



CABLE

SATELLITE

TELECOM

TERRESTRIAL

TWG850 - Residential Voice Gateway

User manual

Important Information

CAUTION

Disconnect power before servicing.

This device is intended for indoor operation only. Telephone jacks Line 1 and Line 2 must not be connected to outside wiring.

CAUTION

To ensure reliable operation and to prevent overheating, provide adequate ventilation for this modem and keep it away from heat sources. Do not locate near heat registers or other heat-producing equipment. Provide for free air flow around the Residential Voice Gateway and its power supply.



This symbol means that your inoperative electronic appliance must be collected separately and not mixed with the household waste. The European Union has implemented a specific collection and recycling system for which producers' are responsible.

This appliance has been designed and manufactured with high quality materials and components that can be recycled and reused. Electrical and electronic appliances are liable to contain parts that are necessary in order for the system to work properly but which can become a health and environmental hazard if they are not handled or disposed of in the proper way. Consequently, please do not throw out your inoperative appliance with the household waste.

If you are the owner of the appliance, you must deposit it at the appropriate local collection point or leave it with the vendor when buying a new appliance.

- If you are a professional user, please follow your supplier's instructions.

- If the appliance is rented to you or left in your care, please contact your service provider.

Help us protect the environment in which we live !

NORTH AMERICAN CABLE INSTALLER:

This reminder is provided to call your attention to Article 820-40 of the National Electrical Code (Section 54 of the Canadian Electrical Code, Part 1) which provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building as close to the point of cable entry as practical.

Euro-PacketCable, Euro-DOCSIS, and DOCSIS compliant

This product was designed according to Euro-PacketCable Specification, Euro-DOCSIS Specifications and Data over Cable Service Interface Specifications.

Operating Information

Operating Temperature: 0 ° - 40 ° C (32 ° - 104 ° F)

Storage Temperature: -20 ° to 70 ° C (-4°F to 158°F)

If you purchased this product at a retail outlet, please read the following:

Product Information

Keep your sales receipt to obtain warranty parts and service and for proof of purchase. Attach it here and record the serial and model numbers in case you need them. The numbers are located on the back of the product.

Model No. _____ Serial No _____

Purchase Date: _____ Dealer/Address/Phone: _____

Table of Contents

Chapter 1: Connections and Setup	1
Introduction	1
Residential Voice Gateway Features	1
What's on the CD-ROM	1
Computer Requirements.....	3
Wall Mounting	4
Residential Voice Gateway TWG850 Overview.....	5
Front Panel.....	5
Rear Panel	6
Relationship among the Devices	7
What the Modem Does	7
What the Modem Needs to Do Its Job.....	7
Contact Your Local Cable Company	8
Connecting the Residential Voice Gateway to a Single Computer.....	10
Attaching the Cable TV Wire to the Residential Voice Gateway	10
Important Connection Information	11
USB Connection to One Computer	11
USB Connection.....	13
Using Windows 2000 for USB Connection	13
Using Windows Me for USB Connection.....	17
Using Windows XP for USB Connection	18
Ethernet Connection to One Computer	20
Connecting More Than Two Computers to the Residential Voice Gateway.....	21
Telephone or Fax Connection	22
Activating the Residential Voice Gateway	23

Chapter 2: Web Configuration.....	24
Accessing the Web Configuration.....	24
Outline of Web Manager	25
Gateway – Status Web Page Group	26
Software.....	26
Connection.....	27
Password.....	27
Diagnostics	28
Event Log	29
Initial Scan	29
Gateway – Network Web Page Group	30
LAN.....	30
WAN.....	31
Computers	31
Gateway – Advanced Web Page Group.....	32
Options	32
IP Filtering.....	33
MAC Filtering	33
Port Filtering	34
Forwarding.....	35
Port Triggers	36
RIP (Routing Information Protocol) Setup	37
Gateway – Firewall Web Page Group	38
Web Content Filtering.....	38
TOD Filtering.....	39
Local Log and Remote Log.....	40

Gateway – Parental Control Web Page Group	41
Basic	41
Gateway – Wireless Web Page Group	42
802.11b/g Basic.....	43
802.11b/g Security	45
Access Control	48
802.11b/g Advanced.....	49
Bridging	51
Guest Network	52
VoIP – Basic Web Page Group	53
Basic LAN	53
Hardware Info	53
Event Log	54
CM State	54
Chapter 3: Additional Information	55
Frequently Asked Questions	55
General Troubleshooting	57
FCC Declaration of Conformity and Industry Canada Information.....	59
Service Information.....	60
Glossary	61

Chapter 1: Connections and Setup

Introduction

Residential Voice Gateway Features

- Support Multiple Provisioning Mode
- Standard RJ-45 connector for 10/100BaseT Ethernet with auto-negotiation and MDIS functions
- USB Connector for USB interface
- Two RJ-11 Foreign Exchange Station (FXS) ports for IP telephony
- Support simultaneous voice and data communications
- Two simultaneous voice conversations in the different FXS ports with different CODEC: PCM A-law, PCM-law, G.723.1, G.729, G.729a, G.729e, G.728, G.726, BV16 and BV32
- Echo Cancellation
- Voice Active Detection (VAD)
- DTMF detection and generation
- Comfort Noise Generation (CNG)
- Support V.90 fax and modem services
- Transparent bridging for IP traffic
- RSA and 56 bit DES data encryption security
- SNMP network management support
- Remote operating firmware downloading
- Support Web pages and private DHCP server for status monitoring
- Clear LED display
- Plug and Play

What's on the CD-ROM

Insert the Residential Voice Gateway CD-ROM into your CD-ROM drive to view troubleshooting tips, the internal diagnostics, and other valuable information.

Note: You might need to use the CD-ROM to install the USB driver if you are connecting via the USB port.

Chapter 1: Connections and Setup

CD-ROM Contents:

- Electronic copy of this user's guide in additional languages (PDF format)
- Adobe Acrobat Reader — application you can load to read PDF format, if you don't have it loaded already
- USB drivers — required if connecting by USB
- Links to Thomson and RCA web sites

DOCSIS and PacketCable are trademarks of Cable Television Laboratories, Inc.

Chapter 1: Connections and Setup

Computer Requirements

For the best possible performance from your Residential Voice Gateway, your personal computer must meet the following minimum system requirements (note that the minimum requirements may vary by cable companies):

	IBM PC COMPATIBLE	MACINTOSH**
CPU	Pentium preferred	PowerPC or higher
System RAM	16MB (32MB preferred)	24MB (32MB preferred)
Operating System	Windows* NT/2000/Me/XP, Linux	Mac OS** 7.6.1 or higher
Available Disk Space	125MB	50MB
Sound Card	Required for audio on CD-ROM	N/A
Video	VGA or better (SVGA preferred)	VGA or better (SVGA built-in preferred)
CD-ROM Drive	Required	Required
Ethernet	10BaseT or 100BaseT An Ethernet card makes it possible for your computer to pass data to and from the internet. You must have an Ethernet card and software drivers installed in your computer. You will also need a standard Ethernet cable to connect the Ethernet card to your Residential Voice Gateway.	
USB Port	USB (Windows 2000/ME/XP only) The Universal Serial Bus is a high speed bus that enables your computer to communicate simultaneously with a variety of peripherals. However, if you have other peripherals that send and receive a lot of information, such as speakers, printers or scanners, we recommend using an Ethernet card to support this modem.	
Software	<ul style="list-style-type: none">• A TCP/IP network protocol for each machine• Microsoft Internet Explorer 4.0 or later or Netscape Navigator 4.0 or later. (5.0 and 4.7 or later, respectively, are strongly recommended.)	

*Windows is a trademark of Microsoft Corporation.

**Macintosh and the Mac OS are trademarks of Apple Computer, Inc.

Chapter 1: Connections and Setup

Wall Mounting

The number of the screw: 2 pcs

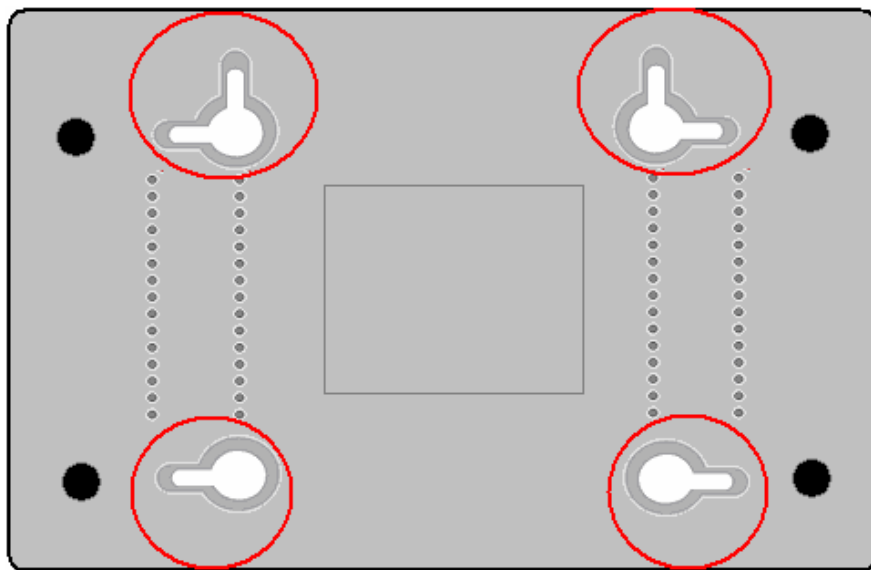
Direction for wall mounting: LED panel upward.

Dimension for the screw: TBD

There are 4 slots on the underside of the EMTA that can be used for wall mounting.

Note: When wall mounting the unit, ensure that it is within reach of the power outlet.

You will need 2 suitable screws which screw diameter would be 4.4 mm to wall mount the Cable Modem or the Battery Pack. Two different wall mount directions could be chosen for the Battery Pack.



To do this:

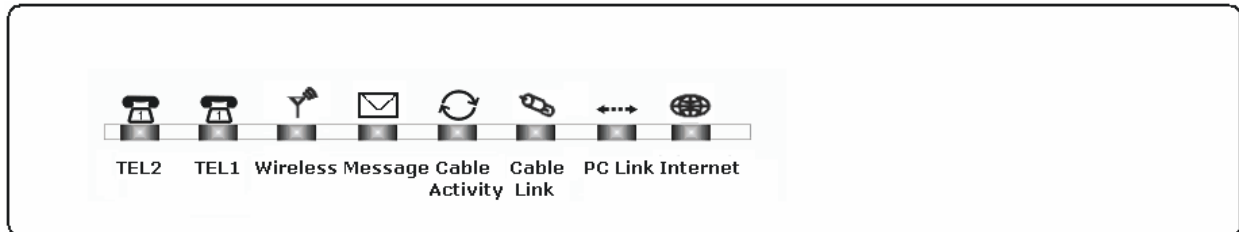
1. Ensure that the wall you use is smooth, flat, dry and sturdy and use the 4 screw holes which are 101.6 mm apart from each other.
2. Fix the screws into wall, leaving their heads 3 mm (0.12 inch) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.

Chapter 1: Connections and Setup

Residential Voice Gateway TWG850 Overview

Front Panel

The following illustration shows the front panel of the TWG850 machine:



The LEDs on the front panel are described in the table below (from left to right):

	Tel 2	Tel 1	Wireless	Message	Cable Activity	Cable Link	PC Link	Internet	Description
Start-up Operation	X	X	X	OFF	OFF	OFF	OFF	FLASH	Tuning (Searching downstream signal)
	X	X	X	OFF	OFF	OFF	FLASH	FLASH	Ranging – Awaiting Response (DS carrier acquire, ranging in process but RNG-RSP has not been detected)
	X	X	X	OFF	OFF	OFF	FLASH	FLASH	Any RNG-RSP detected (Normalizing power level and timing offset)
	X	X	X	OFF	OFF	FLASH	FLASH	FLASH	Connecting (Ranging complete, DHCP in progress)
	X	X	X	OFF	FLASH	FLASH	FLASH	FLASH	Configuring (DHCP complete, configuration file download in process)
	X	X	X	FLASH	FLASH	FLASH	FLASH	FLASH	Registering and Baseline Privacy Initializing (configuration file download complete, initialize BPI if BPI is ON, registration in process)
	X	X	Enter Normal Operation Mode						Registration complete
Normal Operation	X	X	X	X	X	X	X	FLASH ON	NO Cable Link CM is registered
	X	X	X	X	X	X	OFF FLASH ON	X	NO Ethernet/USB carrier present Ethernet/USB TX/RX traffic Ethernet/USB carrier present, no traffic
	X	X	X	X	X	OFF FLASH ON	X	X	NO Cable Link Cable BSS/OSS has set the CM into de-activated state CM is registered
	X	X	X	X	OFF FLASH	X	X	X	Internet ON-OFF switch off/No RF DS/US network traffic RF DS/US network traffic
	X	X	X	OFF FLASH	X	X	X	X	No message is delivered by the MSO Email/Voice Mail is available for the user on the server (Implementation of the message waiting LED will be via Proprietary MIB)
	X	X	OFF ON FLASH	X	X	X	X	X	Wireless initiate fail or disable Wireless initiate success or enable TX/RX Wireless Traffic
No service Operation	X	X	X	X	X	Wink	X	X	NACO =OFF
	X	X	X	3 seconds ON followed by a flash OFF					
MTA initialization	OFF	FLASH	<CM Normal Operation>						MTA DHCP
	FLASH	OFF							MTA SNMP/TFTP
	FLASH	FLASH							RSIP
MTA Operation	ON	ON							Both Lines On-Hook
	ON	FLASH							Tel1 Off-hook, Tel2 On-hook
	FLASH	ON							Tel1 On-hook, Tel2 Off-hook
	FLASH	FLASH							Both Lines Off-Hook
SW Download Operation	X	X	X	FLASH	FLASH	FLASH	FLASH	FLASH	A software download and while updating the FLASH memory
	X	X	X	From Right to Left					

Chapter 1: Connections and Setup

Rear Panel

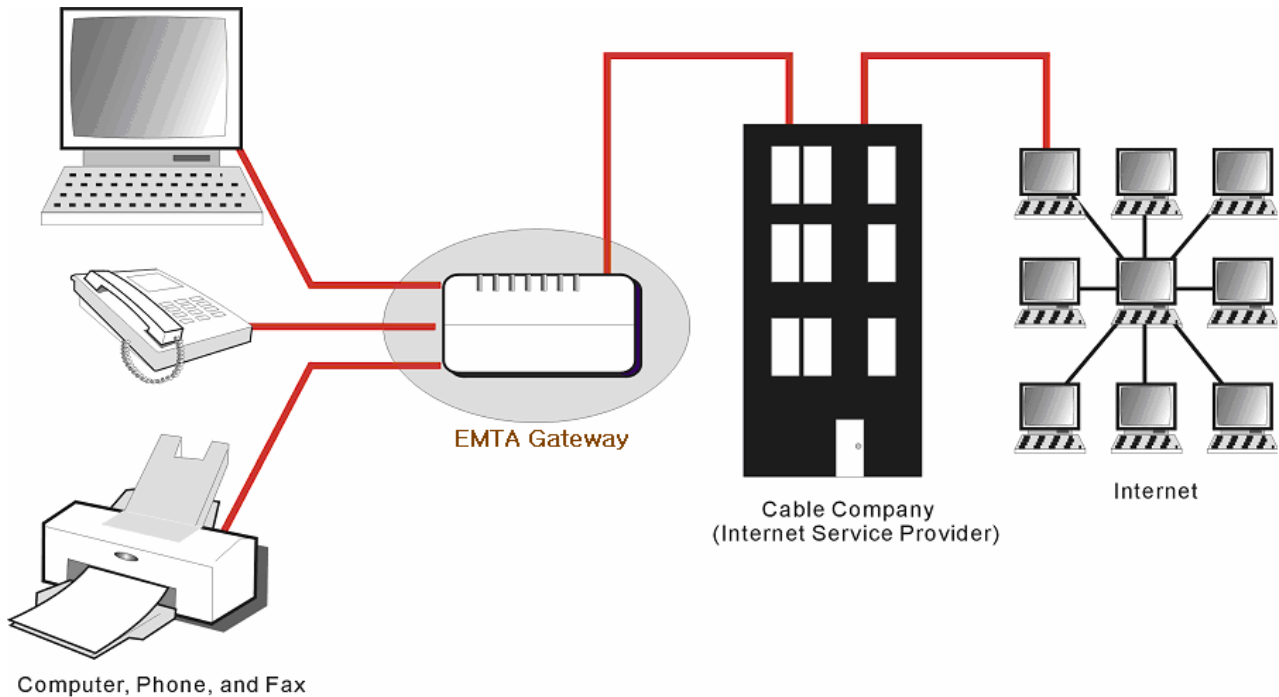


15VDC:	15V DC-IN Power connector
TEL1 & TEL2	Telephony RJ-11 connector
ETHERNET:	Ethernet 10/100BaseT RJ-45 connector
USB:	USB Connector
REBOOT EMTA:	Reboot this Residential Voice Gateway
CABLE:	F-Connector

Chapter 1: Connections and Setup

Relationship among the Devices

This illustration shows a cable company that offers DOCSIS- and PacketCable-compliant voice/data services.



What the Modem Does

The Residential Voice Gateway provides high-speed Internet access as well as cost-effective, toll-quality telephone voice and fax/modem services over residential, commercial, and education subscribers on public and private networks via an existing CATV infrastructure. It can inter-operate with the PacketCable compliant headend equipment and provide the IP-based voice communications. The IP traffic can transfer between the Residential Voice Gateway and DOCSIS compliant headend equipment. The data security secures upstream and downstream communications.

What the Modem Needs to Do Its Job

- **The Right Cable Company:** Make sure your local cable company provides data services that use cable TV industry-standard Euro-DOCSIS or DOCSIS-compliant and Euro-PacketCable or PacketCable-compliant technology.
- **The Internet/Telephony Service Provider (ISP/TSP):** Your cable company provides you access to an Internet Service Provider (ISP) and Telephony Service Provider (TSP). The ISP is your gateway to the Internet and provides you with a pipeline to access Internet content on the World Wide Web (WWW). The TSP provides you with telephony access to other modems or other telephony services over the Public Switched Telephone Network (PSTN).

Illustrations contained in this document are for representation only.

Chapter 1: Connections and Setup

Check with your cable company to make sure you have everything you need to begin; they'll know if you need to install special software or re-configure your computer to make your cable internet service work for you.

Contact Your Local Cable Company

You will need to contact your cable company to establish an Internet account before you can use your gateway. You should have the following information ready (which you will find on the sticker on the gateway):

- The serial number
- The model number
- The Cable Modem (CM) Media Access Control (MAC) address
- The Terminal Adapter (EMTA) MAC address

Chapter 1: Connections and Setup

Please verify the following with the cable company

- The cable service to your home supports Euro-DOCSIS or DOCSIS compliant two-way modem access.
- Your internet account has been set up. (The Media Terminal Adapter will provide data service if the cable account is set up but no telephony service is available.)
- You have a cable outlet near your PC and it is ready for Cable Modem service.

Note: It is important to supply power to the modem at all times. Keeping your modem plugged in will keep it connected to the Internet. This means that it will always be ready whenever you need.

Important Information

Your cable company should always be consulted before installing a new cable outlet. Do not attempt any rewiring without contacting your cable company first.

Chapter 1: Connections and Setup

Connecting the Residential Voice Gateway to a Single Computer

This section of the manual explains how to connect your Residential Voice Gateway to the USB or Ethernet port on your computer and install the necessary software. Please refer to Figure 1 to help you connect your Digital Cable Modem for the best possible connection.

