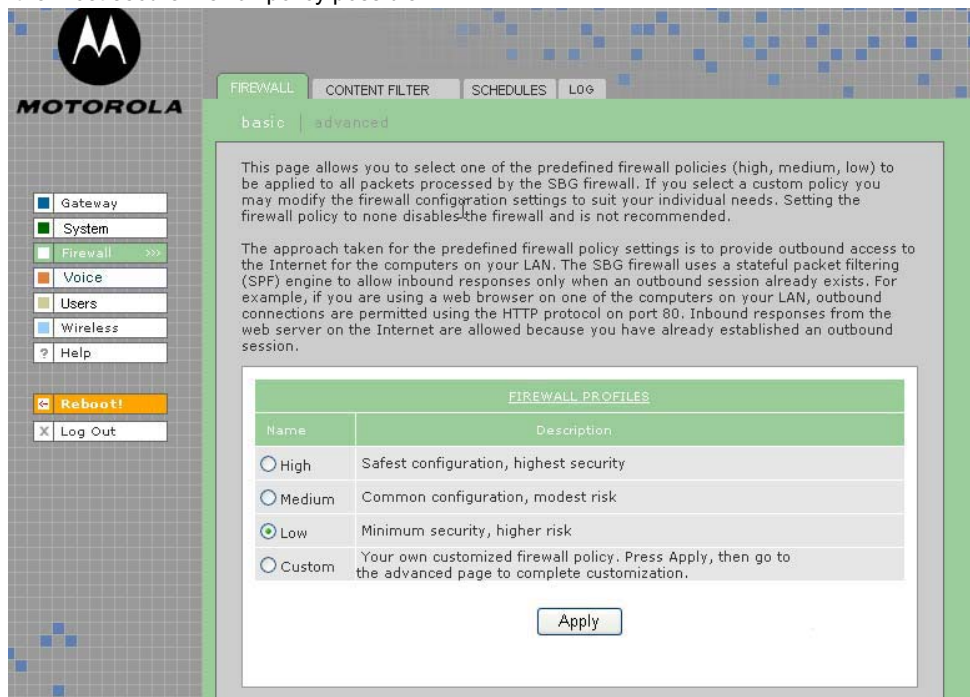
Firewalls are not foolproof. Choose the most secure firewall policy possible. To enable easy network setup, the default firewall policy is None, which provides no security.

The predefined policies provide outbound Internet access for computers on the [VT2400/VT2500](#) LAN. The [voice gateway](#) firewall uses [stateful inspection](#) to allow inbound responses when there already is an outbound session running corresponding to the data flow. For example, if you use a Web browser, outbound HTTP connections are permitted on port 80. Inbound responses from the Internet are allowed because an outbound session is established.

To set up a custom firewall, see [Firewall > FIREWALL — basic](#) in [Advanced Configuration](#).

To select a predefined policy for all data processed by the [VT2400/VT2500](#) firewall:

- 1 After you log in, click **Firewall** on the main menu then click Firewall. The [Firewall > FIREWALL — basic](#) page appears.
- 2 Click the most secure firewall policy possible.



High The safest firewall policy template, that provides the highest security. *We recommend this setting.*

Medium A firewall policy template that provides a common configuration having modest risk.

Low A firewall policy template that provides minimum security, with a higher risk of intrusions.

Custom You may need to create your own custom firewall policy. *Do not create a custom policy unless you have the necessary expertise and the need to do so.*

- 3 Click **Apply** to make your changes.

*After you edit the field and click **Apply** for some settings, you are required to reboot the [VT2400/VT2500](#) for the changes to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.*

For more advanced security, you can:

- View the rules for the High, Medium, and Low predefined policy templates or create a custom policy on the [Firewall > FIREWALL — advanced](#) page.
- View the firewall logs on the [Firewall > LOG](#) page.
- Configure the [VT2500](#) firewall to allow inbound packets without first establishing an outbound session. You will also need to configure a port forwarding entry on the [Gateway > PORT FORWARDING — config](#) page or a DMZ client on the [Gateway > LAN — static leases](#) page.

For information about these options refer to [Advanced Configuration](#). For more information about how the firewall can affect gaming, see [Gaming Configuration Guidelines](#).

Disabling the Wireless Option

If you do not plan to have any wireless devices in your network, make sure the **Enable Wireless Interface** check box is *not* selected on the Wireless > NETWORK page.

Enabling Wireless Security for Wireless Devices

Follow this procedure if you plan to have wireless devices in your network.

- 1 On the Wireless > NETWORK page, select the **Enable Wireless Interface** check box.
- 2 Change the ESSID **name**. Type up to 32 alphanumeric case-sensitive characters.

Caution!



The default ESSID name is Motorola. It is recommended that you change the default immediately upon setting up your WLAN.

- 3 Click **Save Changes**.
- 4 On the Wireless > SECURITY > advanced page, select the **ESSID Broadcast** check box.
- 5 Click **Apply**.
- 6 Go to [Setting Up Your Wireless LAN \(WLAN\)](#) to complete all other required procedures for setting up your WLAN.

Gaming Configuration Guidelines

The following sections provide information about configuring the [voice gateway](#) firewall and a DMZ for gaming.

Configuring the Firewall for Gaming

By default, the [VT2500](#) firewall is disabled. If you enable the firewall, as recommended, refer to the game's documentation to ensure that the necessary ports are open for use by that game.

The predefined [VT2400/VT2500](#) firewall policies affect Xbox *Live*™ as follows:

- | | |
|-----------------------|---|
| Low | Xbox <i>Live</i> data can pass through the firewall. No user action is required. |
| Medium or high | To enable Xbox <i>Live</i> traffic to pass, you must configure: <ul style="list-style-type: none">• Choose Firewall > FIREWALL — advanced to create your own custom firewall• Enter UDP 88:88 and UDP/TCP 3074:3074 on the? |

Configuring Port Triggers

Because the [voice gateway](#) has predefined port triggers for games using any of the following applications, no user action is required to enable them:

- DirectX 7 and DirectX 8
- MSN Games by Zone.com
- Battle.net

For a list of games supported by Battle.net, visit <http://www.battle.net>.

You may need to create custom port triggers to enable other games to operate properly. If you set custom port triggers and enable the firewall, you must customize the firewall to allow traffic through those ports. To create custom port triggers, use the [Gateway > PORT TRIGGERS - custom](#) page.

Configuring a Gaming DMZ Host

Caution!



The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

Some games and game devices require *one* of these:

- The use of random ports
- The forwarding of unsolicited traffic

For example, to connect a PlayStation® 2 for PS2® online gaming, designate it as the gaming DMZ host because the ports required vary from game to game. For these games, we recommend configuring the gaming computer or device as a gaming DMZ device.

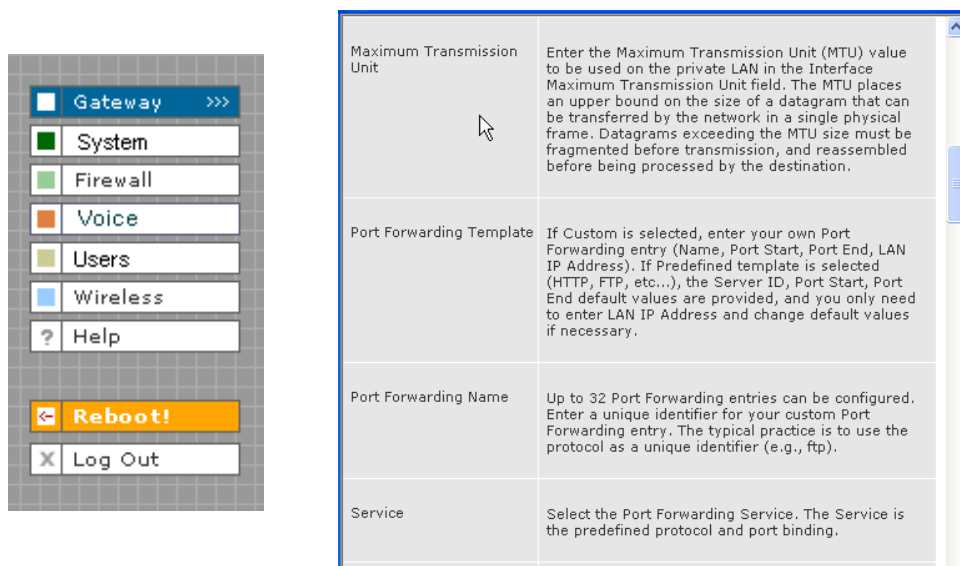
To configure a gaming DMZ device, on the [Gateway > LAN – static leases](#) page:

- 1 Reserve a private IP address for the computer or game device MAC address.
- 2 Designate the device as a DMZ device.

You can reserve IP addresses for multiple devices, but only one device can be designated as the gaming DMZ at a time.

Help

Use this page to obtain Help screens when using the [VT2400/VT2500](#) graphical user interface. For example....



Help page fields

Field or Button

Description

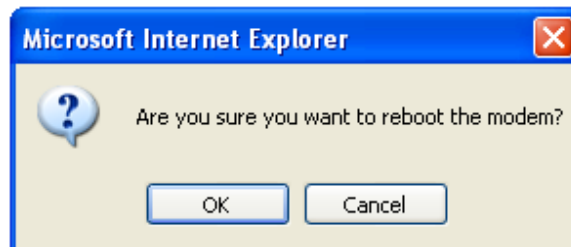
HELP

Generates a help window that contains a description and other information.

Note to reviewers: is there a search option on the Help button?

Rebooting

When you click **Reboot**, this message appears:



Click **OK** to reboot the [VT2400/VT2500](#) voice terminal. The current configuration (or changes you just made using the Apply buttons) will be kept.

Click **Cancel** to cancel the reboot.



Logging Out

When you click **Log Out**, the [VT2400/VT2500](#) Setup Program log in screen appears.

The screenshot shows a web browser window with the address bar displaying `http://192.168.102.1:8081/`. The page content includes a blue header bar with the text "Voice Terminal" on the left and "VT2500" on the right. Below this, the Motorola logo is displayed on the left. To the right of the logo is a login form with the following elements: a "User ID:" label above a text input field containing "admin"; a "Password:" label above a text input field with masked characters (dots); and a "Login" button below the password field. A thick blue horizontal bar is positioned below the login form. The entire page is framed by thin black lines at the top and bottom.

❖ Advanced Configuration

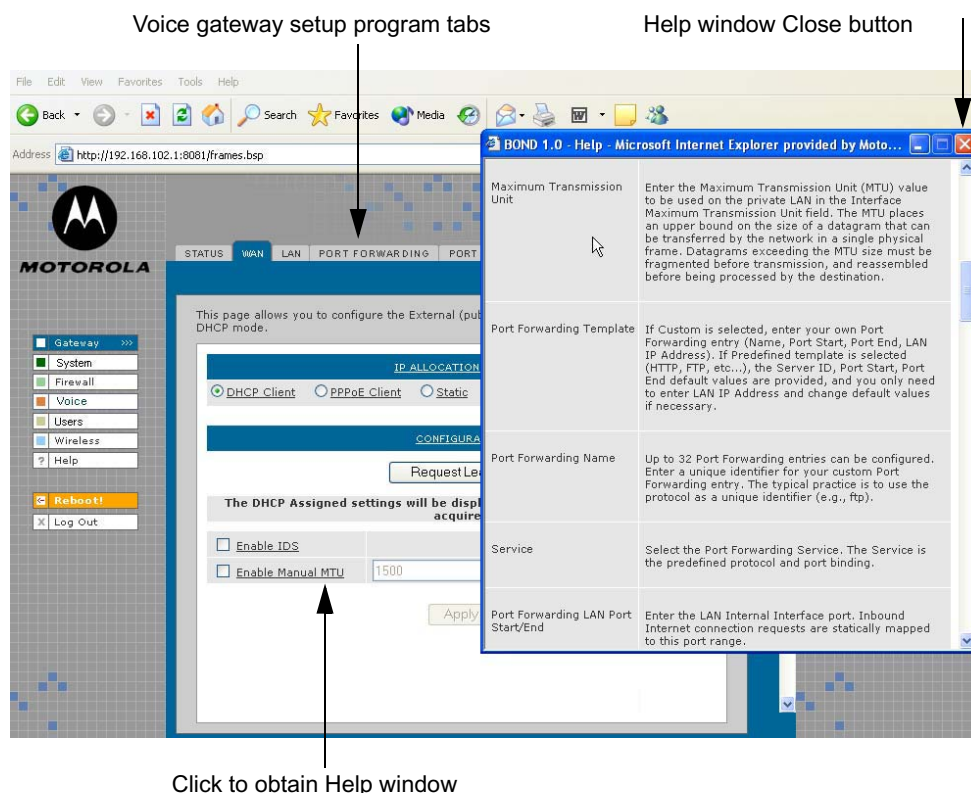
This section describes how to use the configuration pages in the [VT2400/VT2500](#) Setup Program for configuring your local and wide area networks. You will need to refer to the Configuration Worksheet you filled out in [Installation](#) to successfully configure your network.

- [Gateway > STATUS](#)
- [Gateway > WAN — DHCP Client](#)
- [Gateway > WAN — PPPoE Client](#)
- [Gateway > WAN — Static](#)
- [Gateway > LAN — nat config](#)
- [Gateway > LAN — dhcp server config](#)
- [Gateway > LAN — dhcp leases](#)
- [Gateway > LAN — static leases](#)
- [Gateway > PORT FORWARDING — status](#)
- [Gateway > PORT FORWARDING — config](#)
- [Gateway > PORT TRIGGERS - predefined](#)
- [Gateway > PORT TRIGGERS - custom](#)
- [Gateway > DNS](#)
- [Gateway > LOG](#)
- [System > CONTROL](#)
- [System > CONFIGURATION — backup](#)
- [System > CONFIGURATION — restore](#)
- [System > CONFIGURATION — reset](#)
- [System > LOG](#)
- [Firewall > FIREWALL — basic](#)
- [Firewall > FIREWALL — advanced](#)
- [Firewall > CONTENT FILTER — status](#)
- [Firewall > CONTENT FILTER — config](#)
- [Firewall > SCHEDULES — status](#)
- [Firewall > SCHEDULES — config](#)
- [Firewall > LOG](#)
- [Voice > STATUS](#)
- [Voice > SERVICE](#)
- [Users > USERS — status](#)
- [Users > USERS — config](#)
- [Users > USER GROUPS](#)
- [Users > LOG](#)
- [Wireless > STATUS](#)
- [Wireless > NETWORK](#)
- [Wireless > SECURITY — basic](#)
- [Wireless > SECURITY — advanced](#)
- [Wireless > STATISTICS](#)

After you edit the field and click **Apply** for some settings, you are required to reboot the [VT2400/VT2500](#) for the changes to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.

Using the Getting Started Wizard

When you log in to the [VT2400/VT2500](#) setup program, the first screen that appears ([Gateway > STATUS](#)) provides a configuration wizard to help you through the configuration screens. By selecting **Launch Getting Started Wizard** on the [Gateway > STATUS](#) page, you can access a subset of the configuration screens in succession. To use the online help, click any field that is underlined on any wizard screen to obtain a Help window, which provides information to help you configure that particular field.



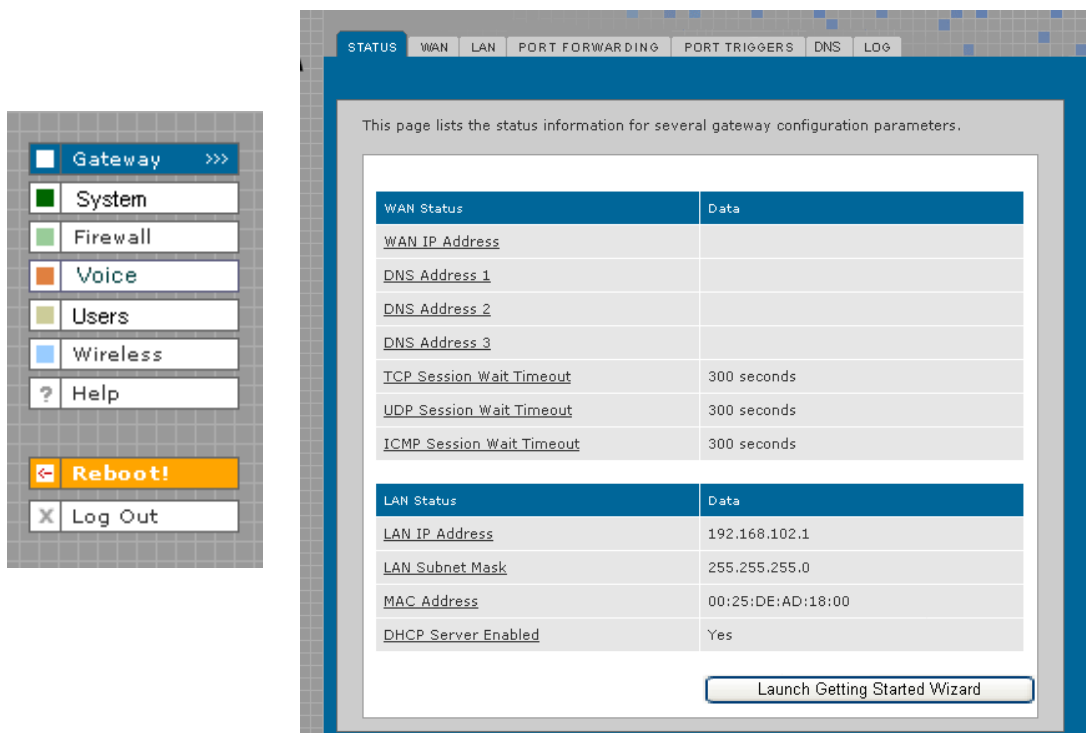
In the example shown, if you click Enable Manual MTU, the Help window displays information about Maximum Transmission Unit (MTU). To close the Help screen, simply click the close button in the upper right corner.

When you finish the current screen, click the next tab at the top of the graphical user interface to continue configuring the voice gateway network. In the example shown, you would click **LAN** after entering all the necessary information on the WAN pages.

Refer to the corresponding configuration pages in this section for more help when configuring the network using the wizard.

Gateway > STATUS

This page displays the status information for several gateway configuration parameters:



STATUS | WAN | LAN | PORT FORWARDING | PORT TRIGGERS | DNS | LOG

This page lists the status information for several gateway configuration parameters.

WAN Status	Data
WAN IP Address	
DNS Address 1	
DNS Address 2	
DNS Address 3	
TCP Session Wait Timeout	300 seconds
UDP Session Wait Timeout	300 seconds
ICMP Session Wait Timeout	300 seconds

LAN Status	Data
LAN IP Address	192.168.102.1
LAN Subnet Mask	255.255.255.0
MAC Address	00:25:DE:AD:18:00
DHCP Server Enabled	Yes

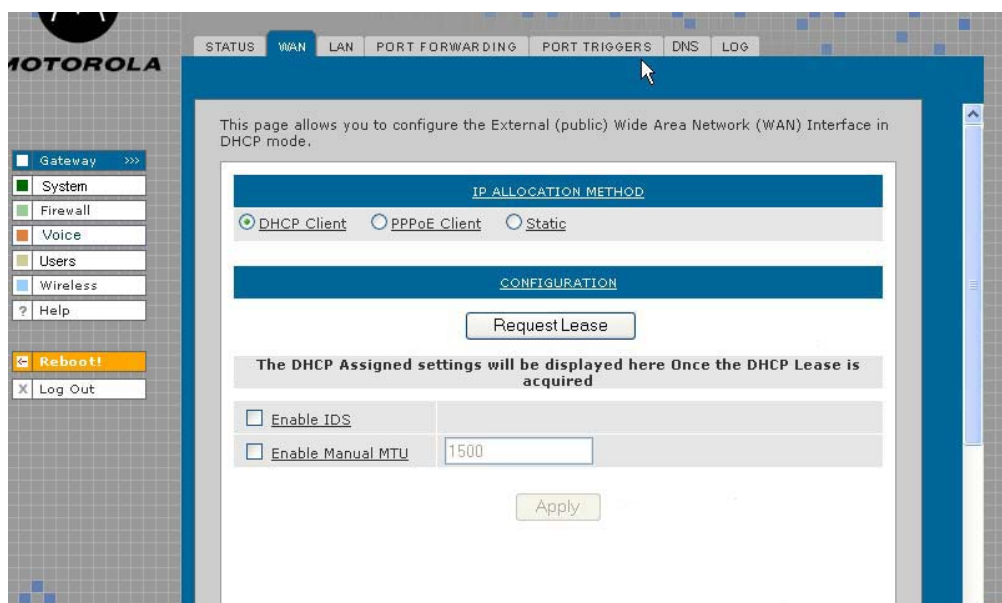
[Launch Getting Started Wizard](#)

To view a definition of any field on the Status page, click the [underlined field](#). A Help screen appears that displays the definition.

You may want to select the Launch Getting Started Wizard, which takes you through the minimum screens you need to verify for any voice gateway network. Refer to ["Using the Getting Started Wizard"](#) for more information.

Gateway > WAN — DHCP Client

Use this page to configure the external (public) wide area network (WAN) interface for an IP Allocation Method of DHCP Client. Refer to your Modem Worksheet in “[Basic Configuration](#)” to determine which type of IP allocation method you must configure.



Gateway > WAN — DHCP Client page fields

Field	Description
-------	-------------

IP ALLOCATION METHOD:

DHCP Client (default)	Use this page if you have a cable Internet provider that uses dynamic IP addressing, which automatically obtains the public IP address, subnet mask, domain name, and DNS server(s). DHCP Client is the default IP allocation method.
------------------------------	---

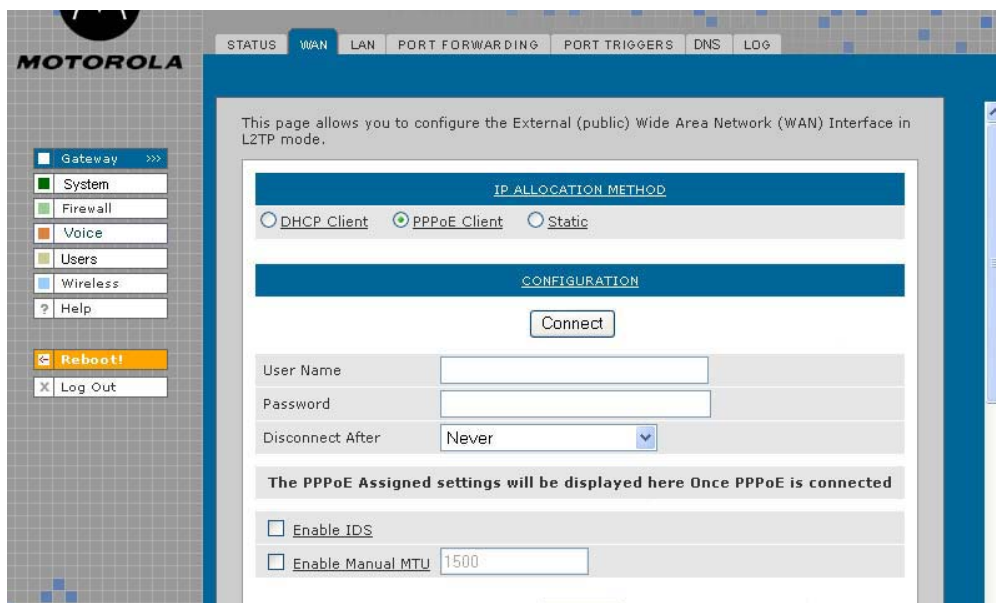
CONFIGURATION

Request Lease	Click this button to obtain a DHCP leased IP address. Once the lease is acquired, the assigned settings are displayed. Up to 64 IP addresses can be leased.
Enable IDS	Enables the intrusion detection system (IDS) which inspects all inbound and outbound network activity.
Enable Manual MTU	Defines the maximum size of the packets sent from your computer to the network. Enter 1500 for an Ethernet LAN (how about for wireless- leave blank?)
Apply (button)	Click Apply to save your changes.

Gateway > WAN — PPPoE Client

Use this page to configure the external (public) wide area network (WAN) interface with an IP Allocation Method of PPPoE Client. Refer to your Modem Worksheet in “[Basic Configuration](#)” to determine which type of IP allocation method you must configure.

:



Gateway > WAN — PPPoE Client page fields

Field

Description

IP ALLOCATION METHOD:

PPPoE Client

Use this page if you have a DSL service provider.

CONFIGURATION

Connect (button)

Click this button to obtain a DHCP leased IP address. Once the lease is acquired, the assigned settings are displayed.

User Name

Type the user name you selected when you set up your user name in the basic configuration procedures.

Password

Type the password you selected when you set up your password in the basic configuration procedures.

Disconnect After

From the list, select the amount of time before being disconnected from the Internet after a period of inactivity.

Note: The default for auto-reconnect is *enabled*. When auto-reconnect is enabled, the disconnect timer is automatically disabled. ([Where is auto reconnect configured?](#))

Enable IDS

Enables the intrusion detection system (IDS), which inspects all inbound and outbound network activity.

Enable Manual MTU

Defines the maximum transmission unit (size of packets) sent from your computer to the network. Enter 1500 for an Ethernet LAN. ([How about for wireless- leave blank?](#))

Apply (button)

Click **Apply** to save your changes.



Gateway > WAN — Static

Use this page to configure the external (public) wide area network (WAN) interface. The default is DHCP Client. Refer to your Modem Worksheet in “[Basic Configuration](#)” to determine which type of IP allocation method you must configure.

The screenshot shows the Motorola Gateway configuration interface. The 'WAN' tab is selected. The 'IP ALLOCATION METHOD' section has 'Static' selected. The 'CONFIGURATION' section has the following fields: IP Address, Subnet Mask, Gateway, Enable IDS (unchecked), and Enable Manual MTU (checked, with a value of 1500). An 'Apply' button is at the bottom.

Gateway > WAN — Static page fields

Field

Description

IP ALLOCATION METHOD:

Static

Use this page if you answered No on the worksheet to “Is the IP address obtained dynamically?”

CONFIGURATION

IP Address

Type the static *IP address* provided by the service provider in [dotted-decimal format](#). The default is None. Example: 192.168.102.150

Subnet Mask

Type the *subnet mask* associated with the static IP address in dotted-decimal format. The default is None.

Gateway

Type the default gateway *IP address* on the WAN for the [VT2400/VT2500](#) in dotted-decimal format.

Enable IDS

Enables the intrusion detection system (IDS), which inspects all inbound and outbound network activity.

Enable Manual MTU

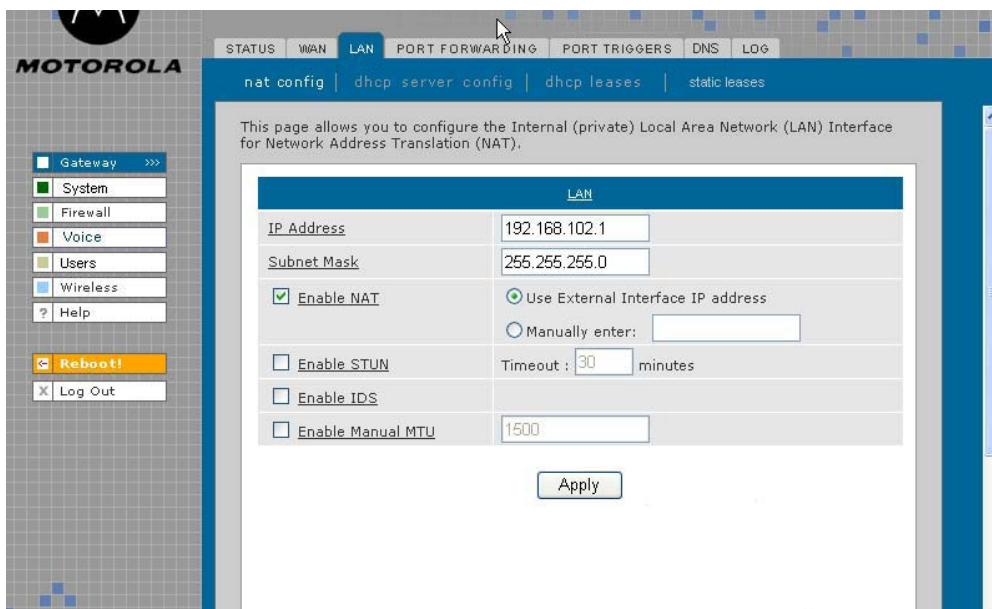
Defines the maximum size of the packets sent from your computer to the network. Enter 1500 for an Ethernet LAN ([How about for wireless?](#)).

Apply (button)

Click **Apply** to save your changes.

Gateway > LAN — nat config

Use this page to enable NAT (Network Address Translation) and add clients to the **CURRENT NAT PASSTHROUGH** list:



The screenshot shows the 'LAN' configuration page for NAT. The 'IP Address' field is set to 192.168.102.1 and the 'Subnet Mask' is 255.255.255.0. The 'Enable NAT' checkbox is checked, and the 'Use External Interface IP address' radio button is selected. The 'Enable STUN' checkbox is unchecked, and the 'Timeout' is set to 30 minutes. The 'Enable IDS' checkbox is unchecked. The 'Enable Manual MTU' checkbox is unchecked, and the 'MTU' is set to 1500. The 'Apply' button is at the bottom.

Gateway > LAN — nat config page fields

Field or Button	Description
LAN	Local Area Network
IP Address	The LAN internet protocol (IP) address assigned by your Internet service provider.
Subnet Mask	The subnet mask assigned by your Internet service provider.
Enable NAT	If enabled, the single HFC IP Address (public IP address) assigned by the service provider is mapped to many private IP addresses on the VT2500 LAN. Use External Interface IP address - Manually enter -
Enable STUN	Enables a protocol for assisting devices behind a NAT firewall or router with their packet routing. STUN allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It provides applications with the ability to determine the public Internet Protocol (IP) addresses allocated to them by the NAT. STUN works with many existing NATs and allows for a wide variety of applications to work through existing NAT infrastructure.
Enable IDS	Enables the intrusion detection system (IDS), which inspects all inbound and outbound network activity.
Enable Manual MTU	Defines the maximum size of the packets sent from your computer to the network. Enter 1500 for an Ethernet LAN (How about for wireless?)
Apply (button)	Click to Apply your changes. You must reboot the VT2500.



Gateway > LAN — dhcp server config

Only experienced network administrators should use this page to perform advanced DHCP server configuration. Use this page to configure the DHCP server programs for your private LAN.

This page allows you to configure the SBG DHCP server parameters for your private LAN.
Note: Only experienced network users should modify these parameters.

DHCP Server

☒ Enable

IP Address Pool

☐ IP Subnet

☒ IP Range

192.168.102.100 - 192.168.102.200

Lease Duration 60 minutes

Wins Server 1 192.168.102.10

Wins Server 2 192.168.102.11

Wins Server 3 0

☐ Enable DNS Proxy

☐ Enable DHCP Relay

Apply

CAUTION!



Do not modify these settings unless you are an experienced network administrator with strong knowledge of IP addressing, subnetting, and DHCP.

Gateway > LAN — dhcp server config page fields

Field

Description

DHCP SERVER

Enable

Select this option to enable the DHCP server settings that follow.

IP Address Pool

You can type the *IP address* of the [VT2400/VT2500](#) for your private LAN. The default is 192.168.102.1.

When you change the LAN IP address, the voice gateway automatically adjusts the address pool to match the new subnet, invalidates any leases which conflict with the new IP address, redirects the active Web logon session to the new address, and moves Telnet to the new address.

IP Subnet

Displays the subnet mask in dotted-decimal format. The default is [255.255.255.0](#).

IP Range

Enter the starting *IP address* and the ending *IP address* in dotted-decimal format to be assigned to clients by the DHCP server. The default lease pool size is 64.

Lease Duration

Sets the *time* in seconds that the VT2500 DHCP server leases an IP address to a client. The default is 86,400 seconds (24 hours).

