DWG855 - Residential Voice Gateway

User manual

RCA by THOMSON

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.

Illustrations contained in this document are for representation only.

PacketCable and DOCSIS compliant

This product was designed according to Data over Cable Service Interface Specifications and PacketCable Voice Over IP Cable Telephony Specifications.
It will operate on any DOCSIS-compliant Hybrid Fiber Coax (HFC) cable system and offers DOCSIS and PacketCable Baseline Privacy to promote secure internet transactions and PC-secure telephone service.

Operating Information

Operating Temperature: 0˚ - 40˚ C (32˚ - 104˚ F)
Storage Temperature: -30˚ to 65˚ C

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

Product Registration

Please fill out the product registration card (packed separately) and return it immediately, or register on-line at rca.com. Registering allows us to contact you if needed.

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

Table of Contents

Table of Contents

Chapter 1: Connections and Setup

Introduction

Residential Voice Gateway Features

- Support Multiple Provisioning Mode
- 4 Standard RJ-45 connectors for 10/100BaseT Ethernet with auto-negotiation and MDIS functions
- Two RJ-11 Foreign Exchange Station (FXS) ports for IP telephony
- IEEE 802.11b/g Wireless interface
- 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, BV32 and SIP
- 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.

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

Chapter 1: Connections and Setup

- Links to RCA or Thomson web sites

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

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/Vista, 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 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.	
Software	• 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.

Wall Mounting

The number of the screw: 2 pcs

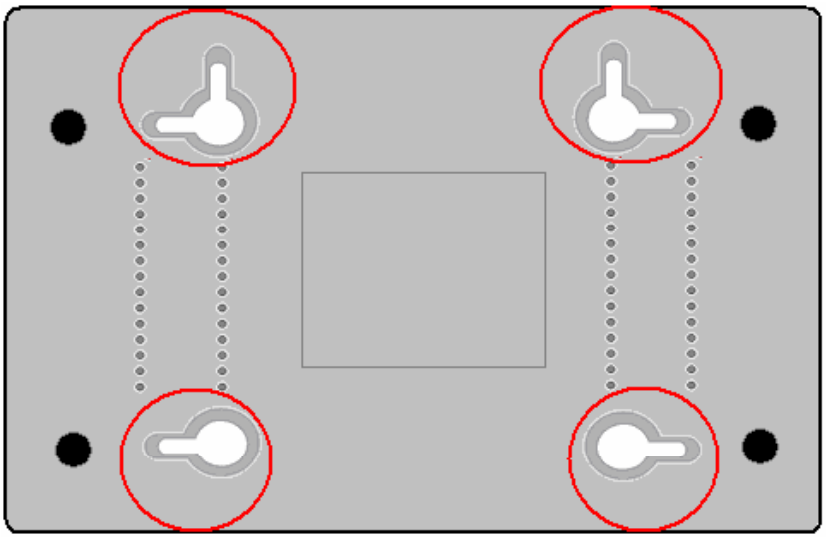
Direction for wall mounting: LED panel upward.

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:

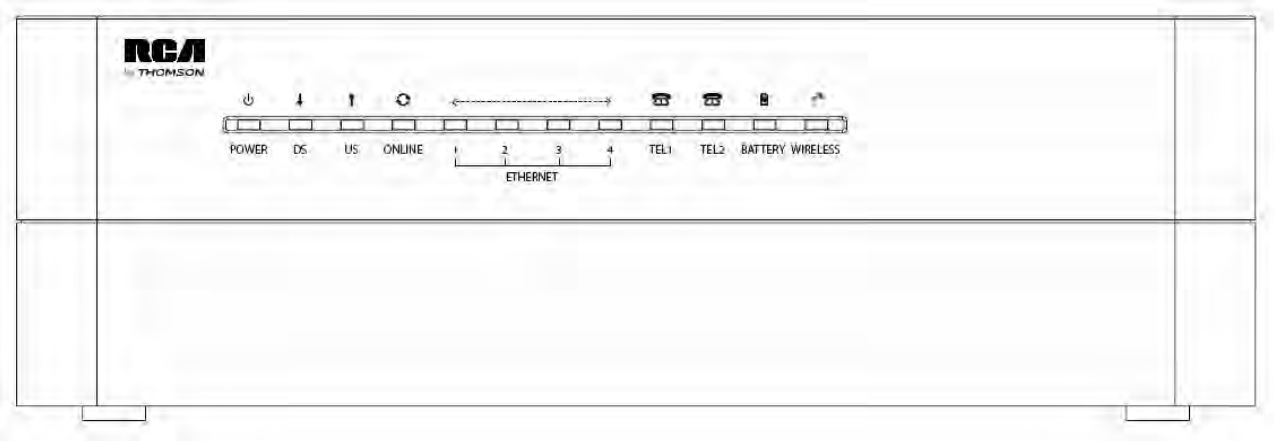
1. Ensure that the wall you use is smooth, flat, dry and sturdy and use the 4 screw holes which are 101.6 mm apart from each other.
2. Fix the screws into wall, leaving their heads 3 mm (0.12 inch) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw heads. When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