Attaching the Cable TV Wire to the Residential Voice Gateway

1. Locate the Cable TV wire. You may find it one of three ways:
 - a. Connected directly to a TV, a Cable TV converter box, or VCR. The line will be connected to the jack which should be labeled either IN, CABLE IN, CATV, CATV IN, etc.
 - b. Connected to a wall-mounted cable outlet.
 - c. Coming out from under a baseboard heater or other location. See Figure 1 for the wiring example.

Notes: For optimum performance, be sure to connect your Residential Voice Gateway to the first point the cable enters your home. The splitter must be rated for at least 1GHz.

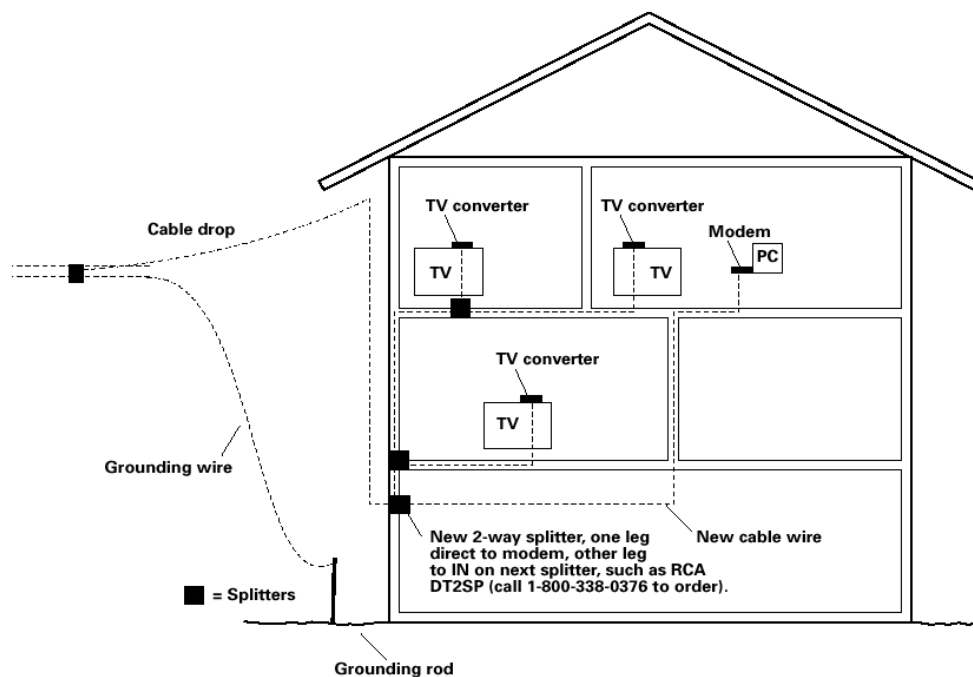


Fig. 1: Basic Home Wiring

Chapter 1: Connections and Setup

Important Connection Information

The Residential Voice Gateway supports Ethernet and USB connections simultaneously.

Below are important points to remember before you connect the Residential Voice Gateway.

- For USB connections, follow the instructions on this page.
- For Ethernet connections, go to page 20.
- For telephone and fax connections, go to page 22.

USB Connection to One Computer

Note: Only use the power supply provided with this unit. Using other power supplies may damage the unit.

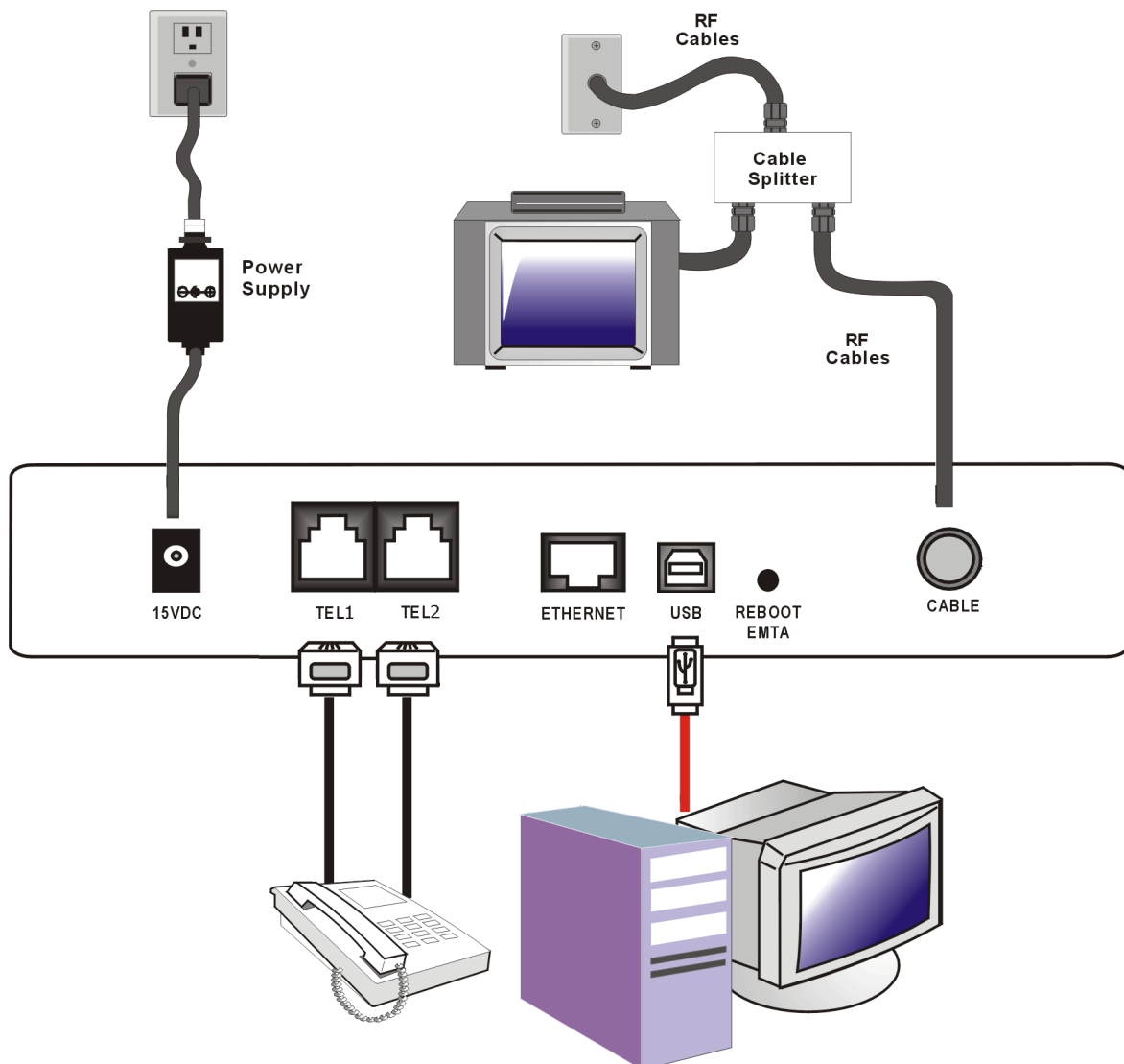


Fig. 2: USB Connection

Illustrations contained in this document are for representation only.

Chapter 1: Connections and Setup

If you received an Installation/Quick Start kit with the purchase of your modem, you should use the software provided in that kit. If not, the Residential Voice Gateway CD included with your modem contains the drivers and other information you need to install your Residential Voice Gateway.

Chapter 1: Connections and Setup

USB Connection

If you do not want to use the CD-ROM, follow instructions 1 through 5 to connect the Residential Voice Gateway to the USB port on your computer. **Instructions must be followed in the order they appear.**

1. Connect one end of the coaxial cable to the cable connection on the wall, and the other end to the CABLE jack on the Residential Voice Gateway.
2. Connect the plug from the AC power supply into the POWER AC ADAPTER jack on the Residential Voice Gateway and plug the power supply into an AC outlet.
3. Insert the supplied Residential Voice Gateway CD-ROM. Wait momentarily for the CD window display.



4. Close **all** open applications and dialog boxes, including the CD window.

Note: Some applications may interfere with your Residential Voice Gateway installation.

5. Connect one end of the USB cable to the USB port located on the back of your computer.
Connect the other end of the USB cable to the USB port on the Residential Voice Gateway.

Note: Use only the power supply that accompanied this unit. Using other power supplies may damage the unit.

Next, you need to install the USB driver for your operating system.

Using Windows 2000 for USB Connection

Follow steps 6 through 14 if you have a Windows 2000 operating system:

Chapter 1: Connections and Setup

6. When the “Found New Hardware Wizard” appears, click “Next” to initiate the search for drivers for your USB device.



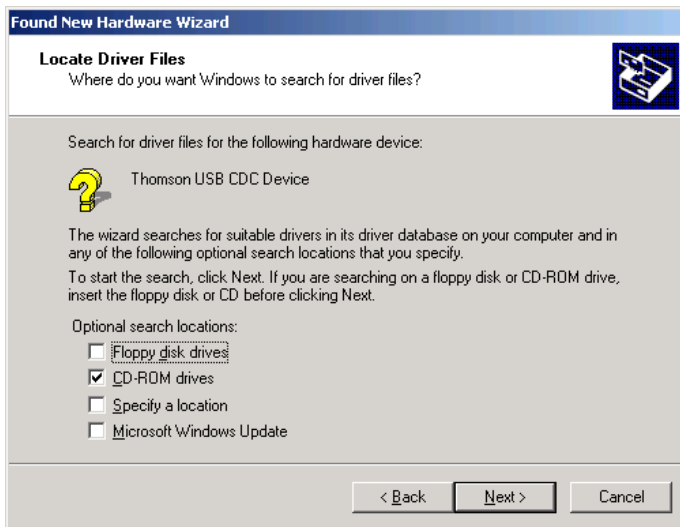
Note: If Windows 2000 does not recognize the presence of the Residential Voice Gateway, your BIOS settings may not permit USB and/or Plug-and-Play devices. Please contact the customer service department of the computer company.

7. Choose the “Search for a suitable driver for my device (recommended)” option, and click “Next”.

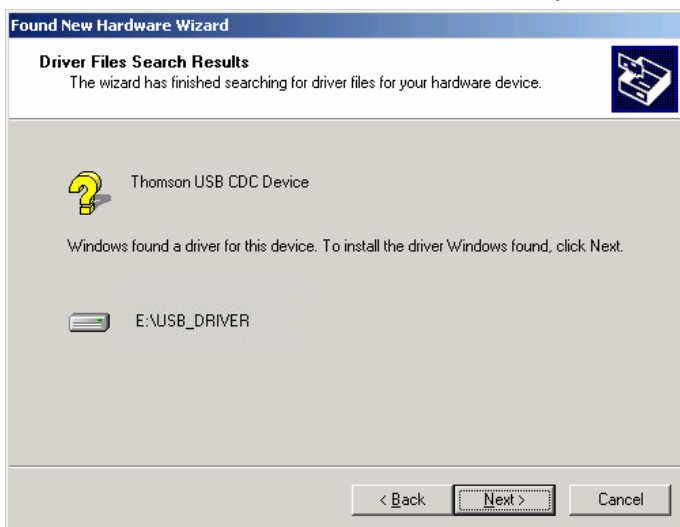


Chapter 1: Connections and Setup

8. Choose **ONLY** the “CD-ROM drives” option and click “Next”.



9. The search should find the driver for the “Thomson USB CDC Devices”. Confirm that this is the case, and click “Next” to continue and proceed to step 11; otherwise, see step 10.



Important: Do NOT continue if the search finds “USB Composite Device” driver. Proceed to step 10.

10. Follow these instructions **ONLY** if the driver found was NOT the “Thomson USB CDC Devices.”
- A. Click “Back” to return to the previous window.
 - B. Ensure that you have selected the “CD-ROM” option.
 - C. In **addition** to the CD-ROM option, choose “Specify a location.” Click on “Next” to continue.
 - D. In the location box, key in your CD-ROM drive. For example, if your CD-ROM is located on the E: drive, type “E:\.” Click “OK” to continue.
 - E. Click “Next” to continue.
 - F. The search should find either “RCA or Thomson USB Cable Modem”.

Chapter 1: Connections and Setup

11. Windows should now prompt you to install the “Thomson USB CDC Devices”. Click “Next” to install the driver.

At this point your PC needs to copy Windows 2000 specific files. If these files are not located on your hard drive, you may need to insert your Windows 2000 installation media (i.e., Windows 2000 CD-ROM), but first remove the Residential Voice Gateway CD-ROM.

12. After the Windows specific files are copied, you may be asked for another USB driver file named “NETRCACM.SYS,” located on the Residential Voice Gateway CD-ROM. Remove the Windows 2000 CD-ROM (if necessary), and reinsert the Residential Voice Gateway CD-ROM that accompanied your Residential Voice Gateway.

13. Click on “Finish” to complete the process.



14. The Residential Voice Gateway installation is now complete. To validate a proper installation, perform the following instructions:
 - A. Click on the “Start” icon in the lower left-hand corner of your screen.
 - B. Select “Settings,” followed by “Control Panel.” The “Control Panel” window appears.
 - C. Double-click on the “System” icon, select the “Hardware” tab, and choose “Device Manager.”
 - D. Scroll down the list until you come to “Network Adapters.” Double-click on “Network Adapters.”
 - E. The “RCA Digital Cable Modem” should exist. If the “RCA or Thomson Digital Cable Modem” does not exist, the Residential Voice Gateway was **NOT** installed correctly. Please install again.

Chapter 1: Connections and Setup

Using Windows Me for USB Connection

Follow steps 6 through 9 if you have a Windows Me operating system:

6. Windows Me will briefly display the “Found New Hardware Wizard,” and automatically proceed to the “Add New Hardware Wizard”.

Choose the “Automatic search for a better driver (Recommended)” option, and click “Next.”

Note: If Windows Me does not recognize the presence of the Residential Voice Gateway, i.e., the “Add New Hardware Wizard” did not automatically appear, your BIOS settings may not permit USB and/or Plug-and-Play devices. Please contact your computer’s customer service department.

7. The automatic search should find and install the driver for the “RCA or Thomson Digital Cable Modem”. Click on “Finish” to complete the process.



8. When the “System Settings Change” window appears, click “Yes” to restart your computer.



9. The Thomson Digital Cable Modem installation is now complete. To validate a proper installation, perform the following instructions:
 - A. Click on the “Start” icon in the lower left-hand corner of your screen.
 - B. Select “Settings,” followed by “Control Panel.” The “Control Panel” window will appear.
 - C. Double-click on the “System” icon, and select the “Device Manager.”
 - D. Scroll down the list until you come to “Network Adapters.” Double-click on “Network Adapters.”
 - E. The “RCA or Thomson Digital Cable Modem” should exist. If “RCA or Thomson Digital Cable Modem” does not exist, the Digital Cable Modem was **NOT** installed correctly.

Chapter 1: Connections and Setup

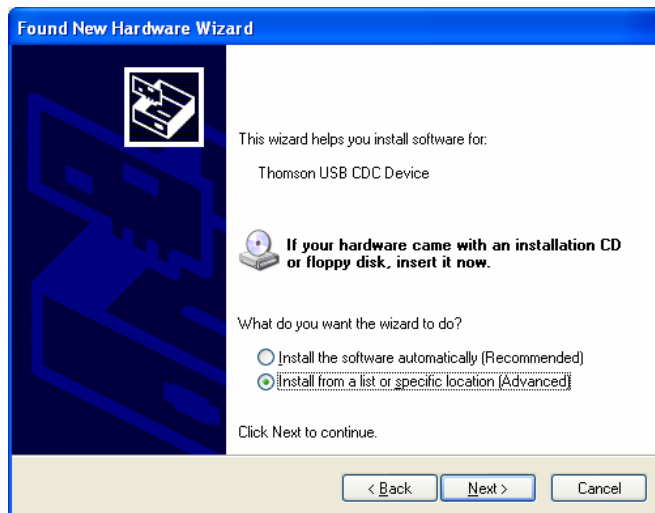
Using Windows XP for USB Connection

Follow steps 6 through 9 if you have a Windows XP operating system:

6. Windows XP will display the “Welcome to the Found New Hardware Wizard” window, and ask whether you would like the Windows to connect to Windows Update to search for software, Choose “No, not this time” and click “Next”.



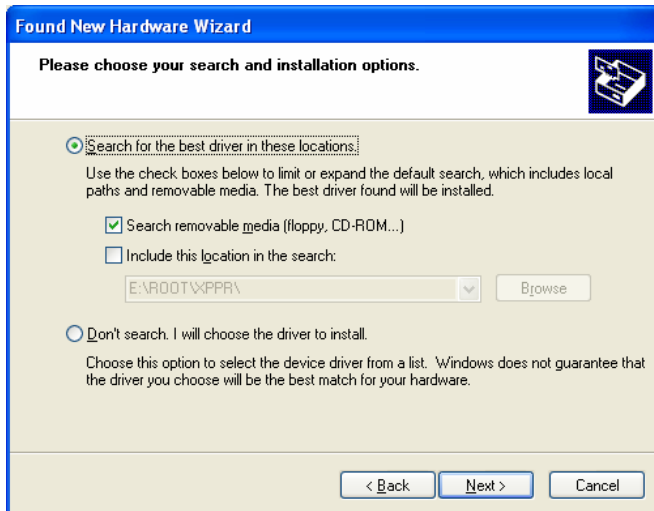
7. The “Found New Hardware Wizard” will then display the device name and ask you to insert the installation CD-ROM that came with the unit. Choose the “Install from a list or specific location (Advanced)” option, and click “Next.”



Note: If Windows XP does not recognize the presence of the Residential Voice Gateway, i.e., the “Welcome to the New Hardware Wizard” did not automatically appear, your BIOS settings may not permit USB and/or Plug-and-Play devices. Please contact the customer service department of the computer company.

8. Select “Search Removable Media (floppy, CD-ROM...)” and click on “Next”, then your computer will install the drivers for the “RCA or Thomson Digital Cable Modem”.

Chapter 1: Connections and Setup



9. When the “Completing the Found New Hardware Wizard” window appears, click “Finish” to complete the process.



10. The Residential Voice Gateway installation is now complete. To validate a proper installation, perform the following instructions:
- Click on the “Start” icon in the lower left-hand corner of your screen.
 - Select “Settings,” followed by “Control Panel.” The “Control Panel” window will appear.
 - Double-click on the “System” icon, and select the “Device Manager.”
 - Scroll down the list until you come to “Network Adapters.” Double-click on “Network Adapters.”
 - The “RCA or Thomson Digital Cable Modem” should exist. If “RCA or Thomson Digital Cable Modem” does not exist, the Residential Voice Gateway was **NOT** installed correctly.

Chapter 1: Connections and Setup

Ethernet Connection to One Computer

Make the connections to the modem in the following sequence:

1. Connect one end of the coaxial cable to the cable connection on the wall, and the other end to the CABLE jack on the Residential Voice Gateway.
2. Connect the plug from the AC power supply into the POWER AC ADAPTER jack on the Residential Voice Gateway, and plug the power supply into an AC outlet.

Note: Use only the power supply that accompanied this unit. Using other adapters may damage the unit.

3. Connect one end of the Ethernet cable (straight-wired, see below) to the Ethernet port on the back of your computer, and the other end to the ETHERNET port on the Residential Voice Gateway.

Make sure that the Ethernet cable is straight-wired (not “null” or crossover-wired). However, you will need a crossover-type cable if you are connecting the modem to a hub, or a hub within a port switch that provides the same function.