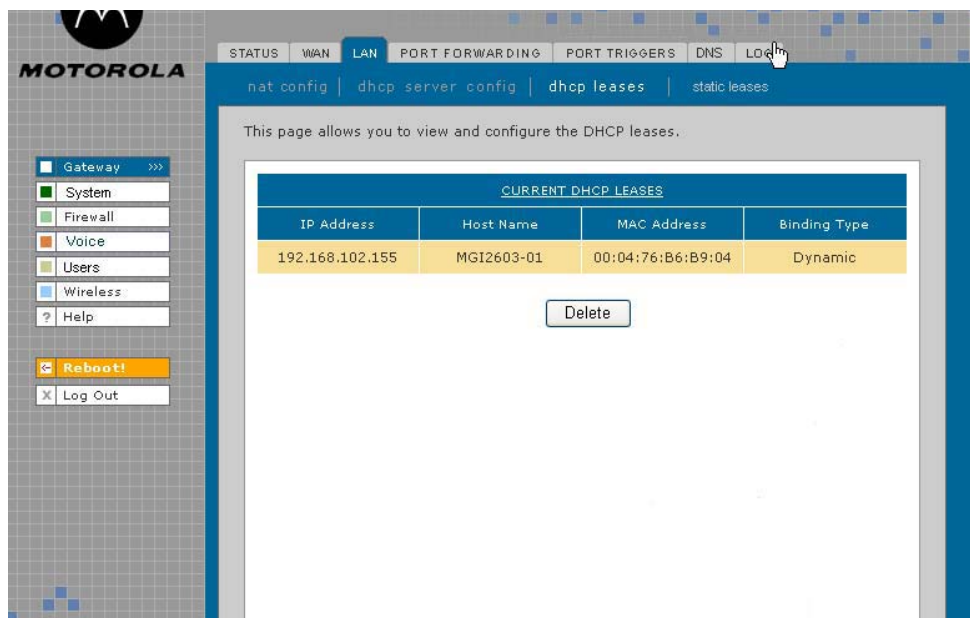


Gateway > LAN — dhcp server config page fields (continued)

Field	Description
Wins Server 1	The IP address of the first Windows Internet Naming Service server that assigns IP addresses dynamically.
Wins Server 2	The IP address of the second Windows Internet Naming Service server that assigns IP addresses dynamically.
Wins Server 3	The IP address of the third Windows Internet Naming Service server that assigns IP addresses dynamically.
Enable DNS Proxy	Enables a server that sits between the client application, such as a Web browser, and a real server. Its job is to improve performance as it intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. A company or household might use a proxy server to prevent its members from accessing a specific set of Web sites.
Enable DHCP Relay	The Gateway can relay the actual DNS queries to some other server. Such relaying of DNS querying to some other server is called a DNS relay.
Apply (button)	Click to apply your changes. You must reboot the VT2400/VT2500.

Gateway > LAN — dhcp leases

Use this page to view and configure DHCP leases.

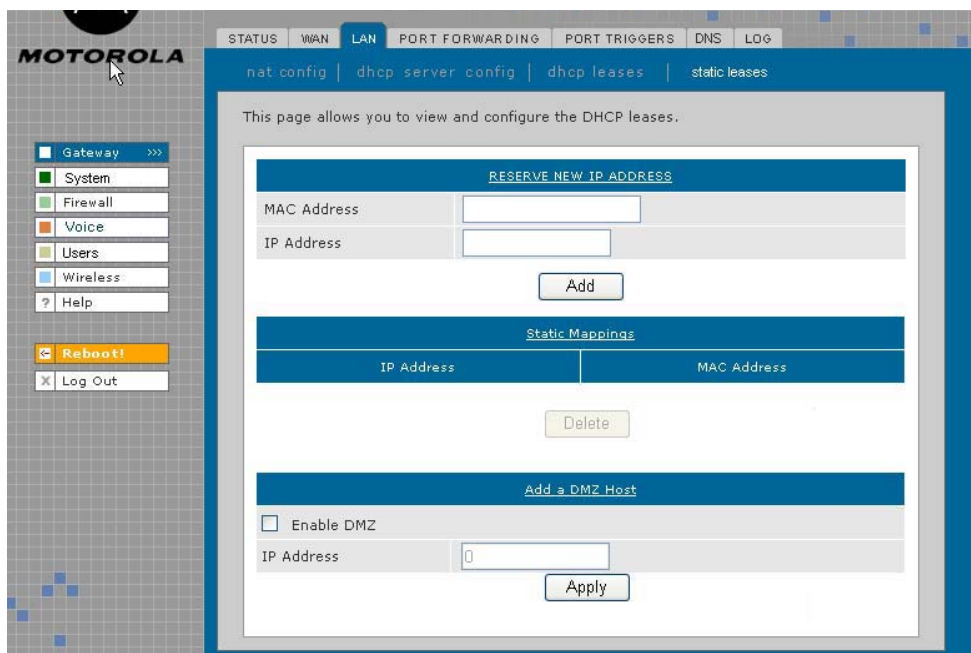


Gateway > LAN — dhcp leases page fields

Field	Description
CURRENT DHCP LEASES	Displays all DHCP clients that have reserved IP addresses. The table entries represent both reserved (static) leases added by the user and dynamic leases automatically assigned by the DHCP server.
IP Address	Displays its reserved IP address.
Host Name	Displays its host name.
MAC Address	Displays the client MAC address.
Binding Type	How the IP address is bound to the network (Dynamic or Static).?
Delete (button)	Select a DHCP lease in the list and click Delete to remove the lease from this list.

Gateway > LAN – static leases

Use this page to configure DHCP static leases, including one for a DMZ device:



Gateway > LAN — static leases page fields

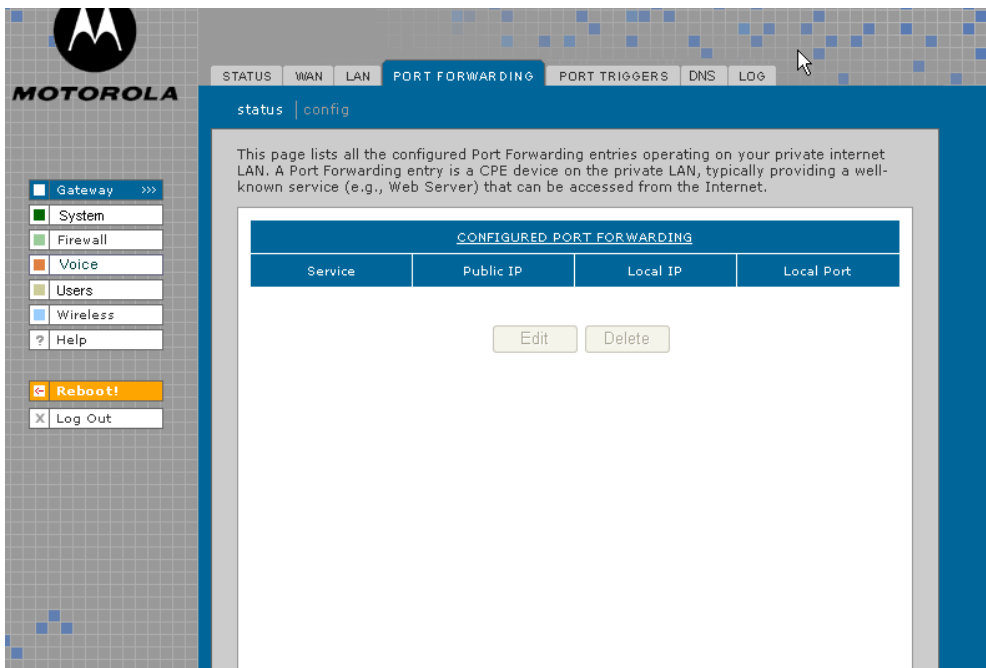
Field	Description
RESERVE NEW IP ADDRESS	You can reserve up to 64 IP addresses assigned by the VT2400/VT2500 DHCP server for specific LAN clients. For example, to ensure that they always receive the same private IP address, you can reserve IP addresses for a private FTP server or gaming DMZ device. You may reserve up to 16 IP addresses for CPEs on your LAN that are assigned by the voice gateway's DHCP server. You may want to reserve an IP address on your LAN for a particular server (such as a private FTP server) to ensure the designated server always receives the same private IP address.
MAC Address	Type the MAC address of the DHCP client for which a reserved IP address is required. The format is 16 hexadecimal numerals. NOTE: If the MAC Address you entered already has an IP Address assigned and is listed in the CURRENT DHCP LEASES table as Dynamic on the Gateway > LAN — dhcp leases page, you must reserve the same IP Address that is listed there for this MAC Address.
IP Address	Sets the host portion of the reserved IP address for the LAN client having the specified MAC address. When the LAN client requests an IP address, the VT2400/VT2500 DHCP server assigns the client this IP address.
Add (button)	After you have entered a MAC address and an IP address, click Add to reserve a new IP address. The IP address and MAC address appear in the STATIC MAPPINGS table.

Gateway > LAN — static leases page fields (continued)

Field	Description
Static Mappings:	You can select a device to always receive the same IP address by adding a static binding/mapping. The IP address you specify for the MAC address will always be the one allocated by the DHCP server.
IP Address	Specify the IP address that should always be mapped to the MAC address displayed alongside it in this table.
MAC Address	This MAC address is always mapped to the IP address displayed alongside it in this table.
Delete (button)	Select an IP/MAC address in the STATIC MAPPINGS table and then click the Delete button to remove it from the list.
Add a DMZ Host:	
Enable DMZ	The gaming DMZ host is a computer with a reserved IP address designated as the default DMZ host. Only one gaming DMZ host can be active at once. <i>The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a computer to be in the DMZ.</i> The benefit of using a gaming DMZ host instead of a NAT passthrough host is that a gaming DMZ host does not require a public IP address as does a NAT passthrough host. If the application requires a public IP address, configure the computer for NAT passthrough on the Gateway > LAN — nat config page.
IP Address	Sets the host portion of the reserved IP address for the LAN client having the specified MAC address. When the LAN client requests an IP address, the VT2500 voice gateway DHCP server assigns the client this IP address.
Apply (button)	Click to apply your changes. You must reboot the VT2400/VT2500 .

Gateway > PORT FORWARDING — status

Use this page to view the configured port forwarding entries for the [VT2400/VT2500](#) LAN. Refer to [Gateway > PORT FORWARDING — config](#) for complete definitions of each field.



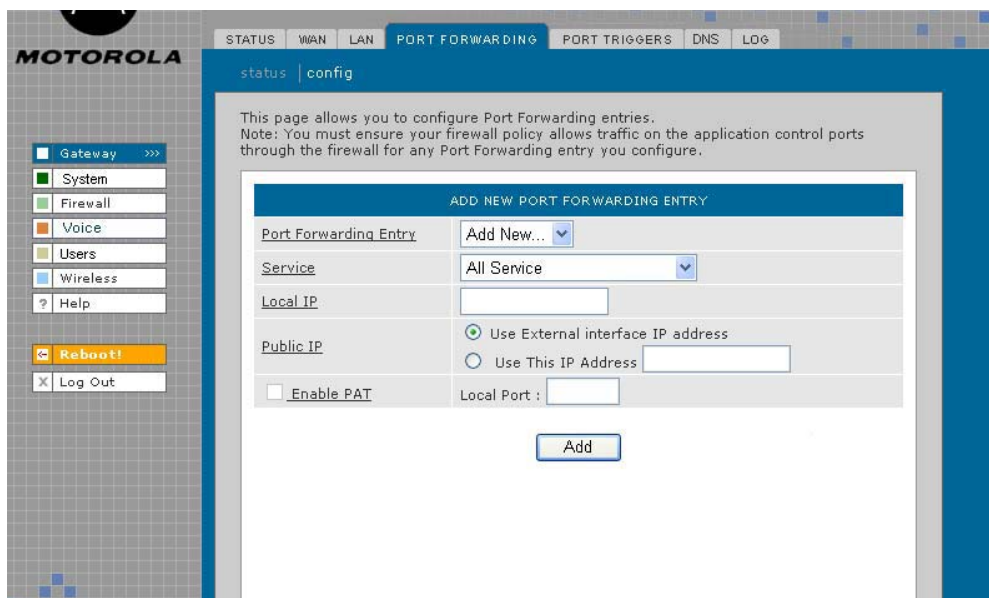
The screenshot shows the Motorola Gateway web interface. The top navigation bar includes tabs for STATUS, WAN, LAN, PORT FORWARDING (selected), PORT TRIGGERS, DNS, and LOG. Below the tabs, there are links for 'status' and 'config'. The main content area has a heading 'CONFIGURED PORT FORWARDING' and a table with columns: Service, Public IP, Local IP, and Local Port. Below the table are 'Edit' and 'Delete' buttons. A sidebar on the left contains a menu with 'Gateway' (selected), 'System', 'Firewall', 'Voice', 'Users', 'Wireless', and 'Help'. At the bottom of the sidebar are 'Reboot!' and 'Log Out' buttons.

This page lists all the configured Port Forwarding entries operating on your private internet LAN. A Port Forwarding entry is a CPE device on the private LAN, typically providing a well-known service (e.g., Web Server) that can be accessed from the Internet.

Service	Public IP	Local IP	Local Port
Edit Delete			

Gateway > PORT FORWARDING — config

Use this page to configure up to 30 virtual servers.



Gateway > PORT FORWARDING — config page fields

Field	Description
ADD NEW PORT FORWARDING ENTRY	You can configure up to 64 virtual servers. If you select Custom, you must set the Name, Port Start, Port End, and LAN IP Address.
Port Forwarding Entry (new)	Type a unique identifier for the custom virtual server. The typical practice is to use the protocol as a unique identifier (for example "ftp").
Service	Sets the LAN internal interface port or the start of a port range. Inbound Internet connection requests are statically mapped to this port. The voice gateway includes predefined port triggers (enabled by default) for many popular applications and protocols, including: DirectX, MS zone.com, Battle.net, Quicktime, Netmeeting H.323, Net2Phone, MSN Messenger, AOL Instant Messenger. In addition, predefined port forwarding templates are provided for many applications, such as: - FTP 20, 21 - HTTP 80 - NTP 123 - Secure Shell 22 - SMTP e-mail 25 - Telnet 23
Local IP	Sets the private LAN IP address for the port forwarding page. An Internet user must know the public IP address to access any port forwarding entry you define on the private LAN.

Gateway > PORT FORWARDING — config page fields (continued)

Field	Description
Public IP	Enter the public IP address for the Port Forwarding service. Note: An Internet user must know this External (public) WAN Interface IP address in order to access any Port Forwarding entry you define on the private LAN. Sets the public LAN IP address for the port forwarding page. An internet user must know the public IP address to access any port forwarding entry you defined on the private LAN.
Use External interface IP address	Select this option if you are using an external (does this mean dynamically assigned addressing?) interface IP address.
Use this IP address	Select this option if you are using a static IP address, then type the address in the field provided.
Enable PAT (Port Address Translation)	Select this box to enable the port forwarding entries to be accessed through network address translation (NAT). Notes: The most common form of address translation between public and private IP addresses is NAT. This represents a mapping of one public IP address to many private IP addresses. Using NAT, you can support up to 253 clients on your private LAN. If NAT is disabled, then the voice terminal DHCP server is also disabled. In this case, none of the client devices on your private internal LAN will be assigned an IP address from the voice terminal DHCP server. Instead, your clients are treated as passthrough devices, and if they are configured to use DHCP, they will attempt to obtain a public IP address from your ISP.
Local Port	
Add (button)	Click Add to save this virtual server to the PORT FORWARDING list. The configured port(s) appear on the Gateway > PORT FORWARDING — status page.

Gateway > PORT TRIGGERS - predefined

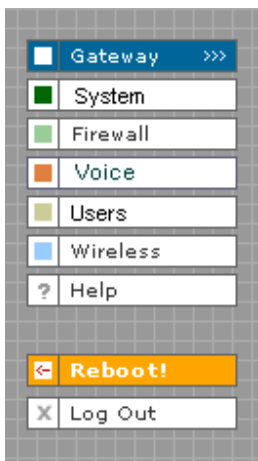
When you run a PC application that accesses the Internet, it communicates with a computer on the Internet. In some applications, especially gaming, the computer on the Internet also communicates with your PC. Because NAT does not normally allow these incoming connections, the [VT2400/VT2500](#) supports port triggering.

The [VT2400/VT2500](#) is preconfigured with port triggering for common applications. You can also configure additional port triggers if needed. Configuring port triggers for an application requires:

- The application transport protocol — TCP or UDP
- The application port number

You can use the default values for the remaining parameters.

Only one computer at a time connected to the [VT2400/VT2500](#) can use an application that requires port triggering. Use this page to view predefined port triggers.



Gateway >>>

System

Firewall

Voice

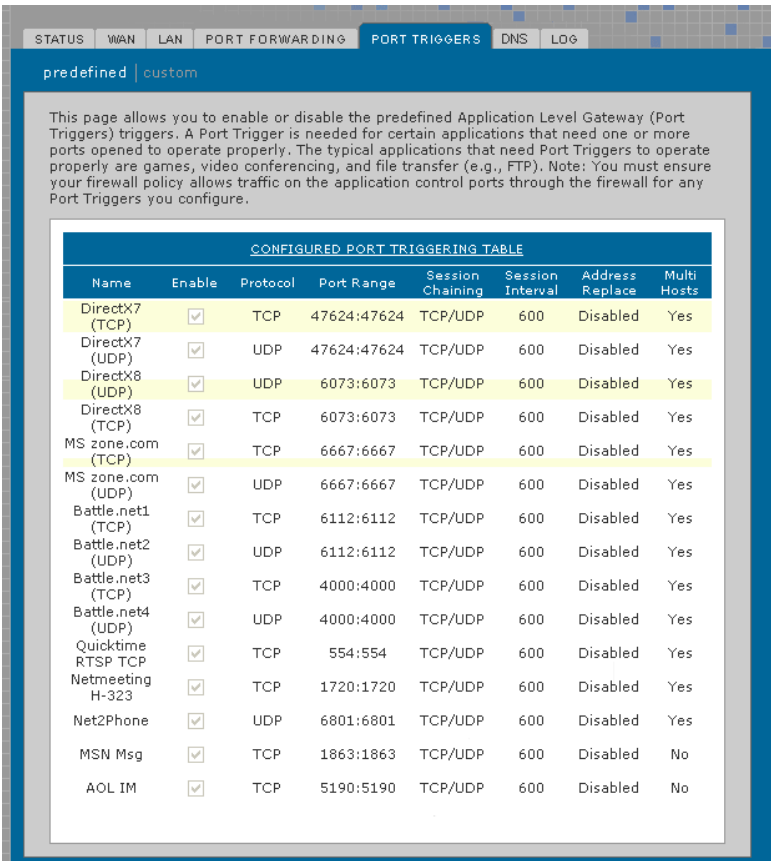
Users

Wireless

Help

Reboot!

Log Out



STATUS WAN LAN PORT FORWARDING **PORT TRIGGERS** DNS LOG

predefined | custom

This page allows you to enable or disable the predefined Application Level Gateway (Port Triggers) triggers. A Port Trigger is needed for certain applications that need one or more ports opened to operate properly. The typical applications that need Port Triggers to operate properly are games, video conferencing, and file transfer (e.g., FTP). Note: You must ensure your firewall policy allows traffic on the application control ports through the firewall for any Port Triggers you configure.

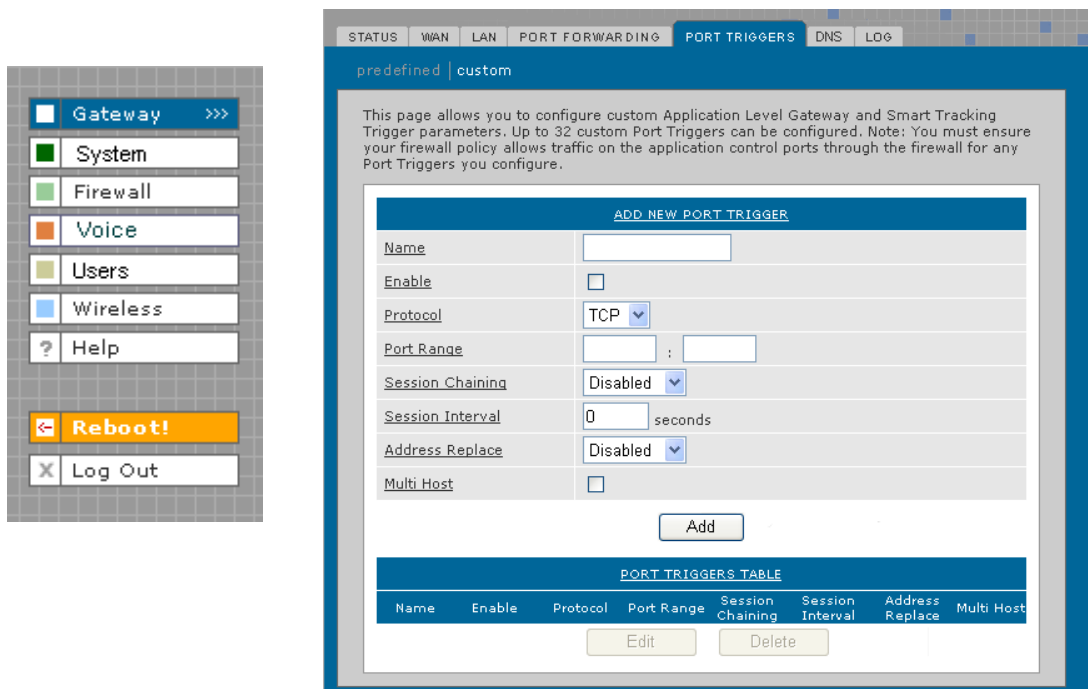
CONFIGURED PORT TRIGGERING TABLE							
Name	Enable	Protocol	Port Range	Session Chaining	Session Interval	Address Replace	Multi Hosts
DirectX7 (TCP)	☒	TCP	47624:47624	TCP/UDP	600	Disabled	Yes
DirectX7 (UDP)	☒	UDP	47624:47624	TCP/UDP	600	Disabled	Yes
DirectX8 (UDP)	☒	UDP	6073:6073	TCP/UDP	600	Disabled	Yes
DirectX8 (TCP)	☒	TCP	6073:6073	TCP/UDP	600	Disabled	Yes
MS zone.com (TCP)	☒	TCP	6667:6667	TCP/UDP	600	Disabled	Yes
MS zone.com (UDP)	☒	UDP	6667:6667	TCP/UDP	600	Disabled	Yes
Battle.net1 (TCP)	☒	TCP	6112:6112	TCP/UDP	600	Disabled	Yes
Battle.net2 (UDP)	☒	UDP	6112:6112	TCP/UDP	600	Disabled	Yes
Battle.net3 (TCP)	☒	TCP	4000:4000	TCP/UDP	600	Disabled	Yes
Battle.net4 (UDP)	☒	UDP	4000:4000	TCP/UDP	600	Disabled	Yes
Quicktime RTSP TCP	☒	TCP	554:554	TCP/UDP	600	Disabled	Yes
Netmeeting H-323	☒	TCP	1720:1720	TCP/UDP	600	Disabled	Yes
Net2Phone	☒	UDP	6801:6801	TCP/UDP	600	Disabled	Yes
MSN Msg	☒	TCP	1863:1863	TCP/UDP	600	Disabled	No
AOL IM	☒	TCP	5190:5190	TCP/UDP	600	Disabled	No

Gateway > PORT TRIGGERS — predefined page fields

Field	Description
CONFIGURED PORT TRIGGERING TABLE	
Name	Displays the unique name for the port triggers. This is typically the protocol name.
Enable	Select this box to activate the port triggers for the predefined application.
Protocol	Displays the transport protocol for the port trigger — TCP or UDP.
Port Range	Displays the port range (From/To) for the port trigger.
Session Chaining	Displays the session chaining selection for the port trigger — Disable, TCP, or TCP/UDP.
Session Interval	Displays the session interval set for the port trigger.
Address Replace	Displays the address replacement method for the port trigger.
Multi Hosts	Displays the multi-host selection for the port trigger.

Gateway > PORT TRIGGERS - custom

Use this page to create a custom port trigger:



Gateway > PORT TRIGGERS — custom page fields

Field	Description
ADD NEW PORT TRIGGER	
Name	Enter the unique name for the port trigger. This is typically the protocol.
Enable	Select this box to enable the custom port trigger.
Protocol	Sets the transport protocol for the port trigger — TCP or UDP.
Port Range (From:To)	Sets the port range for the port trigger. Type the start of the range in the left field and the end in the right field.
Session Chaining	Enable session chaining if the application needs to open one or more ports in different ranges to operate properly. The options are Disable, TCP, or TCP/UDP.
Session Interval	Sets the session interval for the application: - If the port triggers detect traffic on the Port Range within the Session Interval, it is considered to be related to the initial session. - If the port triggers detect traffic on the Port Range after the Session Interval expires, it is considered to be a new and unique session.
Address Replace	Sets the address replacement method for the application.
Multi Host	Select if appropriate for the application.



Gateway > PORT TRIGGERS — custom page fields (continued)

Field

Description

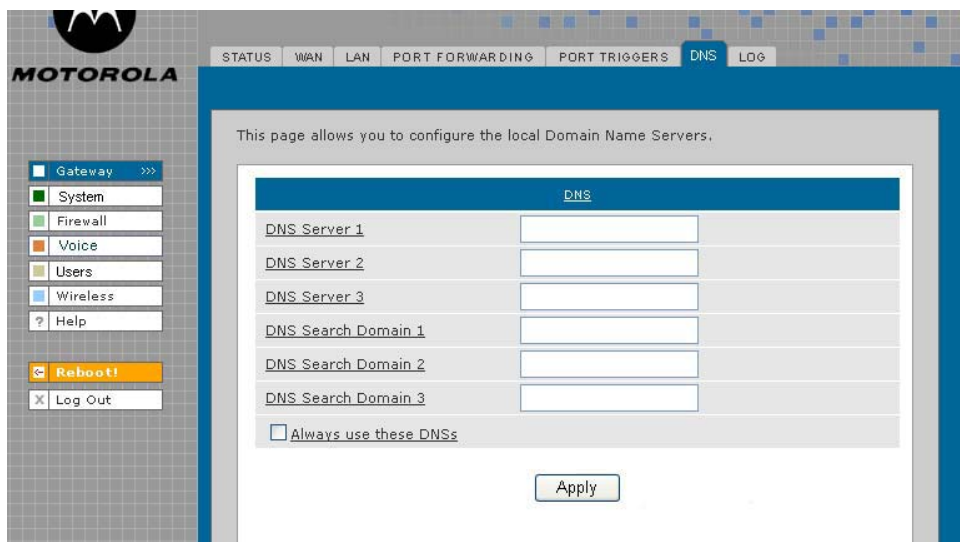
Add

Click to add the port trigger to the PORT TRIGGERS TABLE.

PORT TRIGGERS TABLE Lists all defined port triggers and their parameters.

Gateway > DNS

Use this page to configure the local Domain Name Servers:



Gateway > DNS page fields

Field

Description

DNS

DNS Server 1

Type the IP address for the first DNS server (refer to the Configuration Worksheet you completed in Section 2). Valid numbers are between 0 and 255. The ISP Domain Name Server provides name-to-IP address translation. If your ISP does not automatically assign your DNS addresses from their DHCP server, they will need to provide you with at least one DNS server IP address that you enter in the DNS IP Address fields. You may manually enter two more. **Example:** 192.168.102.1

DNS Server 2

Type the IP address of a second DNS server as described above.

DNS Server 3

Type the IP address of a third DNS server as described above.

DNS Search Domain 1

Type the domain name of DNS Server 1. **Example:** www.example.com

DNS Search Domain 2

Type the domain name of DNS Server 2.

DNS Search Domain 3

Type the domain name of DNS Server 3.

Always use these DNSs

When this check box is selected, the voice gateway will use the DNS Servers specified on the Gateway > DNS page. If not selected, the DNS Servers obtained from external servers are used.

Apply (button)

Click to apply your changes. (Is a reboot required?)

Gateway > LOG

Use this page to view detailed information about the gateway:

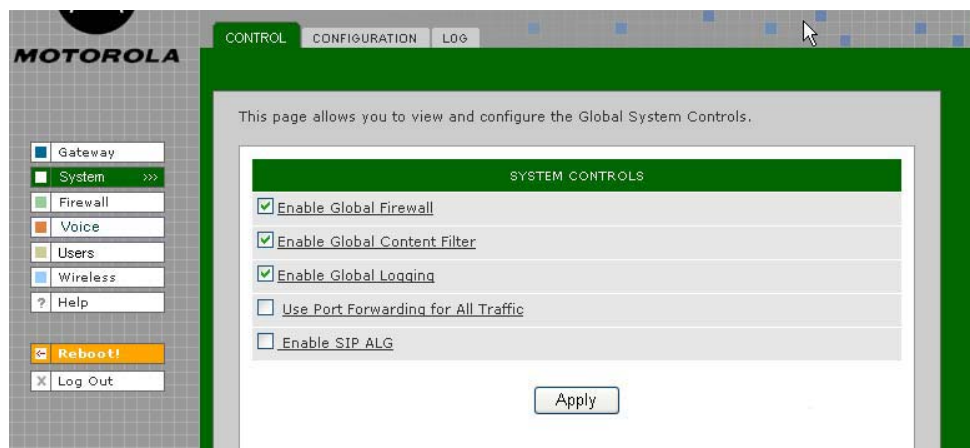


Gateway > LOG page fields

Field	Description
GATEWAY LOG	The table shows the logging information related to gateway activity.
Clear Log (button)	Clears the entries in the log. Types of entries include DHCP server lease information, wireless client associations, and user interface access (log in, etc.) The log can hold up to xx entries.
Time	The date and time of the event in the format yyyy-mm-dd hh:mm:ss
Description	The URL or Web page accessed.
Source Address	The source IP address of the inbound or outbound message.??
Destination Address	The destination IP address of the inbound or outbound message.??
Rule Number	The firewall profile rule applicable to this entry. Refer to Firewall > FIREWALL — advanced for more information about firewall rules.

System > CONTROL

Use this page to view and configure the Global System Controls.



System > CONTROL page fields

Field

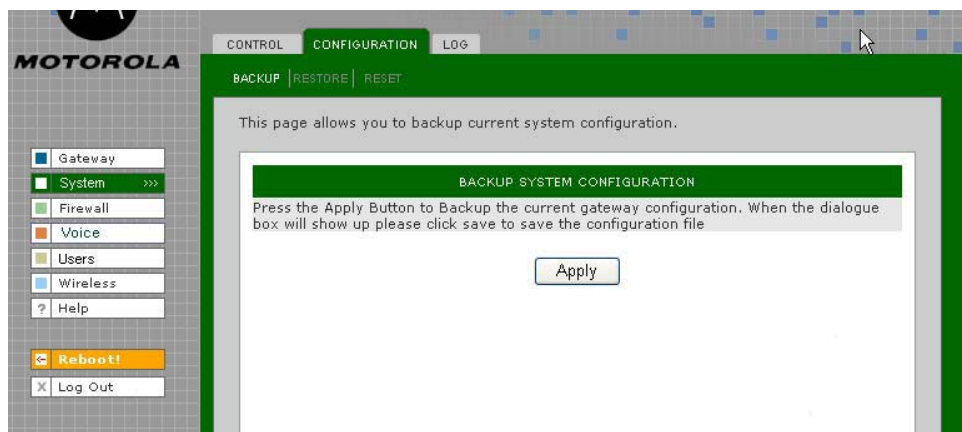
Description

SYSTEM CONTROLS

Enable Global Firewall	If you disable the global firewall, all the traffic will be allowed to pass through the firewall, irrespective of the policy rules configured. Default is
Enable Global Content Filter	Enable the global content filter to use the profiles configured under the Content Filter Profiles.
Enable Global Logging	Enable global logging to log gateway system events, such as
Use Port Forwarding for All Traffic	Applies port forwarding rules to all traffic, as defined on the Gateway > PORT FORWARDING — config page. If this option is enabled, the firewall allows incoming connections to any virtual servers (using port forwarding rules), even if firewall rules are configured to block them. This provides a way to create a port forwarding rule to allow traffic without having to reconfigure the firewall.
Enable SIP ALG	The gateway can act as SIP ALG (Session Initiation Protocol Application Layer Gateway) when enabled. Recommended for interactive communication sessions between users for voice, video, chat, interactive, games, and virtual reality.
Apply (button)	Click Apply to save your changes.