Chapter 1: Connections and Setup

Residential Voice Gateway DWG855 Overview

Front Panel

The following illustration shows the front panel of the DWG855 machine:



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

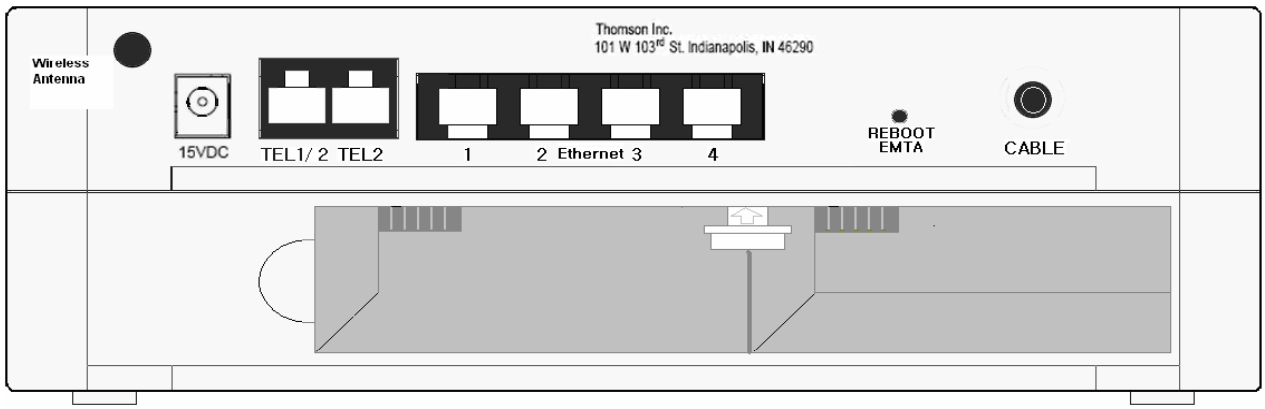
	Power	Internet			Ethernet				Tel 1	Tel 2	Battery	Wireless	Description
		DS	US	Online	1	2	3	4					
Boot-up Operation	ON	ON	ON	ON	ON	ON	ON	ON	ON	ON	X	ON	Power on 0.25 sec
	ON	0.25 second											
	ON	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	From power ON to system initialization complete
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Following system initialization complete to (before) DS scanning
		1 second											
DOCSIS Start-up Operation	ON	FLASH	OFF	OFF	X	X	X	X	X	X	X	X	During DS scanning and acquiring SYNC
	ON	ON	FLASH	OFF	X	X	X	X	X	X	X	X	From SYNC completed, receiving UCD to ranging completed
	ON	ON	ON	FLASH	X	X	X	X	X	X	X	X	During DHCP, configuration file download, registration, and Baseline Privacy initialization
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Operational (NACO=ON)
	ON	FLASH	FLASH	OFF	X	X	X	X	X	X	X	X	Operational(NACO=OFF)
MTA initialization	ON	ON	ON	ON	X	X	X	X	FLASH	OFF	OFF	X	MTA DHCP
	ON	ON	ON	ON	X	X	X	X	OFF	FLASH	OFF	X	MTA SNMP/TFTP
	ON	ON	ON	ON	X	X	X	X	FLASH	FLASH	OFF	X	RSIP
CPE Operation	ON	X	X	X	OFF ON FLASH ON	OFF ON FLASH ON	OFF ON FLASH ON	OFF ON FLASH ON	X	X	X	X	No Ethernet Link Ethernet Link TX/RX Ethernet Traffic Ethernet Collision

Illustrations contained in this document are for representation only.