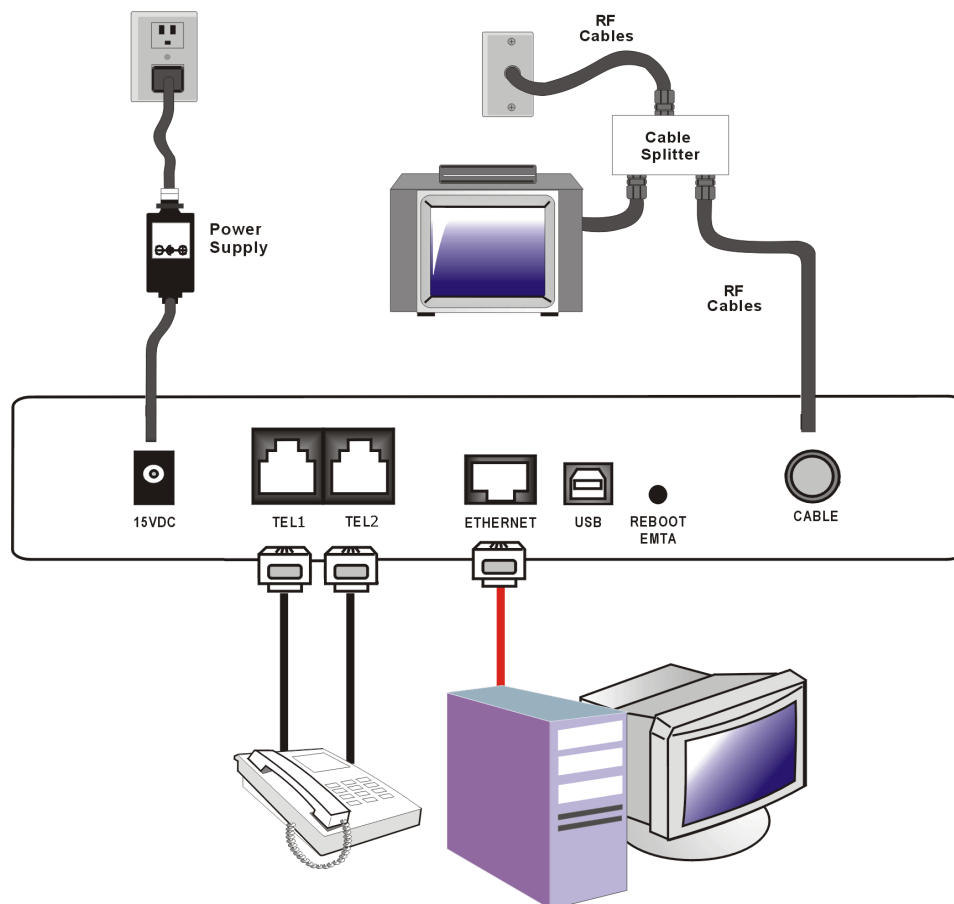


Fig.3: Ethernet Connection

Chapter 1: Connections and Setup

Connecting More Than Two Computers to the Residential Voice Gateway

For TWG 850, if you need to connect more than two computers or if you need to connect two computers, but USB is not available, you'll need the following additional equipment:

- Crossover-wired, or “null,” category 5 Ethernet cable for the EMTA Gateway to be connected to the hub
- 10BaseT or 100BaseT Hub or Switch
- Straight through, or standard, category 5 Ethernet cable (one for each computer to be connected)

If you have a hub with an uplink port*, a straight through cable can be used in combination with that port in lieu of the crossover cable.

*An uplink port has a small switch on it to change the polarity of the connection. It can accept either a crossover or a straight cable, depending on the setting.

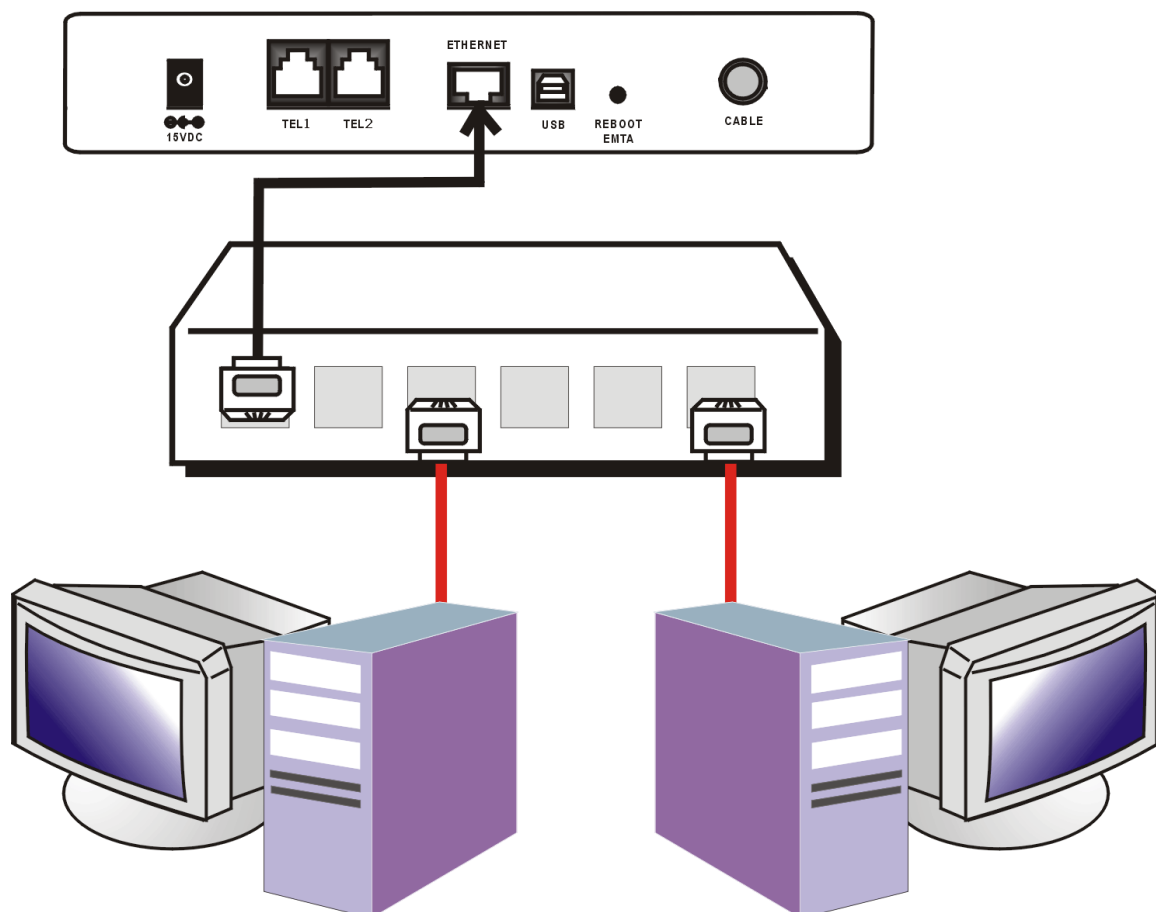


Fig.4: Hub Connection

Note: You may need to check with your service provider in order to connect multiple computers.

Chapter 1: Connections and Setup

Telephone or Fax Connection

When properly connected, most telephony devices can be used with the Residential Voice Gateway just as with conventional telephone service. To make a normal telephone call, pick up the handset; listen for a dial tone, then dial the desired number. For services such as call waiting, use the hook switch (or FLASH button) to change calls. The following procedures describe some of the possible connection schemes for using telephony devices with the Residential Voice Gateway.

1. Connect a standard phone line cord directly from the phone (fax machine, answering machine, caller ID box, etc.) to one of the LINE jacks on the Residential Voice Gateway.
2. If there is a phone line in your home which is NOT connected to another telephone service provider, connect a standard phone line cord from a jack on this line to one of the LINE jacks of the Residential Voice Gateway. Connect a standard phone line cord directly from the phone (fax machine, answering machine, caller ID box, etc.) to one of the other jacks in the house that uses that line.
3. If you have a multi-line telephone, connect a standard phone line cord (not an RJ-14 type line cord) from the phone to the LINE jacks on the Residential Voice Gateway. (Other phones can be added to each line by using standard phone line splitters.

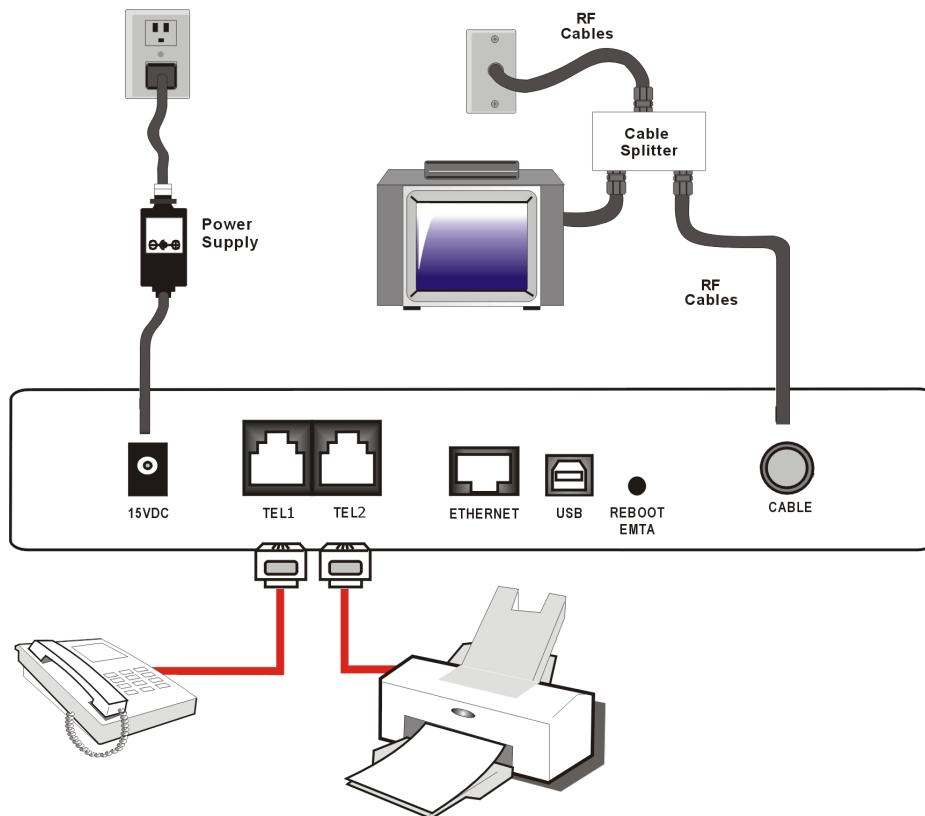


Fig. 5: Phone/Fax Connection

Chapter 1: Connections and Setup

Activating the Residential Voice Gateway

After installing the Residential Voice Gateway and turn it on for the first time (and each time the modem is reconnected to the power), it goes through several steps before it can be used. Each of these steps is represented by a different pattern of flashing lights on the front of the modem.

Note: All indicators flash once before the initialization sequence.

If all of the lights are flashing sequentially, it means the Residential Voice Gateway is automatically updating its system software. Please wait for the lights to stop flashing. You cannot use your modem during this time. Do not remove the power supply or reset the Residential Voice Gateway during this process.

Chapter 2: Web Configuration

Chapter 2: Web Configuration

To make sure that you can access the Internet successfully, please check the following first.

1. **Make sure the connection (through Ethernet or USB) between the Residential Voice Gateway and your computer is OK.**
2. **Make sure the TCP/IP protocol is set properly.**
3. **Subscribe to a Cable Company.**

Accessing the Web Configuration

The **Residential Voice Gateway** offers local management capability through a built in HTTP server and a number of diagnostic and configuration web pages. You can configure the settings on the webpage and apply them to the device.

Once your host PC is properly configured; please proceed as follows:

1. Start your web browser and type the private IP address of the Residential Voice Gateway on the URL field: **192.168.0.1**.
2. After connecting to the device, you will be prompted to enter username and password. By default, the username is “ ” and the password is “**admin**”.



Fig. 6

If you login successfully, the main page will appear.

Chapter 2: Web Configuration

Outline of Web Manager

The main screen will be shown as below.

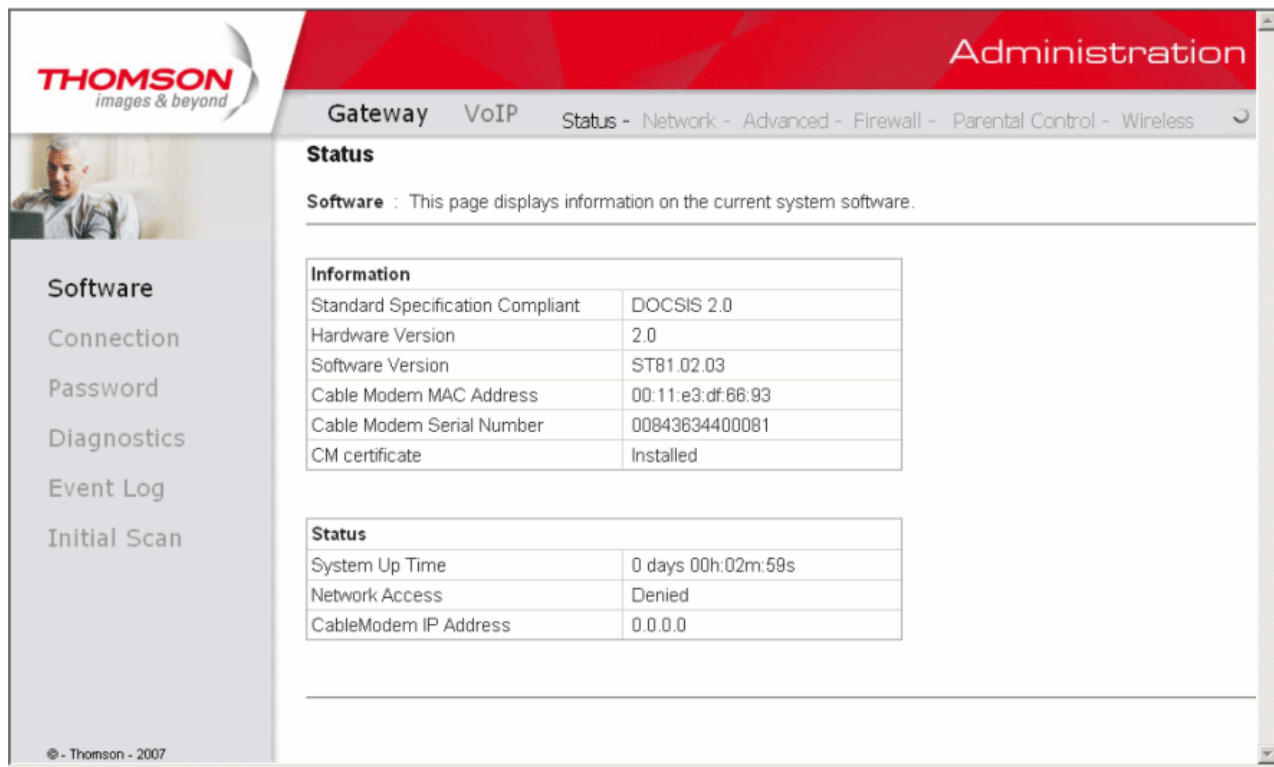


Fig. 7

- Main Menu:** the hyperlinks on the top of the page, including Gateway, VoIP and several sub-menu items
- Title:** the sidebar on the left side of the page, indicates the title of this management interface, e.g., Software in this example
- Main Window:** the current workspace of the web management, containing configuration or status information

For easy navigation, the pages are organized in groups, with group names main menu, individual page names within each group are provided in the sidebar. To navigate to a page, click the group hyperlink at the top, then the page title on the sidebar.

Your cable company may not support the reporting of some items of information listed on your gateway's internal web pages. In such cases, the information field appears blank. This is normal.

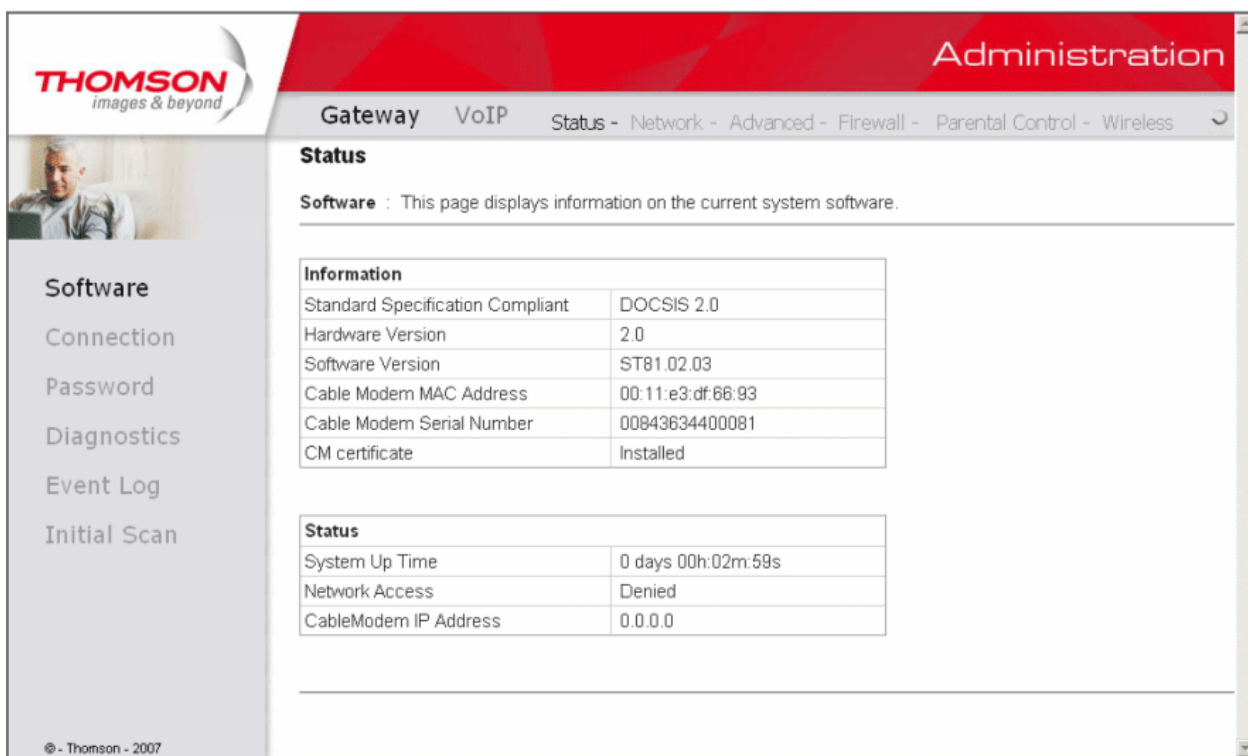
Chapter 2: Web Configuration

Gateway – Status Web Page Group

Software

The information section shows the hardware and software information about your gateway.

The status section of this page shows how long your gateway has operated since last time being powered up, and some key information the Cable Modem received during the initialization process with your cable company. If Network Access shows “Allowed,” then your cable company has configured your gateway to have Internet connectivity. If not, you may not have Internet access, and should contact your cable company to resolve this.