System > CONFIGURATION — backup

Use this page to back up the current system configuration:



System > CONFIGURATION — backup page fields

Field

Description

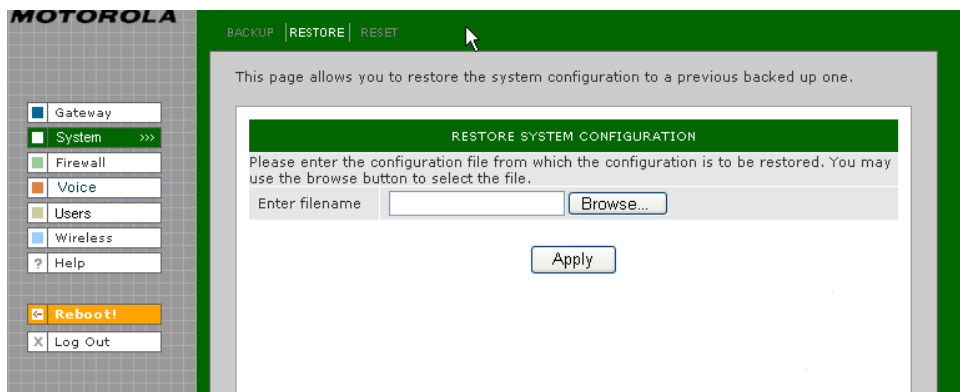
BACK UP SYSTEM CONFIGURATION

Apply (button)

Click **Apply** to back up the current configuration. When the Save dialog appears, click Save to preserve the configuration file.

System > CONFIGURATION — restore

Use this page to restore the system configuration to one that was backed up previously:



System > CONFIGURATION — restore page fields

Field

Description

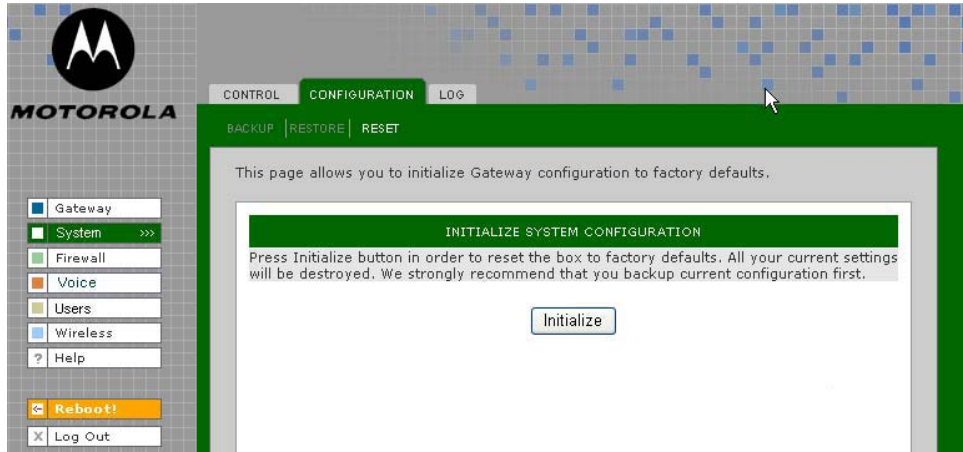
RESTORE SYSTEM CONFIGURATION

Enter Filename	Enter the path of the configuration file from which the configuration is to be restored. Use the Browse button to select the path and file name.
Apply (button)	Click Apply to restore the VT2400/VT2500 configuration to the settings in the file specified in the Enter filename field. This message appears: "Device will be rebooted after configuration restore. Continue?" Click Yes to continue or click Cancel to keep the current configuration.



System > CONFIGURATION — reset

Use this page to reset the current system configuration to the factory default settings.



System > CONFIGURATION — reset page fields

Field

Description

INITIALIZE SYSTEM CONFIGURATION

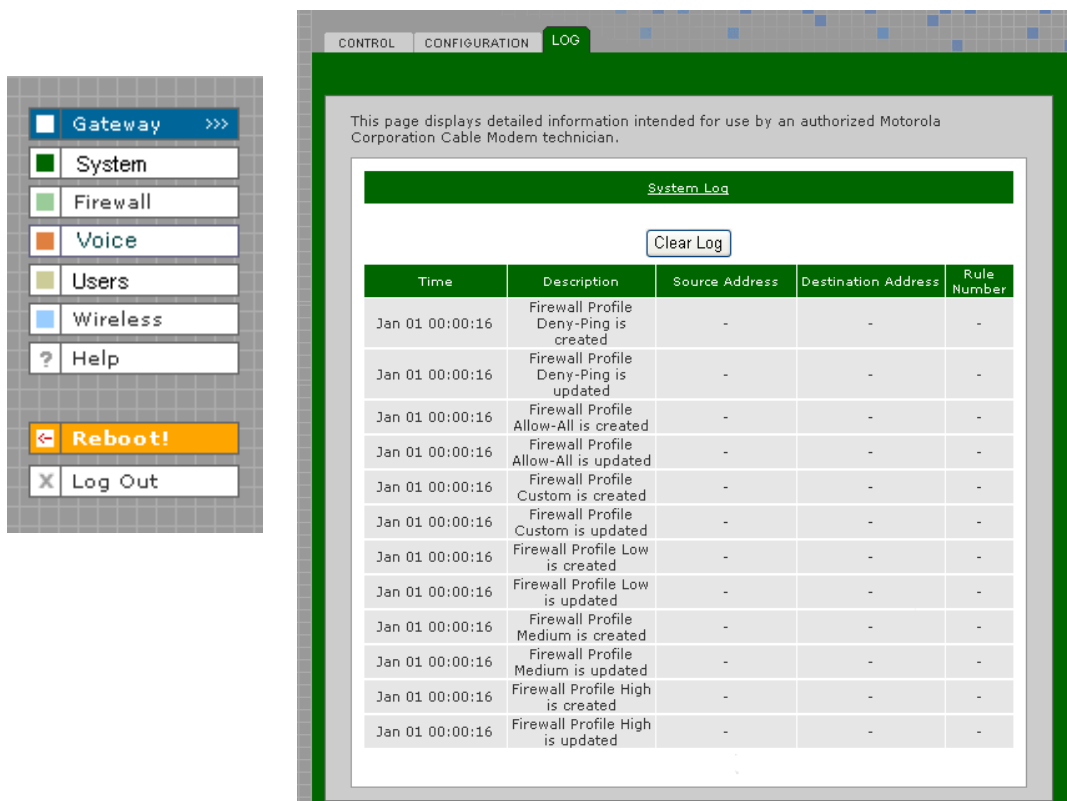
When system configuration is reset, all *Gateway* and *Wireless* feature settings shall not be reset to factory defaults.

Initialize (button)

Click **Initialize** to restore the factory default configuration settings. It is highly recommended that you back up the current configuration before restoring factory defaults. See [System > CONFIGURATION — backup](#) for more information.

System > LOG

Use this page to view detailed information about system activity:



CONTROL CONFIGURATION LOG

This page displays detailed information intended for use by an authorized Motorola Corporation Cable Modem technician.

System Log

Clear Log

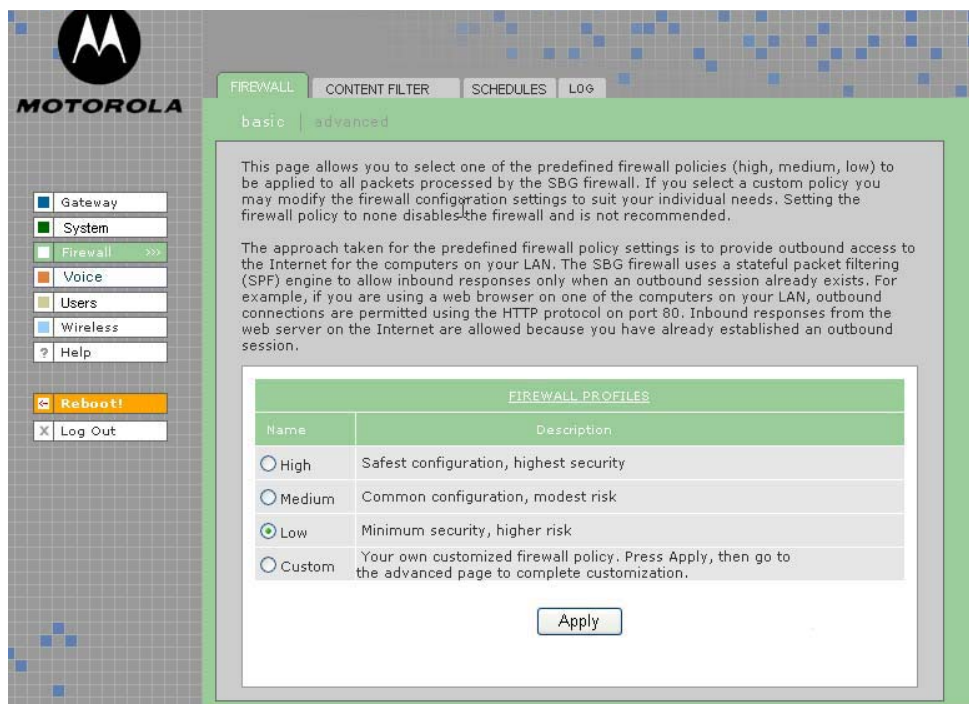
Time	Description	Source Address	Destination Address	Rule Number
Jan 01 00:00:16	Firewall Profile Deny-Ping is created	-	-	-
Jan 01 00:00:16	Firewall Profile Deny-Ping is updated	-	-	-
Jan 01 00:00:16	Firewall Profile Allow-All is created	-	-	-
Jan 01 00:00:16	Firewall Profile Allow-All is updated	-	-	-
Jan 01 00:00:16	Firewall Profile Custom is created	-	-	-
Jan 01 00:00:16	Firewall Profile Custom is updated	-	-	-
Jan 01 00:00:16	Firewall Profile Low is created	-	-	-
Jan 01 00:00:16	Firewall Profile Low is updated	-	-	-
Jan 01 00:00:16	Firewall Profile Medium is created	-	-	-
Jan 01 00:00:16	Firewall Profile Medium is updated	-	-	-
Jan 01 00:00:16	Firewall Profile High is created	-	-	-
Jan 01 00:00:16	Firewall Profile High is updated	-	-	-

System > LOG page fields

Field	Description
SYSTEM LOG	The table shows the logging information related to the system. The Time shows the time of the event was logged. Description column gives a brief description about the event logged. The source and destination addresses specify the source and destination of the packet. The rule number shows the firewall rule number which resulted in the event
Clear Log (button)	Clears the entries in the log. Types of entries include predefined or custom firewall profile changes or additions,?
Time	The date and time of the event in the format yyyy-mm-dd hh:mm:ss
Description	The URL or Web page accessed.
Source Address	The source IP address of the inbound or outbound message.??
Destination Address	The destination IP address of the inbound or outbound message.??
Rule Number	The firewall profile rule applicable to this entry. Refer to Firewall > FIREWALL — advanced for more information about firewall rules.

Firewall > FIREWALL — basic

Use this page to view and edit the existing firewall profiles. Predefined firewall templates are defined in the table following this screen's field definitions.



MOTOROLA

Gateway System **Firewall** Voice Users Wireless Help

Reboot! Log Out

FIREWALL CONTENT FILTER SCHEDULES LOG

basic advanced

This page allows you to select one of the predefined firewall policies (high, medium, low) to be applied to all packets processed by the SBG firewall. If you select a custom policy you may modify the firewall configuration settings to suit your individual needs. Setting the firewall policy to none disables the firewall and is not recommended.

The approach taken for the predefined firewall policy settings is to provide outbound access to the Internet for the computers on your LAN. The SBG firewall uses a stateful packet filtering (SPF) engine to allow inbound responses only when an outbound session already exists. For example, if you are using a web browser on one of the computers on your LAN, outbound connections are permitted using the HTTP protocol on port 80. Inbound responses from the web server on the Internet are allowed because you have already established an outbound session.

FIREWALL PROFILES	
Name	Description
☐ High	Safest configuration, highest security
☐ Medium	Common configuration, modest risk
☒ Low	Minimum security, higher risk
☐ Custom	Your own customized firewall policy. Press Apply, then go to the advanced page to complete customization.

Apply

Firewall > FIREWALL — basic page fields

Field	Description
FIREWALL PROFILES	Use these fields to select one of the predefined firewall profiles for all packets processed by the voice gateway firewall.
Name (chgd)	The name of the firewall profile. Predefined firewall profiles names include High, Medium, and Low.
High	Provides the safest configuration and highest security
Medium	Provides the most common configuration with modest risk
Low	Provides minimum security and higher risk
Custom	Use this to create a customized firewall policy. Press Apply then enter the applicable information (see the Firewall > FIREWALL — advanced page).
Description (chgd)	A description of the profile type
Apply (button)	Select Apply to save your changes.

Predefined Firewall Template Definitions

Firewall

Low

inbound	PSEC-IKE, IPSEC-ESP, IPSEC-AH, ICMP messages, RSVP messages - native and UDP-encapsulated, Kerberos, RTP/RTCP, MGCP, SNMP
outbound	DHCP, ICMP, DNS, FTP, TFTP, SMTP, POP3, HTTP, HTTPS, NNTP, PPTP, L2TP, IPSEC-IKE, IPSEC-ESP, IPSEC-AH, AOL instant messenger, Microsoft instant messenger, Yahoo instant messenger, TFTP, DirectX7-based applications, DirectX8-based applications, Battle.net, Microsoft Zone.com-based applications, RSVP messages (native and UDP-encapsulated), XBox, SYSLOG, Kerberos, RTP/RTCP, MGCP, Gnutella, LineWire, Bearshare, Morpheus, IGMP, H.323, T.120, ICQ, ICQ Chat, Real Player, Microsoft Media Player, Telnet, RIP, SNMP
Denial of Service	SYN Flooding, Land Attach (source IP = destination IP), WinNuke, SMURF, ICMP Flood, Ping Flood, Ping of Death (are these the same for medium)
Intrusions	IMAP Scan, Echo Scan, Chargen Scan, TCP Syn ACK Syn, TCP FIN Scan, TCP RESET Scan, Back Orifice Scan, Net Bus Scan, IP Spoofing UDP Bomb, XMAS Tree (are these the same for medium)

Medium

Medium is not addressed in the specification

inbound
outbound
Denial of Service
Intrusions

High

inbound	PSEC-IKE, IPSEC-ESP, IPSEC-AH, ICMP messages, RSVP messages - native and UDP-encapsulated, Kerberos, RTP/RTCP, MGCP, SNMP
outbound	DHCP, ICMP, DNS, FTP, TFTP, SMTP, POP3, HTTP, HTTPS, NNTP, PPTP, L2TP, IPSEC-IKE, IPSEC-ESP, IPSEC-AH, AOL instant messenger, Microsoft instant messenger, Yahoo instant messenger, TFTP, DirectX7-based applications, DirectX8-based applications, Battle.net, Microsoft Zone.com-based applications, RSVP messages (native and UDP-encapsulated), XBox, SYSLOG, Kerberos, RTP/RTCP, MGCP, Gnutella, LineWire, Bearshare, Morpheus, IGMP, H.323, T.120, ICQ, ICQ Chat, Real Player, Microsoft Media Player, Telnet, RIP, SNMP
Denial of Service	SYN Flooding, Land Attach (source IP = destination IP), WinNuke, SMURF, ICMP Flood, Ping Flood, Ping of Death (are these the same for medium)
Intrusions	MAP Scan, Echo Scan, Chargen Scan, TCP Syn ACK Syn, TCP FIN Scan, TCP RESET Scan, Back Orifice Scan, Net Bus Scan, IP Spoofing UDP Bomb, XMAS Tree (are these the same for medium)

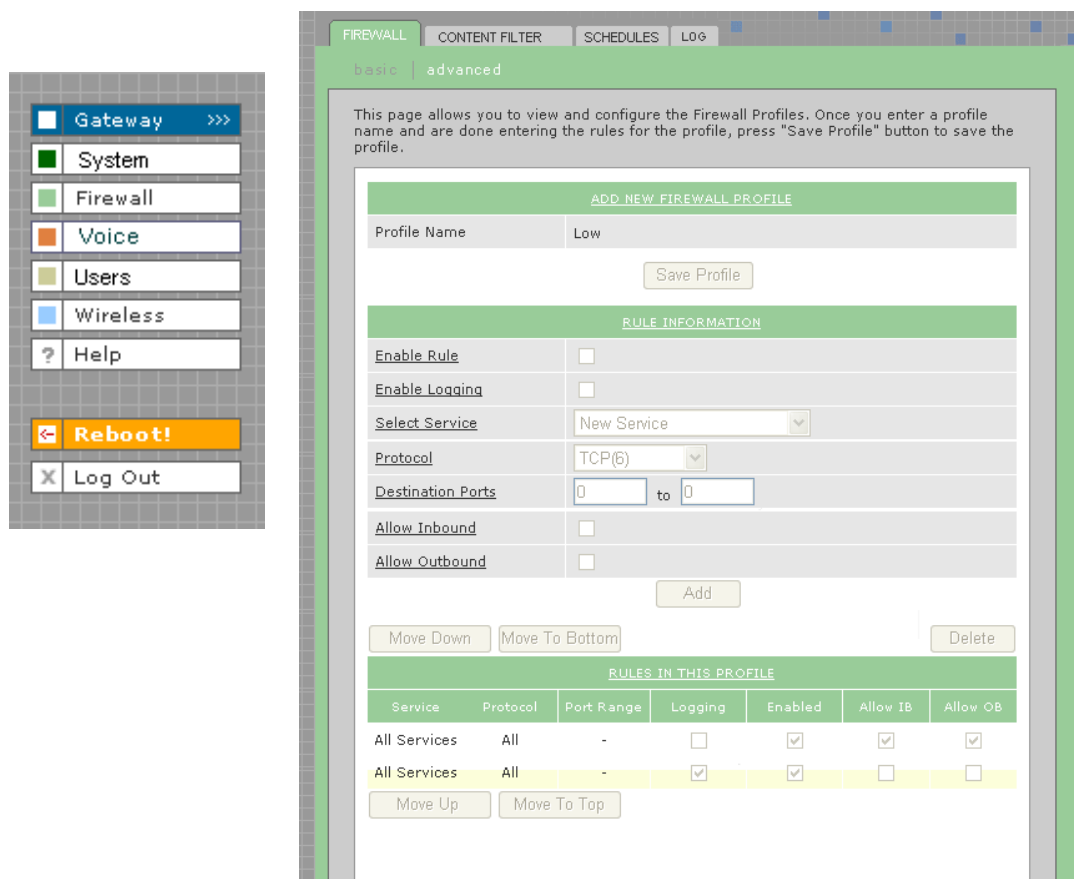
None

Allows all packets through the firewall. The firewall is, in effect, disabled.

Firewall > FIREWALL — advanced

Do not create a custom firewall policy unless you have the expertise necessary to do so. Instead, select one of the predefined policy templates as described in “[Setting Up Minimum Security Network Options](#)”.

Use this page to configure custom firewall profiles. This page also appears when you edit a firewall profile on the [Firewall > FIREWALL — basic](#) page:



Firewall > FIREWALL — advanced page fields

Field	Description
ADD NEW FIREWALL PROFILE	Use these fields to set up one or more custom firewalls <i>if you have the expertise to do so</i> . The voice gateway's predefined firewall is enabled for the “admin” user. See Firewall > LOG to see which firewalls are enabled.
Profile Name	The profile name
Save Profile (button)	Click Save Profile to save the profile name and to continue configuring it. The new name is displayed on the Firewall > FIREWALL — basic page.
RULE INFORMATION	Up to 30 IP filtering rules can be configured.
Enable Rule	Select this box to enable firewall policy filtering for the port using this rule.?

Firewall > FIREWALL — advanced page fields (continued)

Field	Description
Enable Logging	If you enable logging for the firewall, a list is always generated. Any IP address the firewall determines to have breached the active policy is added to the log. The firewall blocks all traffic to and from a denied IP address for 24 hours or until you reboot the VT2400/VT2500 or manually clear the log on the Firewall > LOG page. ??????????
Select Service (new)	From the list, select All Services or a single service to which this new profile applies.
Protocol (new)	Select the protocol type for the service defined.
Destination Ports (new)	Specify the destination port range for this newly created service.
Allow Inbound (new)	Inbound direction indicates WAN to LAN. If you want the selected service to be allowed from WAN to LAN, this check box must be selected
Allow Outbound (new)	Outbound direction indicates LAN to WAN. If you want the selected service to be allowed from LAN to WAN, this check box must be selected

Buttons:

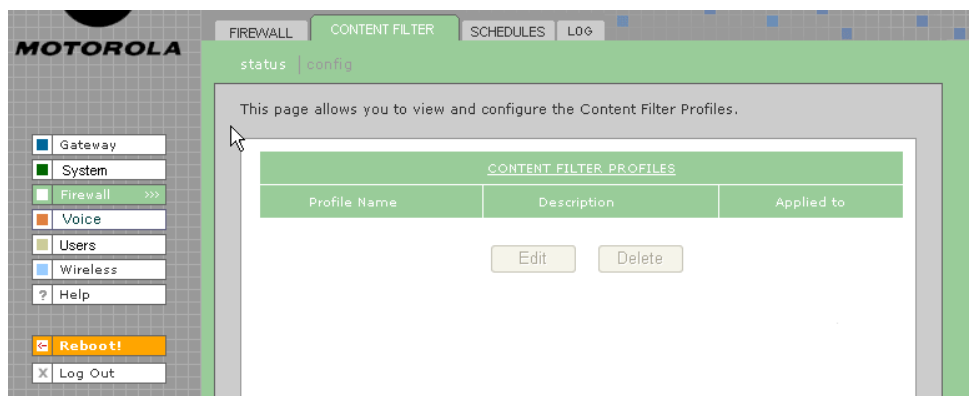
Add	Adds the profile to the Firewall > FIREWALL — basic page.
Move Down, Move to Bottom	Allows you to prioritize rules by moving them up or down (one at a time) after you select one in the list under RULES IN THIS PROFILE.
Delete	Deletes the profile after selecting it in the list under RULES IN THIS PROFILE. This message appears: " Name Firewall Profile is about to be deleted. Are you sure?" Click OK to delete it or Cancel to keep it. Predefined firewall profiles (Low, Medium, High) cannot be deleted

RULES IN THIS PROFILE

Service	The URL types covered by this profile
Protocol	The protocols covered by this profile
Port Range	The ports covered by this profile
Logging	Events are logged or are not logged
Enabled	The rule is enabled or not enabled
Allow 1B	???
Allow 0B	???

Firewall > CONTENT FILTER — status

Use this page to view and edit the existing Content Filter Profiles:

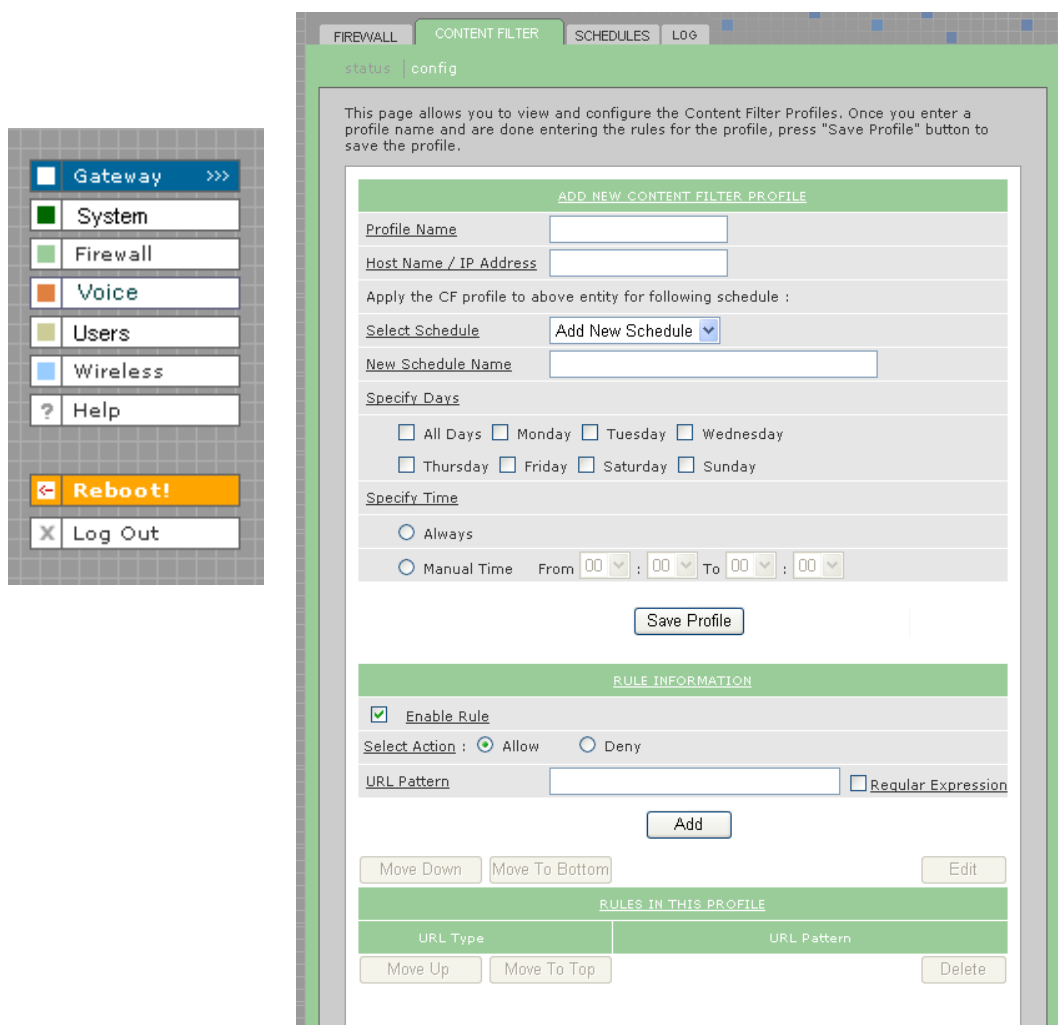


Firewall > CONTENT FILTER— status page fields

Field	Description
CONTENT FILTER PROFILES	
Profile Name	Name for the custom or predefined Content Filter Profile you created or selected on the Firewall > FIREWALL — advanced page.
Low	A filter that provides minimum security with a higher risk of intrusions. See Predefined Firewall Template Definitions in Firewall > FIREWALL — basic section.
Medium	A filter that provides a common configuration that has moderate risk.
High	A filter that provides the highest security. <i>This setting is recommended.</i>
Description	Need
Applied to	Need
URLs	The Uniform Resource Locator (URL) names, such as mon.com , which are protected under the content filter. URLs identify the IP address of Web pages and other resources on the World Wide Web.
Edit (button)	Allows you to edit custom filter profiles. See the Firewall > CONTENT FILTER — config page for more field information. Predefined filter profiles (Low, Medium and High) cannot be edited.
Delete (button)	Allows you to delete custom filter profiles. Predefined filter profiles (Low, Medium and High) cannot be deleted.

Firewall > CONTENT FILTER — config

Use this page to view and configure new Content Filter Profiles, such as parental controls, employee access controls, and so on. **Content filtering does not occur automatically; you must configure it. In addition, profiles must be defined for content filtering to work. Otherwise, all data passes through the firewall unprotected. (TRUE?)**



Firewall > CONTENT FILTER — config page fields

Field	Description
-------	-------------

ADD NEW CONTENT FILTER PROFILE:

Profile Name	Enter a name for the Content Filter Profile. Enter the url rules one by one and then click on Save Profile to save the profile. If Save Profile button is not clicked the profile will not be saved.
Host Name/IP Address	Enter the Host name or IP address of the PC to which this content filter profile has to be applied

Firewall > CONTENT FILTER — config page fields (continued)

Field Description

Apply the CF profile to above entity for following schedule:

Select Schedule	The Content Filter profile will be applied to the specified PC only for the specified schedule. The "Always" schedule is predefined. You can define a new schedule by selecting Add New Schedule from the drop down list.
New Schedule Name	The name of the schedule.
Specify Days	The days during which the schedule is active.
Specify Time	The time of day during which the schedule is active. If you select Always, the schedule is active 24 hours a day, seven days a week. Or you can manually enter the time (in hours and minutes) during which the schedule is active.
Save Profile (button)	Click Save Profile to save the filter profile name and continue configuring it. The new name is displayed on the Firewall > CONTENT FILTER — status page. Select the profile name you just created and then click Edit to continue configuring it. Or click Delete to delete it

RULE INFORMATION:

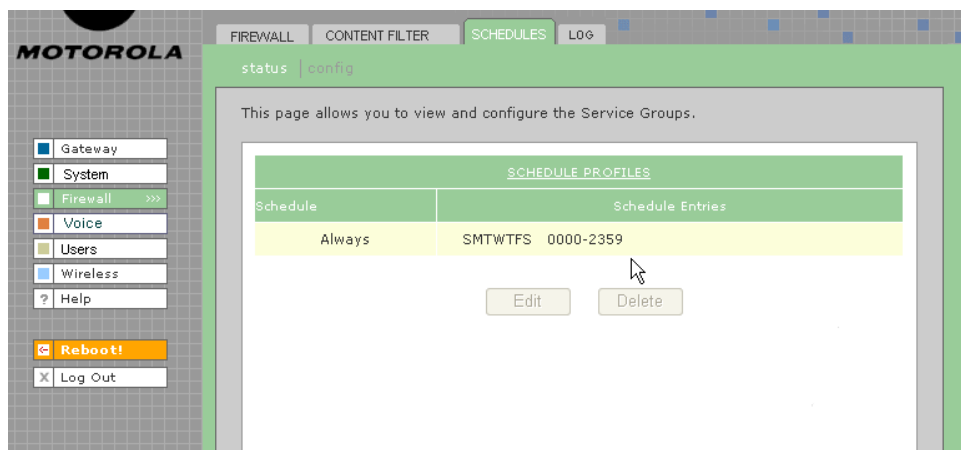
Enable Rule	Select this check box to activate the rule. If not selected, the rule is still created but it won't be in effect.
Select Action:	Select the action (Allow or Deny) to be taken when this rule is applied. You can select a particular URL to be allowed or denied:
Allow	Allows access to the URL by users on the network.
Deny	Denies access to the URL by users on the network.
URL Pattern	Type the URL/Web site pattern to be allowed or denied (for key word filtering?)
Regular Expression	A URL is treated as a regular expression. This option is useful when using wildcards such as *, ? etc.
Add (button)	Adds the URL pattern to the URL PATTERNS IN THIS PROFILE list.
Move Down, Move Up, Move to Bottom, Move to Top (buttons)	Prioritizes the URL pattern in the URL PATTERNS IN THIS PROFILE list after you select it.
Edit (button)	Allows you to edit the URL pattern in the URL PATTERNS IN THIS PROFILE list.
Delete (button)	Allows you to delete the URL pattern in the URL PATTERNS IN THIS PROFILE list.

RULES IN THIS PROFILE

URL Type
URL Pattern

Firewall > SCHEDULES — status

Use this page to view, edit, and delete the existing schedule profiles.



Firewall > SCHEDULES — status page fields

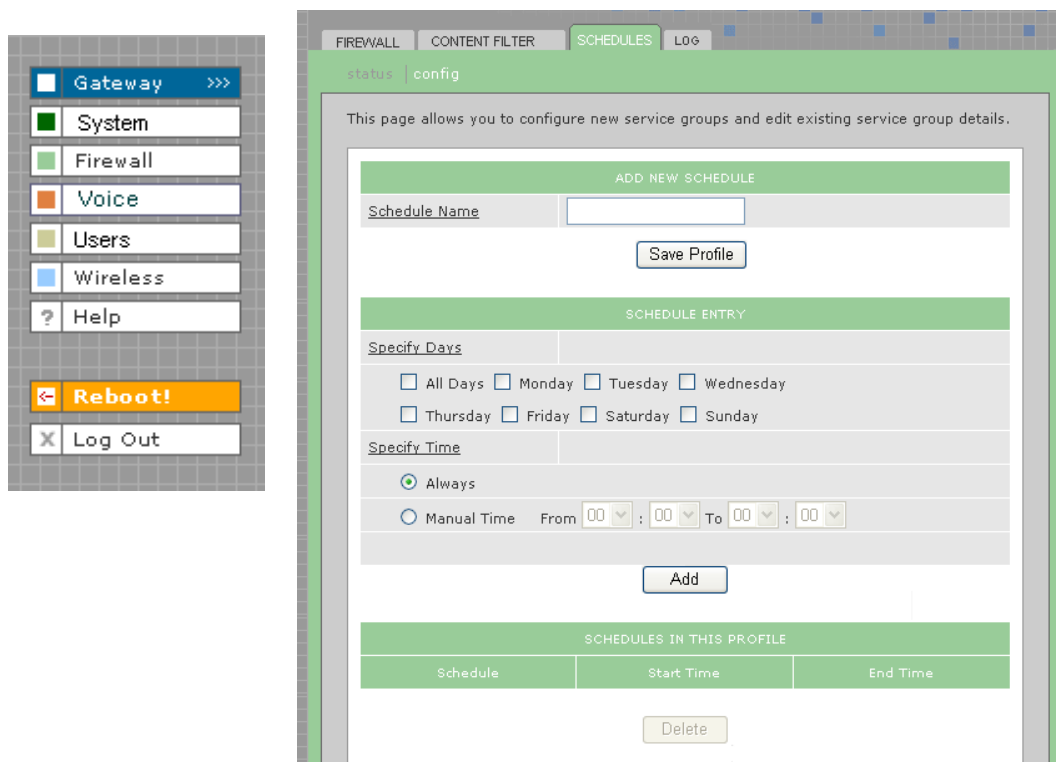
Field or Button	Description
-----------------	-------------

SCHEDULE PROFILES

Schedule	Type the name of the schedule.
Schedule Entries	Enter the days and time range for the schedule
Edit (button)	Select a schedule in the XXXXXXXXXX list and click the Edit button. Refer to Firewall > SCHEDULES — config for changing configuration information.
Delete (button)	Select a schedule profile in the SCHEDULES IN THIS PROFILE list and click Delete . The <i>entire</i> schedule profile is removed from xxxxxxxx on the Firewall > SCHEDULES — status page. NOTE: To remove individual schedules from a profile, select them on the Firewall > SCHEDULES — status page and then click Delete.

Firewall > SCHEDULES — config

Use this page to configure new schedule profiles and edit existing schedule profiles.



Firewall > SCHEDULES — config page fields

Field	Description
-------	-------------

ADD NEW SCHEDULE

Schedule Name Type the name of the schedule profile.

Save Profile (button) Click the **Save Profile** button to save the profile name, which appears on the [Firewall > SCHEDULES — status](#) page. Select the schedule name you just created and then click **Edit** to continue configuring it. Or click **Delete** to delete it.

SCHEDULE ENTRY

Specify Days Select the days for this schedule to be active.

Specify Time: **Always** - select for the schedule to be active 24 hours per day, seven days a week.

Manual Time- select to specify a time range and then select the hours and minutes in the **From** and **To** lists.

Add (button) When you finish specifying or changing days and time, click the **Add** button to add the new schedule information to the profile.

SCHEDULES IN THIS PROFILE:

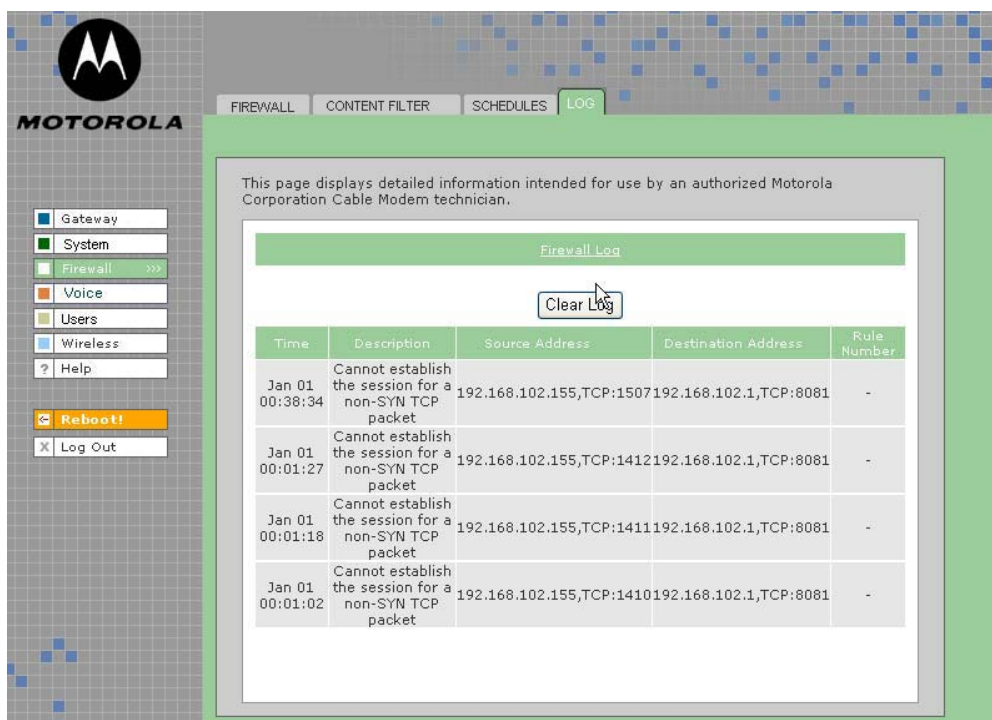


Firewall > SCHEDULES — config page fields (continued)

Field	Description
Schedule	The schedule name
Start Time	The time the schedule begins
End Time	The time the schedule ends
Delete (button)	To delete a schedule from the profile, select it in the SCHEDULES IN THIS PROFILE list and click Delete .

Firewall > LOG

This page displays activity related to the firewall:



Firewall > LOG page fields

Field

Description

Firewall LOG

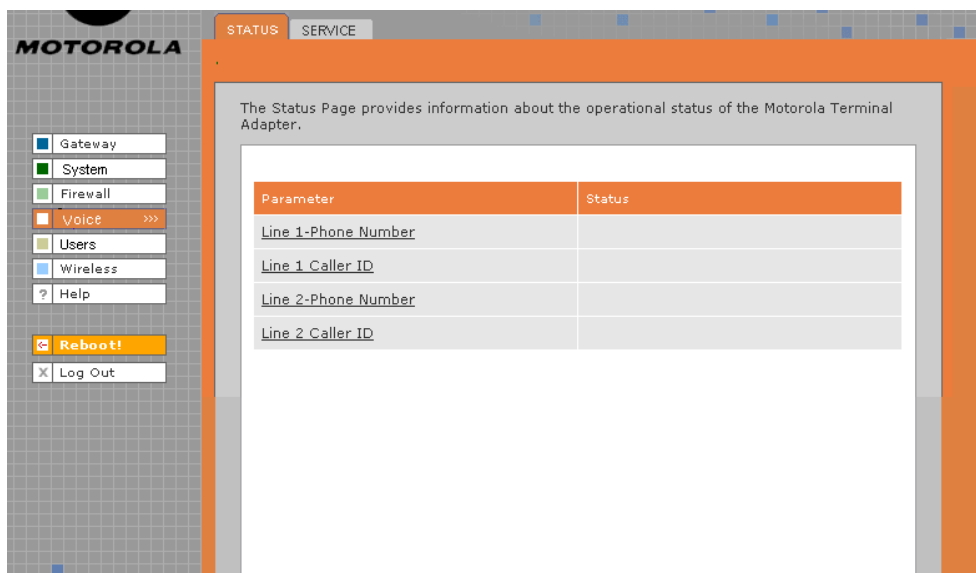
Allows up to 250 entries. Subsequent entries overwrite the oldest entries in the log. (Not sure if this definition is the same for the URL Log and the Log under USERS.)

Clear Log (button)

Clears all entries from the log.

Voice > STATUS

Use this page to view the operational status of the voice gateway:



Voice > STATUS page fields

Field

Description

Parameter

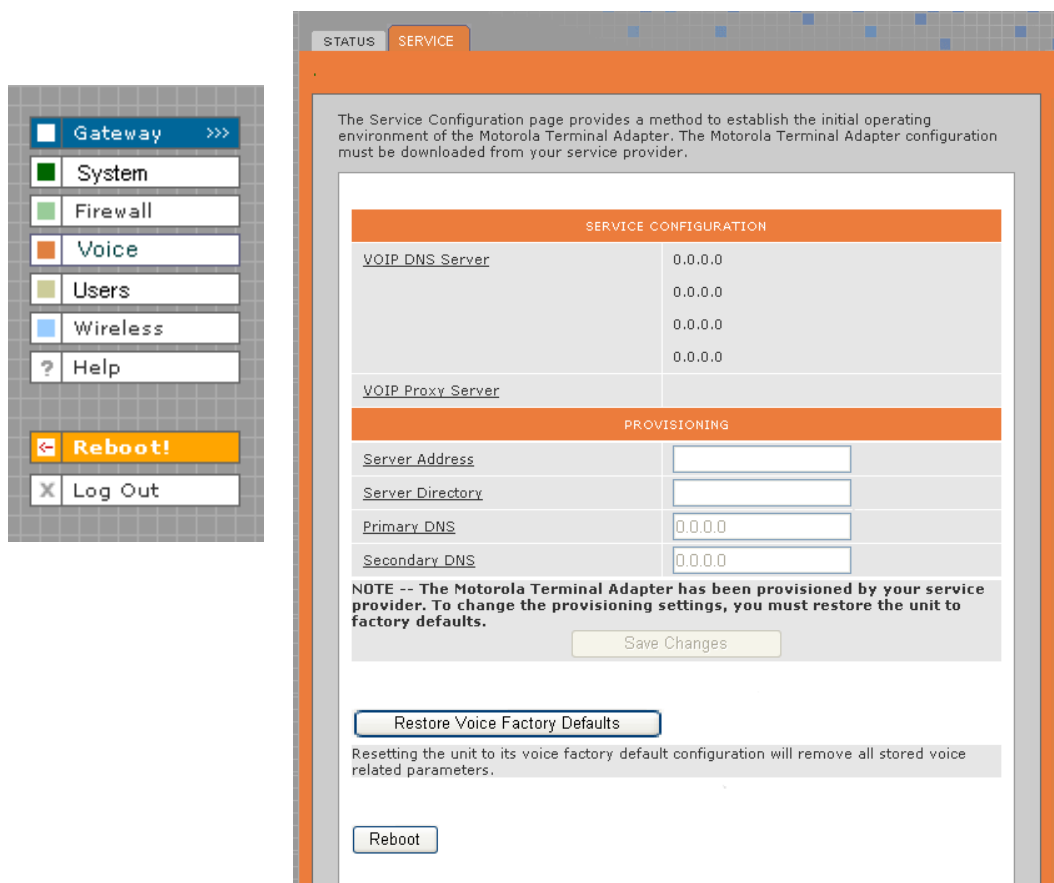
The voice feature, such as line number, caller ID, call forwarding, etc.

Status

The status of the voice feature (*enabled, disabled* ????)

Voice > SERVICE

Use this page to view and edit the service provider's configuration.



Voice > SERVICE page fields

Field	Description
-------	-------------

SERVICE CONFIGURATION

VOIP DNS Server	Voice Over IP DNS Server IP Address
VOIP Proxy Server	The IP address of the SIP Proxy Server assigned by your voice service provider

PROVISIONING

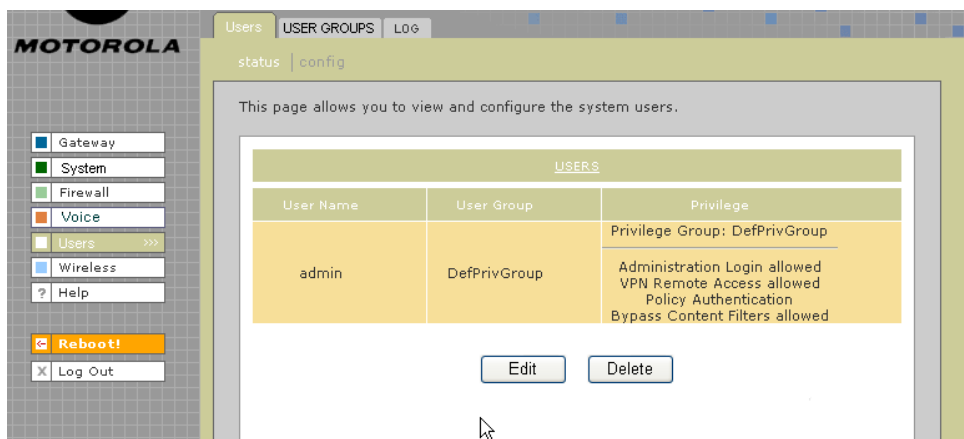
Server Address	Enter the IP address of the TFTP server
Server Directory	Enter the directory of the TFTP server
Primary DNS	The Internet Service Provider Domain Name Server provides a primary name-to-IP address resolution. If your ISP does not automatically assign your DNS addresses from their DHCP server, they will need to provide you with at least one DNS server IP address that you enter in the DNS IP address fields.

**Voice > SERVICE page fields (continued)**

Field	Description
Secondary DNS	The Internet Service Provider Domain Name Server provides a secondary name-to-IP address resolution. If your ISP does not automatically assign your DNS addresses from their DHCP server, they will need to provide you with at least one DNS server IP address that you enter in the DNS IP Address fields.
Save Changes (button)	Select to save your changes.
Restore Voice Factory Defaults (button)	Select to restore factory defaults for VoIP. <i>Do not select this button unless your service provider advises you to do so.</i>
Reboot (button)	Reboots the voice gateway.

Users > USERS — status

Use this page to view, edit, and delete existing users and user groups.

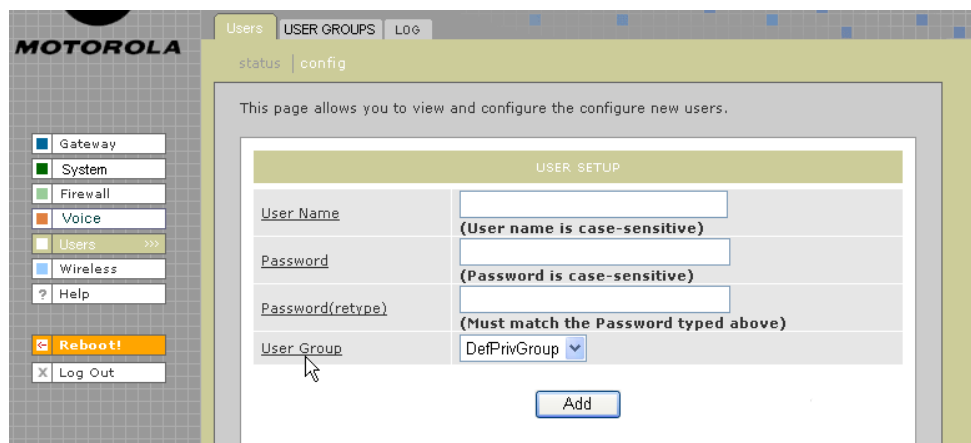


Users > USERS — status page fields

Field	Description
USERS	
User Name	Displays the names of all users.
User Group	The user group to which the user belongs. See Users > USER GROUPS for more information about user groups.
Privilege	The privileges assigned to this user. See Users > USERS — config for more information about available privileges.
Edit (button)	Edits the selected user in the USERS list. See Users > USERS — config for more information about editing configuration options.
Delete (button)	Deletes the selected user in the USERS list.

Users > USERS — config

Use this page to configure new users.

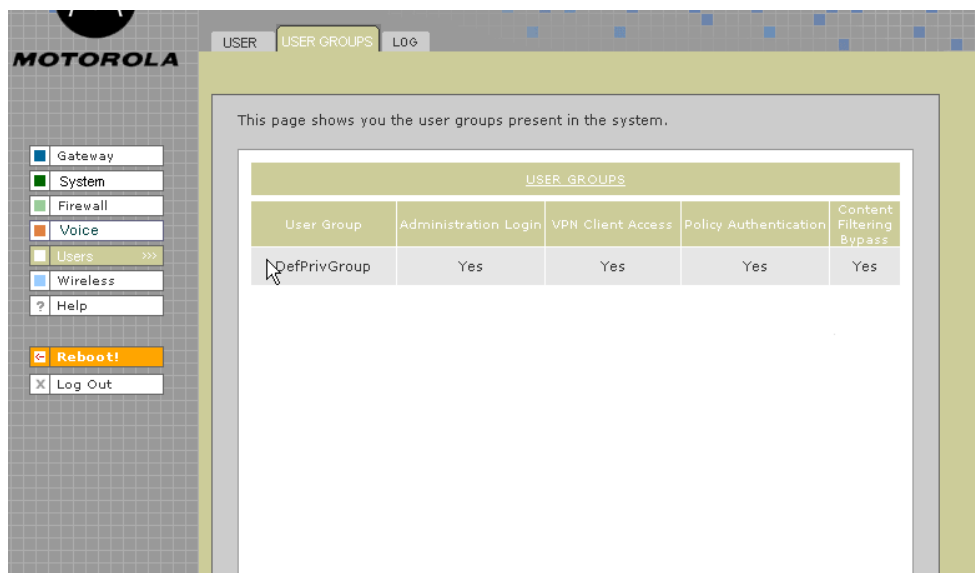


Users > USERS — config page fields

Field	Description
USER SETUP	
User Name	Type the user name as it will be entered by the user to log on to the network.
Password	Type at least four characters for the user's password.
Password (retype)	Retype the user's password.
User Group	Select a user group from the list. The user is given all the privileges assigned to that group. See Users > USER GROUPS for more information about user groups.
Add (button)	Click Add when you finish entering user setup information. The user name is added to the USERS list on the Firewall > FIREWALL — advanced page.

Users > USER GROUPS

Use this page to configure user groups to which users belong.



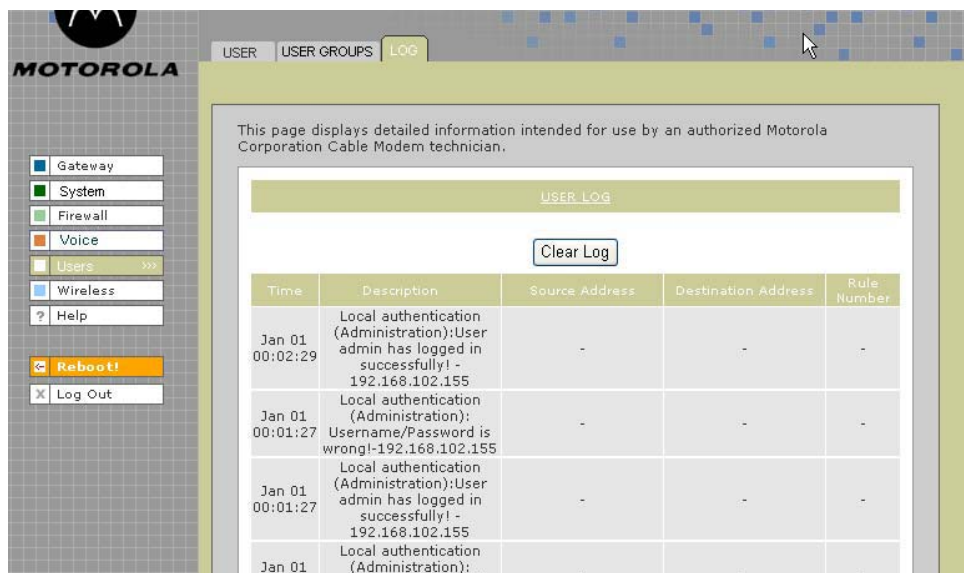
Users > USER GROUPS page fields

Field	Description
USER GROUPS	Will this page include a way to create user groups?
User Group	Help screens not provided
Administration Login	
VPN Client Access	
Policy Authentication	
Content Filtering Bypass	

NOTE: page 25 of spec says the product supports VPN pass through for IPSEC, PPTP, and L2TP.

Users > LOG

Use this page to view a log of user activity:



Users > LOG page fields

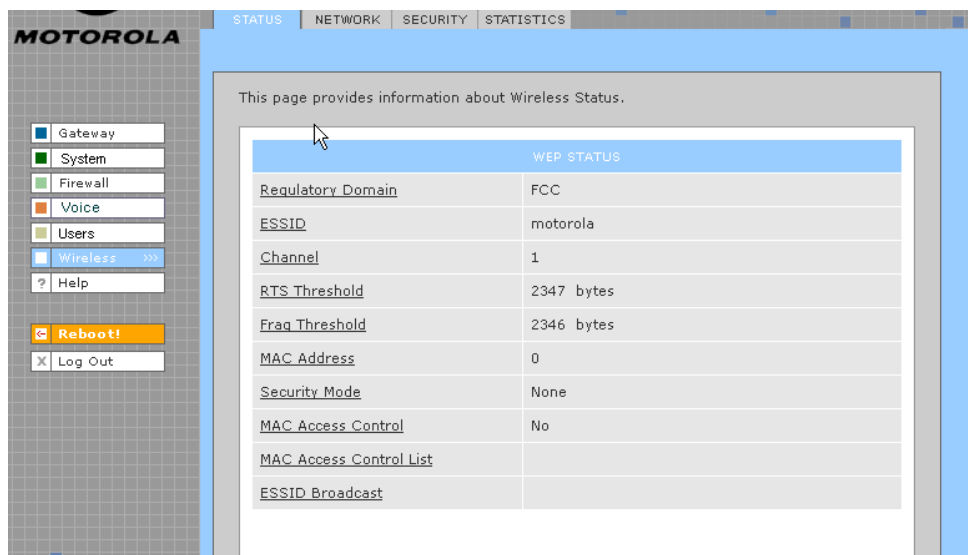
Field	Description
-------	-------------

USER LOG

Clear Log (button)	Clears all entries in the log.
Time	The time frame that a user accessed a particular destination address.
Description	The URL or Web page accessed.
Source Address	The source IP address of the inbound or outbound message.
Destination Address	The destination IP address of the inbound or outbound message.
Rule Number	The firewall profile rule applicable to this user. Refer to Firewall > FIREWALL — advanced for more information about firewall rules.

Wireless > STATUS

This page provides wireless status information.



This page provides information about Wireless Status.

WEP STATUS	
<u>Regulatory Domain</u>	FCC
<u>ESSID</u>	motorola
<u>Channel</u>	1
<u>RTS Threshold</u>	2347 bytes
<u>Frag Threshold</u>	2346 bytes
<u>MAC Address</u>	0
<u>Security Mode</u>	None
<u>MAC Access Control</u>	No
<u>MAC Access Control List</u>	
<u>ESSID Broadcast</u>	

Refer to “[Setting Up Your Wireless LAN \(WLAN\)](#)” for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > NETWORK

This page allows you to configure wireless network settings. The default configuration parameters are set to permit IEEE 802.11 wireless network operation without additional changes. Any 802.11 conforming device may operate on the network.

Gateway
>>>

System
 Firewall
 Voice
 Users
 Wireless
 Help

← Reboot!

X Log Out

STATUS
NETWORK
SECURITY
STATISTICS

This page allows you to configure wireless network settings. The default configuration parameters have been set to permit IEEE 802.11 wireless network operation without additional changes.

An access point is the term used to describe the cable modem when it is providing wireless local area network connectivity to wireless client devices.

A station or client device is any 802.11 conformant device operating on the wireless local area network.

WIRELESS

<u>Enable Wireless Interface</u>	☒
<u>ESSID</u>	motorola
<u>Channel</u>	1 ▾
<u>Operating Mode</u>	Compatibility ▾

ADVANCED SETUP

<u>Transmit Power</u>	100 ▾ percent
<u>RTS Threshold</u>	2347 bytes
<u>Fragmentation Threshold</u>	2346 bytes
<u>Beacon Period</u>	100 milliseconds
<u>DTIM Period</u>	3 beacons

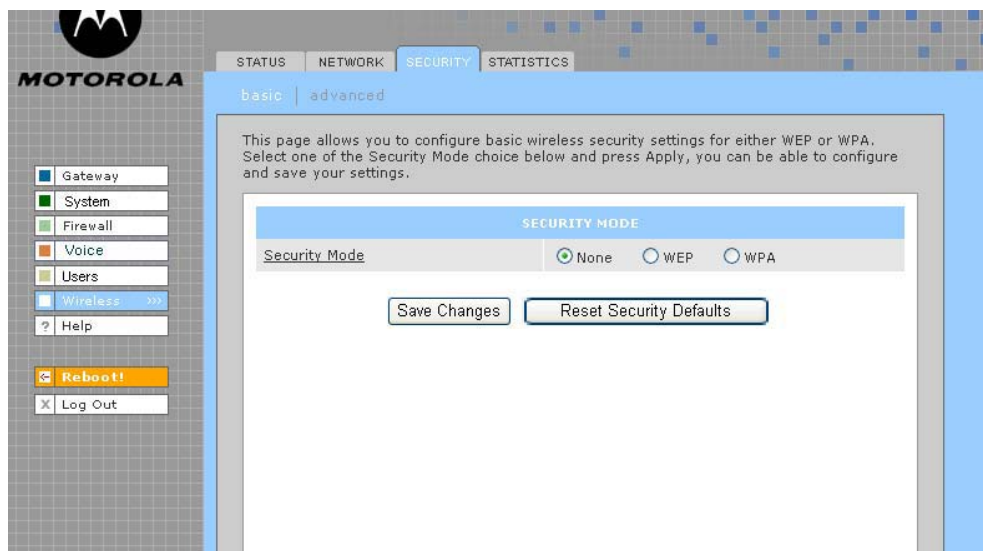
Save Changes

Reset Wireless Defaults

Refer to "[Setting Up Your Wireless LAN \(WLAN\)](#)" for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > SECURITY – basic

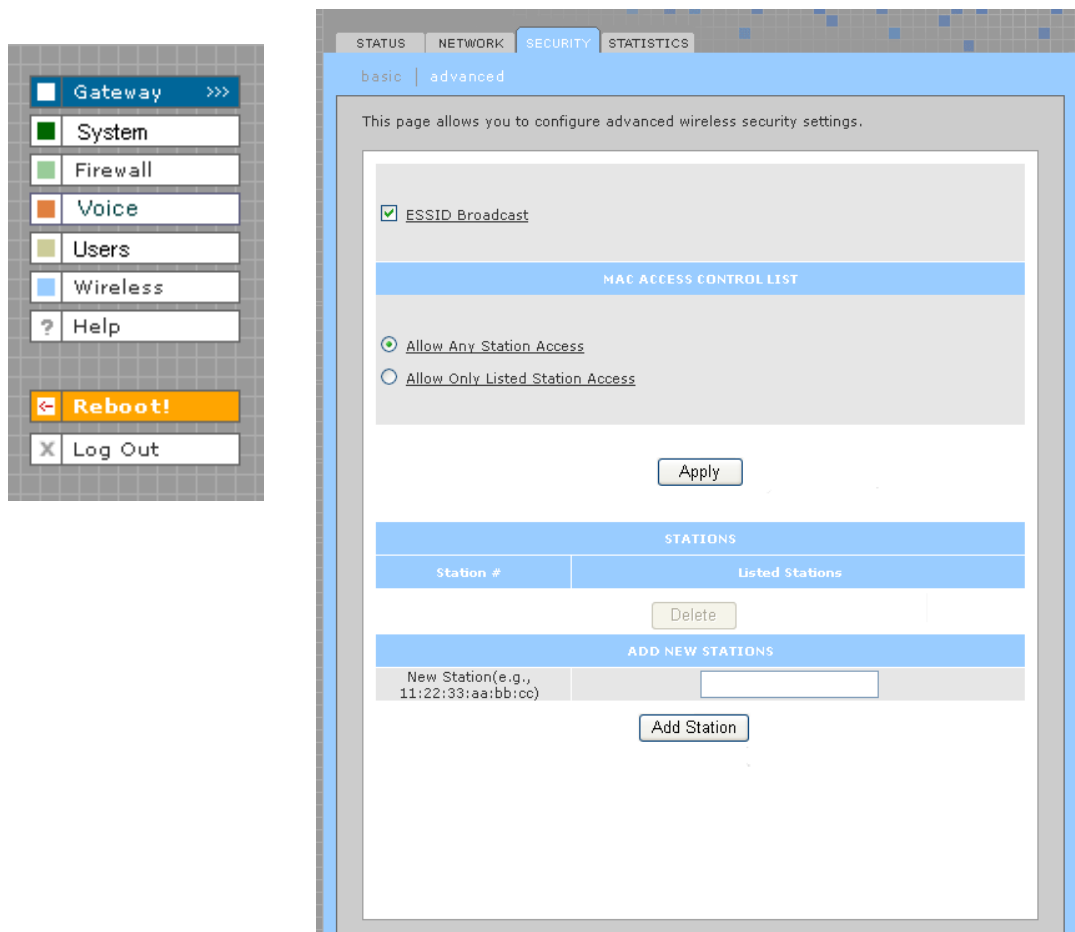
This page allows you to configure basic wireless security settings for WEP or WPA.



Refer to “[Configuring WPA on the VT2500](#)” or “[Configuring WEP on the VT2500](#)” under “[Setting Up Your Wireless LAN \(WLAN\)](#)” for a description of each field. Or, mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > SECURITY – advanced

This page allows you to configure advanced wireless security settings.



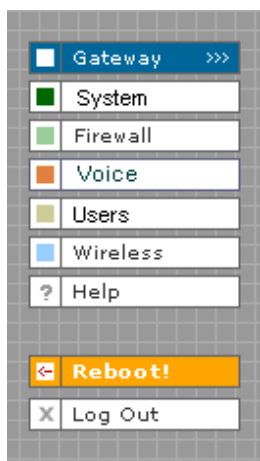
The screenshot displays the Motorola Voice Gateway configuration interface. On the left is a sidebar menu with options: Gateway >>>, System, Firewall, Voice, Users, Wireless, Help, Reboot!, and Log Out. The main content area is titled 'SECURITY' and has tabs for STATUS, NETWORK, SECURITY, and STATISTICS. The 'SECURITY' tab is active, and the 'advanced' sub-tab is selected. The page contains the following sections:

- ESSID Broadcast:** A checkbox that is checked.
- MAC ACCESS CONTROL LIST:** A section with two radio button options:
 - ☒ Allow Any Station Access
 - ☐ Allow Only Listed Station Access
- Apply:** A button to save the changes.
- STATIONS:** A table with two columns: 'Station #' and 'Listed Stations'. Below the table is a 'Delete' button.
- ADD NEW STATIONS:** A section with a text input field for 'New Station(e.g., 11:22:33:aa:bb:cc)' and an 'Add Station' button.

Refer to “[Setting Up Your Wireless LAN \(WLAN\)](#)” for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > STATISTICS

This page provides information about wireless statistics.