The screenshot displays the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', and 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The left sidebar lists 'Software', 'Connection', 'Password', 'Diagnostics', 'Event Log', and 'Initial Scan'. The main content area is titled 'Status' and contains a 'Software' section with the following information:

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	2.0
Software Version	ST81.02.03
Cable Modem MAC Address	00:11:e3:df:66:93
Cable Modem Serial Number	00843634400081
CM certificate	Installed

Status	
System Up Time	0 days 00h:02m:59s
Network Access	Denied
CableModem IP Address	0.0.0.0

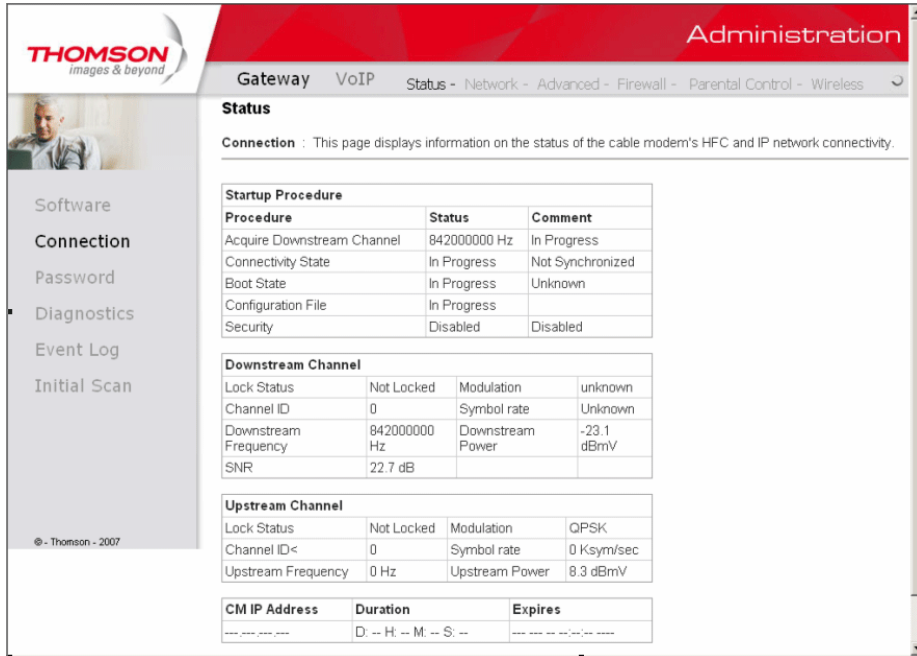
© - Thomson - 2007

Fig. 8

Chapter 2: Web Configuration

Connection

This page reports current connection status containing startup procedures, downstream and upstream status, CM online information, and so on. The information can be useful to your cable company's support technician if you're having problems.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes links for Gateway, VoIP, Status, Network, Advanced, Firewall, Parental Control, and Wireless. The left sidebar contains links for Software, Connection, Password, Diagnostics, Event Log, and Initial Scan. The main content area is titled 'Status' and contains a description: 'This page displays information on the status of the cable modem's HFC and IP network connectivity.' Below this, there are three tables: 'Startup Procedure', 'Downstream Channel', and 'Upstream Channel'. At the bottom, there is a table for 'CM IP Address'.

Procedure	Status	Comment
Acquire Downstream Channel	842000000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Configuration File	In Progress	
Security	Disabled	Disabled

Lock Status	Channel ID	Modulation	Symbol rate
Not Locked	0	unknown	Unknown
Downstream Frequency	842000000 Hz	Downstream Power	-23.1 dBmV
SNR	22.7 dB		

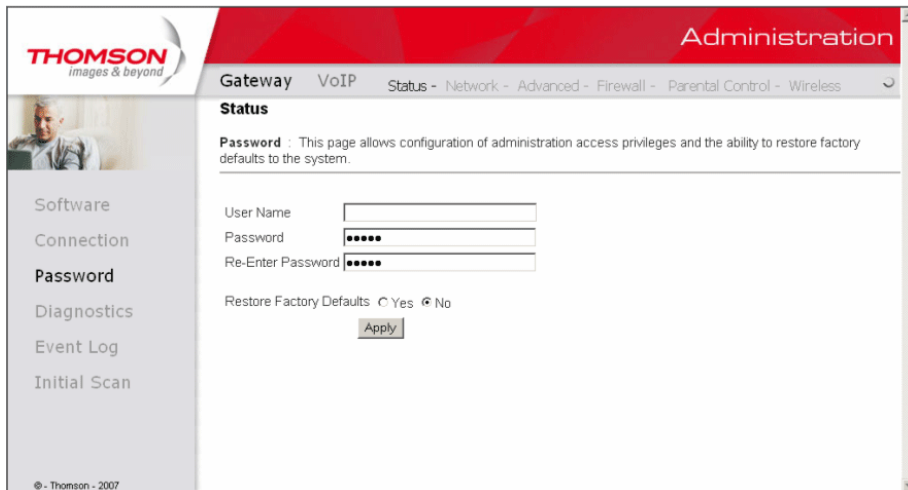
Lock Status	Channel ID	Modulation	Symbol rate
Not Locked	0	QPSK	0 Ksym/sec
Upstream Frequency	0 Hz	Upstream Power	8.3 dBmV

CM IP Address	Duration	Expires
---	D: -- H: -- M: -- S: --	---

Fig. 9

Password

This page is used to change the password that enables you to access the gateway web pages next time. The default User ID is “”(EMPTY), and the password is “admin”. The password can be a maximum of 8 characters and is case sensitive. In addition, this page can be used to restore the gateway to its original factory settings. Use this with caution, as all the settings you have made will be lost. To perform this reset, set **Restore Factory Defaults** to **Yes** and click **Apply**. This has the same effect as a factory reset using the rear panel reset switch, where you hold in the switch for 15 seconds, then release.



The screenshot shows the Thomson Gateway Administration web interface, specifically the Password section. The top navigation bar and left sidebar are the same as in Figure 9. The main content area is titled 'Password' and contains a description: 'This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.' Below this, there are input fields for 'User Name', 'Password', and 'Re-Enter Password'. There is also a checkbox for 'Restore Factory Defaults' with radio buttons for 'Yes' and 'No'. An 'Apply' button is located at the bottom.

User Name:

Password:

Re-Enter Password:

Restore Factory Defaults ☐ Yes ☒ No

Fig. 10

Chapter 2: Web Configuration

Diagnostics

This page offers basic diagnostic tools for you to utilize when connectivity problems occur. When you ping an Internet device, you send a packet to its TCP/IP stack, and it sends one back to yours. To use the ping Test, enter the information needed and press **Start Test**; the Result will be displayed in the lower part of the window. Press **Abort Test** to stop, and **Clear Results** to clear the result contents.

Note: Firewalls may cause pings to fail but still provide you TCP/IP access to selected devices behind them. Keep this in mind when pinging a device that may be behind a firewall. Ping is most useful to verify connectivity with PCs have no firewall, such as the PCs on your LAN side.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Status' section is active, displaying the 'Diagnostics' page. The 'Ping Test Parameters' section includes input fields for 'Ping Target' (192.168.0.1), 'Ping Size' (64 bytes), 'No. of Pings' (3), and 'Ping Interval' (1000 ms). Below these fields are buttons for 'Start Test', 'Abort Test', and 'Clear Results'. The 'Results' section shows a box with the text 'Waiting for input...' and a red message at the bottom: 'To get an update of the results you must REFRESH the page.' The Thomson logo and '© - Thomson - 2007' are visible in the bottom left corner.

Fig. 11

Chapter 2: Web Configuration

Event Log

This page displays the contents of the SNMP event log. Press “**Clear Log**” button to clear the logs.

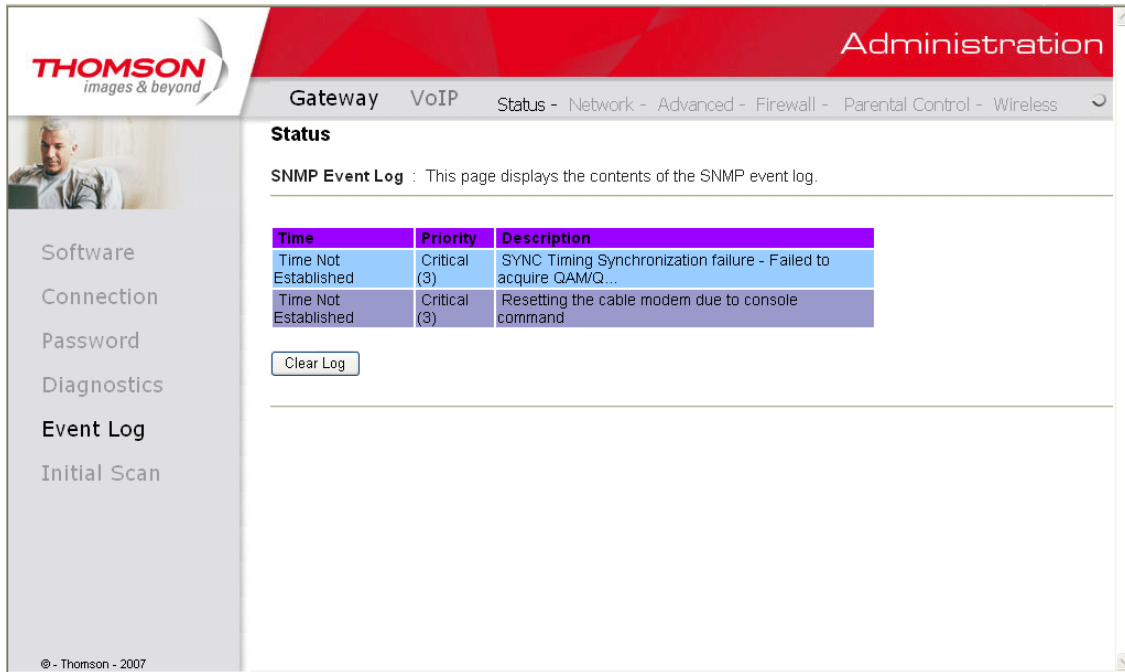


Fig. 12

Initial Scan

To speed up the modem's first time startup, enter known downstream frequency and/or upstream channel ID information here. Then click “**Apply and Reboot**” button to start scanning the cable network beginning with the values supplied here.

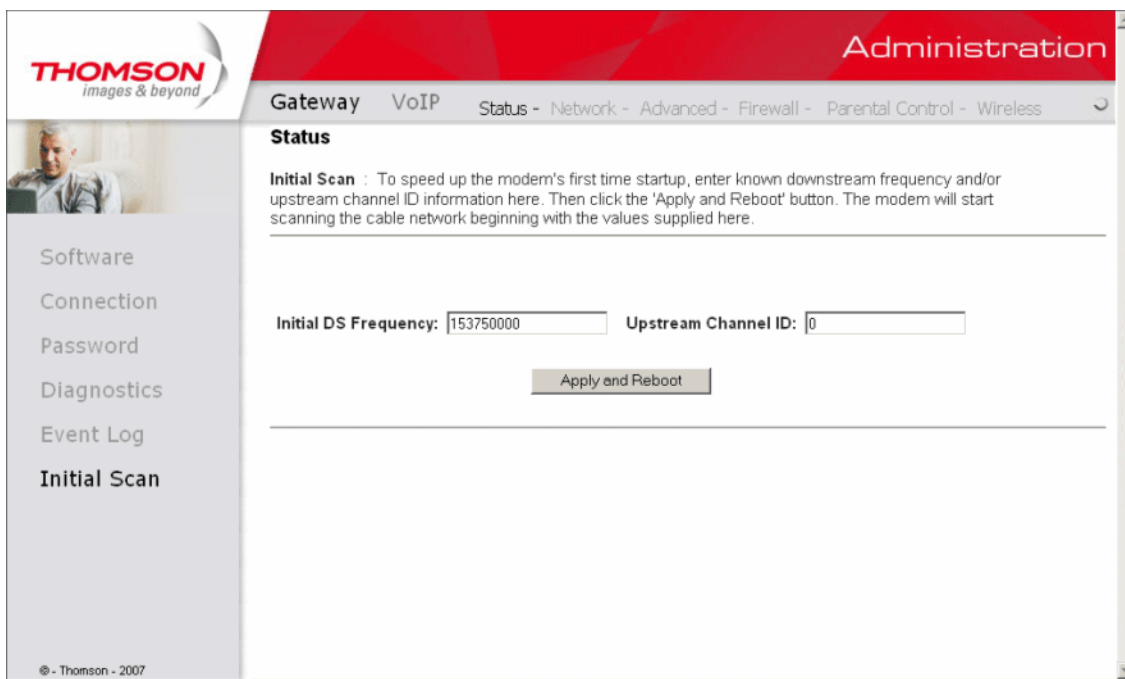


Fig. 13

Chapter 2: Web Configuration

Gateway – Network Web Page Group

LAN

You can activate the DHCP server function for the LAN on this page.

With this function activated, your cable company's DHCP server provides one IP address for your gateway, and your gateway's DHCP server provides IP addresses, starting at the address you set in IP Address on the LAN page, to your PCs. A DHCP server leases an IP address with an expiration time.

To change the lowest IP address that your gateway will issue to your PCs, enter it into the IP Address box and then click **Apply**.

The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Network' section is active, showing 'LAN' configuration. The 'Network Configuration' section includes fields for IP Address (192.168.0.1), Subnet Mask (255.255.255.0), MAC Address (00:11:e3:df:66:97), DHCP Server (Yes), Starting Local Address (192.168.0.10), Number of CPEs (245), and Lease Time (604800). An 'Apply' button is at the bottom.

Network Configuration	
IP Address	192 . 168 . 0 . 1
Subnet Mask	255.255.255.0
MAC Address	00:11:e3:df:66:97
DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
Starting Local Address	192.168.0.10
Number of CPEs	245
Lease Time	604800
<input type="button" value="Apply"/>	

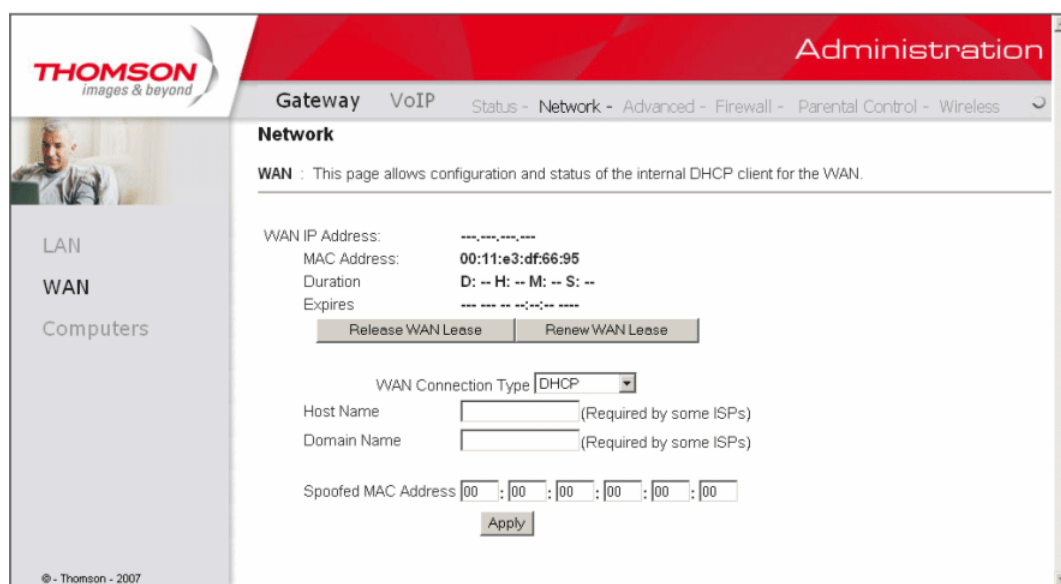
Fig. 14

Chapter 2: Web Configuration

WAN

You can configure the optional internal DHCP server for the WAN on this page. Select different WAN Connection Type will lead to different contents. Take the WAN connection type-DHCP for example, you can release and renew the WAN lease by pressing the buttons.

You can enter a spoofed MAC address that causes your gateway networking stack to use that MAC address when communicating instead of the usual WAN MAC address, e.g., if the MAC address is `00:11:e3:df:66:95`, this spoofed MAC address could be `00:11:e3:df:66:97` or any desired MAC address.

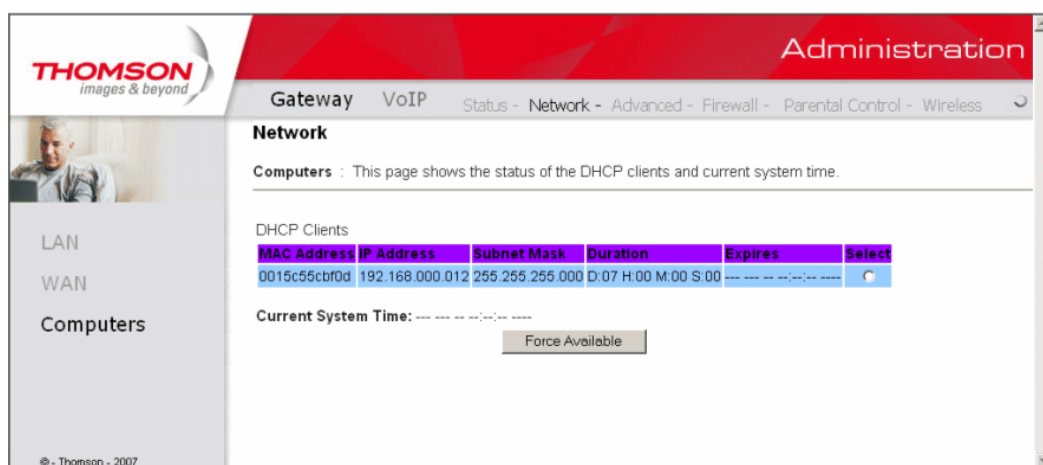


The screenshot shows the Thomson Administration web interface. The left sidebar has a menu with 'LAN', 'WAN', and 'Computers'. The main content area is titled 'Administration' and has a sub-menu with 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Network' section is active, showing 'WAN' configuration. The text says: 'WAN : This page allows configuration and status of the internal DHCP client for the WAN.' Below this, there are fields for 'WAN IP Address' (---:---:---:---), 'MAC Address' (00:11:e3:df:66:95), 'Duration' (D: -- H: -- M: -- S: --), and 'Expires' (---:---:---:---). There are two buttons: 'Release WAN Lease' and 'Renew WAN Lease'. Below these is a 'WAN Connection Type' dropdown menu set to 'DHCP'. There are also fields for 'Host Name' and 'Domain Name', both with a note '(Required by some ISPs)'. At the bottom, there is a 'Spoofed MAC Address' field with six input boxes (00, 00, 00, 00, 00, 00) and an 'Apply' button. The footer shows '© - Thomson - 2007'.

Fig. 15

Computers

This page displays the status of the DHCP clients and current system time. You can cancel an IP address lease by selecting it in the DHCP Client Lease Info list and then clicking the **Force Available** button. If you do so, you may have to perform a DHCP Renew on that PC, so that it can obtain a new lease.



The screenshot shows the Thomson Administration web interface for the 'Computers' section. The left sidebar has a menu with 'LAN', 'WAN', and 'Computers'. The main content area is titled 'Administration' and has a sub-menu with 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Computers' section is active, showing 'Computers : This page shows the status of the DHCP clients and current system time.' Below this, there is a table titled 'DHCP Clients' with the following data:

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
0015c55cbf0d	192.168.000.012	255.255.255.000	D:07 H:00 M:00 S:00	---	<input type="checkbox"/>

Below the table, there is a 'Current System Time' field (---:---:---:---) and a 'Force Available' button. The footer shows '© - Thomson - 2007'.

Fig. 16

Chapter 2: Web Configuration

Gateway – Advanced Web Page Group

Options

This page allows you to enable/disable some features of the Residential Voice Gateway.