WIRELESS STATISTICS	
<u>Transmitted Fragment Count</u>	1263
<u>Multicast Transmitted Fragment Count</u>	1262
<u>Failed Count</u>	1
<u>Retry Count</u>	0
<u>Multiple Retry Count</u>	0
<u>Frame Duplicate Count</u>	1
<u>Request to Send Success Count</u>	3341
<u>Request to Send Failure Count</u>	1996
<u>Acknowledge Failed Count</u>	0
<u>Received Fragment Count</u>	11
<u>Multicast Received Fragment Count</u>	11
<u>Frame Check Sequence Error Count</u>	10155
<u>Transmitted Frame Count</u>	1265
<u>WEP Undecryptable Count</u>	0

Refresh

Refer to "[Setting Up Your Wireless LAN \(WLAN\)](#)" for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

❖ Configuring TCP/IP

You must be sure all client computers are configured for [TCP/IP](#) (a protocol for communication between computers). Perform *one* of these:

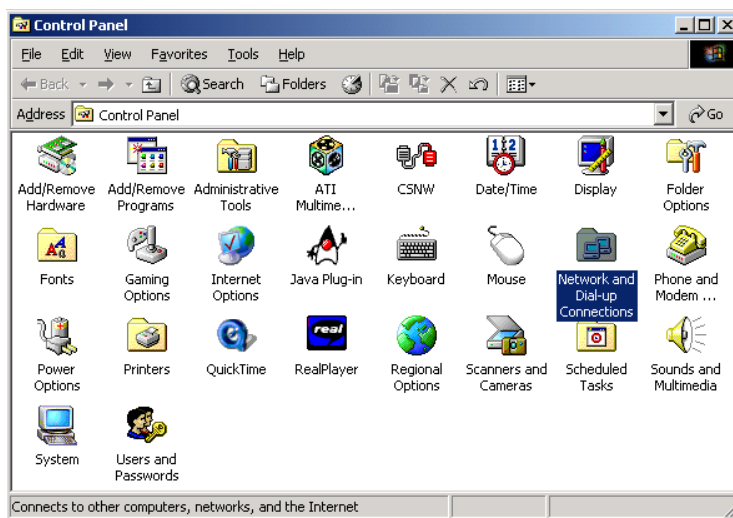
- [Configuring TCP/IP in Windows 95, Windows 98, or Windows Me](#)
- [Configuring TCP/IP in Windows 2000](#)
- [Configuring TCP/IP in Windows XP](#)
- Follow the instructions in your Macintosh or UNIX user manual

After configuring TCP/IP, perform *one* of the following to verify the [IP address](#):

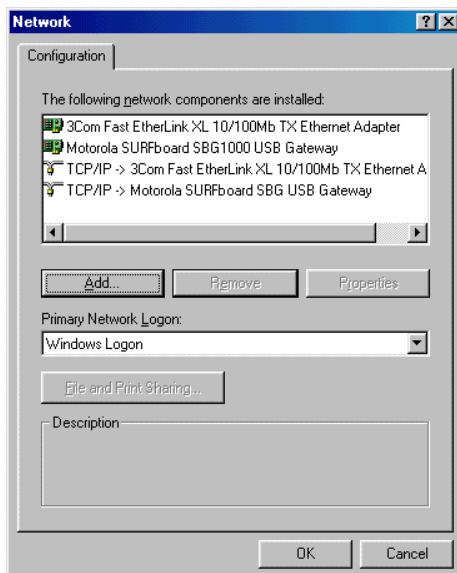
- [Verifying the IP Address in Windows 95, Windows 98, or Windows Me](#)
- [Verifying the IP Address in Windows 2000 or Windows XP](#)
- Follow the instructions in your Macintosh or UNIX user manual

Configuring TCP/IP in Windows 95, Windows 98, or Windows Me

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:

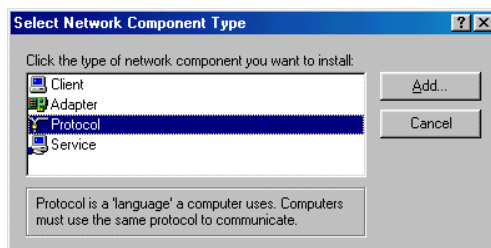


- 3 Double-click the **Network** icon to display the Network window:

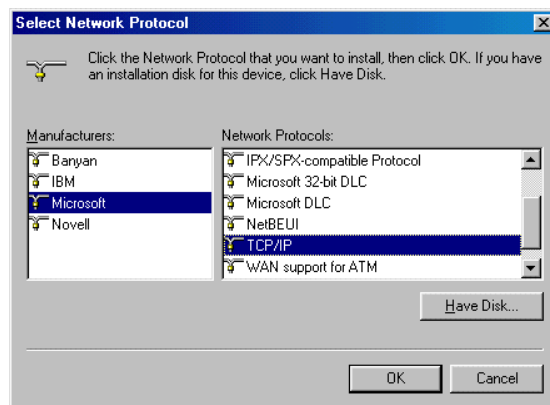


Although your VT model number may be different than in the images in this guide, the procedure is the same.

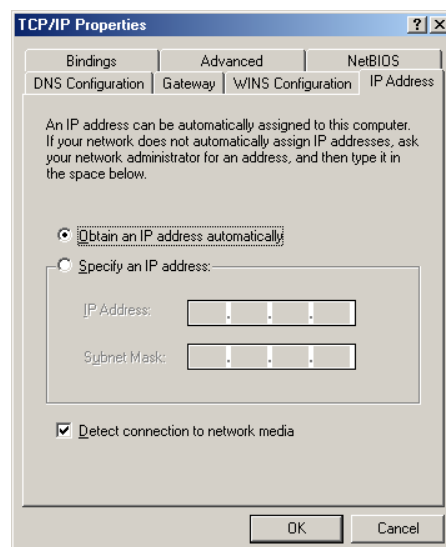
- 4 Select the **Configuration** tab.
- 5 Verify that TCP/IP is installed for the adapter used to connect to the VT2500. If TCP/IP is installed, skip to step 10. If TCP/IP is not installed for the adapter, continue with step 6.
- 6 Select the adapter to use for the VT2500 connection and click **Add**. The Select Network Component Type window is displayed:



- 7 Click **Protocol** and click **Add**. The Select Network Protocol window is displayed:



- 8 Click **Microsoft** in the Manufacturers section and click **TCP/IP** in the Network Protocols section.
- 9 Click **OK**.
- 10 Click **TCP/IP** on the Network window. If there is more than one TCP/IP entry, choose the one for the Ethernet card or USB port connected to the VT2500.
- 11 Click **Properties**. The TCP/IP Properties window is displayed:

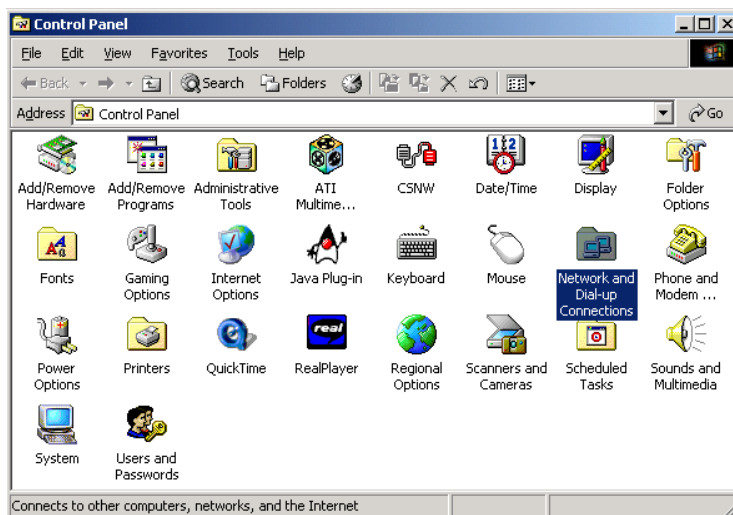


- 12 Click the **IP Address** tab.
- 13 Click **Obtain an IP address automatically**.
- 14 Click **OK** to accept the TCP/IP settings.
- 15 Click **OK** to close the Network window.
- 16 Click **OK** when prompted to restart the computer and click **OK** again.

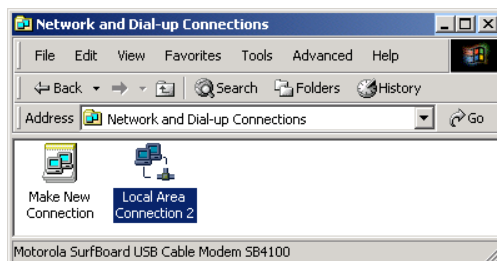
When you complete TCP/IP configuration, go to ["Verifying the IP Address in Windows 95, Windows 98, or Windows Me"](#).

Configuring TCP/IP in Windows 2000

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:



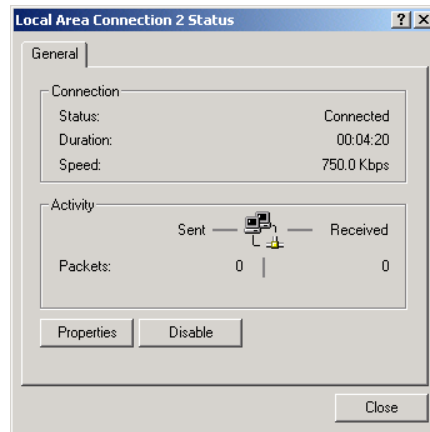
- 3 Double-click the **Network and Dial-up Connections** icon to display the Network and Dial-up Connections window:



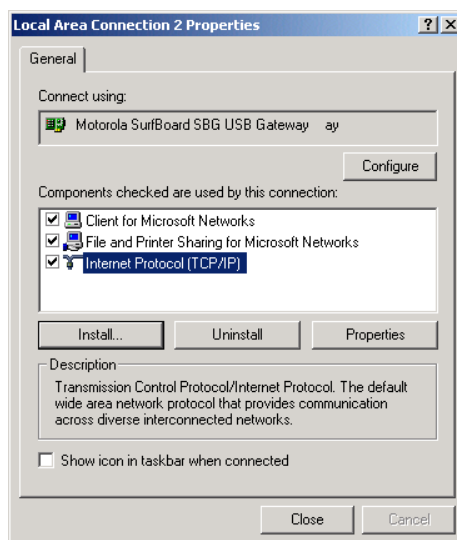
In the steps that follow, a connection *number* like 1, 2, 3, etc., is a reference that is displayed on computers with multiple network interfaces. Computers with only one network interface may only see the label: Local Area Connection.



- 4 Click **Local Area Connection number**. The value of *number* varies from system to system. The Local Area Connection *number* Status window is displayed:

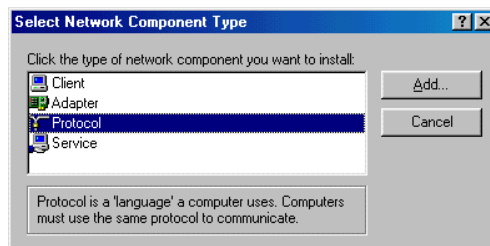


- 5 Click **Properties**. Information similar to the following window is displayed:

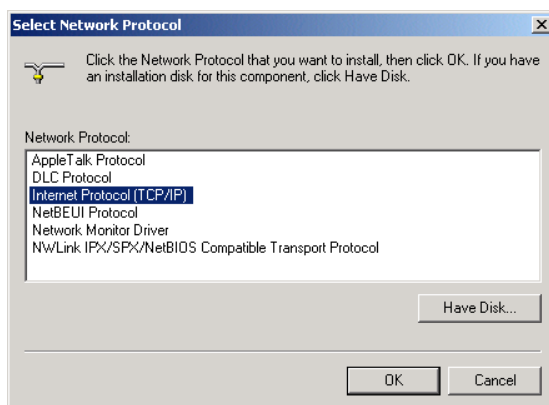


- 6 If Internet Protocol (TCP/IP) is in the list of components, TCP/IP is installed. You can skip to step 10.

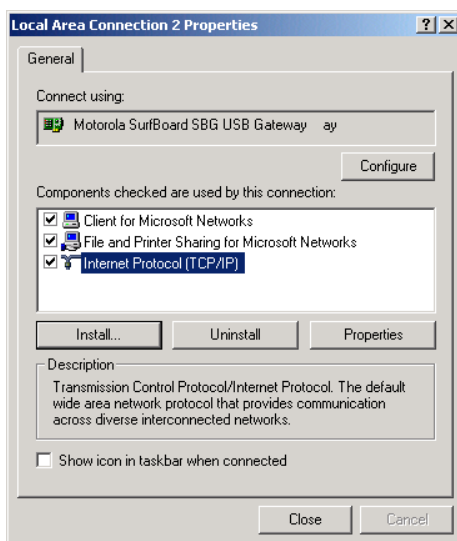
If Internet Protocol (TCP/IP) is not in the list, click **Install**. The Select Network Component Type window is displayed:



- 7 Click **Protocol** on the Select Network Component Type window and click **Add**. The Select Network Protocol window is displayed:

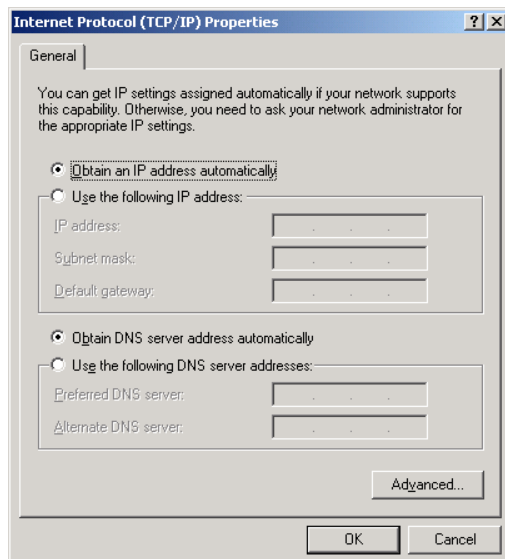


- 8 Click **Internet Protocol (TCP/IP)**.
- 9 Click **OK**. The Local Area Connection *number* Properties window is re-displayed.



- 10 Be sure the box next to Internet Protocol (TCP/IP) is selected.

- 11** Click **Properties**. The Internet Protocol (TCP/IP) Properties window is displayed:



- 12** Be sure **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.

- 13** Click **OK** to accept the TCP/IP settings.

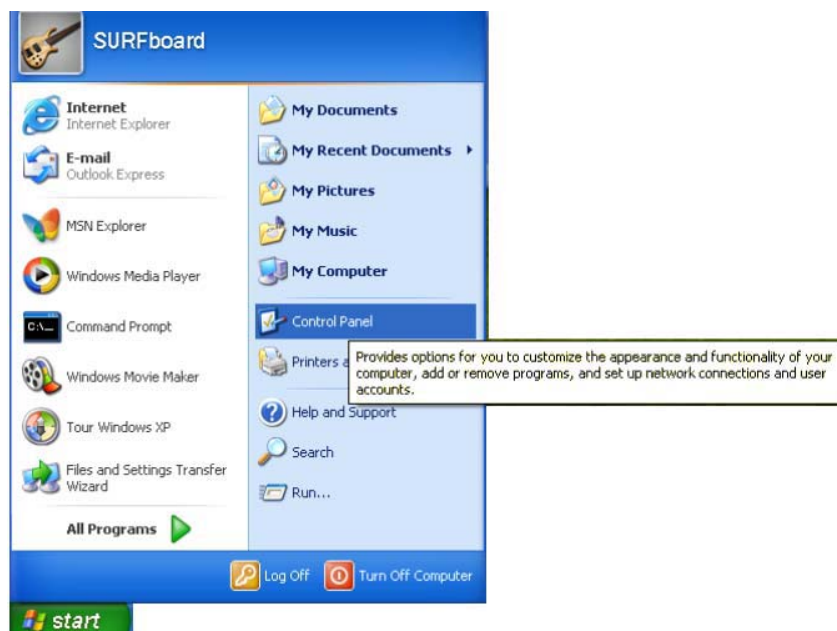
- 14** Click **Close** to close the Local Area Connection *number* Properties window.

- 15** Click **OK** when prompted to restart the computer and click **OK** again.

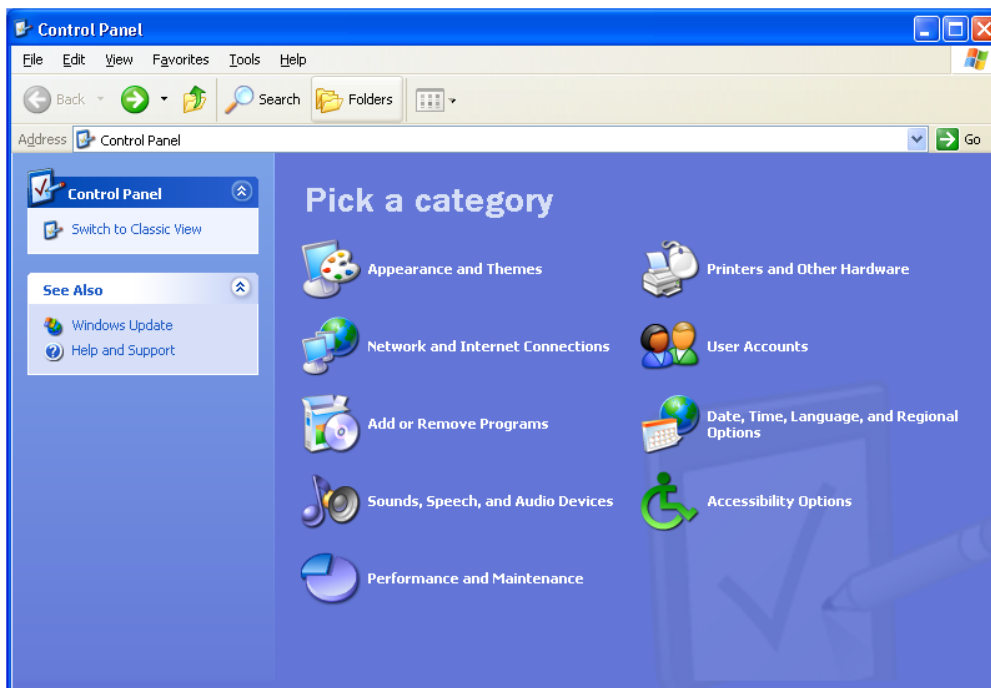
When you complete the TCP/IP configuration, go to "[Verifying the IP Address in Windows 2000 or Windows XP](#)".

Configuring TCP/IP in Windows XP

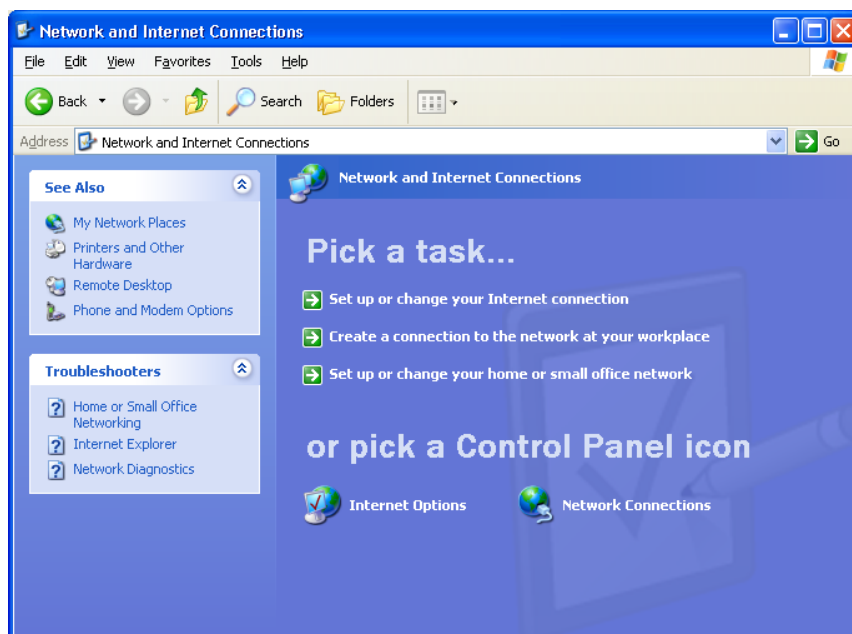
- 1 On the Windows desktop, click **Start** to display the Start window:



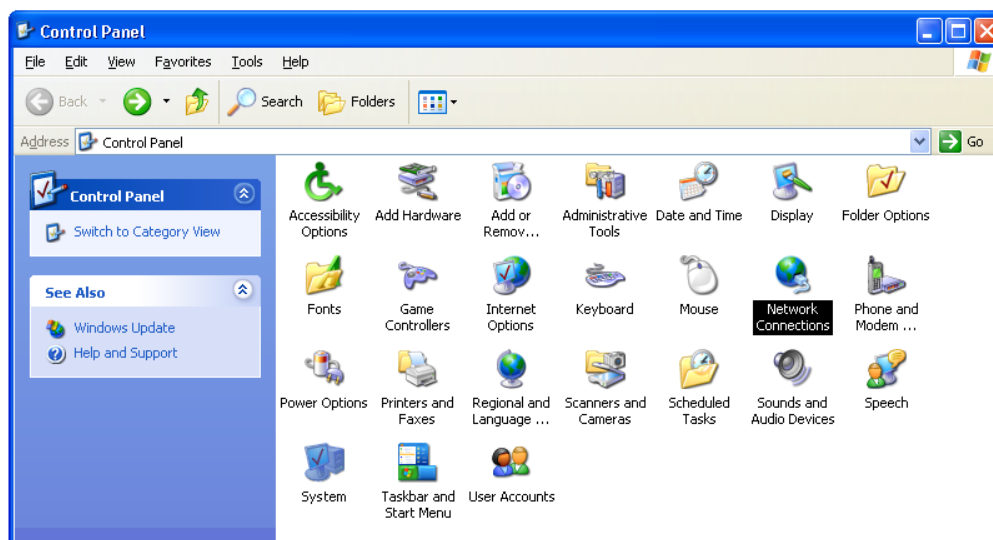
- 2 Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options. If the display is a Category view as shown below, continue with step 3. Otherwise, skip to step 5.



- 3 Click **Network and Internet Connections** to display the Network and Internet Connections window:

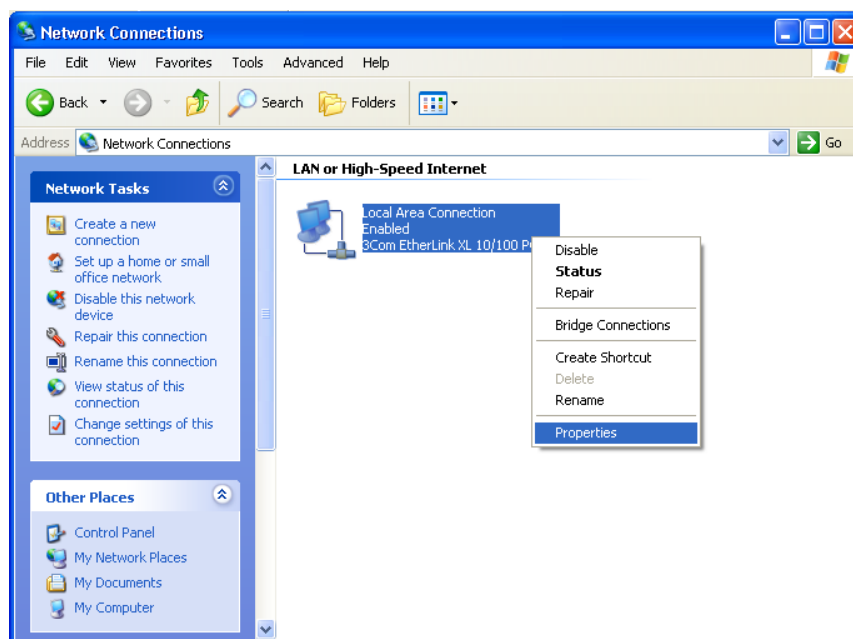


- 4 Click **Network Connections** to display the LAN or High-speed Internet connections. Skip to step 7.
- 5 If a classic view similar to below is displayed:

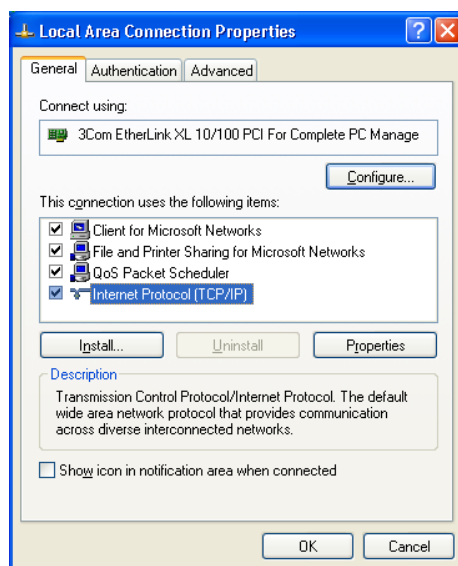


- 6 Double-click **Network Connections** to display the LAN or High-speed Internet connections.

- 7 Right-click on the network connection. If more than one connection is displayed, be sure to select the one for your network interface:

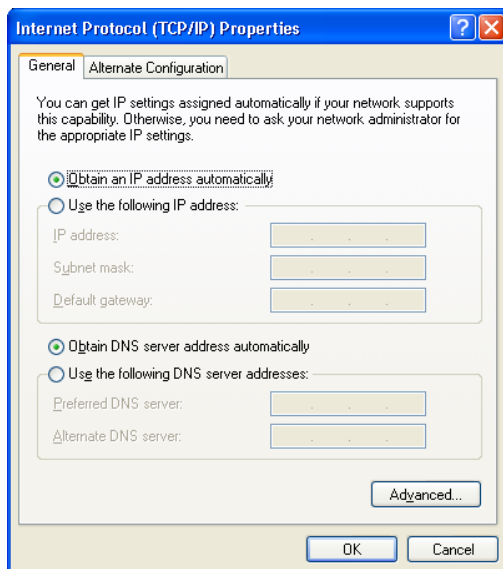


- 8 Select **Properties** from the pop-up menu to display the Local Area Connection Properties window:



- 9 On the Local Area Connection Properties window, select **Internet Protocol (TCP/IP)** if it is not selected.

- 10** Click **Properties** to display the Internet Protocol (TCP/IP) Properties window:



- 11** Verify that the settings are correct, as shown above.
- 12** Click **OK** to close the TCP/IP Properties window.
- 13** Click **OK** to close the Local Area Connection Properties window.

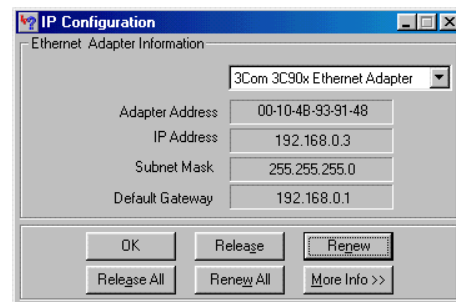
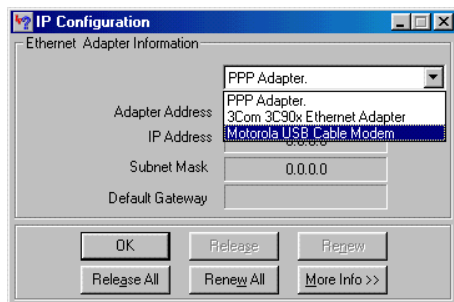
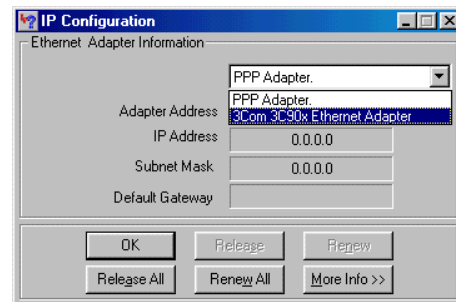
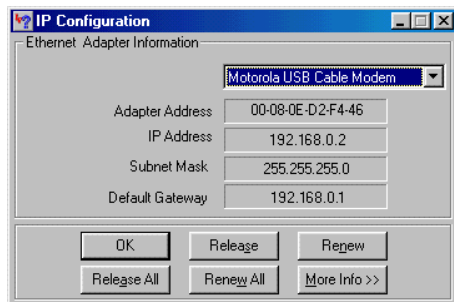
When you complete the TCP/IP configuration, go to [“Verifying the IP Address in Windows 2000 or Windows XP”](#).



Verifying the IP Address in Windows 95, Windows 98, or Windows Me

To check the IP address:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **winipcfg.exe** and click **OK**. The IP Configuration window is displayed. The Ethernet Adapter Information field will vary depending on the system, as shown in the following examples:



The values for Adapter Address, IP Address, Subnet Mask, and Default Gateway on the PC will be different than in the images.

In Windows 98, if "Autoconfiguration" is displayed before the IP Address as in the following image, call your service provider.

Adapter Address	00-80-C6-E7-59-E6
IP Autoconfiguration Address	169.254.191.251

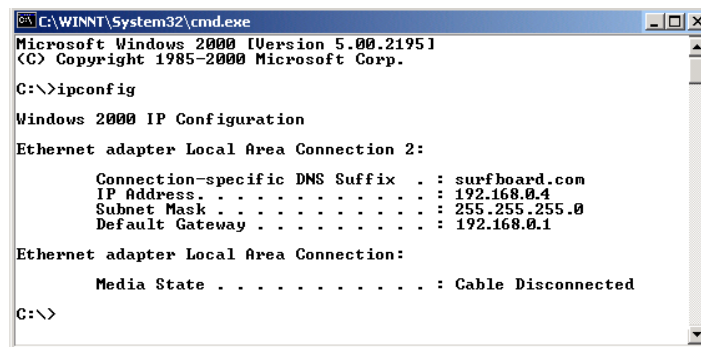
- 4 Select the adapter name — the Ethernet card or USB device.
- 5 Click **Renew**.
- 6 Click **OK** after the system displays an IP address.

If after performing this procedure the computer cannot access the Internet, call your cable provider for help.

Verifying the IP Address in Windows 2000 or Windows XP

To check the IP address:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **cmd** and click **OK** to display a command prompt window.
- 4 Type **ipconfig** and press **ENTER** to display the IP configuration. A display similar to the following indicates a normal configuration:



```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

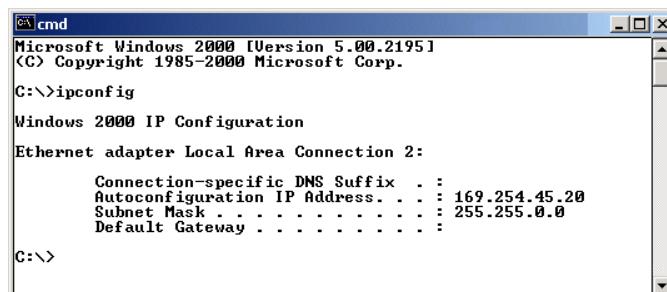
    Connection-specific DNS Suffix  . : surfboard.com
    IP Address. . . . . : 192.168.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Cable Disconnected

C:\>
  
```

If an Autoconfiguration IP Address is displayed as in the following window, there is an incorrect connection between the PC and the VT2500 or there are cable network problems. Check the cable connections and determine if you can view cable-TV channels on your television:



```

cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

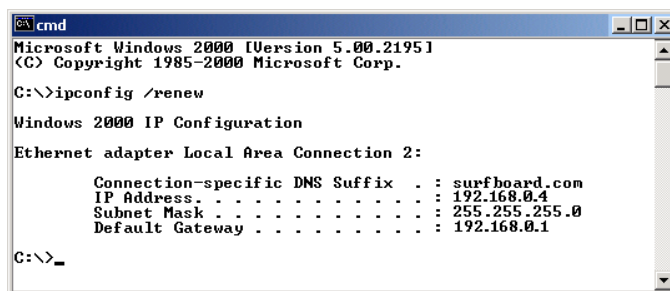
    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.45.20
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

C:\>
  
```

After verifying the cable connections and proper cable-TV operation, renew the IP address.

To renew the IP address:

- 1 Type **ipconfig /renew** and press **ENTER**. If a valid IP address is displayed as shown, Internet access should be available.



```
cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : surfboard.com
    IP Address . . . . . : 192.168.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\>
```

- 2 Type **exit** and press **ENTER** to return to Windows.

If after performing this procedure the computer cannot access the Internet, call your cable provider for help.



❖ Setting Up Your Wireless LAN (WLAN)

You can use the [VT2500](#) as an access point for a wireless LAN (WLAN) without changing its default settings.

Caution!



To prevent unauthorized eavesdropping or access to WLAN data, you must enable wireless security. The default [VT2500](#) settings provide no wireless security. After your WLAN is operational, be sure to enable wireless security.

To enable security for your WLAN, you can do the following on the [VT2500](#):

To	Perform	Use in Setup Program
Encrypt wireless transmissions and restrict WLAN access	Encrypting Wireless LAN Transmissions	Wireless > SECURITY — basic page
Further prevent unauthorized WLAN intrusions	Restricting Wireless LAN Access	Wireless > SECURITY — advanced page

Connect at least one computer to the [VT2500](#) Ethernet port to perform configuration. Do not attempt to configure the [VT2500](#) over a wireless connection.

You need to configure each wireless client (station) to access the [VT2500](#) LAN as described in “[Configuring the Wireless Clients](#)”.

Caution!



Never provide your ESSID, WPA or WEP passphrase, or WEP key to anyone who is not authorized to use your WLAN.

For descriptions of all wireless configuration fields, see “[Wireless Pages in the VT2500 Setup Program](#)”.

Another step to improve wireless security is to place wireless components away from windows. This decreases the signal strength outside the intended area.