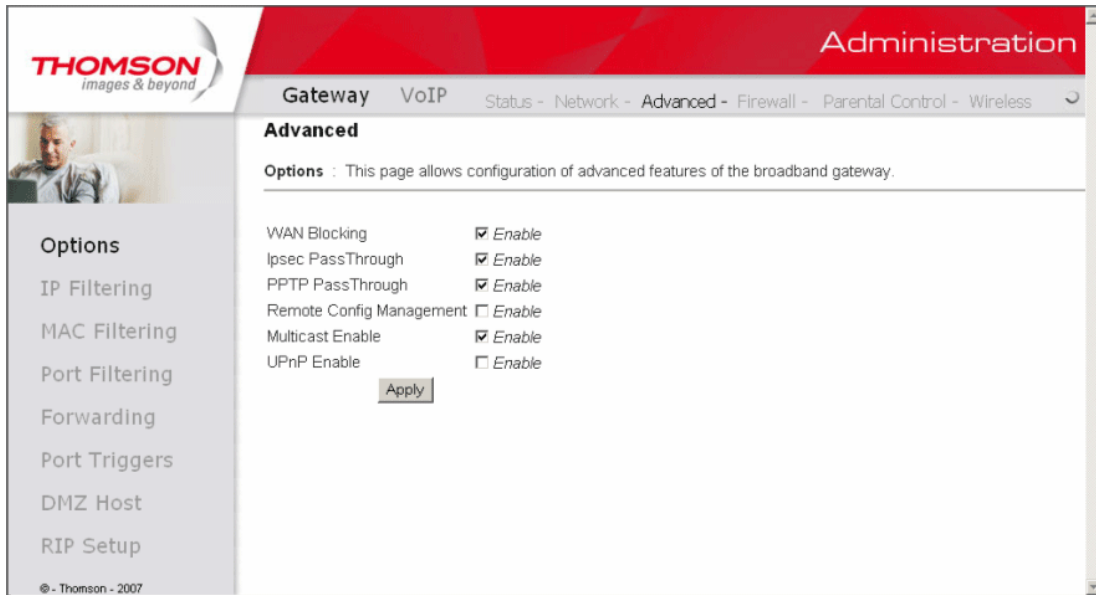


Fig. 17

WAN Blocking prevents others on the WAN side from being able to ping your gateway. With WAN Blocking enabled, your gateway will not respond to pings it receives, effectively “hiding” your gateway.

Ipsec PassThrough enables IpSec type packets to pass WAN ⇔ LAN. IpSec (IP Security) is a security mechanism used in Virtual Private Networks (VPNs).

PPTP PassThrough enables PPTP type packets to pass WAN ⇔ LAN. PPTP (Point to Point Tunneling Protocol) is another mechanism sometimes used in VPNs.

Remote Config Management makes the configuration web pages in your gateway accessible from the WAN side. Note that page access is limited to only those who know the gateway access password. When accessing your gateway from a remote location, you must use HTTP port 8080 and the WAN IP address of the gateway. For example, if the WAN IP address is 157.254.5.7, you would navigate to <http://157.254.5.7:8080> to reach your gateway.

Multicast Enable enables multicast traffic to pass WAN⇔ LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet.

Chapter 2: Web Configuration

IP Filtering

This page enables you to enter the IP address ranges of PCs on your LAN that you don't want to have outbound access to the WAN. These PCs can still communicate with each other on your LAN, but packets they originate to WAN addresses are blocked by the gateway.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Advanced' section is selected, and the 'IP Filtering' sub-section is active. A sidebar on the left lists various options: Options, IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers, DMZ Host, and RIP Setup. The main content area for IP Filtering includes a description: 'IP Filtering : This page allows the configuration of IP Address filters in order to block internet traffic to specific network devices on the LAN.' Below this is a table with three columns: 'Start Address', 'End Address', and 'Enabled'. The table contains ten rows, each with a text input field for the start address, another for the end address, and a checkbox for the 'Enabled' status. All start and end address fields are pre-filled with '192.168.0.0'. An 'Apply' button is located at the bottom of the table.

Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Fig. 18

MAC Filtering

This page enables you to enter the MAC address of specific PCs on your LAN that you wish to NOT have outbound access to the WAN. As with IP filtering, these PCs can still communicate with each other through the gateway, but packets they send to WAN addresses are blocked.

The screenshot shows the Thomson Gateway Administration interface for MAC Filtering. The top navigation bar and sidebar are identical to the IP Filtering page. The 'MAC Filtering' sub-section is active. The main content area includes a description: 'MAC Filtering : This page allows configuration of MAC Address filters in order to block internet traffic to specific network devices on the LAN.' Below this is a table titled 'MAC Address Filters' with two columns. Each column contains ten rows, each with a label (e.g., 'MAC 01', 'MAC 02') followed by a text input field for the MAC address. The input fields are pre-filled with '00:00:00:00:00:00'. An 'Apply' button is located at the bottom of the table.

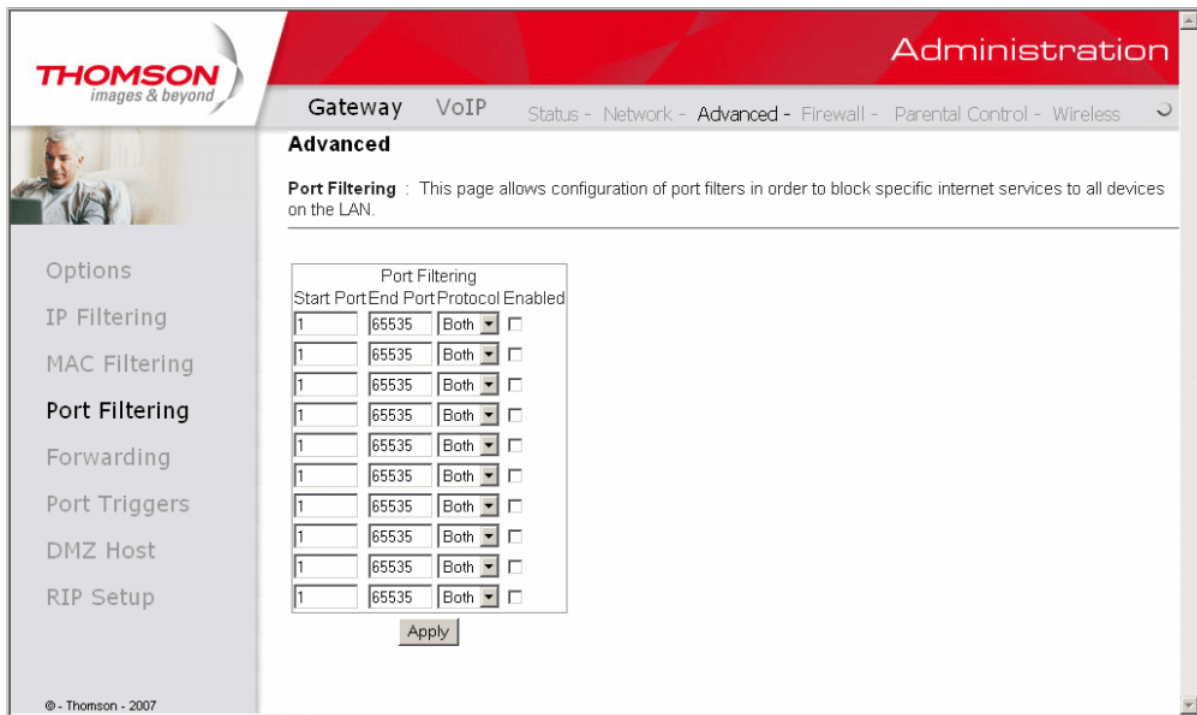
MAC Address Filters	
MAC 01	MAC 02
MAC 03	MAC 04
MAC 05	MAC 06
MAC 07	MAC 08
MAC 09	MAC 10
MAC 11	MAC 12
MAC 13	MAC 14
MAC 15	MAC 16
MAC 17	MAC 18
MAC 19	MAC 20

Fig. 19

Chapter 2: Web Configuration

Port Filtering

This page allows you to enter ranges of destination ports (applications) that you don't want your LAN PCs to send packets to. Any packets your LAN PCs send to these destination ports will be blocked. For example, you could block access to worldwide web browsing (http = port 80) but still allow email service (SMTP port 25 and POP-3 port 110). To enable port filtering, set Start Port and End Port for each range, and click Apply. To block only one port, set both Start and End ports the same.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Advanced' section is selected, and the 'Port Filtering' page is displayed. The page title is 'Port Filtering' and the description states: 'This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.' The configuration table has columns for 'Start Port', 'End Port', 'Protocol', and 'Enabled'. The table contains 10 rows, each with a '1' in the 'Start Port' column, '65535' in the 'End Port' column, 'Both' in the 'Protocol' column, and an unchecked 'Enabled' checkbox. An 'Apply' button is located below the table. The left sidebar contains a list of options: 'Options', 'IP Filtering', 'MAC Filtering', 'Port Filtering' (highlighted), 'Forwarding', 'Port Triggers', 'DMZ Host', and 'RIP Setup'. The Thomson logo and 'images & beyond' tagline are in the top left corner. The copyright notice '© - Thomson - 2007' is in the bottom left corner.

Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Apply

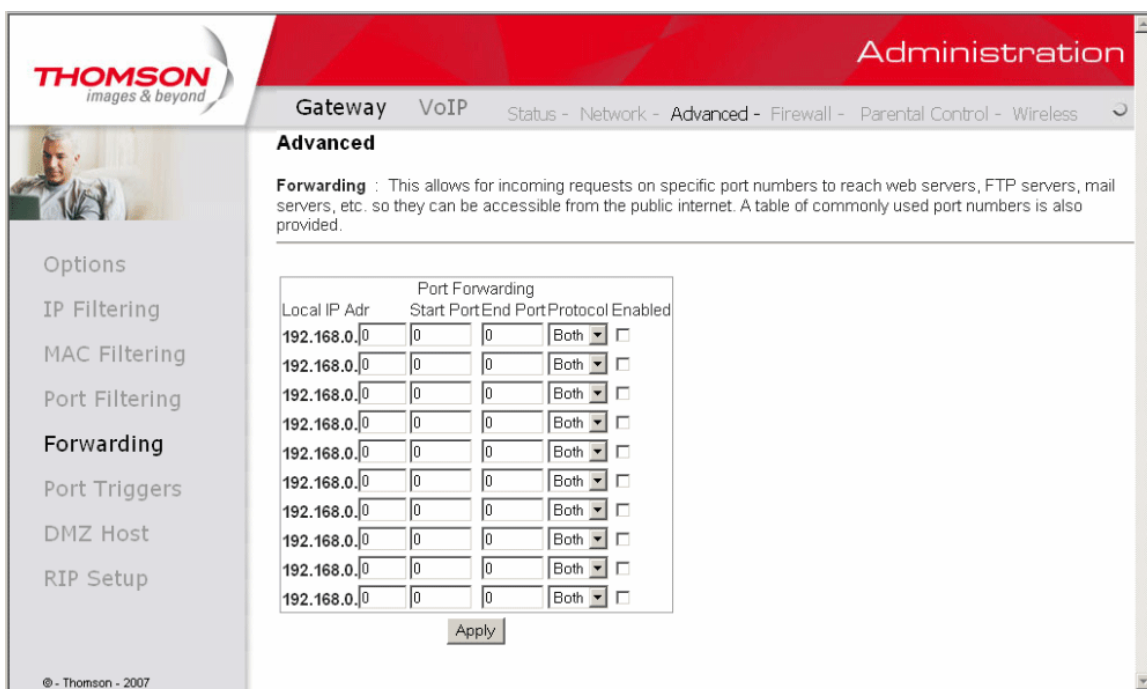
Fig. 20

Chapter 2: Web Configuration

Forwarding

For LAN ↔ WAN communications, the gateway normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one you specify.

This page allows you to specify up to 10 such rules. For example, to specify that outsiders should have access to an FTP server you have running at 192.168.0.5, create a rule with that address and Start Port = 20 and End Port = 21 (FTP port ranges) and Protocol = TCP (FTP runs over TCP and the other transport protocol, UDP), and click Apply. This will cause inbound packets that match to be forwarded to that PC rather than blocked. As these connections are not tracked, no entry is made for them in the Connection Table. The same IP address can be entered multiple times with different ports.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', and a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Advanced' section is active, displaying the 'Forwarding' configuration page. A sidebar on the left lists various options, with 'Forwarding' highlighted. The main content area features a table for 'Port Forwarding' with columns: 'Local IP Addr', 'Start Port', 'End Port', 'Protocol', and 'Enabled'. The table contains 10 rows, each with a '192.168.0.' IP address, '0' for both start and end ports, a 'Both' protocol dropdown, and an unchecked 'Enabled' checkbox. An 'Apply' button is located at the bottom of the table.

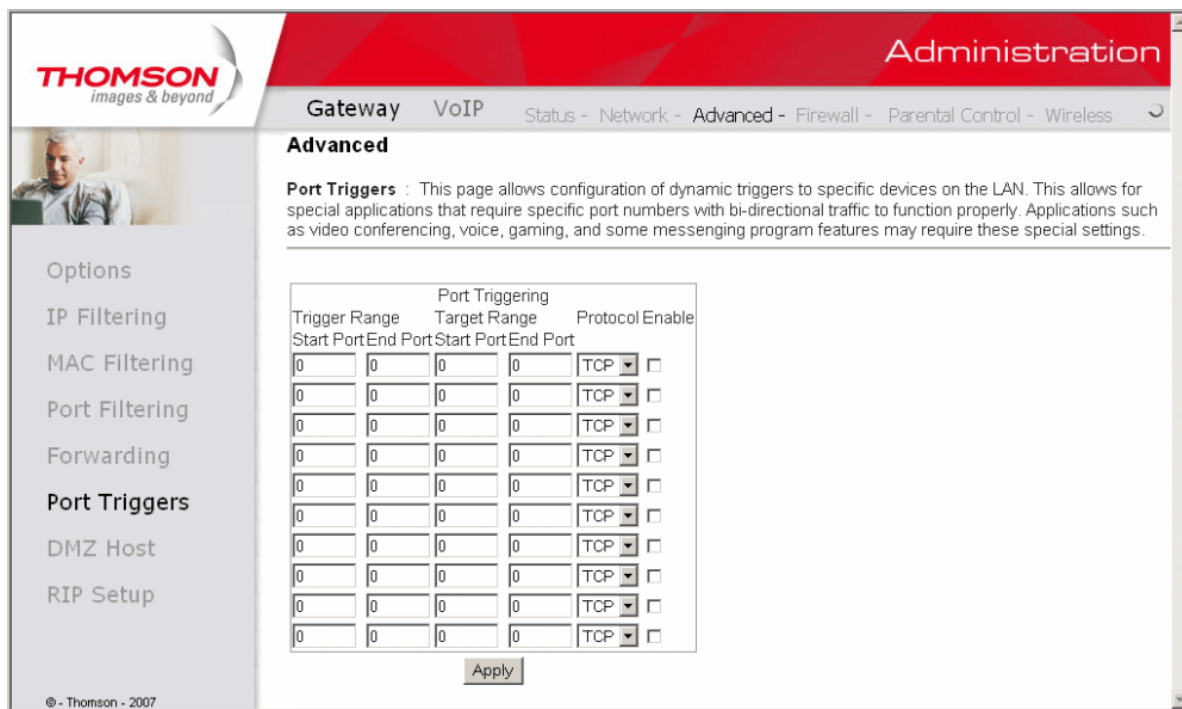
Local IP Addr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Fig. 21

Chapter 2: Web Configuration

Port Triggers

Some Internet activities, such as interactive gaming, require that a PC on the WAN side of your gateway be able to originate connections during the game with your game playing PC on the LAN side. You could use the Advanced-Forwarding web page to construct a forwarding rule during the game, and then remove it afterwards (to restore full protection to your LAN PC) to facilitate this. Port triggering is an elegant mechanism that does this work for you, each time you play the game.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', and a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Advanced' section is active, displaying the 'Port Triggers' configuration page. A sidebar on the left lists various options, with 'Port Triggers' highlighted. The main content area contains a description of Port Triggers and a table for configuring them.

Port Triggers : This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>

Apply

Fig. 22

Port Triggering works as follows. Imagine you want to play a particular game with PCs somewhere on the Internet. You make one time effort to set up a Port Trigger for that game, by entering into **Trigger Range** the range of destination ports your game will be sending to, and entering into **Target Range** the range of destination ports the other player (on the WAN side) will be sending to (ports your PC's game receives on). Application programs like games publish this information in user manuals. Later, each time you play the game, the gateway automatically creates the forwarding rule necessary. This rule is valid until 10 minutes after it sees game activity stop. After 10 minutes, the rule becomes inactive until the next matched outgoing traffic arrives.

For example, suppose you specify Trigger Range from 6660 to 6670 and Target Range from 113 to 113. An outbound packet arrives at the gateway with your game-playing PC source IP address 192.168.0.10, destination port 666 over TCP/IP. This destination port is within the Trigger destined for port 113 to your game-playing PC at 192.168.0.10.

You can specify up to 10 port ranges on which to trigger.

Chapter 2: Web Configuration

DMZ Host

Use this page to designate one PC on your LAN that should be left accessible to all PCs from the WAN side, for all ports. For example, if you put an HTTP server on this machine, anyone will be able to access that HTTP server by using your gateway IP address as the destination. A setting of “0” indicates NO DMZ PC. “Host” is another Internet term for a PC connected to the Internet.

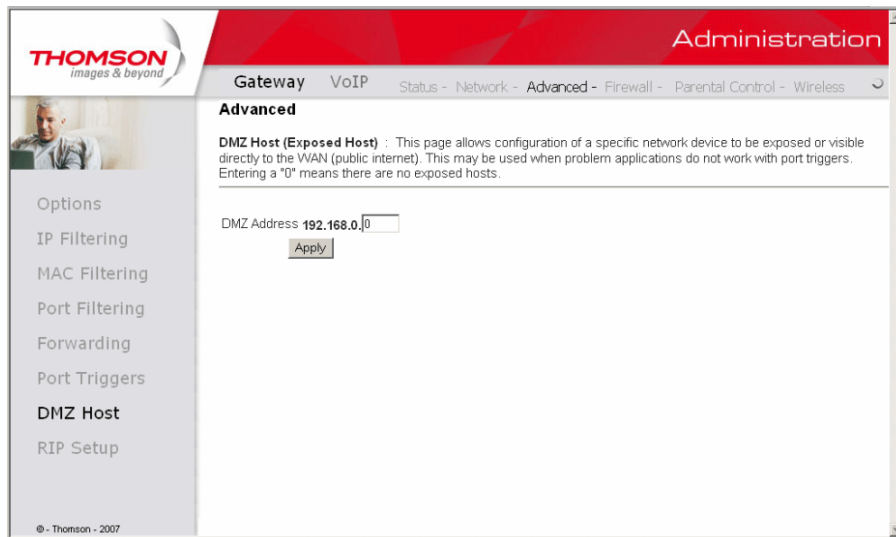


Fig. 23

RIP (Routing Information Protocol) Setup

This feature enables the gateway to be used in small business situations where more than one LAN (local area network) is installed. The RIP protocol provides the gateway a means to “advertise” available IP routes to these LANs to your cable operator, so packets can be routed properly in this situation.

Your cable operator will advise you during installation if any setting changes are required here.

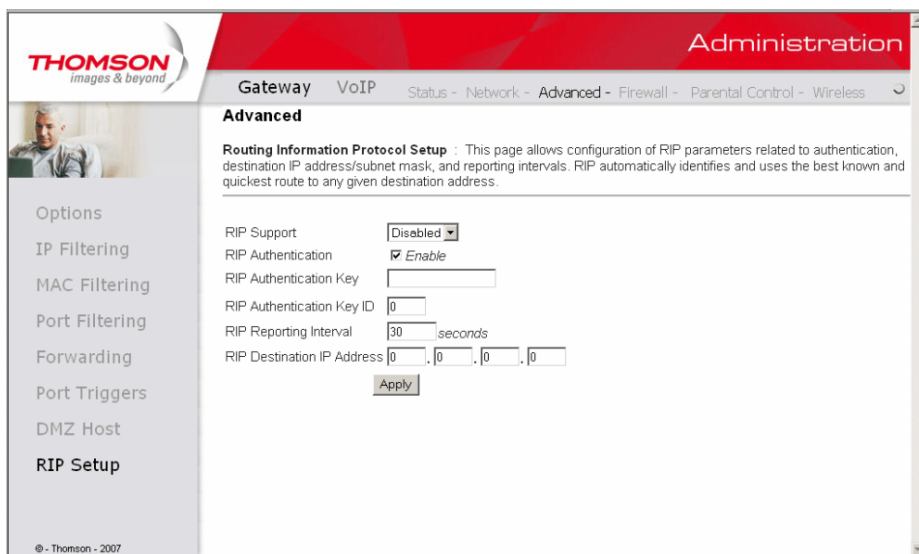


Fig. 24

Chapter 2: Web Configuration

Gateway – Firewall Web Page Group

Web Content Filtering

These pages allow you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking Apply.

The web-related filtering features you can activate from the Web Content Filter page include Filter Proxy, Filter Cookies, Filter Java Applets, Filter ActiveX, Filter Popup Windows, and Firewall Protection.

If you want the gateway to exclude your selected filters to certain computers on your LAN, enter their MAC addresses in the Trusted Computers area of this page.

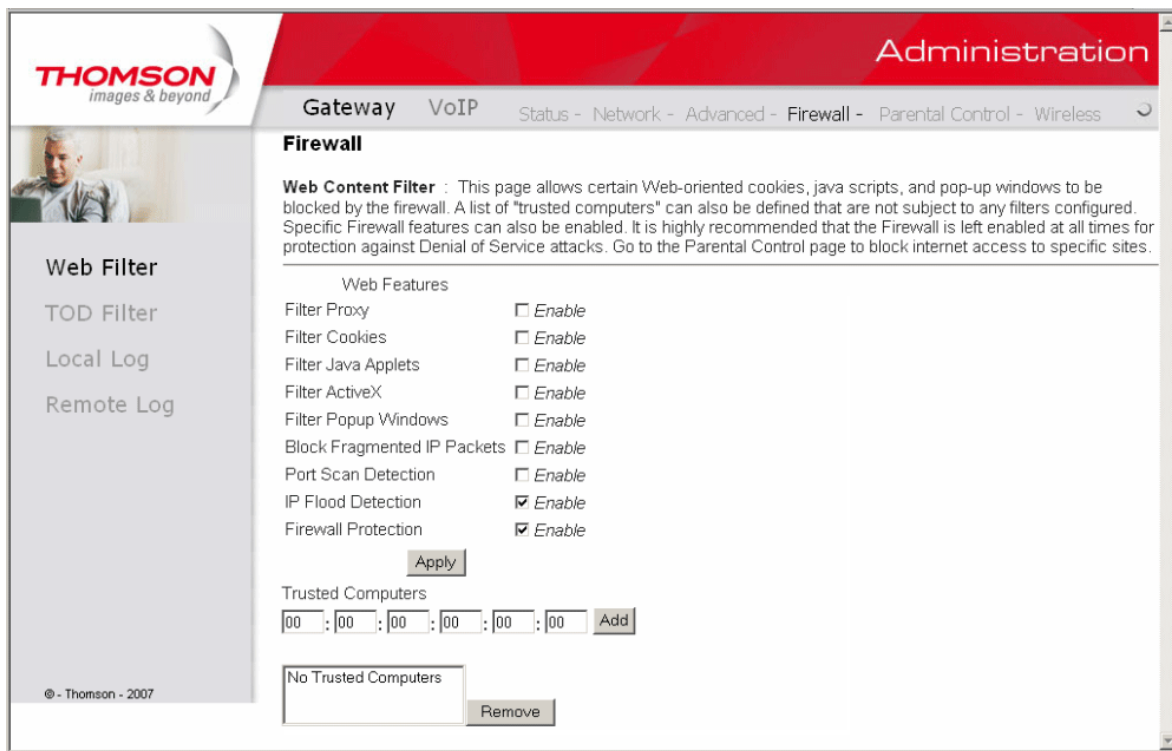
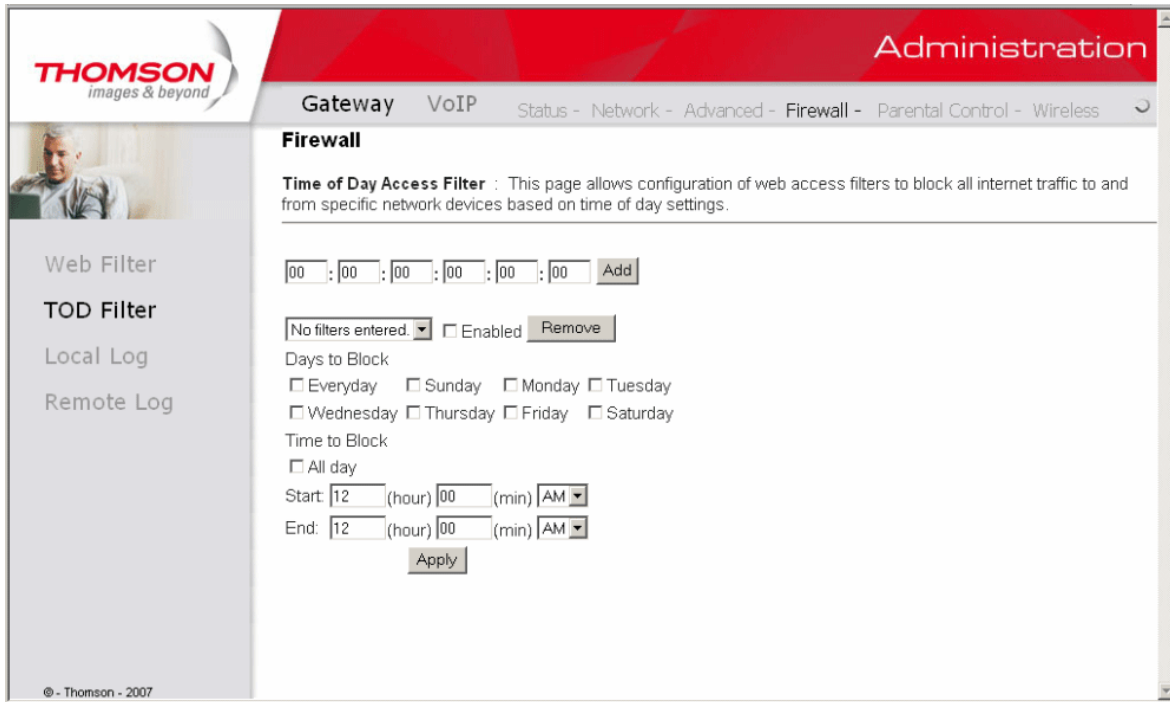


Fig. 25

Chapter 2: Web Configuration

TOD Filtering

Use this page to set rules that will block specific LAN side PCs from accessing the Internet, but only at specific days and times. Specify a PC by its hardware MAC address, and then use the tools to specify blocking time. Finally, click the Apply button to save your settings.



The screenshot displays the Thomson Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The left sidebar contains links for 'Web Filter', 'TOD Filter', 'Local Log', and 'Remote Log'. The main content area is titled 'Firewall' and contains the 'Time of Day Access Filter' configuration page. This page includes a description, a time selection tool with an 'Add' button, a list of days to block, and a time range selector with 'Start' and 'End' fields and an 'Apply' button.

THOMSON
images & beyond

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Firewall

Time of Day Access Filter : This page allows configuration of web access filters to block all internet traffic to and from specific network devices based on time of day settings.

00 : 00 : 00 : 00 : 00 : 00 Add

No filters entered. ☐ Enabled Remove

Days to Block

☐ Everyday ☐ Sunday ☐ Monday ☐ Tuesday

☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Time to Block

☐ All day

Start: 12 (hour) 00 (min) AM

End: 12 (hour) 00 (min) AM

Apply

© - Thomson - 2007

Fig. 26

Chapter 2: Web Configuration

Local Log and Remote Log

The gateway builds a log of firewall blocking actions that Firewall has taken.

Using the Local Log page lets you specify an email address to which you want the gateway to email this log. You must also tell the gateway your outgoing (i.e. SMTP) email server's name, so it can direct the email to it. Enable Email Alerts has the gateway forward email notices when Firewall protection events occur. Click **E-mail Log** to immediately send the email log. Click **Clear Log** to clear the table of entries for a fresh start.

The log of these events is also visible on the screen. For each blocking event type that has taken place since the table was last cleared, the table shows Description, Count, Last Occurrence, Target, and Source.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Firewall' section is active. The 'Local Log' page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system. It includes fields for 'Contact Email Address' and 'SMTP Server Name', an 'E-mail Alerts' checkbox with an 'Enable' option, and an 'Apply' button. Below these is a table with headers: Description, Count, Last Occurrence, Target, and Source. At the bottom, there are buttons for 'E-mail Log' and 'Clear Log'.

Fig. 27

The Remote Log page allows you to specify the IP address where a SysLog server is located and select different types of firewall events that may occur. Then, each time such an event occurs, notification is automatically sent to this log server.

The screenshot shows the Thomson Gateway Administration interface, specifically the 'Remote Log' configuration page. The top navigation bar is the same as in Fig. 27. The 'Remote Log' page allows optional configuration of events to be sent to a local SysLog server. It includes a section for 'Send selected events' with checkboxes for 'Permitted Connections', 'Blocked Connections', 'Known Internet Attacks', and 'Product Configuration Events'. Below this is a field for 'to SysLog server at 192.168.0.0' and an 'Apply' button.

Fig. 28

Chapter 2: Web Configuration

Gateway – Parental Control Web Page Group

Basic

This page allows you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking Apply.

Here are some of your choices on the Parental Control page:

- ◆ Activate **Keyword Blocking** and specify some keywords in the Keyword List to cause blocking of web pages on the WAN side with the specified keyword in the content.
- ◆ Activate **Domain Blocking** and specify some Domain Names (e.g. disney.com) in the Domain List.

The screenshot displays the Thomson Gateway Administration web interface. The top navigation bar is red with the 'Administration' title. Below it, a breadcrumb trail shows 'Gateway' > 'VoIP' > 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The main content area is titled 'Parental Control' and includes a 'Basic Setup' section. This section contains two checkboxes: 'Content Filtering' (checked) and 'Keyword Blocking' (unchecked). Below these are two text input fields for 'Keyword List' and 'Blocked Domain List', each with 'Add' and 'Remove' buttons. The left sidebar features the Thomson logo and a 'Basic' tab. The bottom left corner of the interface shows the copyright notice '© - Thomson - 2007'.

Fig. 29

Chapter 2: Web Configuration

Gateway – Wireless Web Page Group

Important: Changes to the wireless web pages should be made from a PC that is hard wired to the gateway.

The Wireless web pages group enables a variety of settings that can provide secure and reliable wireless communications for even the most demanding tech-savvy user.

The TWG850 gateway offers a choice of 802.1x, WPA and WPA-PSK authentication of your PCs to the gateway, 64 and 128 bit WEP encryption of communication between the gateway and your PCs to guaranty security, and an Access Control List function that enables you to restrict wireless access to only your specific PCs.

The wireless function will probably work in your home as shipped from the factory, but without the security features activated. In addition, the factory default wireless channel setting may not provide optimum changes are recommended from the factory defaults, to secure your wireless communications and provide optimum performance.

Performance

Because your wireless communication travels through the air, the factory default wireless channel setting may not provide optimum performance in your home if you or your neighbors have other interfering 2.4GHz devices such as cordless phones. If your wireless PC is experiencing very sluggish or dramatically slower communication compared with the speed you achieve on your PC that is wired to the gateway, try changing the channel number. See the 802.11b/g Basic Web Page discussion below for details.

Authentication

Authentication enables you to restrict your gateway from communicating with any remote wireless PCs that aren't yours. The following minimum authentication-related changes to factory defaults are recommended. See the 802.11b/g Basic and Access Control Web Page discussions below for details.

Network Name (SSID) – Set a unique name you choose

Network Type – Set to Open

Access Control List – Enter your wireless PCs' MAC addresses

Chapter 2: Web Configuration

Security

Security secures or scrambles messages traveling through the air between your wireless PCs and the gateway, so they can't be observed by others. The following minimum security setting changes to factory defaults are recommended. See the 802.11b/g Security Web Page discussion below for details.

Data Encryption – Set to WEP (64-bit)

PassPhrase – Use this feature to generate security keys

802.11b/g Basic

To set the basic configuration for the wireless features, click **Basic** from the **Wireless** menu. These must match the settings you make on your wireless-equipped PC on the LAN side.

The SSID is your Network Name. Change the factory default to a name of your choice up to 32 characters long. The wireless radio in your gateway can be completely de-activated by changing Interface to Disabled. Click the Apply button to save your settings.

The Network Type control is used to hide or reveal your network name to any remote, wireless equipped PC in the area that may be scanning WiFi channels to find available WiFi networks. The gateway WiFi radio frequently transmits a beacon signal which can contain this network name (SSID). If you set Network Type to Open, your SSID is included in that beacon, and is therefore detectable by any nearby wireless equipped PCs in the area. The benefit of using Open is it can speed your WiFi setup on some PCs. If you set Network Type to Closed, your SSID is not included in the beacon. This hides your network name, but as a result may require a bit more effort on your part to set up your wireless PCs. Details of all settings on the 802.11b/g Basic Web Page are provided in Table 1.

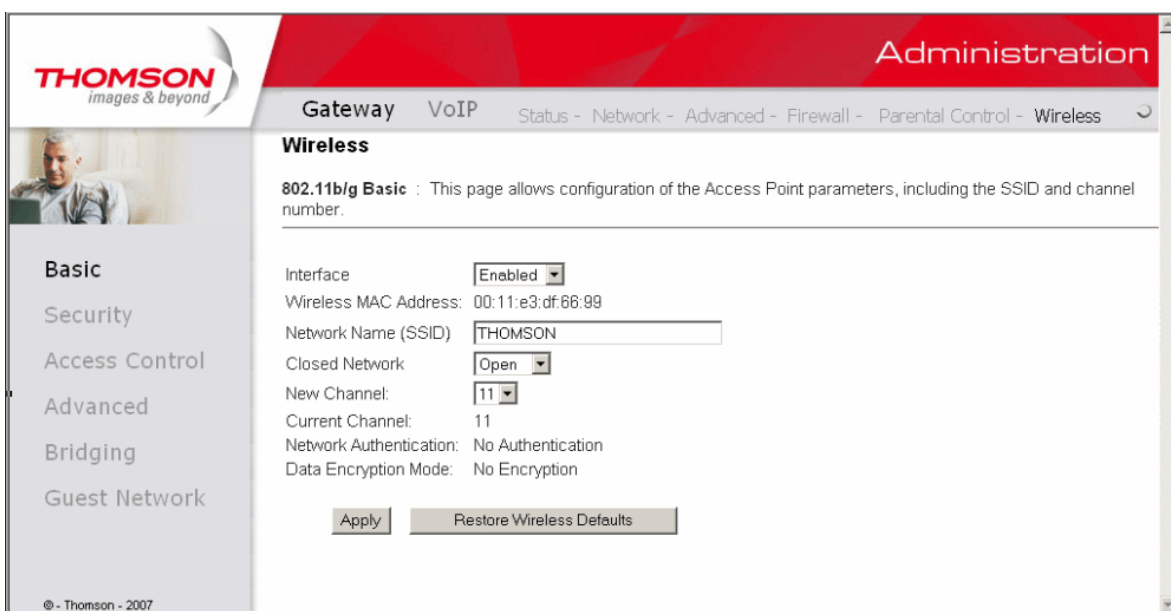


Fig. 30

Chapter 2: Web Configuration

Setting	Description	Value List or Range	Default
Network Name (SSID)	Set the Network Name (also known as SSID) of this network.	Up to 32-character string containing ASCII characters with codes between 0x20 and 0x7e	THOMSON
Network Type	Select Closed to hide the network from active scans. Select Open to reveal the network to active scans.	Open, Closed	Open
New Channel	Select a particular channel on which to operate.	1-13	11
Interface	Enable or disable the wireless interface.	Enabled, Disabled	Enabled

Table1. Basic Settings Definitions

Chapter 2: Web Configuration

802.11b/g Security

This page allows you to configure the Network Authentication. Here provides several different modes of wireless security. You will have to enter proper information according to the mode you select.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Wireless' section is active, displaying the '802.11b/g Security' configuration page. The page title is 'Wireless' and the description states: '802.11b/g Security : This page allows configuration of the WEP keys and/or passphrase.' The configuration options are as follows:

- WPA: Disabled (dropdown)
- WPA-PSK: Disabled (dropdown)
- WPA2: Disabled (dropdown)
- WPA2-PSK: Disabled (dropdown)
- WPA/WPA2 Encryption: Disabled (dropdown)
- WPA Pre-Shared Key: [Text input field]
- RADIUS Server: [Text input field, value: 0.0.0.0]
- RADIUS Port: [Text input field, value: 1812]
- RADIUS Key: [Text input field]
- Group Key Rotation Interval: [Text input field, value: 0]
- WPA/WPA2 Re-auth Interval: [Text input field, value: 3600]
- WEP Encryption: Disabled (dropdown)
- Shared Key Authentication: Optional (dropdown)
- 802.1x Authentication: Disabled (dropdown)
- Network Key 1: [Text input field]
- Network Key 2: [Text input field]
- Network Key 3: [Text input field]
- Network Key 4: [Text input field]
- Current Network Key: [Dropdown menu, value: 1]
- PassPhrase: [Text input field]
- Buttons: 'Generate WEP Keys' and 'Apply'

Fig. 31

WPA (Wi-Fi Protected Access)/WPA2:

It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than none WPA modes. **WPA2** is the second generation of **WPA** security

WPA-PSK (WPA-Pre-Shared Key) /WPA2-PSK (WPA2-Pre-Shared Key):

It is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.

WEP Encryption:

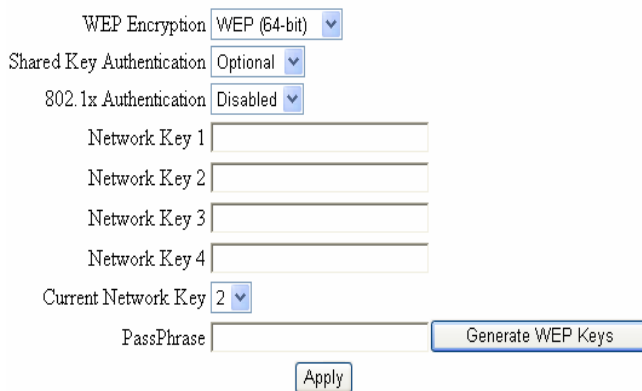
You can choose **64-bit** or **128-bit** according to your needs. If you choose **Disabled**, the Network Keys will not be shown on this page. If selected, the data is encrypted using the key before being transmitted. For example, if you set 128-bit in this field, then the receiving station must be set to use the 128 Bit Encryption, and have the same Key value too. Otherwise, it will not be able to decrypt the data.

Apply:

After proper configuration, click Apply to invoke the settings.

Chapter 2: Web Configuration

WEP Encryption



The screenshot shows the WEP Encryption configuration interface. It includes a dropdown menu for 'WEP Encryption' set to 'WEP (64-bit)', a dropdown for 'Shared Key Authentication' set to 'Optional', and a dropdown for '802.1x Authentication' set to 'Disabled'. Below these are four text input fields for 'Network Key 1', 'Network Key 2', 'Network Key 3', and 'Network Key 4'. A dropdown for 'Current Network Key' is set to '2'. There is a text input field for 'PassPhrase' and a 'Generate WEP Keys' button. At the bottom, there is an 'Apply' button.