Encrypting Wireless LAN Transmissions

To prevent unauthorized viewing of data transmitted over your WLAN, you must encrypt your wireless transmissions.

Use the [Wireless > SECURITY — basic](#) to encrypt your transmitted data. Choose *one* of:

Configure on the VT2500

If all of your wireless clients support Wi-Fi Protected Access (WPA), we recommend you follow [Configuring WPA on the VT2500](#)

Otherwise, perform [If you need to restore the wireless defaults, click Reset Security Defaults.](#)

Required On Each Wireless Client

If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase to the [VT2500](#) on each wireless client. Home and small-office settings typically use a local passphrase.

Configuring a RADIUS server requires specialized knowledge that is beyond the scope of this guide. For more information, contact your network administrator.

You must configure each wireless client with the [VT2500's](#) WEP key (must be identical)

If all of your wireless clients support WPA encryption, we recommend using WPA instead of WEP because WPA:

- Provides much stronger encryption and is more secure
- Provides authentication to ensure that *only* authorized users can log on to your WLAN
- Is much easier to configure
- Uses a standard algorithm on all compliant products to generate a key from a textual passphrase
- Will be incorporated into the new IEEE 802.11i wireless networking standard

For new wireless LANs, we recommend purchasing client adapters that support WPA, such as the [Motorola Wireless Notebook Adapter WN825G](#), [Wireless PCI Adapter WPCI810G](#), and [Wireless USB Adapter WU830G](#).

For more information about the benefits of WPA, see the Wi-Fi Protected Access Web page:

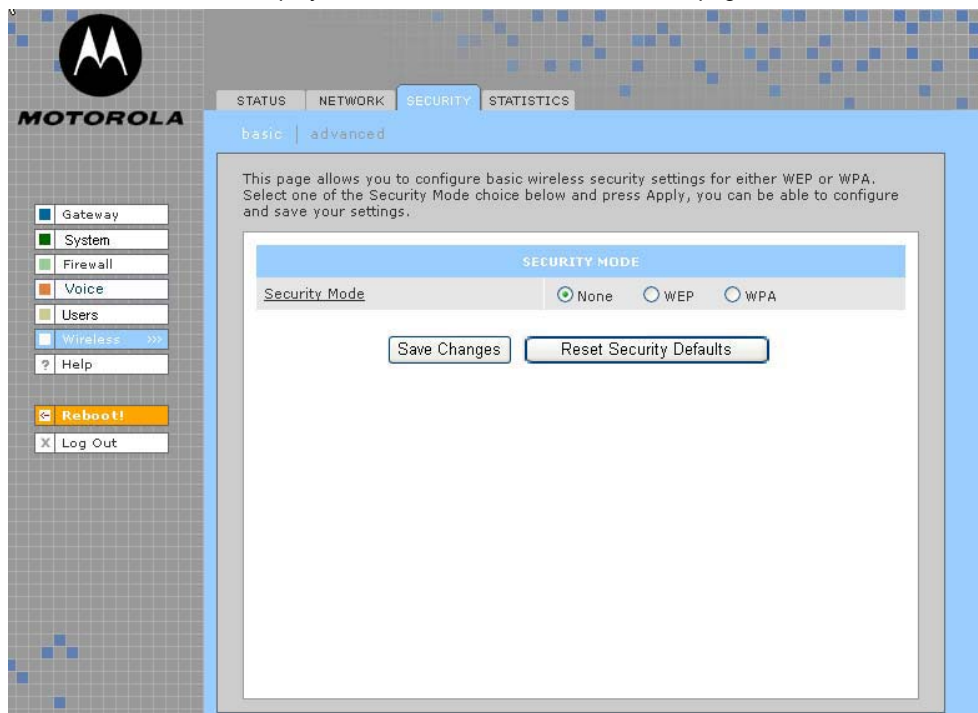
http://www.wifialliance.org/OpenSection/protected_access.asp.

Configuring WPA on the VT2500

After you enable and configure WPA on the VT2500, you must configure each WLAN client as described in the subsections under “[Configuring the Wireless Clients](#)”.

To enable WPA and set the key on the [VT2500](#):

- 1 On the [VT2500](#) Setup Program menu, click **Wireless**.
- 2 Click the **SECURITY** tab to display the [Wireless > SECURITY — basic](#) page:



- 3 In the **Security Mode** field, select **WPA** and click **Apply**.
- 4 Under WPA CONFIGURATION, choose one **WPA Encryption** type. *Because performance may be slow with TKIP, we recommend choosing AES if your clients support AES:*

TKIP	Temporal Key Integrity Protocol provides data encryption including a per-packet key mixing function, message integrity check (MIC), initialization vector (IV), and re-keying mechanism.
AES	The Advanced Encryption Standard algorithm implements symmetric key cryptography as a block cipher using 128-bit keys. We recommend this setting if all of your wireless clients support AES. The Motorola client adapters shown in “ Optional Accessories ” support AES.
Group Rekey Interval	Set the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying. The value should be from 0 - (2^32 - 1).

5 Choose the **WPA Authentication** type:

- Remote (Radius)** If a Remote Authentication Dial-In User Service (RADIUS) server is available, you can select this option and go to step 6. A RADIUS server is typically used in a large corporate location.
- Local (WPA-PSK)** If you choose Pre-Shared Key (PSK) local authentication, if the passphrase on any client supporting WPA matches the PSK Passphrase set on the [VT2500](#), the client can access the [VT2500](#) WLAN. To set the PSK Passphrase, go to step 7. A local key is typically used in a home or small office.

6 For **Remote (Radius)** authentication *only*, set:

- Radius Port** The port used for remote authentication through a RADIUS server. It can be from 0 to 65535.
- Radius Key** The key for remote authentication. It can be from 0 to 255 ASCII characters.
- Radius Server Type** Currently IPv4 *only*.
- Radius Server** The RADIUS server IP address in dotted-decimal format (example: 192.168.102.155).

7 For **Local (WPA-PSK)** authentication *only*, set:

- PSK Passphrase** The PSK password containing from 8 to 63 ASCII characters. You must set the identical passphrase on each WLAN client (see "[Configuring a Wireless Client for WPA](#)").

8 Click **Save Changes**.

If you need to restore the wireless defaults, click **Reset Security Defaults**.



Configuring WEP on the VT2500

After you enable and configure WEP on the VT2500, you must configure each WLAN client as described in the subsections under “[Configuring the Wireless Clients](#)”.

Use Wired Equivalent Privacy (WEP) only if you have wireless clients that do not support WPA.

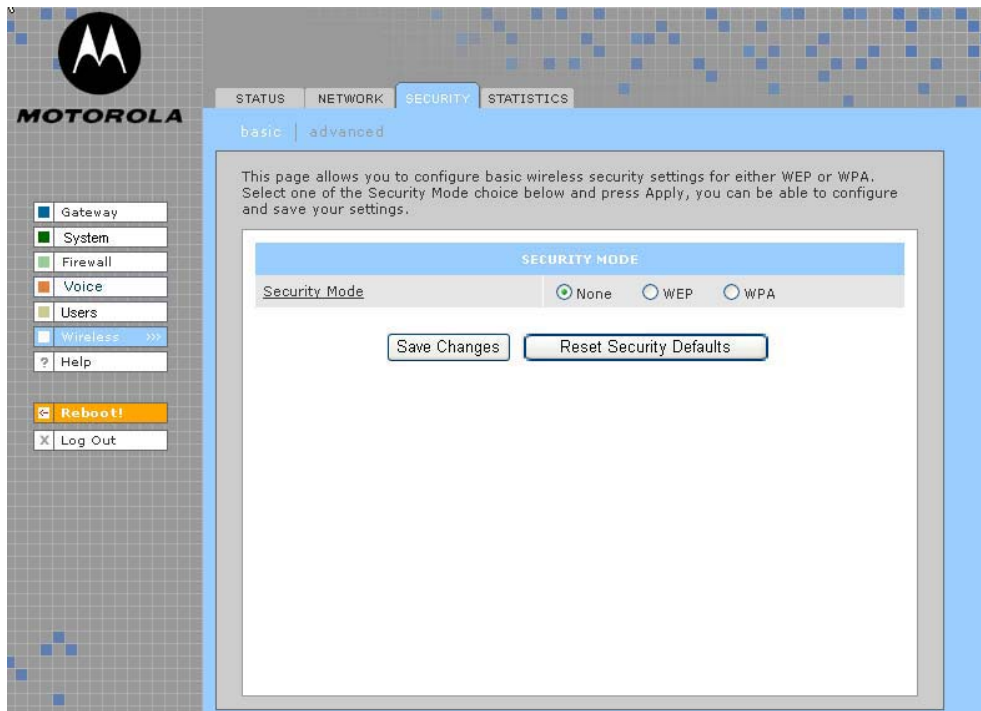
Caution!



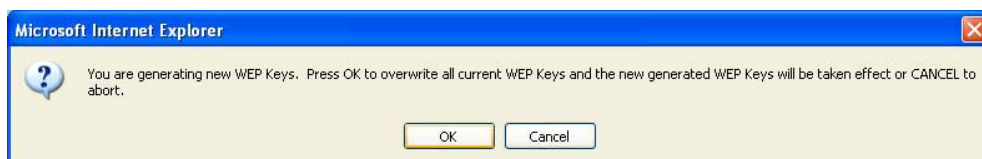
If you use WEP encryption, you must configure the same WEP key on the [VT2500 access point](#) and all wireless clients (stations). *Never provide your WEP key or passphrase to anyone who is not authorized to use your WLAN.*

To enable WEP and set the key on the [VT2500](#):

- 1 On the [VT2500](#) Setup Program menu, click **Wireless**.
- 2 Click the **SECURITY** tab to display the [Wireless > SECURITY — basic](#) page:



- 3 In the **Security Mode** field, select **WEP** and click **Apply**.
- 4 In the **WEP Passphrase** field, type a passphrase containing from 8 to 31 ASCII characters. For privacy, your passphrase displays as dots.
- 5 Click **Generate WEP Keys**. The following window is displayed:





- 6 Click **OK**. The WEP CONFIGURATION fields now appear something like this:

WEP CONFIGURATION		
WEP Passphrase	••••••••••	Generate WEP Keys
WEP Authentication	☐ Open	☒ Shared Key
Encryption	☒ Enable 64-Bit	☐ Enable 128-Bit
Key Type	Enter 10 HEX chars or 5 ASCII chars	Enter 26 HEX chars or 13 ASCII chars
☒ Key 1	e704d8bce7	e704d8bce78be042718adca8b2
☐ Key 2	718adca8b2	8f4c696d44d10d6b8222d1f978
☐ Key 3	8f4c696d44	ffb5918a1b024e93bd2475dc7
☐ Key 4	8222d1f978	cc1ad6dbfc137c898233206332

Before performing step 7, consider the following:

- If all of your wireless adapters support 128-bit encryption, you can select **Enable 128 Bit**. Otherwise, you must select **Enable 64 Bit**.
- For a WLAN client equipped with a Motorola wireless adapter, you can enter the WEP Passphrase when you perform “[Configuring a Wireless Client for WEP](#)”. For all other wireless adapters, you will probably need to enter the generated WEP key that you designate in step 7.

- 7 Under WEP CONFIGURATION, set:

WEP Authentication	Sets whether shared key authentication is enabled to provide data privacy on the WLAN: • Open System — Any WLAN client can transmit data to any other client without authentication. It is the default, if the Security Mode is set to WEP. • Shared Key — The VT2500 authenticates and transfers data to and from all clients having shared key authentication enabled. <i>We recommend this setting.</i>
Encryption	Use a WEP key length that is compatible with your wireless client adapters. Choose <i>one</i> of: • Enable 64-Bit — Use only if you have wireless clients that do not support 128-bit encryption • Enable 128-Bit — We recommend this setting for stronger encryption; it is supported by the Motorola WN825G and WPCI810G wireless adapters and most current wireless adapters
Key Type (Key 1 to Key 4)	Select the active key (1 to 4). Only <i>one</i> key can be active. You can generate WEP keys from a passphrase as described in steps 4 to 6 or type non-case-sensitive hexadecimal characters 0 to 9 and A to F to define up to: • Four 10-character long key 64-bit WEP keys • Four 26-character long 128-bit WEP keys <i>We recommend changing the WEP keys frequently. Never provide the WEP key to anyone who is not authorized to use your WLAN.</i>

- 8 Click **Save Changes** to save your changes.

If you need to restore the wireless defaults, click **Reset Security Defaults**.



Restricting Wireless LAN Access

The default [VT2500](#) wireless settings enable any computer having a compatible wireless adapter to access your WLAN. To protect your network from unauthorized intrusions, you can restrict access to your WLAN to a limited number of computers on the [Wireless > SECURITY — advanced](#) page.

You can configure one or both of:

Configure on the VT2500

Perform [Configuring the Wireless Network Name on the VT2500](#) to disable Extended Service Set Identifier (ESSID) broadcasting to enable closed network operation

Perform [Configuring a MAC Access Control List on the VT2500](#) to restrict access to wireless clients with known MAC addresses

Required On Each Wireless Client

You must configure each wireless client with the [VT2500](#)'s ESSID network name (must be identical).

No configuration is required on the client.

Configuring the Wireless Network Name on the VT2500

If you disable ESSID broadcasting on the [VT2500](#), it does not transmit the network name (ESSID). This provides additional protection because:

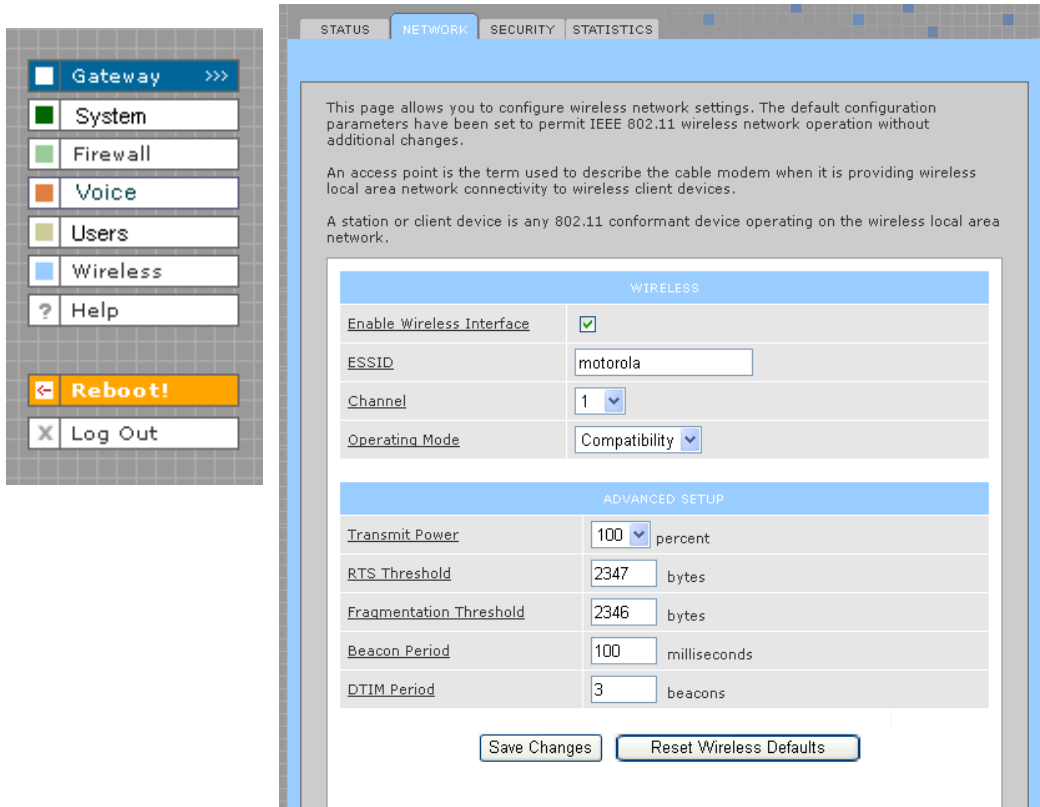
- Only wireless clients configured with your network name can communicate with the [VT2500](#)
- It is more difficult for unauthorized individuals who scan for unsecured WLANs to access your WLAN

Closed network operation is an enhancement of the IEEE 802.11b and IEEE 802.11g standards.

If you select Disable ESSID Broadcast, you must also perform [Configuring a Wireless Client with the Network Name \(ESSID\)](#) on all WLAN [clients](#) (stations). Never provide your ESSID to anyone who is not authorized to use your WLAN.

To configure the ESSID on the [VT2500](#):

- 1 Start the [VT2500](#) Setup Program as described in “[Starting the VT2400/VT2500 Voice Gateway Setup Program](#)”.
- 2 On the Setup Program menu, click **Wireless**.
- 3 Click the **NETWORK** tab to display the [Wireless > NETWORK](#) page:



This page allows you to configure wireless network settings. The default configuration parameters have been set to permit IEEE 802.11 wireless network operation without additional changes.

An access point is the term used to describe the cable modem when it is providing wireless local area network connectivity to wireless client devices.

A station or client device is any 802.11 conformant device operating on the wireless local area network.

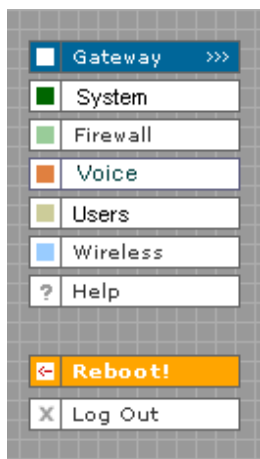
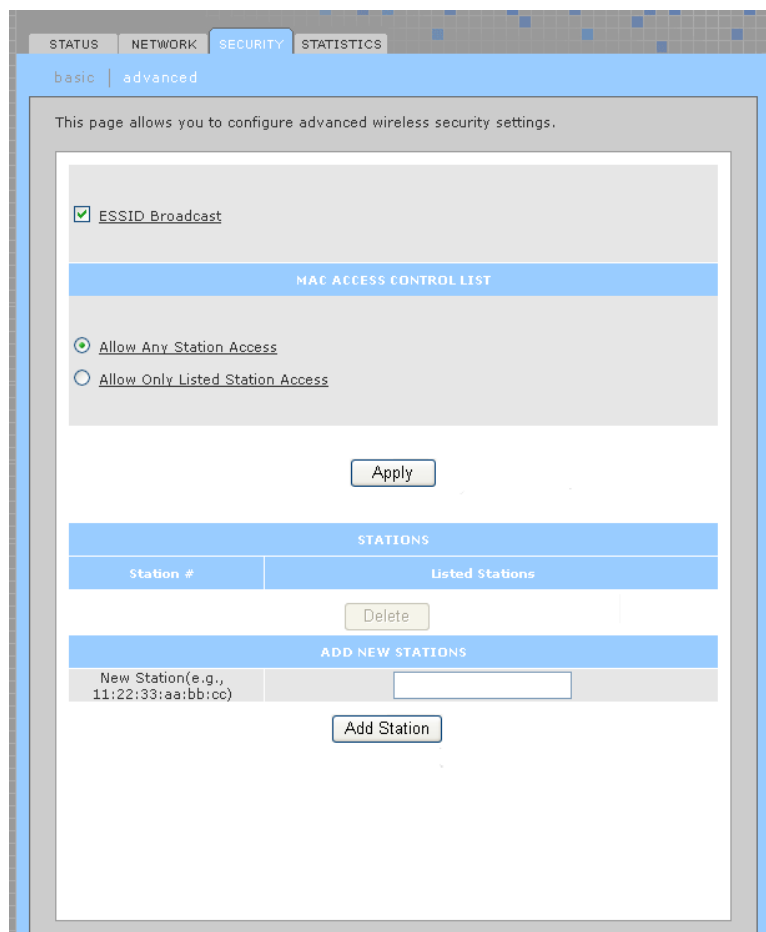
WIRELESS	
Enable Wireless Interface	☒
ESSID	motorola
Channel	1
Operating Mode	Compatibility

ADVANCED SETUP	
Transmit Power	100 percent
RTS Threshold	2347 bytes
Fragmentation Threshold	2346 bytes
Beacon Period	100 milliseconds
DTIM Period	3 beacons

Save Changes Reset Wireless Defaults

- 4 In the **ESSID** field, type a unique **name**. It can be any alphanumeric, case-sensitive string up to 32 characters. The default is “Motorola.” *Do not use the default ESSID.*
- 5 Click **Save Changes** to save your changes.

- 6 To restrict WLAN access to clients configured with the same Network Name (ESSID) as the [VT2500](#), click the **SECURITY** tab.
- 7 Click **advanced** to display the [Wireless > SECURITY — advanced](#) page:

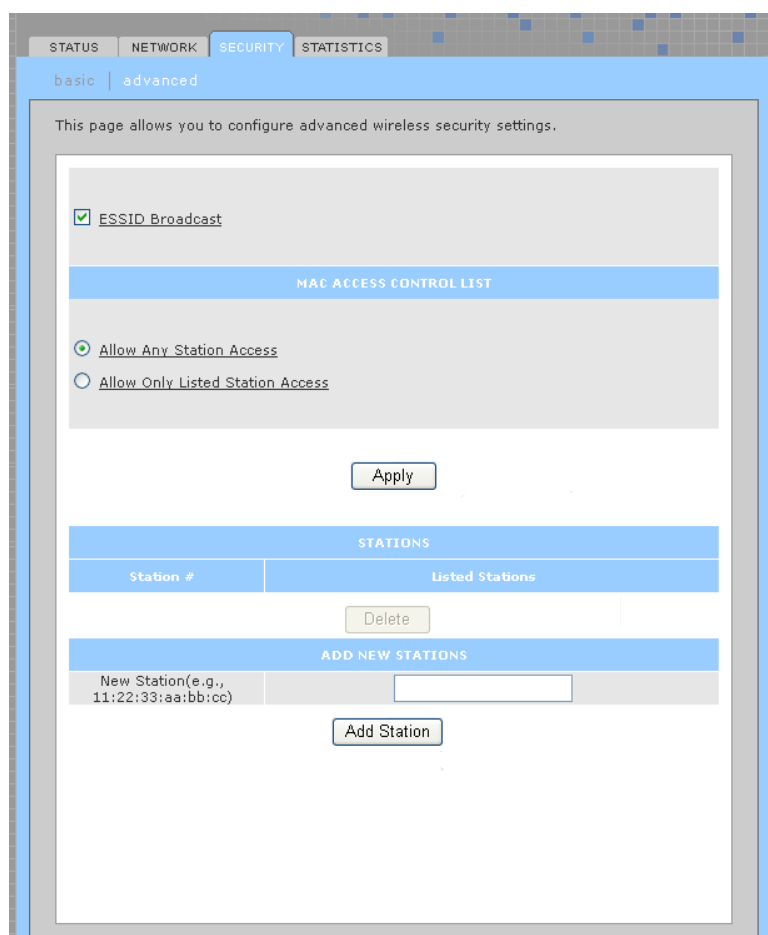
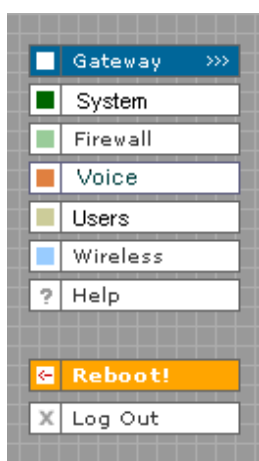
- 8 Select **ESSID Broadcast** to restrict WLAN access to clients configured with the same Network Name (ESSID) as the [VT2500](#).
- 9 Click **Apply** to save your changes.

Configuring a MAC Access Control List on the VT2500

You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.

To configure a MAC access control list:

- 1 On the [VT2500](#) Setup Program menu, click **Wireless**.
- 2 Click the **SECURITY** tab.
- 3 Click **advanced** to display the [Wireless > SECURITY — advanced](#) page:



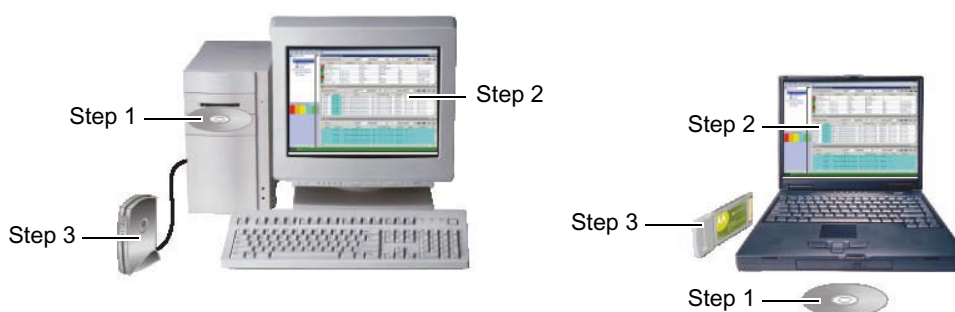
- 4 To restrict wireless access to systems in the MAC access control list, select **Allow Only Listed Stations Access** and click **Apply**.
- 5 To add a wireless client, type its MAC address in the format **xx:xx:xx:xx:xx:xx** in the **New Station** field and click **Add Station**.

You can add up to 32 wireless clients to the MAC access control list.

Configuring the Wireless Clients

For each wireless client computer (station), install the wireless adapter — such as a Motorola [WN825G](#), [WPCI810G](#), or [WU830G](#) — following the instructions supplied with the adapter. Be sure to:

- 1 Insert the CD-ROM for the adapter in the CD-ROM drive on the client.
- 2 Install the device software from the CD.
- 3 Insert the adapter in the PCMCIA or PCI slot or connect it to the USB port.



Configure the adapter to obtain an IP address automatically. The Motorola wireless adapters are supplied with a client configuration program called Wireless Client Manager, which is installed in the Windows Startup group.

On a PC with Wireless Client Manager installed, the  icon is displayed on the Windows task bar. Double-click the icon to launch the utility.

You may need to do the following to use a wireless client computer to surf the Internet:

If You Performed:

Configuring WPA on the VT2500

If you need to restore the wireless defaults, click Reset Security Defaults.

Configuring the Wireless Network Name on the VT2500

Configuring a MAC Access Control List on the VT2500

On Each Client, You Need to Review:

“Configuring a Wireless Client for WPA”

“Configuring a Wireless Client for WEP”

“Configuring a Wireless Client with the Network Name (ESSID)”

No configuration on client required



Configuring a Wireless Client for WPA

If you enabled WPA and set a PSK Passphrase by “[Configuring WPA on the VT2500](#)”, you must configure the same passphrase (key) on each wireless client. The VT2500 cannot authenticate a client if:

- WPA is enabled on the VT2500 but not on the client
- The client passphrase does not match the VT2500 PSK Passphrase

For information about the WPA support in Windows XP, visit:

WPA Wireless Security for Home Networks

<http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp>

Overview of the WPA Wireless Security Update in Windows XP

<http://support.microsoft.com/?kbid=815485>

You can download the Microsoft Windows XP Support Patch for WPA from

<http://www.microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en>.

Caution!



Never provide the PSK Passphrase to anyone who is not authorized to use your WLAN.

Configuring a Wireless Client for WEP

If you enabled WEP and set a key by [If you need to restore the wireless defaults, click Reset Security Defaults.](#), you must configure the same WEP key on each wireless client. The VT2500 cannot authenticate a client if:

- Shared Key Authentication is enabled on the VT2500 but not on the client
- The client WEP key does not match the VT2500 WEP key

On a WLAN client equipped with a Motorola wireless adapter, you can enter the WEP Passphrase you set when you configured the VT2500. For all other wireless adapters, you must enter the 64-bit or 128-bit WEP key generated by the VT2500.

Caution!



Never provide the WEP key to anyone who is not authorized to use your WLAN.

Configuring a Wireless Client with the Network Name (ESSID)

To distinguish it from other nearby WLANs, you should identify your WLAN with a unique network name (also known as a network identifier or ESSID). As you configure a wireless client, you will be prompted for the network identifier, network name, or ESSID; type the same **name** that appears in the ESSID field on the [Wireless > NETWORK](#) page in the VT2500 Setup Program (see [Wireless > NETWORK](#) for details). If the network name is not configured yet, see “[Configuring the Wireless Network Name on the VT2500](#)” to configure it.

After you specify the network name, many wireless cards or adapters automatically scan for an access point such as the VT2500 and the proper channel and data rate. If your card requires you to manually start scanning for an access point, do so following the instructions in the documentation supplied with the card.



Wireless Pages in the VT2500 Setup Program

Use the Wireless pages to control and monitor the wireless interface:

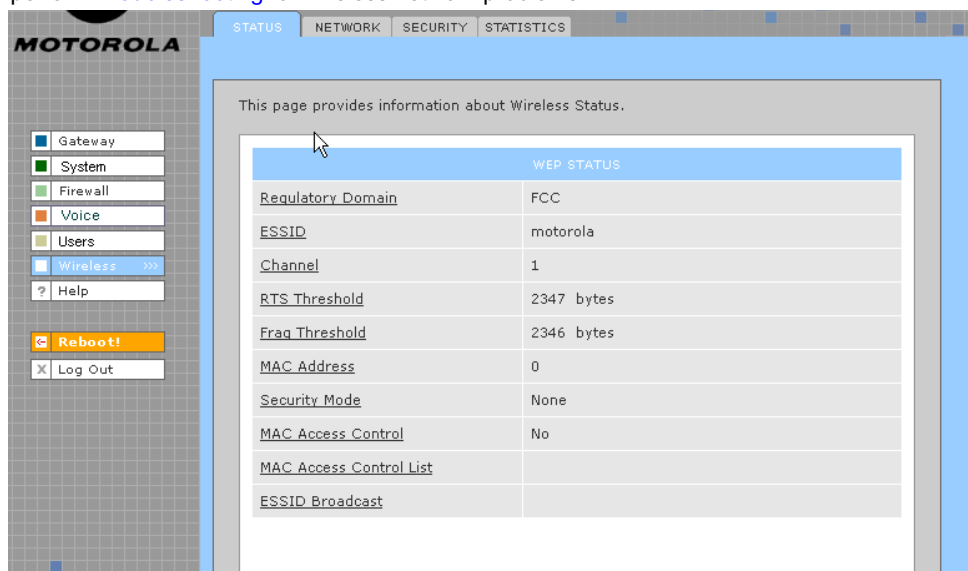
- [Wireless > STATUS](#) page
- [Wireless > NETWORK](#) page
- [Wireless > SECURITY — basic](#) page
- [Wireless > SECURITY — advanced](#) page
- [Wireless > STATISTICS](#) page

After you edit some fields and click Apply, you are required to reboot your voice gateway for your changes to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.

Wireless > STATUS

You can use this read-only page to:

- View the wireless interface status
- Help perform [Troubleshooting](#) for wireless network problems



Wireless > STATUS Page Fields

Regulatory Domain	Indicates the country for which the VT2500 is manufactured. The list of channels depends on the country's standards for operation of wireless devices. Depending on the domain set at the factory, USA FCC, Europe, Spain, France, Japan, or some other country name is displayed. The equipment version marketed in the United States is restricted to usage of channels 1 through 11 only.
ESSID	Displays the ESSID set on the Wireless > NETWORK page. For more information, see " Configuring the Wireless Network Name on the VT2500 ". <i>Never provide the ESSID to anyone who is not authorized to use your WLAN.</i>
Channel	Displays the radio channel for the access point. If you encounter interference, you can set a different channel on the Wireless > NETWORK page.
RTS Threshold	Displays the Request to Send Threshold set on the Wireless > NETWORK page.
Frag Threshold	Displays the Fragmentation Threshold set on the Wireless > NETWORK page.
MAC Address	Displays the VT2500 MAC address.
Security Mode	Displays the enabled wireless encryption type. For more information, see " Configuring WPA on the VT2500 " or " Configuring WEP on the VT2500 ".
MAC Access Control	Displays the MAC Access Control setting (see " Configuring a MAC Access Control List on the VT2500 "): • Allow Listed — Only clients in the MAC access control list can access the WLAN. • Allow Any Station Access — Any wireless client can access the WLAN.



Wireless > STATUS Page Fields (continued)

MAC Access Control List Displays the MAC addresses of wireless clients having access (see "[Configuring a MAC Access Control List on the VT2500](#)").