Fig. 32

If you select WEP (64-bit or 128-bit), you can adjust the following settings–

Shared Key Authentication:

Decide whether to set the shared key **Optional** or **Required** by selecting from the drop-down menu.

Network Key 1 to 4:

The system allows you to enter four sets of the WEP key. For **64-bit** WEP mode, the key length is 5 characters or 10 hexadecimal digits. As for **128-bit** WEP mode, the key length is 13 characters or 26 hexadecimal digits.

Current Network Key:

Select one set of the network key (from 1 to 4) as the default one.

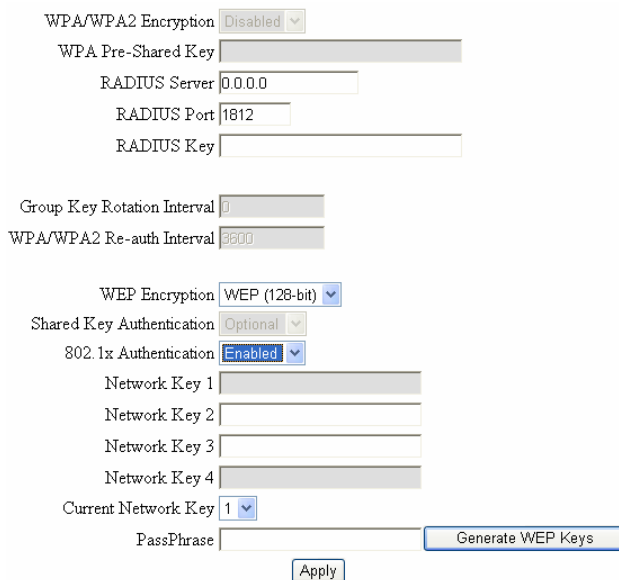
PassPhrase:

You can enter ASCII codes into this field. The range is from 8 characters to 64 characters. For **ASCII** characters, you can key in **63** characters in this field. If you want to key in **64** characters, only **hexadecimal** characters can be used.

Generate WEP Keys:

Click this button to generate the PassPhrase.

802.1x Authentication



The screenshot shows the 802.1x Authentication configuration interface. It includes a dropdown for 'WPA/WPA2 Encryption' set to 'Disabled', a text input for 'WPA Pre-Shared Key', a text input for 'RADIUS Server' set to '0.0.0.0', a text input for 'RADIUS Port' set to '1812', and a text input for 'RADIUS Key'. Below these are two text input fields for 'Group Key Rotation Interval' and 'WPA/WPA2 Re-auth Interval'. A dropdown for 'WEP Encryption' is set to 'WEP (128-bit)', a dropdown for 'Shared Key Authentication' is set to 'Optional', and a dropdown for '802.1x Authentication' is set to 'Enabled'. Below these are four text input fields for 'Network Key 1', 'Network Key 2', 'Network Key 3', and 'Network Key 4'. A dropdown for 'Current Network Key' is set to '1'. There is a text input field for 'PassPhrase' and a 'Generate WEP Keys' button. At the bottom, there is an 'Apply' button.

Fig. 33

If you enable the **802.1x authentication** function, you will have to offer the following information–

RADIUS Server:

RADIUS Server is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. Please key in the IP Address for the RADIUS Server.

RADIUS Port:

Besides the IP address of the RADIUS Server, you have to enter the port number for the server. Port 1812 is the reserved RADIUS-authentication port described in RFC 2138. Earlier AP (RADIUS clients) use port 1945. The default value will be shown on this box. You can keep and use it.

RADIUS Key:

A RADIUS Key is like a password, which is used between IAS and the specific RADIUS client to verify identity. Both IAS and the RADIUS client must be use the same RADIUS Key for successful communication to occur. Enter the RADIUS Key.

Chapter 2: Web Configuration

WPA/WPA2

WPA Enabled

WPA-PSK Disabled

WPA2 Disabled

WPA2-PSK Disabled

WPA/WPA2 Encryption TKIP

WPA Pre-Shared Key

RADIUS Server 0.0.0.0

RADIUS Port 1812

RADIUS Key

Group Key Rotation Interval 0

WPA/WPA2 Re-auth Interval 3600

Fig. 34

For the WPA/WPA2 network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, RADIUS Server, RADIUS Port, RADIUS Key, Group Key Rotation Interval, and WPA/WPA2 Re-auth Interval.

WPA/WPA2 Encryption:

There are three types that you can choose, **TKIP***, **AES****, **TKIP+AES**.

*** TKIP** takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. Then it regularly changes and rotates the encryption keys so that the same encryption key will never be used twice

**** AES** provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.

RADIUS Server/RADIUS Port/RADIUS Key:
Please refer to the previous page.

Group Key Rotation Interval:

Key in the time for the WAP group key rotation interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

WPA/WPA2 Re-auth Interval:

When a wireless client has associated with the Residential Voice Gateway for a period of time longer than the setting here, it would be disconnected and the authentication will be executed again. The default value is 3600, you may modify it.

WPA-PSK/ WPA2-PSK

WPA Disabled

WPA-PSK Enabled

WPA2 Disabled

WPA2-PSK Enabled

WPA/WPA2 Encryption TKIP

WPA Pre-Shared Key

RADIUS Server 0.0.0.0

RADIUS Port 1812

RADIUS Key

Group Key Rotation Interval 0

WPA/WPA2 Re-auth Interval 3600

Fig. 35

For the WPA-PSK/WPA2-PSK network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, WPA Pre-Shared Key, and Group key Rotation Interval.

WPA Pre-Shared Key:

Please type the key to be between 8 and 63 characters, or 64 hexadecimal digits. Only the devices with a matching key that you set here can join this network.

WPA/WPA2 Encryption & WPA Group Rekey Interval:

Please refer to the WPA/WPA2 part.

Chapter 2: Web Configuration

Access Control

This page allows you to make access control to the AP or connected clients by offering the MAC Addresses of the clients.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Wireless' section is active, displaying the '802.11b/g Access Control' configuration page. The page title is 'Wireless'. The description states: 'This page allows the configuration of the Access Control to the AP as well as status on the connected clients.' The 'MAC Restrict Mode' is set to 'Disabled'. Below this, there are eight input fields for 'MAC Addresses' arranged in two columns of four. An 'Apply' button is located below the input fields. At the bottom, the 'Connected Clients' section shows a table with headers: 'MAC Address', 'Age(s)', 'RSSI(dBm)', 'Type', 'IP Addr', and 'Host Name'. The table content indicates 'No wireless clients are connected.' The Thomson logo and '© - Thomson - 2007' are visible in the bottom left corner.

Fig. 36

MAC Restrict Mode:

Click **Disabled** to welcome all of the clients on the network; select **Allow** to permit only the clients on the list to access the cable modem; or choose **Deny** to prevent the clients on the list to access this device.

MAC Address:

Your Gateway identifies wireless PCs by their WiFi MAC Address. This address consists of a string of 6 pairs of numbers 0–9 and letters A–F, such as 00 90 4B F0 FF 50. It is usually printed on the WiFi card of the device (e.g. the PCMCIA card in a laptop). It can also be determined from a Windows DOS prompt as explained below.

Enter the MAC addresses of the connected clients into the fields, and then click Apply to add them to the list for access control.

Apply:

After proper configuration, click Apply to invoke the settings.

Connected Clients:

The information of currently connected clients will be displayed here.

Chapter 2: Web Configuration

802.11b/g Advanced

This page allows you to configure some advanced settings. The factory default values should provide good results in most cases. We don't recommend you change these settings unless you have technical knowledge of 802.11b wireless technology.

For expert users, details of all settings on this web page are provided below.

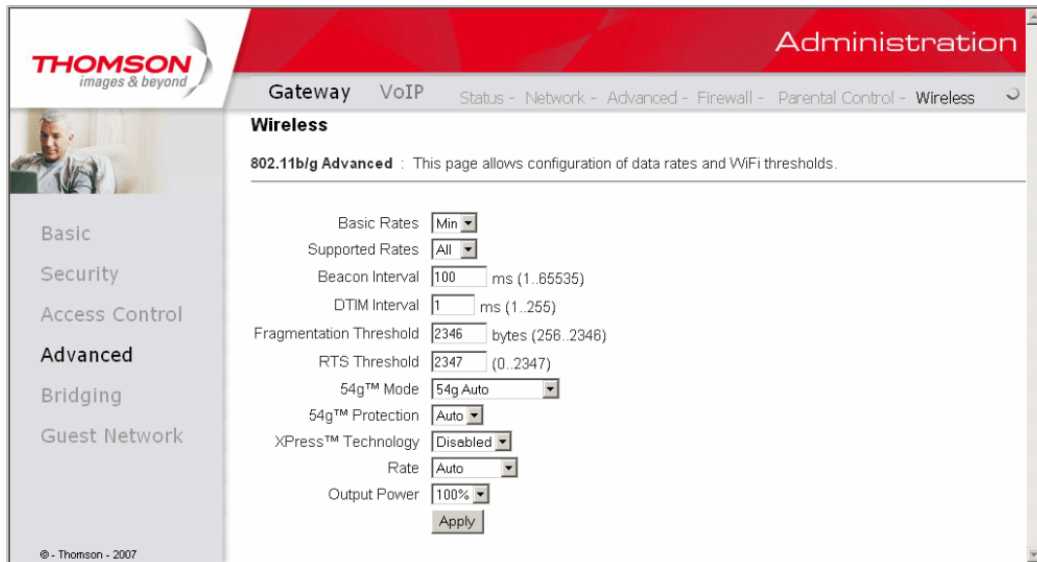


Fig. 37

Beacon Interval:

Set the period of beacon transmissions to allow mobile stations to locate and identify a BSS. The measure unit is "time units" (TU) of 1024 microseconds. (Value range: 1~65535)

DTIM Interval:

The value you set here is used to inform mobile stations when multicast frames that have been buffered at the Residential Voice Gateway will be delivered and how often that delivery occurs. (Value range: 1~255)

Fragmentation Threshold:

Set the number of the fragmenting frames to make the data to be delivered without errors induced by the interference. Frames longer than the value you set here are fragmented before the initial transmission into fragments no longer than the value of the threshold. (Value range: 256~ 2346)

RTS Threshold:

Set the value for sending a request to the destination. All the frames of a length greater than the threshold that you set here will be sent with the four-way frame exchange. And, a length less than or equal to the value that you set will not be proceeded by RTS. (Value range: 0~ 2347)

54g™ Network Mode:

There are three modes for you to choose, please check the specification of your wireless card and choose a proper setting.

54g™ Protection:

Select **Auto** to turn on the 54g™ protection; select **Off** to turn down the protection.

Xpress™ Technology:

When Xpress is turned on, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by **up to 27%** in 802.11g-only networks, and **up to 75%** in mixed networks comprised of 802.11g and 802.11b standard equipment.

Chapter 2: Web Configuration

Rate:

It decides the speed of data transmission. There are several rates provided here for you to choose. Choose any one of it according to your needs by using the drop-down menu.

Output Power:

This setting decides the output power of this device. You may use it to economize on electricity by selecting lower percentage of power output.

Chapter 2: Web Configuration

Bridging

The Bridging page provides a location where settings can be adjusted related to the wireless WDS (**Wireless Distribution System**) feature.

WDS is a system that enables the interconnection of access points wirelessly. It may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging).

The wireless gateway can be placed in a mode that allows the gateway to communicate with other “extender” wireless access points either exclusively or mixed with communications to local PCs. Use this page to designate the Remote Bridges the gateway is allowed to communicate with, and to select the Wireless Bridging mode.

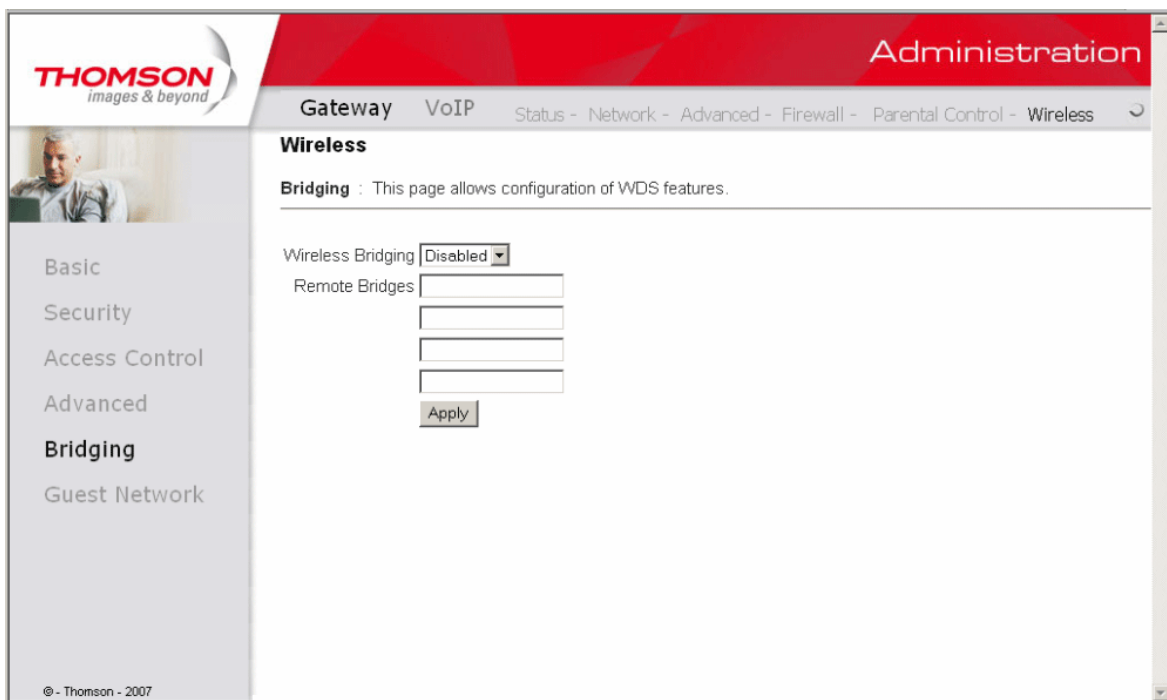


Fig. 38

Wireless Bridging:

Choose **Disabled** to shutdown this function; select **Enabled** to turn on the function of WDS.

Remote Bridges:

Enter the MAC Addresses of the remote Bridges to relay the signals for each other.

Apply:

After proper configuration, click Apply to invoke the settings.

Chapter 2: Web Configuration

Guest Network

This page allows you to configure a guest network.

You can refer to the details described in previous sections to make the WiFi security settings and guest LAN settings.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Wireless' tab is selected. The main content area is titled 'Wireless' and contains the '802.11b/g Guest Network' configuration page. The page is divided into two main sections: 'Guest WiFi Security Settings' and 'Guest LAN Settings'. The 'Guest WiFi Security Settings' section includes fields for 'Guest Network' (Disabled), 'Guest Network Name (SSID)' (BROADCOM_GUEST), 'Use Multiple BSSIDs' (Enabled), 'WPA' (Disabled), 'WPA-PSK' (Disabled), 'WPA2' (Disabled), 'WPA2-PSK' (Disabled), 'WPAWPA2 Encryption' (Disabled), 'WPA Pre-Shared Key', 'RADIUS Server' (0.0.0.0), 'RADIUS Port' (1812), 'RADIUS Key', 'Group Key Rotation Interval' (0), and 'WPAWPA2 Re-auth Interval' (3600). The 'Guest LAN Settings' section includes fields for 'DHCP Server' (Disabled), 'IP Address' (192.168.2.1), 'Subnet Mask' (255.255.255.0), 'Lease Pool Start' (192.168.2.10), 'Lease Pool End' (192.168.2.99), and 'Lease Time' (86400). There are 'Apply' and 'Restore Guest Network Defaults' buttons. The bottom of the page has a 'Generate WEP Keys' button and an 'Apply' button. The left sidebar contains a menu with 'Basic', 'Security', 'Access Control', 'Advanced', 'Bridging', and 'Guest Network' (selected). The Thomson logo and 'images & beyond' tagline are in the top left corner. The copyright notice '© - Thomson - 2007' is at the bottom left.

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Wireless

802.11b/g Guest Network : This page allows configuration of a guest network.

Guest WiFi Security Settings

Guest Network

Guest Network Name (SSID)

Use Multiple BSSIDs

WPA

WPA-PSK

WPA2

WPA2-PSK

WPAWPA2 Encryption

WPA Pre-Shared Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPAWPA2 Re-auth Interval

WE P Encryption

Shared Key Authentication

802.1x Authentication

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

Guest LAN Settings

DHCP Server

IP Address

Subnet Mask

Lease Pool Start

Lease Pool End

Lease Time

© - Thomson - 2007

Fig. 39

Chapter 2: Web Configuration

VoIP – Basic Web Page Group

Basic LAN

This page displays the basic LAN status of this device, including the downstream and upstream status, device information, and interface parameters. You can select specific interface from the Interface Name drop-down menu.

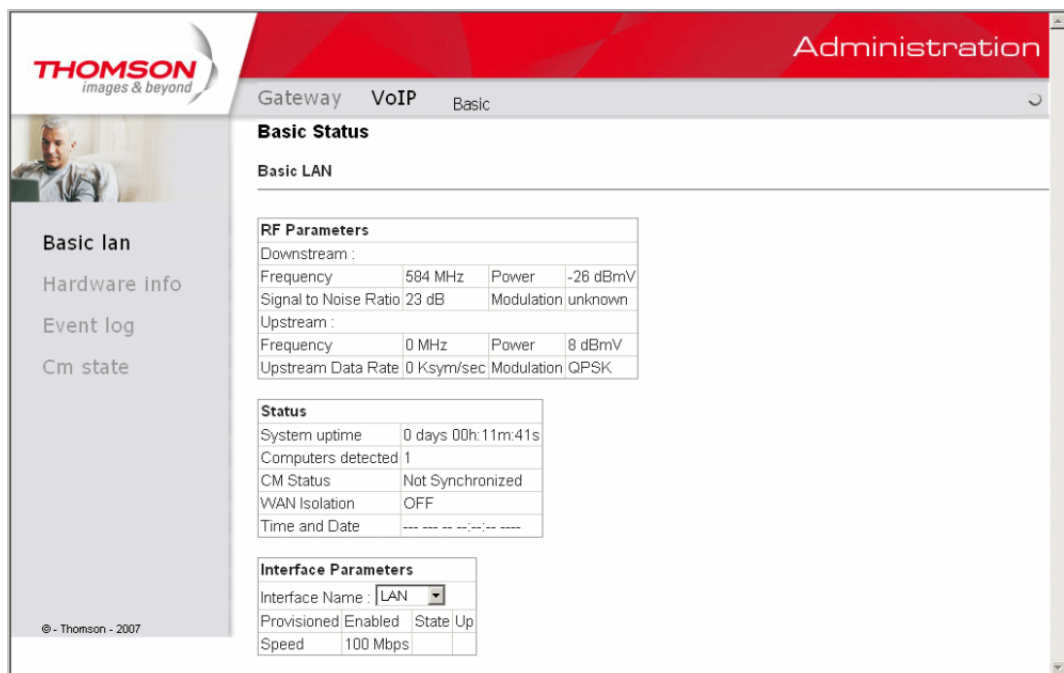


Fig. 40

Hardware Info

The hardware Info is displayed on this page.

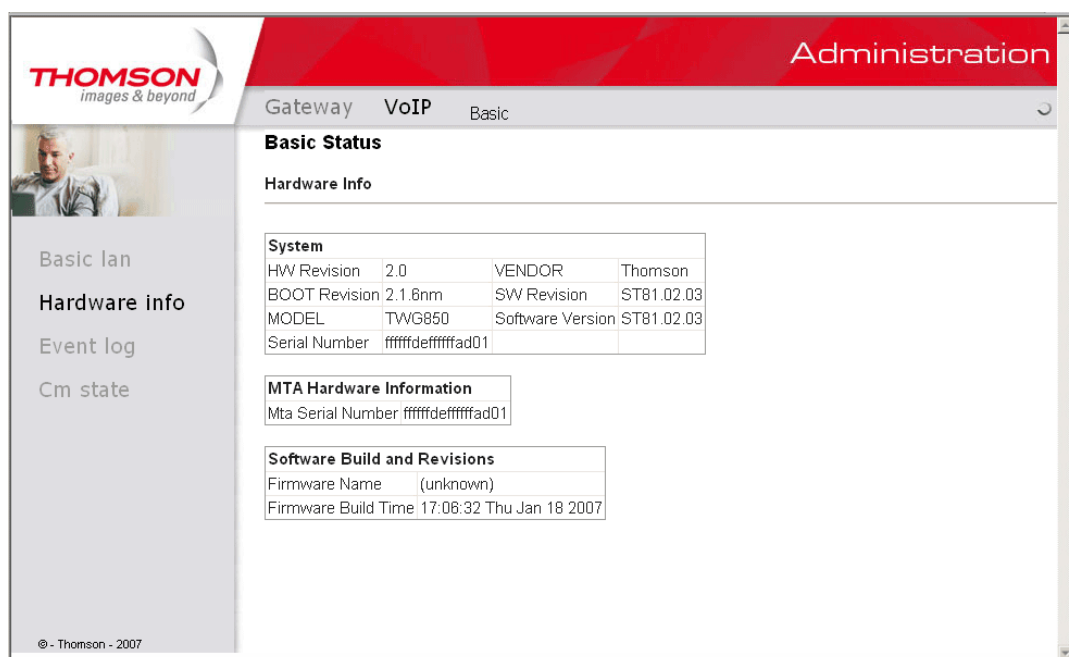
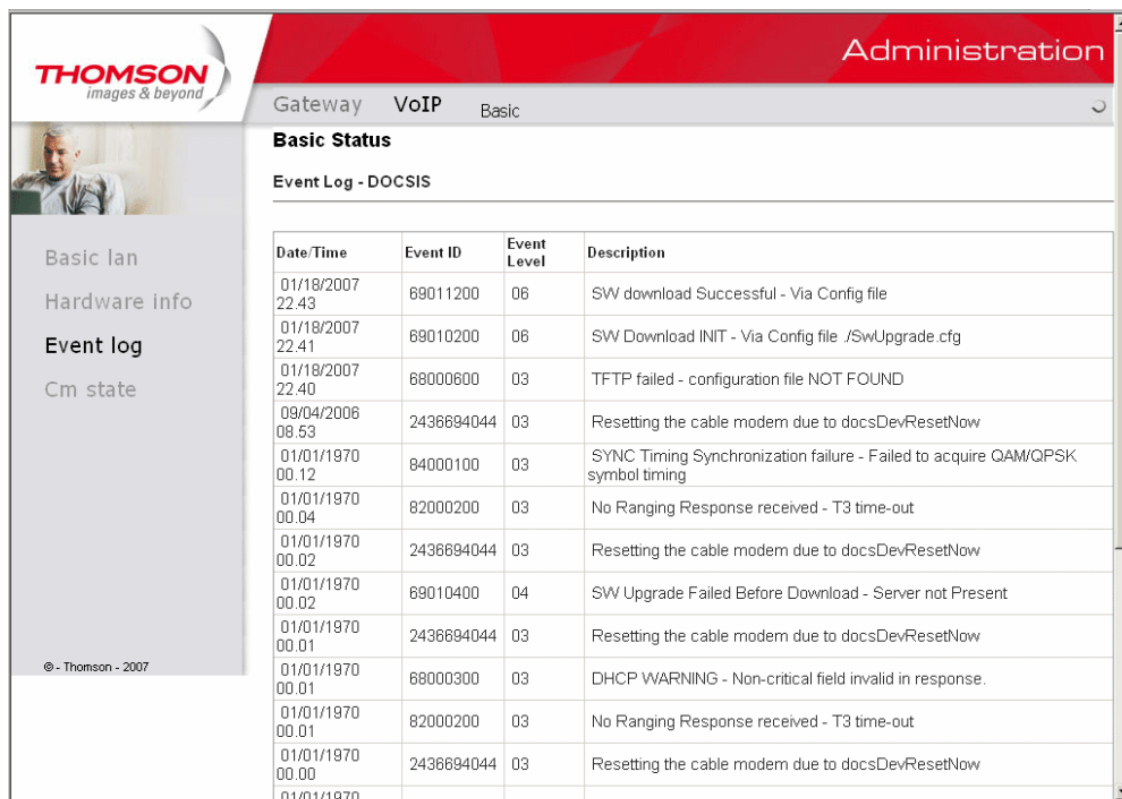


Fig. 41

Chapter 2: Web Configuration

Event Log

The event logs are displayed on this web page. You can check them whenever you need.



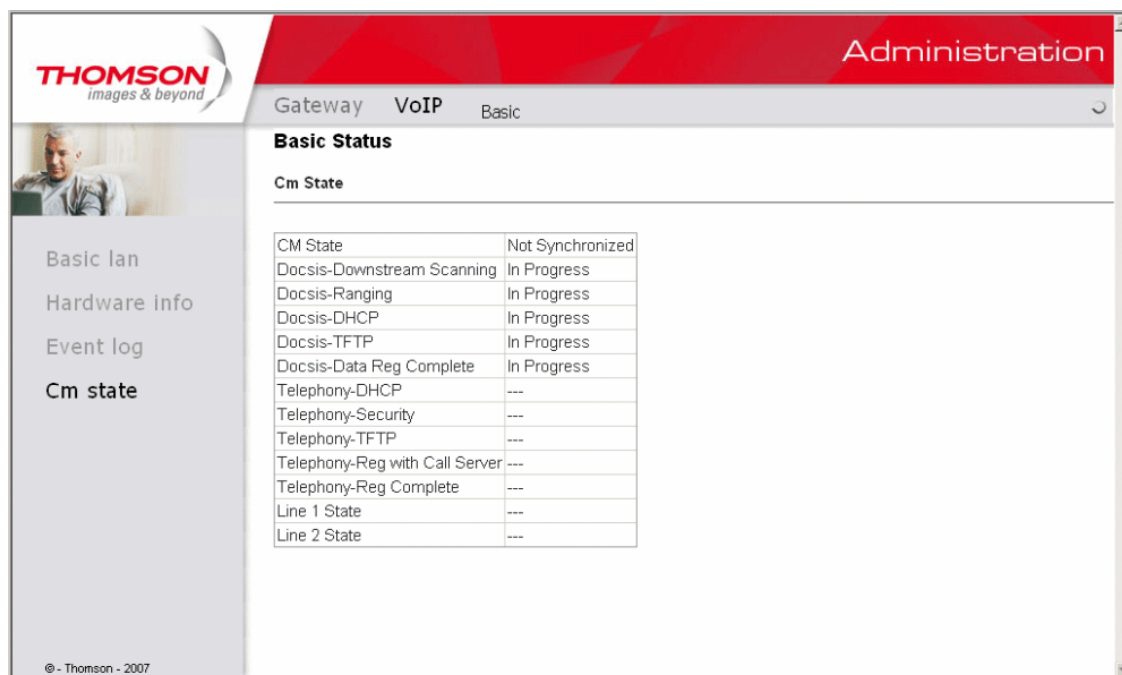
The screenshot shows the Thomson Administration web interface. The top navigation bar includes the Thomson logo and the word "Administration". Below this, there are tabs for "Gateway", "VoIP", and "Basic". The "Basic" tab is selected, and the "Basic Status" section is active. The "Event Log - DOCSIS" page displays a table of events.

Date/Time	Event ID	Event Level	Description
01/18/2007 22.43	69011200	06	SW download Successful - Via Config file
01/18/2007 22.41	69010200	06	SW Download INIT - Via Config file /SwUpgrade.cfg
01/18/2007 22.40	68000600	03	TFTP failed - configuration file NOT FOUND
09/04/2006 08.53	2436694044	03	Resetting the cable modem due to docsDevResetNow
01/01/1970 00.12	84000100	03	SYNC Timing Synchronization failure - Failed to acquire QAM/QPSK symbol timing
01/01/1970 00.04	82000200	03	No Ranging Response received - T3 time-out
01/01/1970 00.02	2436694044	03	Resetting the cable modem due to docsDevResetNow
01/01/1970 00.02	69010400	04	SW Upgrade Failed Before Download - Server not Present
01/01/1970 00.01	2436694044	03	Resetting the cable modem due to docsDevResetNow
01/01/1970 00.01	68000300	03	DHCP WARNING - Non-critical field invalid in response.
01/01/1970 00.01	82000200	03	No Ranging Response received - T3 time-out
01/01/1970 00.00	2436694044	03	Resetting the cable modem due to docsDevResetNow
01/01/1970			

Fig. 42

CM State

This page shows the current state of the cable modem.



The screenshot shows the Thomson Administration web interface. The top navigation bar includes the Thomson logo and the word "Administration". Below this, there are tabs for "Gateway", "VoIP", and "Basic". The "Basic" tab is selected, and the "Basic Status" section is active. The "Cm State" page displays a table of the current state of the cable modem.

CM State	Not Synchronized
Docsis-Downstream Scanning	In Progress
Docsis-Ranging	In Progress
Docsis-DHCP	In Progress
Docsis-TFTP	In Progress
Docsis-Data Reg Complete	In Progress
Telephony-DHCP	---
Telephony-Security	---
Telephony-TFTP	---
Telephony-Reg with Call Server	---
Telephony-Reg Complete	---
Line 1 State	---
Line 2 State	---

Fig. 43

Chapter 3: Additional Information

Chapter 3: Additional Information

Frequently Asked Questions

Q. What if I don't subscribe to cable TV?

A. If cable TV is available in your area, data and voice service may be made available with or without cable TV service. Contact your local cable company for complete information on cable services, including high-speed internet access.

Q. How do I get the system installed?

A. Professional installation from your cable provider is strongly recommended. They will ensure proper cable connection to the modem and your computer. However, your retailer may have offered a self installation kit, including the necessary software to communicate with your cable ISP.

Q. Once my Residential Voice Gateway is connected, how do I get access to the Internet?

A. Your local cable company provides your internet service*, offering a wide range of services including email, chat, and news and information services, and a connection to the World Wide Web.

Q. Can I watch TV, surf the Internet, and talk to my friends through the Residential Voice Gateway at the same time?

A. Absolutely!

Q. What do you mean by "Broadband?"

A. Simply put, it means you'll be getting information through a "bigger pipe," with more bandwidth, than a standard phone line can offer. A wider, "broader" band means more information, more quickly.

Q. What is EURO-DOCSIS/DOCSIS and what does it mean?

A. "Data over Cable Service Interface Specifications" is the industry standard that most cable companies are adopting as they upgrade their systems. Should you ever decide to move, the Cable Modem will work with all upgraded cable systems that are EURO-DOCSIS/DOCSIS-compliant.

Chapter 3: Additional Information

Q. What is Euro-PacketCable/PacketCable and what does it mean?

A. Like DOCSIS, Euro-PacketCable/PacketCable is the industry standard for telephony services that most cable companies are adopting as they upgrade their systems. Should you ever decide to move, the Residential Voice Gateway will work with all upgraded cable systems that are Euro-PacketCable/PacketCable-compliant.

Q. What is SecureEasySetup and what does it mean?

A. The software radically simplifies Wi-Fi® wireless LAN configuration, allowing even first-time Wi-Fi users to setup and secure their wireless networks with the push of a button. Whereas a typical Wi-Fi installation requires a user to manually configure several technical settings on each wireless device, SecureEasySetup simply requires a user to push a button on the wireless router/Access Point, and a corresponding button on the PC or other client device. This automates the connection process and activates Wi-Fi Protected Access (WPA), the strongest security standard available to protect home and small business wireless networks from unauthorized use.

Q. What is Xpress Technology and what does it mean?

A. It is one of the popular performance-enhancing WiFi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks. When Xpress is turned on, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by **up to 27%** in 802.11g-only networks, and **up to 75%** in mixed networks comprised of 802.11g and 802.11b standard equipment. The technology achieves higher throughput by re-packaging data, reducing the number of overhead control packets, so that more useful data can be sent during a given amount of time.

* Monthly subscription fee applies.

Chapter 3: Additional Information

General Troubleshooting

You can correct most problems you have with your product by consulting the troubleshooting list that follows.

I can't access the internet.

- Check all of the connections to your Residential Voice Gateway.
- Your Ethernet card or USB port may not be working. Check each product's documentation for more information.
- The Network Properties of your operating system may not be installed correctly or the settings may be incorrect. Check with your ISP or cable company.

All of the lights are flashing in sequence.

- This means the Residential Voice Gateway is automatically updating its system software. Please wait for the lights to stop flashing. The updating process typically lasts less than one minute.
- Do not remove the power supply or reset the Residential Voice Gateway during this process.

I can't get the modem to establish an Ethernet connection.

- Even new computers don't always have Ethernet capabilities – be sure to verify that your computer has a properly installed Ethernet card and the driver software to support it.
- Check to see that you are using the right type of Ethernet cable.

The modem won't register a cable connection.

- If the modem is in Initialization Mode, the INTERNET light will be flashing. Call your Cable Company if it has not completed this 5-step process within 30 minutes, and note which step it is getting stuck on. (See page 5 for details.)
- The modem should work with a standard RG-6 coaxial cable, but if you're using a cable other than the one your Cable Company recommends, or if the terminal connections are loose, it may not work. Check with your Cable Company to determine whether you're using the correct cable.
- If you subscribe to video service over cable, the cable signal may not be reaching the modem. Confirm that good quality cable television pictures are available to the coaxial connector you are using by connecting a television to it. If your cable outlet is "dead", call your Cable Company.

Chapter 3: Additional Information

- Verify that the Cable Modem service is DOCSIS-compliant and PacketCable-compliant by calling your cable provider.

I don't hear a dial tone when I use a telephone.

- Telephone service is not activated. If the rightmost light on the Residential Voice Gateway stays on while others flash, check with your TSP or cable company.
- If the Residential Voice Gateway is connected to existing house telephone wiring, make sure that another telephone service is not connected. The other service can normally be disconnected at the Network Interface Device located on the outside of the house.
- If using the second line on a two-line telephone, use a 2-line to 1-line adapter cable.

For more Usage and Troubleshooting Tips use the web site links provided on the CD-ROM:

<http://www.cable-modem.rca.com/help>

Chapter 3: Additional Information

FCC Declaration of Conformity and Industry Canada Information

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.

Trade Name:	Thomson Model: TWG850
Equipment Classification:	Computing Device Accessory
Responsible Party:	Thomson Inc. 10330 N. Meridian Street Indianapolis, IN 46290 Telephone 317-415-4151

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and 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 this 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.

FCC regulations state that unauthorized changes or modifications to this equipment may void the user's authority to operate it.

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

Chapter 3: Additional Information

Service Information

If you purchased or leased your Residential Voice Gateway directly from your cable company, then warranty service for the Digital Cable Modem may be provided through your cable provider or its authorized representative. For information on 1) Ordering Service, 2) Obtaining Customer Support, or 3) Additional Service Information, please contact your cable company. If you purchased your Residential Voice Gateway from a retailer, see the enclosed warranty card.

Chapter 3: Additional Information

Glossary

10BaseT – Unshielded, twisted pair cable with an RJ-45 connector, used with Ethernet LAN (Local Area Network). “10” indicates speed (10 Mbps), “Base” refers to baseband technology, and “T” means twisted pair cable.

Authentication - The process of verifying the identity of an entity on a network.

DHCP (Dynamic Host Control Protocol) – A protocol which allows a server to dynamically assign IP addresses to workstations on the fly.

Ethernet card – A plug-in circuit board installed in an expansion slot of a personal computer. The Ethernet card (sometimes called a Network Interface Card or NIC) takes parallel data from the computer, converts it to serial data, puts it into a packet format, and sends it over the 10BaseT or 100BaseT LAN cable.

EURO-DOCSIS/ DOCSIS (Data Over Cable Service Interface Specifications) – A project with the objective of developing a set of necessary specifications and operations support interface specifications for Cable Modems and associated equipment.

F Connector – A type of coaxial connector, labeled CABLE IN on the rear of the Residential Voice Gateway, that connects the modem to the cable system.

HTTP (HyperText Transfer Protocol) – Invisible to the user, HTTP is used by servers and clients to communicate and display information on a client browser.

Hub – A device used to connect multiple computers to the Residential Voice Gateway.

IP Address – A unique, 32-bit address assigned to every device in a network. An IP (Internet Protocol) address has two parts: a network address and a host address. This modem receives a new IP address from your cable operator via DHCP each time it goes through Initialization Mode.

Key exchange - The swapping of mathematical values between entities on a network in order to allow encrypted communication between them.

MAC Address – The permanent “identity” for a device programmed into the Media Access Control layer in the network architecture during the modem’s manufacture.

Network Driver – A file that is loaded on the computer to allow the computer to recognize the Ethernet card or USB port.

NID - Network Interface Device, the interconnection between the internal house telephone wiring and a conventional telephone service provider’s equipment. These wiring connections are normally housed in a small plastic box located on an outer wall of the house. It is the legal demarcation between the subscriber’s property and the service provider’s property.

Euro-PacketCable/ PacketCable – A project with the objective of developing a set of necessary telephony specifications and operations support interface specifications for Residential Voice Gateways and associated equipment used over the DOCSIS-based cable network.

Chapter 3: Additional Information

PSTN (Public Switched Telephone Network) – The worldwide voice telephone network which provides dial tone, ringing, full-duplex voice band audio and optional services using standard telephones.

Provisioning - The process of enabling the Media Terminal Adapter (MTA) to register and provide services over the network.

SecureEasySetup – The software radically simplifies Wi-Fi® wireless LAN configuration, allowing even first-time Wi-Fi users to setup and secure their wireless networks with the push of a button. Whereas a typical Wi-Fi installation requires a user to manually configure several technical settings on each wireless device, SecureEasySetup simply requires a user to push a button on the wireless router/ Access Point, and a corresponding button on the PC or other client device. This automates the connection process and activates Wi-Fi Protected Access (WPA), the strongest security standard available to protect home and small business wireless networks from unauthorized use.

TCP/IP (Transmission Control Protocol/Internet Protocol) – A networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TFTP - Trivial File Transfer Protocol, the system by which the Media Terminal Adapter's configuration data file is downloaded.

TSP - Telephony Service Provider, an organization that provides telephone services such as dial tone, local service, long distance, billing and records, and maintenance.

Universal Serial Bus (USB) – USB is a “plug-and-play” interface between a computer and add-on devices, such as a Residential Voice Gateway.

Xpress Technology - One of the popular performance-enhancing WiFi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks.

Please do not send any products to the Indianapolis address listed in this manual or on the carton. This will only add delays in service for your product.

Thomson Inc.

10330 North Meridian Street

Indianapolis, IN 46290

For more information

Thomson | 46, quai Alphonse Le Gallo | 92100 Boulogne-Billancourt | France
Tel. : 33 (0) 1 41 86 50 00 | Fax : 33 (0) 1 41 86 56 59 | www.thomson-broadband.com

© 2007 Thomson Inc. - Trademark(s) * Registered \ - Marca(s) Registrada(s) \
Photos and features subject to change without notice.
Illustration of product finish may vary from actual color.