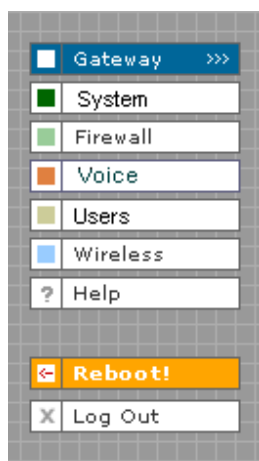
ESSID Broadcast If you disable ESSID broadcast, the network name (ESSID) will not be transmitted in the 802.11 beacon frame. This provides some additional protection for your network because only 802.11 stations that know your network name can be configured to associate with the SBG. Note: Disable ESSID broadcast operation is not part of the IEEE 802.11 standard.

Wireless > NETWORK

Use this page for:

- Enabling the wireless interface
- Configuring the wireless network name (also see [Configuring the Wireless Network Name on the VT2500](#))
- Configuring other WLAN settings

You can use the [VT2500](#) to operate a WLAN without changing its default settings.



STATUS
NETWORK
SECURITY
STATISTICS

This page allows you to configure wireless network settings. The default configuration parameters have been set to permit IEEE 802.11 wireless network operation without additional changes.

An access point is the term used to describe the cable modem when it is providing wireless local area network connectivity to wireless client devices.

A station or client device is any 802.11 conformant device operating on the wireless local area network.

WIRELESS	
Enable Wireless Interface	☒
ESSID	motorola
Channel	1
Operating Mode	Compatibility

ADVANCED SETUP	
Transmit Power	100 percent
RTS Threshold	2347 bytes
Fragmentation Threshold	2346 bytes
Beacon Period	100 milliseconds
DTIM Period	3 beacons

Save Changes
Reset Wireless Defaults

Wireless > NETWORK page fields

Field	Description
-------	-------------

WIRELESS

Wireless > NETWORK page fields (continued)

Field	Description
Enable Wireless Interface	Select this box to enable the wireless interface.
ESSID	Sets a unique network name for the VT2500 WLAN to distinguish between multiple WLANs in the vicinity. <i>If you select Disable ESSID Broadcast on the Wireless > SECURITY — advanced page, all clients on the WLAN must have the same ESSID (network name) as the VT2500.</i> It can be any alphanumeric, case-sensitive string up to 32 characters. The default is “Motorola.” <i>We strongly recommend not using the default. Never provide the ESSID to anyone who is not authorized to use your WLAN.</i>
Channel	Sets the wireless radio channel. You can change the channel if you encounter interference on the default channel. The default is 1 (one), except in countries where the first channel permitted for wireless operation is not one.
Operating Mode	Sets how the VT2500 communicates with wireless clients (stations): 11b/11g Standard — Enables all IEEE 802.11b and IEEE 802.11g clients to work with the VT2500. <i>We recommend using this default setting in most cases because it is more flexible.</i> 11g Enhanced — Choose this option only if all IEEE 802.11g client adapters on the network support the performance-enhancing features of the IEEE 11g Enhanced mode. It is not supported by all IEEE 802.11g adapters.

ADVANCED SETUP

Transmit Power	Sets the VT2500 wireless transmission power — 3, 6, 12, 25, 50, 75, or 100%. The default is 100%. You can lower the Transmit Power to: - Decrease “leakage” into outside areas, such as the street - Improve performance if you usually position your computer or laptop close to your VT2500 Transmission power control is an optional IEEE 802.11 feature.
RTS Threshold	The Request To Send Threshold sets the minimum packet size for which the VT2500 issues an RTS before sending a packet. A low RTS threshold can help when many clients are associated with the VT2500, or the clients are far apart and can detect the VT2500 but not each other. It can be 0 to 2347 bytes. The default is 2347.
Fragmentation Threshold	Sets the size at which packets are fragmented (sent as several packets instead of as one packet). A low fragmentation threshold can help when communication is poor or there is a significant interference. It can be 256 to 2346 bytes. The default is 2346.
Beacon Period	Sets the time between beacon frames sent by the VT2500 for wireless network synchronization. It can be from 1 to 999 ms. The default is 100 ms.

SECOND PAGE ONLY

DTIM Period	The delivery traffic indication message (DTIM) period is the number of beacon periods that elapse before a wireless client operating in power save mode “listens” for buffered broadcast or multicast messages from the VT2500. It can be from 1 to 99999. The default is 3.
--------------------	--

[Save Changes \(button\)](#)

[Reset Wireless Defaults \(button\)](#)



Wireless > SECURITY — basic

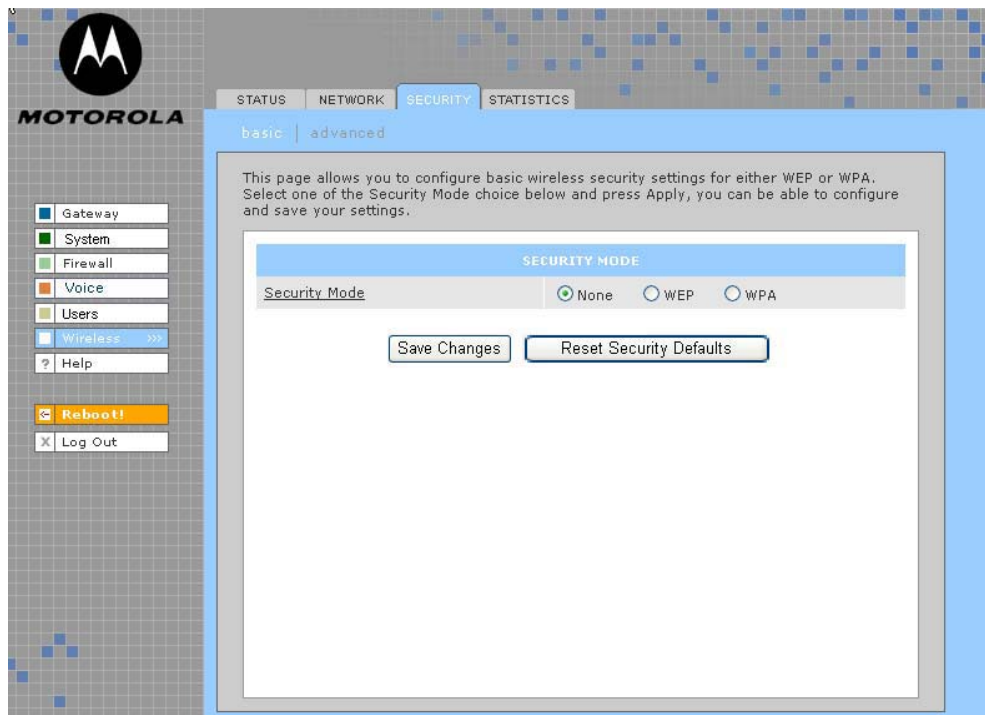
Use this page to configure how your [VT2500](#) encrypts wireless transmissions. For information about using this page, review “[Encrypting Wireless LAN Transmissions](#)” in this section of the manual.

After you enable and configure WEP or WPA on the [VT2500](#) by performing “[Configuring WPA on the VT2500](#)” or “[Configuring WEP on the VT2500](#)” (all options on the [Wireless > SECURITY — basic](#) page are described in these procedures), you must configure each WLAN client as described in the subsections under “[Configuring the Wireless Clients](#)”.

Caution!

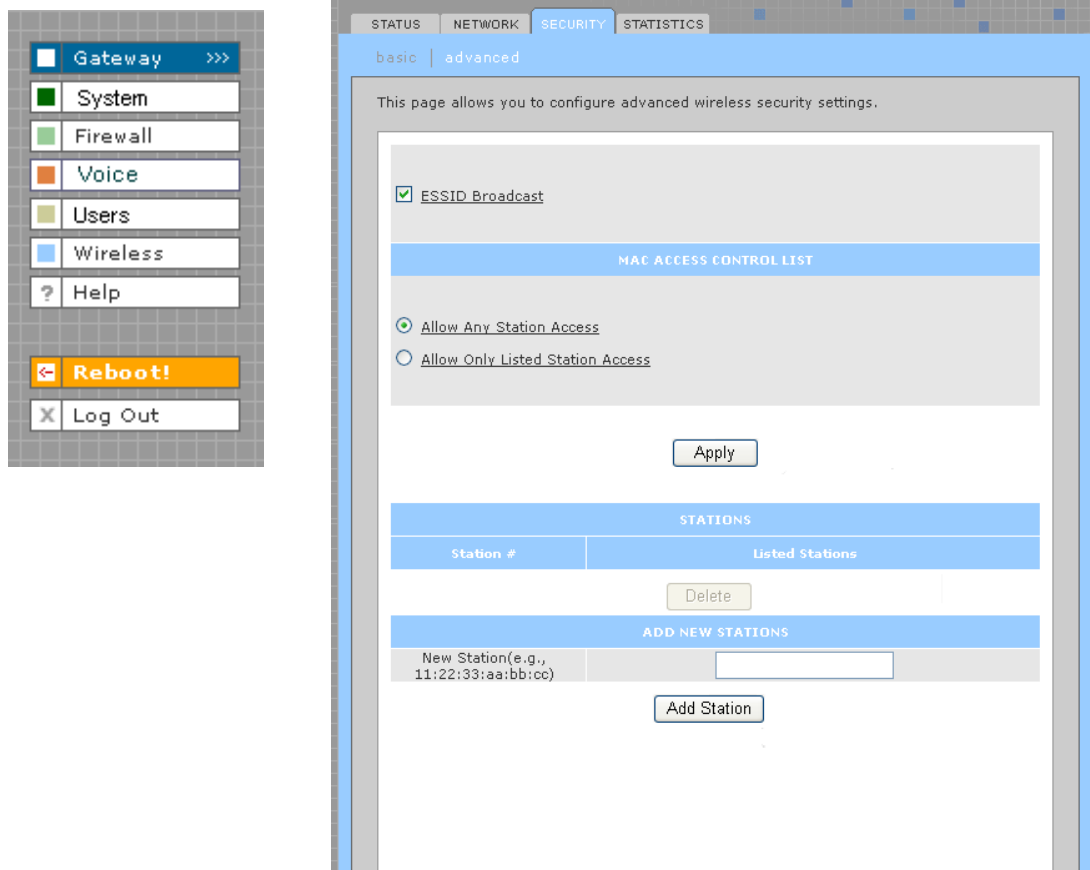


The default Security Mode setting None provides no security for transmitted data.



Wireless > SECURITY — advanced

Use this page to configure advanced wireless security settings.



Wireless > Security — ADVANCED page fields

Field or Button	Description
ESSID Broadcast	If selected, only wireless clients (stations) having the same Network Name (ESSID) as the VT2500 can communicate with the VT2500 . Closed network operation is a VT2500 enhancement to IEEE 802.11b. The default is not selected (off).
MAC ACCESS CONTROL LIST	You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.
Allow Any Station Access	If selected, any wireless client can access the VT2500 WLAN.
Allow Only Listed Stations Access	If selected, only wireless clients in the MAC access control list can access the VT2500 WLAN.
Apply (button)	Click to apply your change.
Station #	
Listed Stations	Lists the wireless clients in the MAC access control list having access if Allow Only Listed Stations Access is selected.

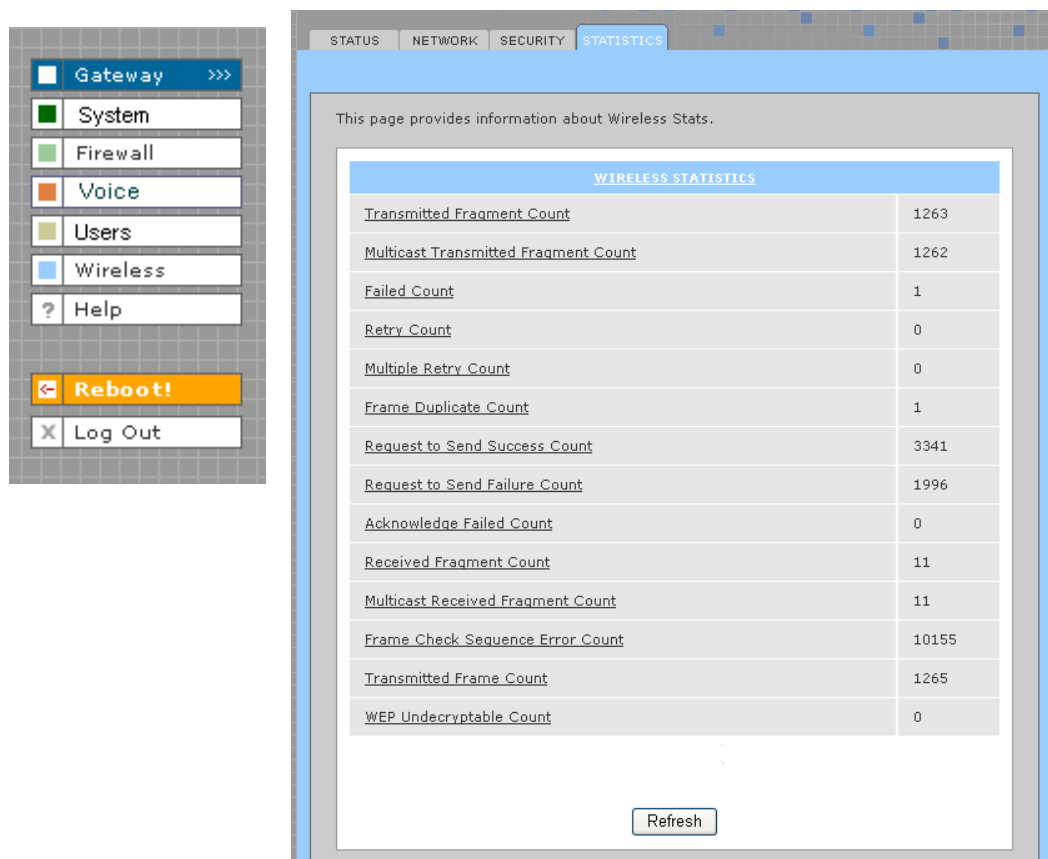


Wireless > Security — ADVANCED page fields (continued)

Field or Button	Description
Delete (button)	To delete a wireless client from the MAC access control list, select its Delete check box and click the Delete button.
ADD NEW STATIONS	
New Station (now Station #?)	Type the MAC address of the wireless client to add to the MAC access control list. Use the format xx:xx:xx:xx:xx:xx. The MAC access control list can contain one to 32 clients.
Add Station (button)	Click to add the New Station to the MAC access control list.

Wireless > STATISTICS

Use this page to display wireless statistics.



STATUS NETWORK SECURITY **STATISTICS**

This page provides information about Wireless Stats.

WIRELESS STATISTICS	
Transmitted Fragment Count	1263
Multicast Transmitted Fragment Count	1262
Failed Count	1
Retry Count	0
Multiple Retry Count	0
Frame Duplicate Count	1
Request to Send Success Count	3341
Request to Send Failure Count	1996
Acknowledge Failed Count	0
Received Fragment Count	11
Multicast Received Fragment Count	11
Frame Check Sequence Error Count	10155
Transmitted Frame Count	1265
WEP Undecryptable Count	0

Refresh

Wireless > STATISTICS page fields

Field or Button Description

WIRELESS STATISTICS

Transmitted Fragment Count	The number of acknowledged MAC protocol data units (MPDUs) with an address in the address 1 field or an MPDU with a multicast address in the address 1 field of type data or management.
Multicast Transmitted Fragment Count	The number of transmitted fragments when the multicast bit is set in the destination MAC address of a successfully transmitted MAC service data unit (MSDU). When operating as a STA in an ESS, where these frames are directed to the AP, this implies having received an acknowledgment to all associated MPDUs.
Failed Count	The number of MSDUs not transmitted successfully because the number of transmit attempts exceeded the IEEE 802.11b short or long retry limit.
Retry Count	The number of successfully transmitted MSDUs after one or more retransmissions.

Wireless > STATISTICS page fields (continued)

Field or Button	Description
Multiple Retry Count	The number of successfully transmitted MSDUs after more than one retransmission.
Frame Duplicate Count	The number of frames received where the Sequence Control field indicated the frame was a duplicate.
Request To Send Success Count	The number of CTS messages received in response to RTS messages.
Request To Send Failure Count	The number of CTS messages not received in response to RTS messages.
Acknowledge Failed Count	The number of acknowledgment messages not received when expected from a data message transmission.
Received Fragment Count	The number of successfully received MPDUs of type Data or Management.
Multicast Received Fragment Count	The number of MSDUs received when the multicast bit was set in the destination MAC address.
Frame Check Sequence Error Count	The number of FCS errors detected in a received MPDU.
Transmitted Frame Count	The number of successfully transmitted MSDUs.
WEP Undecryptable Count	This number of frames received with the WEP subfield of the Frame Control field set to one and the WEP On key value mapped to the client MAC address. This indicates that the frame should not have been encrypted or was discarded due to the receiving client not having WEP enabled.
Refresh (button)??	Click to collect new data.

Troubleshooting

If the solutions listed here do not solve your problem, contact your cable provider. Before calling your cable provider, try pressing the reset button on the rear panel. Resetting the VT2500 may take 5 to 30 minutes. Your service provider may ask for the status of the lights as described in [“Front-Panel Lights and Error Conditions”](#).

Problem	Possible Solutions
Green POWER light is off	Check that the AC power adapter is properly plugged into the electrical outlet and the VT2400/VT2500. Check that the electrical outlet is working.
Cannot send or receive data or phone calls or	Be sure the telephone line cord is connected to the VT2400/VT2500. Check all other cabling between the modem, the VT2400/VT2500, and the computer. Be sure you used the cables provided with the VT2400/VT2500. All Ethernet cables must be straight-through cables.
No dial tone	Check the lights on the modem front panel. For information, see your broadband modem user guide. Check the POWER light (see “Front Panel” on page 5).
A wireless client(s) cannot send or receive data (VT2500 only)	• Be sure that your wireless adapter (PCI card, Notebook or Ethernet adapter) on the PC is installed correctly and is active. • Be sure that your wireless adapter's radio signal is enabled. Review your adapter's documentation for further instructions. • Be sure that your wireless adapter for your PC and the wireless router security settings are the same so that it will allow your computer to access the wireless network. Also, verify that the list of <i>Restricted Wireless MAC Addresses</i> (on the WIRELESS Page of the Web-based Configuration Utility is not configured to block your PC. For details on adjusting your security settings, please refer to the descriptions of the WIRELESS and SECURITY Pages in Section 3: Configuration. • Be sure that your wireless adapter is within range of the voice gateway and is not behind an obstruction. For example, metal structures will interfere with the signal, as will 2.4 GHz cordless phones and microwaves. • Be sure that the PC's wireless adapter antenna is properly connected.
A wired client cannot send or receive data (VT2400/VT2500)	• If you have cable TV, check that the TV is working and the picture is clear. If you cannot receive regular TV channels, the data service will not function. • Check the coaxial cable at the SBG900 and wall outlet. Hand-tighten if necessary. • Check the IP address. Follow the steps for verifying the IP address for your system. See “Configuring TCP/IP”. Call your cable provider if you need an IP address. • Check that the Ethernet cable is properly connected to the SBG900 and the computer.
Slow wireless transmission speed with SPA enabled	• On the Wireless > SECURITY — basic page, check whether the WPA Encryption type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES as described in step 4 in “Configuring WPA on the VT2500” on page 96.”

Front-Panel Lights: Status and Error Conditions

Light	Color	Description
Power	Green	Indicates if the product has power.
Status	Green	Indicates the state the product is in: One blink (every two seconds) - performing initial boot sequence Two blinks - obtaining network IP address Three blinks - Downloading its configuration profile from your VoIP provider
WLAN	Green	Indicates activity on the wireless interface
WAN	Green and Amber	Indicates activity on the WAN and link speed Green = 100baseT, Amber = 10baseT
LAN1	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
LAN2	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
LAN3	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
LAN4	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
Line 1 and Line 2	Green	Indicates status of line 1: Off - service is not present on the line One blink - The line is off the hook Continuous blink - Attempting to reregister with your VoIP provider after an interruption in service (see PSTN failover in " Rear Panel " on page 7) Solid - Successfully registered with your VoIP provider



Contact Us

If you need assistance while working with the [VT2400/VT2500](#), contact your cable provider. For more information about customer service, technical support, or warranty claims, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the [VT2400/VT2500](#).

For answers to typical questions, see "[Frequently Asked Questions](#)" on page 119.

For more information about Motorola consumer cable products, education, and support, visit <http://broadband.motorola.com/consumers>.

Frequently Asked Questions

If you do not understand a term or acronym, check the [Glossary](#).

Q What does the Motorola voice terminal do?

- A** The [VT2400/VT2500 Voice Gateway](#) is part stand-alone media terminal adapter (S-MTA) and part home broadband router:
- As an S-MTA, it converts analog voice signals to and from a standard telephone to digital data that can be transmitted through a broadband connection across the Internet. It provides an alternate means to make voice calls.
 - It provides basic routing to enable simultaneous voice and data communication.

Q Will the [VT2400/VT2500 Voice Gateway](#) work with a cable modem or DSL modem?

- A** Yes. The [VT2400/VT2500 Voice Gateway](#) supports [DHCP](#), which is specified for [DOCSIS](#) cable modems, and [PPPoE](#), which is used by most DSL providers.

Q Can end users operate a virtual private network (VPN) application behind the [VT2400/VT2500](#)?

- A** Yes. The [VT2400/VT2500 Voice Gateway](#) supports [IPSEC](#) and [PPTP](#), the most common VPN protocols.

Q Can the end user play online games through their [VT2400/VT2500](#)?

- A** By default, the [VT2400/VT2500 Voice Gateway](#) blocks all unsolicited messages to the computer or end-user network as a standard security measure. However, for online games that require some unsolicited messages to be transmitted through the [VT2400/VT2500](#), the end user can specify ports and IP addresses on which to allow unsolicited messages. The [VT2400/VT2500 Voice Gateway](#) enables the end user to set up virtual servers or a [DMZ](#).

Q How does the end user configure the [VT2400/VT2500](#)?

- A** *Most end users who perform the appropriate installation procedure in “[Connecting the VT2400/VT2500 to a Network](#)” can send and receive calls immediately!* Configuring your home or office network is done through a GUI where configuration options are selected using a connected PC configured to use DHCP to obtain its network IP address (see “[Gateway > WAN — DHCP Client](#)” on page 34). Or, the user can configure the computer statically to 192.169.102.xxx (xxx is from 2 to 254), subnet 255.255.255.0, and default gateway 192.168.102.1 (see “[Gateway > WAN — Static](#)” on page 36). Or, the user can configure a DSL connection by using the PPPoE Client configuration method (see “[Gateway > WAN — PPPoE Client](#)” on page 35).

Q What is included with the built-in Ethernet router and wireless access point?

- A** The [VT2400/VT2500 Voice Gateway](#) supports a firewall, RIP, parental control, port triggers, advanced ALGs such as RSVP, POP3, **SNMP**, and streaming media. No separate routers or wireless access points are needed.

Q Is any Quality of Service (QoS) implemented on the [VT2400/VT2500 Voice Gateway](#)?

- A** Although VoIP service is typically best-effort, the [VT2400/VT2500](#) provides upstream voice prioritization to ensure that upstream voice data has priority over other Web data. This ensures good voice quality even during heavy upstream data transfers, such as e-mail synchronization or file sharing.



Q What voice protocols and CODECs does the [VT2400/VT2500 Voice Gateway](#) support?

A Refer to [“Supported VoIP Protocols, Codecs, and Calling Features”](#) on page 1.

Specifications

General

WAN and PC interfaces	1 WAN 10/100BASE-T 4 PC/LAN 10/100BASE-T
Data protocol	TCP/IP
Dimensions	1.6" inch (H) x 5.5" inch (W) x 6.5" (L)
Input power	12 VDC

Telephony

Phone lines	Two RJ-11 ports for one or two analog telephones
Fax support	T.38 fax and g.711 fax send-and-receive Adaptive jitter buffer Optional PSTN failover
Services	Call waiting, caller ID, call blocking, 3-way conference calling, call forwarding, etc.
Codecs supported	g.711 (A-law and  -law), g.726, g.726 (reverse nibble), g.729ab, g.729e, g.723.1, g.728
Maximum line length (one-way)	 1000 ft. (maximum)

Wireless ()

CPE wireless interface	802.11b/g; WiFi certified
Quality of service	802.11e WMM/WME for wireless QOS

Routing

CPE network interface	Ethernet 10/100Base-T NAPT, DMZ, port forwarding, VPN pass-through
Security	Firewall with stateful packet inspection, Dynamic port triggers, parental controls
Session initiation protocol	SIP RFC 2543/3261 compatibility; extensive support for SIP methods and extensions STUN, TURN, and outbound proxy support for NAT traversal
IP addressing	DHCP, static IP, or PPPoE

Electrical

Input voltage range	100 – 240 VAC, 50 – 60 Hz
Power consumption	9 watts (nominal)

Environmental

Operating temperature	32° to 113° F (0° to 40° C)
Storage temperature	–40° to 149° F (–40° to 65° C)
Operating humidity	5% to 95% R.H. (non-condensing) 32° to 95° F (0° to 35° C)



Storage humidity 95% R.H.

Antennas

LED Indicators

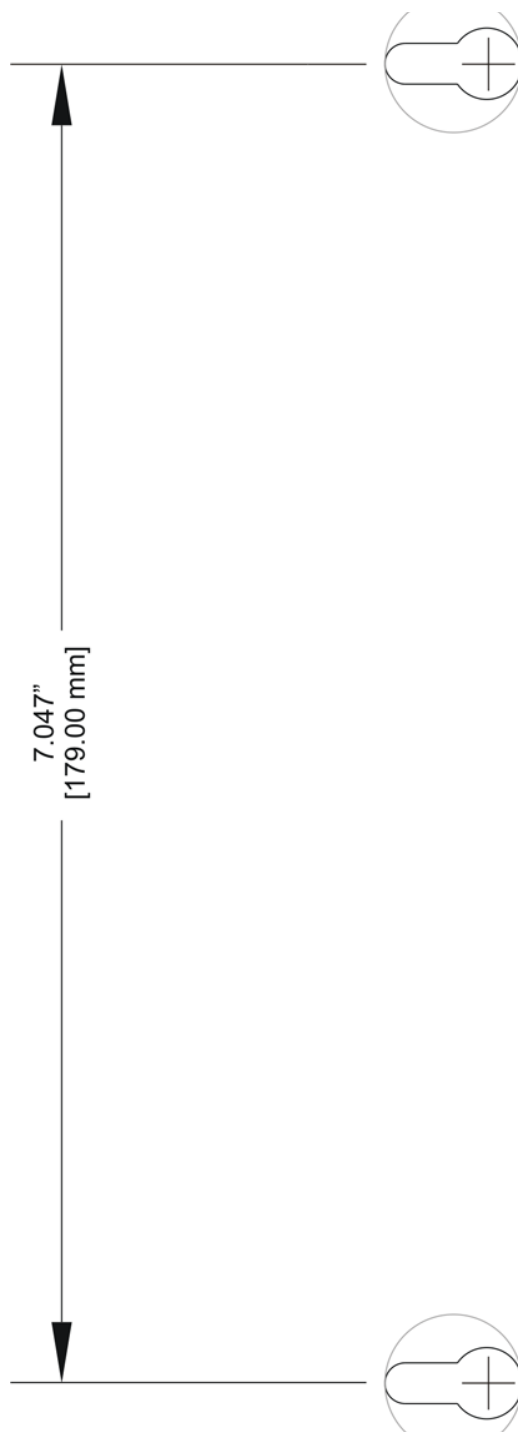
Physical Dimensions

width

height

Wall Mounting Template

Print out the template below to perform the wall mounting procedure in section 2.



Glossary

This glossary defines terms and lists acronyms used with the [VT2400/VT2500 Voice Gateway](#).

To return to your previous page, click the Acrobat Go to Previous View  button.

A

access point	A device that provides WLAN connectivity to wireless clients (stations). The VT2500 acts as a wireless access point.
adapter	A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A <i>wireless adapter</i> connects a computer to the WLAN.
address translation	See <i>NAT</i> .
ALG	Application level gateway triggers are required by some file transfer (for example, FTP), game, and video conferencing applications to open one or more ports to enable the application to operate properly.
American Wire Gauge (AWG)	A standard system used to designate the size of electrical conductors; gauge numbers are inverse to size.
ANSI	The American National Standards Institute is a non-profit, independent organization supported by trade organizations, industry, and professional societies for standards development in the United States. This organization defined ASCII and represents the United States to the International Organization for Standardization.
ANX	Automotive Network Exchange
ARP	Address Resolution Protocol broadcasts a datagram to obtain a response containing a MAC address corresponding to the host IP address. When it is first connected to the network, a client sends an ARP message. The VT2500 responds with a message containing its MAC address. Subsequently, data sent by the computer uses the VT2500 MAC address as its destination.
ASCII	The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.
asynchronous timing	The VT2500 uses synchronous timing for upstream data transmissions. The CMTS broadcasts messages that bandwidth is available. The VT2500 reserves data bytes requiring x-number of mini-slots. The CMTS replies that it can receive data at a specified time (synchronized). At the specified time, the VT2500 transmits the x-number of data bytes.
attenuation	The difference between transmitted and received power resulting from loss through equipment, transmission lines, or other devices; usually expressed in decibels.
authentication	A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.
authorization	Part of the process between a CMTS and the cable modem or gateway to enable Baseline Privacy.
auto-MDIX	Automatic medium-dependent interface crossover detects and corrects cabling errors by automatically reversing the send and receive pins on any port. It enables the use of straight-through wiring between the VT2500 Ethernet port and any computer, printer, or hub.

B To return to your previous page, click the Acrobat Go to Previous View  button.

bandwidth	The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.
Baseline Privacy	An optional feature that encrypts data between the CMTS and the cable modem or gateway. Protection of service is provided by ensuring that a cable modem or gateway, uniquely identified by its MAC address, can only obtain keys for services it is authorized to access.
baud	The analog signaling rate. For complex modulation modes, the digital bit rate is encoded in multiple bits per baud; for example, 64 QAM encodes 6 bits per baud and 16 QAM encodes 4 bits per baud.
BCP	Binary Communication Protocol
BER	The bit error rate is the ratio of the number of erroneous bits or characters received from some fixed number of bits transmitted.
binary	A numbering system that uses two digits, 0 and 1.
bit rate	The number of bits (digital 0s and 1s) transmitted per second in a communications channel. It is usually measured in bits per second bps.
BPKM	Baseline Protocol Key Management encrypts data flows between a cable modem or gateway and the CMTS. The encryption occurs after the cable modem or gateway registers to ensure data privacy across the RF network.
bps	bits per second
bridge	An OSI layer 2 networking device that connects two LANs using similar protocols. It filters frames based on the MAC address to reduce the amount of traffic. A bridge can be placed between two groups of hosts that communicate a lot together, but not so much with the hosts in the other group. The bridge examines the destination of each packet to determine whether to transmit it to the other side. See also <i>switch</i> .
broadband	High bandwidth network technology that multiplexes multiple, independent carriers to carry voice, video, data, and other interactive services over a single cable. A communications medium that can transmit a relatively large amount of data in a given time period. A frequently used synonym for cable TV that can describe any technology capable of delivering multiple channels and services.
broadband Internet provider	A company that provides high-speed cable data or DSL service.
BTI	Broadband telephony interface. See MTA and S-MTA .
broadcast	Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing. See also <i>multicast</i> and <i>unicast</i> .

C To return to your previous page, click the Acrobat Go to Previous View  button.

CableHome	A project of CableLabs and technology suppliers to develop interface specifications for extending high-quality cable-based services to home network devices. It addresses issues such as device interoperability, QoS, and network management. CableHome will enable cable service providers to offer more services over HFC. It will improve consumer convenience by providing cable-delivered services throughout the home.
CableLabs	A research consortium that defines the interface requirements for cable modems and acknowledges that tested equipment complies with DOCSIS.
cable modem	A device installed at a subscriber location to provide data communications over an HFC network. Unless otherwise specified, all references to "cable modem" in this documentation refers to DOCSIS or Euro-DOCSIS cable modems <i>only</i> .
cable modem configuration file	File containing operational parameters that a cable modem or gateway downloads from the cable provider's TFTP server during registration.
circuit-switched	Network-connection scheme used in the traditional PSTN telephone network where each connection requires a dedicated path for its duration. An alternative is packet-switched.
CLASS	Customer Local Area Signaling Service. One of an identified group of network-provided enhanced services. A CLASS group for a given network usually includes several enhanced service offerings, such as incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls.
Class C network	An IP network containing up to 253 hosts. Class C IP addresses are in the form "network.network.network.host."
client	In a client/server architecture, a client is a computer that requests files or services such as file transfer, remote login, or printing from the server. Also called a CPE. On a WLAN, a client is any host that can communicate with the access point. A wireless client is also called a "station."
CMTS	A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connecting IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.
CNR	carrier to noise ratio
coaxial cable (coax)	A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.
CODEC	COmpression/DECompression. A software-only or a hardware-assisted scheme that is used to process digital video or audio files. The amount of data required to represent moving pictures with sound is reduced by a CODEC, which normally discards redundant data on compression.
CoS	Class of service traffic management or scheduling functions are performed when transferring data upstream or downstream on HFC.
CPE	Customer premise equipment, typically computers, printers, etc., are connected to the cable modem or gateway at the subscriber location. CPE can be provided by the subscriber or the cable provider. Also called a client.
crosstalk	Undesired signal interfering with the desired signal.
CSMA/CD	carrier sense multiple access with collision detection

D To return to your previous page, click the Acrobat Go to Previous View  button.

datagram	In RFC 1594, a datagram is defined as “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” For the most part, it has been replaced by the term packet.
default route	The route by which packets are forwarded when other routes in the routing table do not apply.
dB	decibel
dBc	Signal level expressed in dB relative to the unmodulated carrier level desired.
DBm	A unit of measurement referenced to one milliwatt across specified impedance. 0dBm = 1 milliwatt across 75 ohms.
dBmV	Signal level expressed in dB as the ratio of the signal power in a 75-ohm system to a reference power when 1 mV is across 75 ohms.
demodulation	An operation to restore a previously modulated wave and separate the multiple signals that were combined and modulated on a subcarrier.
DHCP	A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses. <i>The VT2500 is simultaneously a DHCP client and a DHCP server.</i> • A DHCP server at the cable system headend assigns a public IP address to the VT2500 and optionally to clients on the VT2500 LAN. • The VT2500 contains a built-in DHCP server that assigns private IP addresses to clients.
distortion	An undesired change in signal waveform within a transmission medium. A nonlinear reproduction of the input waveform.
DMZ	A “de-militarized zone” is one or more hosts logically located between a private LAN and the Internet. A DMZ prevents direct access by outside users to private data. (The term comes from the geographic buffers located between some conflicting countries, such as North and South Korea.) In a typical small DMZ configuration, the DMZ host receives requests from private LAN users to access external web sites and initiates sessions for these requests. The DMZ host cannot initiate a session back to the private LAN. Internet users outside the private LAN can access only the DMZ host. You can use a DMZ to set up a web server or for gaming without exposing confidential data.
DNS	The Domain Name System is the Internet system for converting domain names to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.
DOCSIS	The CableLabs Data-Over-Cable Service Interface Specification defines interface standards for cable modems, gateways, and supporting equipment to deliver data between an HFC network and computer systems or television sets. To emphasize its use as a cable modem standard, DOCSIS is now called CableLabs Certified Cable Modems. Euro-DOCSIS is DOCSIS adapted for use in Europe.
domain name	A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses.
dotted-decimal format	Method of representing an IP address or subnet mask using four decimal numbers called octets. Each octet represents eight bits. In a class C IP address, the octets are “network.network.network.host.” The first three octets together represent the network address and the final octet is the host address. In the VT2500 LAN default configuration, 192.168.100 represents the network address. In the final octet, the host address can be from 2 to 254.

download	To copy a file from one computer to another. You can use the Internet to download files from a server to a computer. A DOCSIS or Euro-DOCSIS cable modem or gateway downloads its configuration file from a TFTP server during start-up.
downstream	In a cable data network, the direction of data received by the computer from the Internet.
driver	Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum is an IEEE 802.11b RF modulation protocol.
dynamic IP address	An IP address that is temporarily leased to a host by a DHCP server. The opposite of <i>static IP address</i> .

E To return to your previous page, click the Acrobat Go to Previous View  button.

encapsulate	To include data into some other data unit to hide the format of the included data.
encode	To alter an electronic signal so that only an authorized user can unscramble it to view the information.
encrypt	To encode data.
endpoint	A VPN endpoint terminates the VPN at the router so that computers on the VT2500 LAN do not need VPN client software to tunnel through the Internet to the VPN server.
ESSID	The Extended Service Set Identifier or network name is a unique identifier that wireless clients use to associate with an access point to distinguish between multiple WLANs in the same area. All clients on a WLAN must have the same ESSID as the access point. On the VT2500, you can set the ESSID on the Wireless > NETWORK page.
Ethernet	The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable." Each Ethernet port has a physical address called the MAC address.
Euro-DOCSIS	A tComLabs standard that is DOCSIS adapted for use in Europe
event	A message generated by a device to inform an operator or the network management system that something has occurred.
expansion slot	A connection point in a computer where a circuit board can be inserted to add new capabilities.
EAP	Extensible Authentication Protocol

F To return to your previous page, click the Acrobat Go to Previous View  button.

FCS	frame check sequence
F-type connector	A type of connector used to connect coaxial cable to equipment such as the VT2500.
firewall	A security software system on the VT2500 that enforces an access control policy between the Internet and the VT2500 LAN.
flash	To press the flash button on the telephone, which allows you to retrieve or go between two calls.
flow	A data path moving in one direction.
FEC	Forward error correction is a technique to correct transmission errors without requiring the transmitter to resend any data.
FDMA	Frequency Division Multiple Access is a method to allow multiple users to share a specific radio spectrum. Each active user is assigned an individual RF channel (or carrier) with the carrier frequency of each channel offset from its adjacent channels by an amount equal to the channel spacing, which allows the required bandwidth per channel.
FQDN (Fully Qualified Domain Name)	A fully qualified domain name consists of a host and domain name, including top-level domain. For example, www.motorola.com is a fully qualified domain name. www is the host, motorola is the second-level domain, and .com is the top level domain.
frame	A unit of data transmitted between network nodes that contains addressing and protocol control data. Some control frames contain no data.
frequency	Number of times an electromagnetic signal repeats an identical cycle in a unit of time, usually one second, measured in Hz, kHz, MHz, or GHz.
FTP	File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.
full-duplex	The ability to simultaneously transmit and receive data. See also <i>half-duplex</i> .

G To return to your previous page, click the Acrobat Go to Previous View  button.

gain	The extent to which a signal is boosted. A high gain antenna increases the wireless signal level to increase the distance the signal can travel and remain usable.
gateway	A device that enables communication between networks using different protocols. See also <i>router</i> . The VT2500 enables up to 253 computers supporting IEEE 802.11b, Ethernet, or USB to share a single broadband Internet connection.
gateway IP address	The address of the default gateway router on the Internet. Also known as the “giaddr.”
GHz	Gigahertz — one billion cycles per second.
GUI	graphical user interface

H To return to your previous page, click the Acrobat Go to Previous View  button.

H.323	A suite of protocols created by the ITU for interactive video-conferencing, data sharing, and audio applications such as VoIP.
half-duplex	Network where only one device at a time can transmit data. See also <i>full-duplex</i> .
headend	A location that receives TV programming, radio programming, data, and telephone calls that it modulates onto the HFC network. It also sends return data and telephone transmissions. Headend equipment includes transmitters, preamplifiers, frequency terminals, demodulators, modulators, and other devices that amplify, filter, and convert incoming broadcast TV signals to wireless and cable channels.
header	The data at the beginning of a packet that identifies what is in the packet.
hexadecimal	A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.
HFC	A hybrid fiber/coaxial cable network uses fiber-optic cable as the trunk and coaxial cable to the subscriber premises.
hop	The interval between two routers on an IP network. The number of hops a packet traverses toward its destination (called the hop count) is saved in the packet header. For example, a hop count of six means the packet has traversed six routers. The packet hop count increases as the time-to-live (TTL) value decreases.
host	In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address. Host also can mean: • A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals • A company that provides this service • In IBM environments, a mainframe computer
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol. The client-server TCP/IP used for exchanging HTML documents on the World Wide Web.
hub	On a LAN, a hub is a device that connects multiple hosts to the LAN. A hub performs no data filtering. See also <i>bridge</i> and <i>router</i>. An IP hub is typically a unit on a rack or desktop. On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.
Hz	Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.

I To return to your previous page, click the Acrobat Go to Previous View  button.

IANA	The Internet Numbering Address Authority (IANA) is an organization under the Internet Architecture Board (IAB) of the Internet Society that oversees IP address allocation. It is under a contract from the U.S. government.
ICMP	Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.

ICSA	The International Computer Security Association is the security industry's main source of research, intelligence, and product certification.
IEEE	The Institute of Electrical and Electronics Engineers, Inc. (http://www.ieee.org) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI.
IEEE 802.11b IEEE 802.11g	IEEE wireless network standards.
IEEE 802.3	See <i>Ethernet</i> .
IETF	The Internet Engineering Task Force (http://www.ietf.org) is an open international community of network designers, operators, vendors, and researchers to develop and maintain Internet architecture. Technical working groups issue working documents called Internet-Drafts. The IETF publishes review versions of the drafts called requests for comments (RFCs).
IGMP	Internet Group Membership Protocol — the Internet multicasting standard. IGMP establishes and maintains a database of group multicast addresses and interfaces to which a multicast router forwards multicast packets. IGMP runs between multicast hosts and their immediately-neighboring multicast routers.
IGMP spoofing	A process where a router acts as an IGMP querier for multicast hosts and an IGMP host to a multicast router.
impedance	The total opposition to AC electron current flow within a device. Impedance is typically 75 ohms for coax cable and other CATV components.
impulse noise	Noise of very short duration, typically of the order of 10 microseconds. It is caused by electrical transients such as voltage spikes, electric motors turning on, and lightning or switching equipment that bleed over to the cable.
ingress noise	Noise typically caused by discrete frequencies picked up by the cable plant from radio broadcasts or an improperly grounded or shielded home appliance such as a hair dryer. Ingress is the major source of cable system noise.
Internet	A worldwide collection of interconnected networks using TCP/IP.
Internetwork	A collection of interconnected networks allowing communication between all devices connected to any network in the collection.
IP	Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

To return to your previous page, click the Acrobat Go to Previous View  button.

IP address	A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address. An IP address has two parts: • The network address is assigned by IANA. • The VT2500 network administrator assigns a host address to each host connected to the VT2500, automatically using its DHCP server as a static IP address. For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format, it appears "network.network.network.host." If you enable the VT2500 DHCP client on the WAN page, the cable provider automatically assigns the network address, subnet mask, domain name, and DNS server to provide a continuous Internet connection.
IPSec	The Internet Protocol Security protocols are IETF authentication and encryption standards for secure packet exchange over the Internet. IPSec works at OSI layer 3 and secures everything on the network.



IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	The International Organization for Standardization (http://www.iso.ch) is a worldwide federation of national standards bodies from approximately 140 countries. ISO is a non-governmental organization established in 1947 to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity.
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider. A company that provides VoIP telephone service. It may be the same as or different from the end-user broadband Internet provider. Also referred to as a "VoIP provider" or "voice provider."
ITU	International Telecommunications Union

KTo return to your previous page, click the Acrobat Go to Previous View  button.

kHz kilohertz — one thousand cycles per second

L To return to your previous page, click the Acrobat Go to Previous View  button.

L2F	Layer 2 Forwarding is an OSI layer 2 protocol that establishes a secure tunnel across the Internet to create a virtual PPP connection between the user and the enterprise network. L2F is the most established and stable layer 2 tunneling protocol.
L2TP	Layer 2 Tunnel Protocol is a PPP extension that enables ISPs to operate VPNs. L2TP merges the best features of the PPTP and L2F. L2TP is the emerging IETF standard.
LAC	An L2TP access concentrator is a device to which the client directly connects through which PPP frames are tunneled to the LNS. The LAC need only implement the media over which L2TP operates to transmit traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F NAS.
LAN	A local area network provides a full-time, high-bandwidth connection over a limited area, such as a building or campus. Ethernet is the most widely used LAN standard.
layer	In networks, layers are software protocol levels. Each layer performs functions for the layers above it. OSI is a reference model having seven functional layers.
LCP	Link Control Protocol establishes, configures, and tests data link connections used by PPP.
latency	The time required for a signal to pass through a device. It is often expressed in a quantity of symbols.
LED	light-emitting diode
LNS	An L2TP network server is a termination point for L2TP tunnels where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS can have a single LAN or WAN interface but can terminate calls arriving at any of the LACs full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.
loopback	A test that loops the transmit signal to the receive signal. Usually the loopback test is initiated on a network device. The test is used to verify a path or to measure the quality of a signal on that path.

M To return to your previous page, click the Acrobat Go to Previous View  button.

MAC address	The Media Access Control address is a unique, 48-bit value permanently saved in ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on the bottom of the VT2400 or VT2500. You need to provide the HFC MAC address to the cable provider. Also called an Ethernet address, physical address, hardware address, or NIC address.
MB	One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.
Mbps	Million bits per second (megabits per second). A rate of data transfer.
media	The various physical environments through which signals pass; for example, coaxial, unshielded twisted-pair (UTP), or fiber-optic cable.
MIB	A management information base is a unique hierarchical structure of software objects used by the SNMP manager and agent to configure, monitor, or test a device.
MHz	Megahertz — one million cycles per second. A measure of radio frequency.
MPDU	MAC protocol data unit (PDU)
MSDU	MAC service data unit
MSO	Multiple Systems Operator. A company that owns and operates more than one cable system. Also called a group operator.
MTA	Multimedia Terminal Adapter. See S-MTA .
MTU	The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission, and reassembled at the destination.
multicast	A data transmission sent from one sender to multiple receivers. See also <i>broadcast</i> and <i>unicast</i> .
mW	milliwatts

N To return to your previous page, click the Acrobat Go to Previous View  button.

NAS	network access server
NAT	Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. NAT provides some security because the IP addresses of VT2500 LAN computers are invisible on the Internet. If NAT is enabled on the Gateway page, there is a one-to-one mapping between each public IP address and client IP address.
NAPT	Network Address Port Translation is the most common form of address translation between public and private IP addresses. NAPT is a mapping of one public IP address to many private IP addresses. If NAPT is enabled on the Gateway page, one public IP address is mapped to an individual private IP address for up to 245 LAN clients.
NEC	National Electrical Code (in the United States) are the regulations for construction and installation of electrical wiring and apparatus, suitable for mandatory application by a wide range of state and local authorities.
network	Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.
network driver	Software packaged with a NIC that enables the computer to communicate with the NIC.



network layer	Layer 3 in the OSI architecture that provides services to establish a path between open systems. The network layer knows the address of the neighboring nodes, packages output with the correct network address data, selects routes, and recognizes and forwards to the transport layer incoming messages for local host domains.
NIC	A network interface card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.
node	On a LAN, a generic term for any network device. On an HFC network, the interface between the fiber-optic trunk and coaxial cable feeders to subscriber locations. A node is typically located in the subscriber neighborhood.
noise	Random spurts of electrical energy or interface. May produce a salt-and-pepper pattern on a television picture.

O To return to your previous page, click the Acrobat Go to Previous View  button.

ohm	A unit of electrical resistance.
OOB DTMF	Out-of-band dual tone multi-frequency signals are generated when you press the keys of an ordinary telephone. In the United States, it is referred to as a "touch-tone" phone (formerly a registered trademark of AT&T).
OSI	The Open Systems Interconnection reference model is an illustrative model describing how data moves from an application on the source host through a network to an application on the destination host. It is a conceptual framework developed by ISO that is now the primary model for intercomputer communications. OSI is a model <i>only</i> ; it does not define a specific networking interface.

P To return to your previous page, click the Acrobat Go to Previous View  button.

packet	The unit of data that is routed between the sender and destination on the Internet or other packet-switched network. When data such as an e-mail message or other file is sent over the Internet, IP on the sender divides the data into uniquely-numbered packets. The packet header contains the source and destination IP addresses. The individual packets may travel different routes. When all packets arrive at the destination, IP at that end reassembles the packets. The header and the data can vary in length. Packet and datagram are similar in meaning.
packet-switched	A scheme to handle transmissions on a connectionless network such as the Internet. An alternative is circuit-switched.
PacketCable	A CableLabs-led project to define a common platform to deliver advanced real-time multimedia services over two-way HFC cable plant. Built on DOCSIS 1.1, PacketCable networks use IP technology as the basis for a highly-capable multimedia architecture.
pass-through	A pass-through client on the VT2500 LAN obtains its public IP address from the cable provider DHCP server.
PAT	Port Address Translation
PCI	
PCMCIA	The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet connectivity.
PDA	personal desktop assistant
PDU	A protocol data unit is a message containing operational instructions used for SNMP. The basic SNMP V2 PDU types are get-request, get-next-request, get-bulk-request, response, set-request, inform-request, and trap.
Peer-to-peer network	A network in which each computer is independent and can serve the others or act as a workstation. Peripherals connected to any computer networked in this fashion are available to any of the other peer computers connected.
periodic ranging	Ranging that is performed on an on-going basis after initial ranging has taken place.
physical layer	Layer 1 in the OSI architecture. It provides services to transmit bits or groups of bits over a transmission link between open systems. It entails the electrical, mechanical, and handshaking procedures.
piggybacking	A process that occurs when a cable modem simultaneously transmits data and requests additional bandwidth.
PING	A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for "Packet InterNet Groper."
PMD	The physical media-dependent sublayer of the physical layer which transmits bits or groups of bits over particular types of transmission links between open systems. It entails the electrical, mechanical, and handshaking procedures.
point-to-point	Physical connection made from one point to another.
POTS	The "plain old telephone service" offered through the PSTN; basic analog telephone service. POTS uses the lowest 4 kHz of bandwidth on twisted pair wiring.
port	On a computer or other electronic device, a port is a socket or plug used to physically connect it to the network or to other devices. in TCP/IP, a port is a number from 0 to 65536 used logically by a client program to specify a server program. Ports 0 to 1024 are reserved.

port mirroring	A feature that enables one port (source) on the VT2500 to be copied to another port (destination) to be studied. The destination mirrors the transmitted (from) or received (to) data on the source port to enable the person managing the network to monitor activity.
port triggering	A mechanism that allows incoming communication with specified applications. Primarily used for gaming applications.
PPP	Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.
PPPoE	Point-to-Point Protocol over Ethernet. A specification for connecting to the Internet with DSL modems.
PPTP	Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.
private IP address	An IP address assigned to a computer on the VT2500 LAN by the DHCP server on the VT2500 for a specified lease time. Private IP addresses are used by the VT2500 LAN only; they are invisible to devices on the Internet. See also <i>public IP address</i> .
protocol	A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.
provisioning	The process of autodiscovery or manually configuring a cable modem on the CMTS.
PSTN	The public switched telephone network is the traditional circuit-switched, voice-oriented telephone network. See also <i>POTS</i> .
public IP address	The IP address assigned to the VT2500 by the cable provider. A public IP address is visible to devices on the Internet. See also <i>private IP address</i> .

Q To return to your previous page, click the Acrobat Go to Previous View  button.

QAM	Quadrature Amplitude Modulation uses amplitude and phase modulation to encode multiple bits of data in one signaling element. QAM achieves faster data transfer than amplitude or phase modulation alone, but the signal is more prone to errors caused by noise. QAM requires a transmission circuit with a higher CNR than alternate modulation formats such as QPSK. Two types of QAM are: • 16 QAM encodes four bits per symbol as one of 16 possible amplitude and phase combinations. • 64 QAM encodes six bits per symbol as one of 64 possible amplitude and phase combinations.
QPSK	Quadrature Phase Shift Key (QPSK) modulation sends two bits of information per symbol period with one symbol 90 degrees out of phase with other symbols. The four constellation points represented by the coordinates (0,0 - 0,1 - 1,0 - 1,1) represent the four possible combinations.
QoS	Quality of service describes the priority, delay, throughput, and bandwidth of a connection.

R To return to your previous page, click the Acrobat Go to Previous View  button.

RADIUS	Remote Authentication Dial-In User Service server typically used in large corporate settings.
RAS	Remote Access Server
registration	How a cable modem makes itself known to the CMTS. The cable modem configuration file and authorization are verified and the CoS is negotiated.
return loss	A measurement of the quality of the match of the device to the cable system. Return loss is the ratio of the amount of power reflected by the device. A return loss of 20 dB or greater is preferred.
RF	Radio Frequency — signals used by the CMTS transmitter and receiver to send data over HFC. The carrier is modulated to encode the digital data stream for transmission across the cable network.
RFC	Request for Comments published on the IETF or other websites. Many RFCs become international standards.
RJ-11	The most common type of connector for household or office phones.
RJ-45	An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.
ROM	read-only memory
router	On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a <i>gateway</i> between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them. A router is often included as part of a network switch. A router can also be implemented as software on a computer.
routing table	A table listing available routes that is used by a router to determine the best route for a packet.
RTP	A protocol that enables real-time data, such as voice traffic, to be carried in packets over the Internet.
RTCP	A protocol for monitoring RTP performance.
RTS	request to send

S To return to your previous page, click the Acrobat Go to Previous View  button.

server	In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients.
scope	The set of IP addresses that a DHCP server can lease to clients.
service provider	A company providing cable data services to subscribers.
SDP	A protocol that describes multimedia sessions for the purpose of session announcement, session invitation, and other forms of multimedia initiation.
SDU	service data unit
SID	A service ID is a unique 14-bit identifier the CMTS assigns to a cable modem or gateway that identifies the traffic type it carries (for example, data or voice). The SID provides the basis for the CMTS to allocate bandwidth to the cable modem and implement CoS.
SIP	Session Initiation Protocol. SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Such sessions include voice, video, chat, interactive games, and virtual reality.
SME	small and medium enterprise
S-MTA	Stand-Alone Multiservice Terminal Adapter. A device that converts analog voice signals to and from a standard telephone to digital data that can be transmitted through a broadband connection over the Internet. An SMTA is typically connected through Ethernet.
SMTP	Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.
SNMP	Simple Network Management Protocol is a standard to monitor and manage networks and network devices. Data is exchanged using PDU messages.
SOHO	small office home office
spectrum	A specified range of frequencies used for transmission of electromagnetic signals.
spectrum allocation	An allocation of portions of the available electromagnetic spectrum for specific services, such as AM, FM, or personal communications.
splitter	A device that divides the signal from an input cable between two or more cables.
stateful inspection	A type of firewall that tracks each connection traversing all firewall interfaces to ensure validity. In addition to examining the source and destination in the packet header based on static rules, a stateful inspection firewall: • Examines packet headers on context established by previous packets that traversed the firewall • Monitors the connection state and saves it in a table • Closes ports until a connection to a specific port is requested • May examine the packet contents up through the application layer to determine more than just the source and destination A stateful-inspection firewall is more advanced than a static filter firewall.
static filter	A type of firewall that examines the source and destination in the packet header based on administrator-defined rules <i>only</i> .
static IP address	An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of dynamic IP address.
static route	A manually-defined route.
station	IEEE 802.11b term for wireless client.
STUN	Simple Traversal of UDP through NAT - an intrusion detection system which inspects all inbound and outbound network activity.



subscriber	A home or office user who accesses television, data, or other services from a cable provider.
subnet mask	A bit mask that is logically ANDed with the destination IP address of a packet to determine the network address. A router routes packets using the network address.
subnetwork	A part of a network; commonly abbreviated "subnet." When subnetting is used, the host portion of the IP address is divided into a subnet and host number. Hosts and routers use the subnet mask to identify the bits used for the network and subnet number.
switch	On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.
symbol rate	Also known as baud rate, is a measure of the number of times per second a signal in a communications channel varies, or makes a transition between states (states being frequencies, voltage levels or phase angles). Usually measured in symbols per second (sps).
SYSLOG	A de-facto UNIX standard for logging system events.

T To return to your previous page, click the Acrobat Go to Previous View  button.

TBCP	Tagged Binary Communication Protocol
TCP	Transmission Control Protocol on OSI transport layer four, provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.
TCP/IP	The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide internetworking standard and the basic communications protocol of the Internet.
Telnet	The Internet standard protocol for remote terminal connection service. Telnet allows a user at one site to interact with a system at another site as if the user's terminal were directly connected to the host computer.
TFTP	Trivial File Transfer Protocol is a very simple protocol used to transfer files.
THDD	Telephony Hardware Device Driver.
TKIP	Temporal Key Integrity Protocol
transparent bridging	A method to enable all hosts on the wired Ethernet LAN, WLAN, and USB connection to communicate as if they were all connected to the same physical network.
transport layer	Layer of the OSI concerned with protocols for error recognition and recovery. This layer also regulates information flow.
trunk	Electronic path over which data is transmitted.
TTL	The time to live is the number of routers (or hops) a packet can traverse before being discarded. When a router processes a packet, it decreases the TTL by 1. When the TTL reaches zero, the packet is discarded.
tunnel	To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network. Tunneling requires the following protocol types: • A carrier protocol, such as TCP, used by the network over which the data travels • An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data • A passenger protocol, such as IP, for the original data
two-way	A cable system that can transmit signals in both directions to and from the headend and the subscriber.

U-Z To return to your previous page, click the Acrobat Go to Previous View  button.

UDP	User Datagram Protocol
unicast	A point-to-point data transmission sent from one sender to one receiver. This the normal way you access websites. See also <i>broadcast</i> and <i>multicast</i> .
upstream	In a cable data network, upstream describes the direction of data sent from the subscriber computer through the cable modem to the CMTS and the Internet.
USB	Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port.
UTP	unshielded twisted pair (wire)
VCM	In a telecommunications connection, the segment of the bandwidth allocated to transmitting voice messages.
VLAN	A virtual local area network is group of devices on different LAN segments that are logically configured to communicate as if they are connected to the same wire.
VoIP	Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.
VoIP Provider	A company that provides voice-over internet protocol telephone service.
VPN	A virtual private network is a private network that uses “virtual” connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.
WAN	A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.
WAP	Wireless access point or Wireless Access Protocol. See also <i>access point</i> .
WECA	The Wireless Ethernet Compatibility Alliance is a trade organization that works to ensure that all wireless devices — computer cards, laptops, air routers, PDAs, etc — can communicate with each other.
WEP	Wired Equivalent Privacy encryption protects the privacy of data transmitted over a WLAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b. <i>Because WEP can be difficult to use and does not provide very strong encryption, we recommend using WPA if possible.</i>
WiFi	Wireless fidelity (pronounced y-phi) brand name applied to products supporting IEEE 802.11b.
Wireless Access Point (WAP)	A device that provides network connectivity to one or more client computers using radio signals over a wireless connection.
Wireless Cable Modem Gateway	A single device, such as the SBG9000, that combines a cable modem, router, Ethernet switch, wireless access point, and DHCP server for SOHO or SME use.
Wireless Voice Gateway	A single device, such as the VT2500, that provides two telephone lines for voice-over-data, a built-in wireless access point and router, and connection to a modem.
WLAN	wireless LAN



world wide web An interface to the Internet that you use to navigate and hyperlink to information.

WPA Wi-Fi Protected Access (WPA) encryption, as described on the Wi-Fi Alliance [Wi-Fi Protected Access](http://www.wifialliance.org/OpenSection/protected_access.asp) web page http://www.wifialliance.org/OpenSection/protected_access.asp. It is a far more robust form of encryption than WEP. *We recommend using WPA if all of your client hardware supports WPA.*

Software License

SOFTWARE LICENSE

Motorola, Inc., [Connected Home Solutions](#) ("Motorola") 101 Tournament Drive, Horsham, PA 19044

IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE ("LICENSE") CAREFULLY BEFORE YOU INSTALL, DOWNLOAD OR USE ANY APPLICATION SOFTWARE, USB DRIVER SOFTWARE, FIRMWARE AND RELATED DOCUMENTATION ("SOFTWARE") PROVIDED WITH MOTOROLA'S VOICE GATEWAY PRODUCT (THE "VOICE GATEWAY PRODUCT"). BY USING THE VOICE GATEWAY PRODUCT AND/OR INSTALLING, DOWNLOADING OR USING ANY OF THE SOFTWARE, YOU INDICATE YOUR ACCEPTANCE OF EACH OF THE TERMS OF THIS LICENSE. UPON ACCEPTANCE, THIS LICENSE WILL BE A LEGALLY BINDING AGREEMENT BETWEEN YOU AND MOTOROLA. THE TERMS OF THIS LICENSE APPLY TO YOU AND TO ANY SUBSEQUENT USER OF THIS SOFTWARE.

IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE (I) DO NOT INSTALL OR USE THE SOFTWARE AND (II) RETURN THE VOICE GATEWAY PRODUCT AND THE SOFTWARE (COLLECTIVELY, "PRODUCT"), INCLUDING ALL COMPONENTS, DOCUMENTATION AND ANY OTHER MATERIALS PROVIDED WITH THE PRODUCT, TO YOUR POINT OF PURCHASE OR SERVICE PROVIDER, AS THE CASE MAY BE, FOR A FULL REFUND.

The Software includes associated media, any printed materials, and any "online" or electronic documentation, as well as any updates, revisions, bug fixes, or drivers obtained by you from Motorola or your service provider. Software provided by 3rd parties may be subject to separate end-user license agreements from the manufacturers of such Software.

The Software is never sold. Motorola licenses the Software to the original customer and to any subsequent licensee for personal use only on the terms of this License. Motorola and its 3rd party licensors retain the ownership of the Software.

You may:

USE the Software only in connection with the operation of the Product.

TRANSFER the Software (including all component parts and printed materials) permanently to another person, but only if the person agrees to accept all of the terms of this License. If you transfer the Software, you must at the same time transfer the Product and all copies of the Software (if applicable) to the same person or destroy any copies not transferred.

TERMINATE this License by destroying the original and all copies of the Software (if applicable) in whatever form.

You may not:

(1) Loan, distribute, rent, lease, give, sublicense or otherwise transfer the Software, in whole or in part, to any other person, except as permitted under the TRANSFER paragraph above. (2) Copy or translate the User Guide included with the Software, other than for personal use. (3) Copy, alter, translate, decompile, disassemble or reverse engineer the Software, including but not limited to, modifying the Software to make it operate on non-compatible hardware. (4) Remove, alter or cause not to be displayed, any copyright notices or startup message contained in the Software programs or documentation. (5) Export the Software or the Product components in violation of any United States export laws.

The Product is not designed or intended for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; or in design, construction, operation or maintenance of any nuclear facility. MOTOROLA AND ITS 3rd PARTY LICENSORS DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH USES. YOU REPRESENT AND WARRANT THAT YOU SHALL NOT USE THE PRODUCT FOR SUCH PURPOSES.

Title to this Software, including the ownership of all copyrights, mask work rights, patents, trademarks and all other intellectual property rights subsisting in the foregoing, and all adaptations to and modifications of the foregoing shall at all times remain with Motorola and its 3rd party licensors. Motorola retains all rights not expressly licensed under this License. The Software, including any images, graphics, photographs, animation, video, audio, music and text incorporated therein is owned by Motorola or its 3rd party licensors and is protected by United States copyright laws and international treaty provisions. Except as otherwise expressly provided in this License, the copying, reproduction, distribution or preparation of derivative works of the Software, any portion of the Product or the documentation is strictly prohibited by such laws and treaty provisions. Nothing in this License constitutes a waiver of Motorola's rights under United States copyright law.



This License and your rights regarding any matter it addresses are governed by the laws of the Commonwealth of Pennsylvania, without reference to conflict of laws principles. THIS LICENSE SHALL TERMINATE AUTOMATICALLY if you fail to comply with the terms of this License.

Motorola is not responsible for any 3rd party software provided as a bundled application, or otherwise, with the Software.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Product and documentation is provided with RESTRICTED RIGHTS. The use, duplication or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at 52.227-7013. The contractor/manufacturer is Motorola, Inc., [Connected Home Solutions](#), 101 Tournament Drive, Horsham, PA 19044.

Visit our website at:
www.motorola.com



521569-001
7/05
MGBI