	Power	Internet			Ethernet				Tel 1	Tel 2	Battery	Wireless	Description
		DS	US	Online	1	2	3	4					
CPE Operation	ON	X	X	X	X	X	X	X	X	X	X	OFF ON FLASH ON	No Wireless Link Wireless Link TX/RX Wireless Traffic Wireless init fail
AC Good Battery Good	ON	<CM Normal Operation>							ON	ON	ON	<CM Normal Operation>	Both Lines On-Hook
	ON								FLASH	ON			Tel1 Off-hook, Tel2 On-hook
	ON								ON	FLASH			Tel1 On-hook, Tel2 Off-hook
	ON								FLASH	FLASH			Both Lines Off-Hook
AC Good Battery Low	ON								ON	ON	FLASH		Both Lines On-Hook
	ON								FLASH	ON			Tel1 Off-hook, Tel2 On-hook
	ON								ON	FLASH			Tel1 On-hook, Tel2 Off-hook
	ON								FLASH	FLASH			Both Lines Off-Hook
AC Good Battery Bad	ON								ON	ON	OFF		Both Lines On-Hook
	ON								FLASH	ON			Tel1 Off-hook, Tel2 On-hook
	ON								ON	FLASH			Tel1 On-hook, Tel2 Off-hook
	ON								FLASH	FLASH			Both Lines Off-Hook
AC Fail Battery Good	FLASH	OFF							ON	ON	OFF	OFF	Both Lines On-Hook
									FLASH	ON			Tel1 Off-hook, Tel2 On-hook
									ON	FLASH			Tel1 On-hook, Tel2 Off-hook
									FLASH	FLASH			Both Lines Off-Hook
AC Fail Battery Low									ON	ON	FLASH		Both Lines On-Hook
									FLASH	ON			Tel1 Off-hook, Tel2 On-hook
									ON	FLASH			Tel1 On-hook, Tel2 Off-hook
									FLASH	FLASH			Both Lines Off-Hook
AC Fail Battery Bad	< All LEDs may be unlit due to lack of battery power>										OFF	< All LEDs may be unlit due to lack of battery power>	Both Lines On-Hook
													Tel1 Off-hook, Tel2 On-hook
													Tel1 On-hook, Tel2 Off-hook
													Both Lines Off-Hook
SW Download Operation	ON	FLASH	FLASH	ON	X	X	X	X	X	X	X	X	A software download and while updating the FLASH memory

Chapter 1: Connections and Setup

Rear Panel

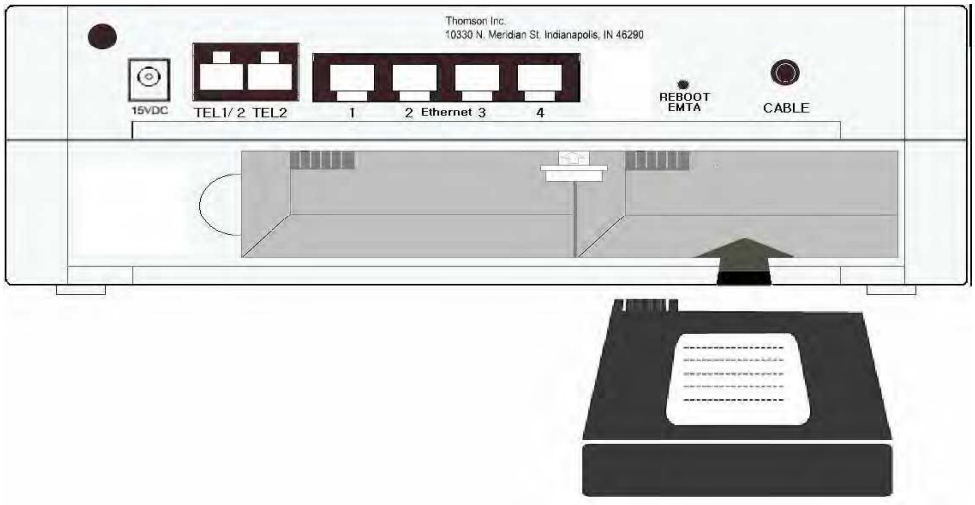


TEL1 & TEL2	Telephony RJ-11 connector
ETHERNET 1-4:	Ethernet 10/100BaseT RJ-45 connector
REBOOT EMTA:	Reboot this Residential Voice Gateway
CABLE:	F-Connector
15VDC:	Power connector

Installing the Battery

This section provides information on installing batteries into the modem. Follow the steps below:

1. Ensure the power cord is unplugged.
2. Remove the battery cover on the rear panel. There are two battery compartments. You may install a single battery into either compartment.



Illustrations contained in this document are for representation only.

Flank Panel

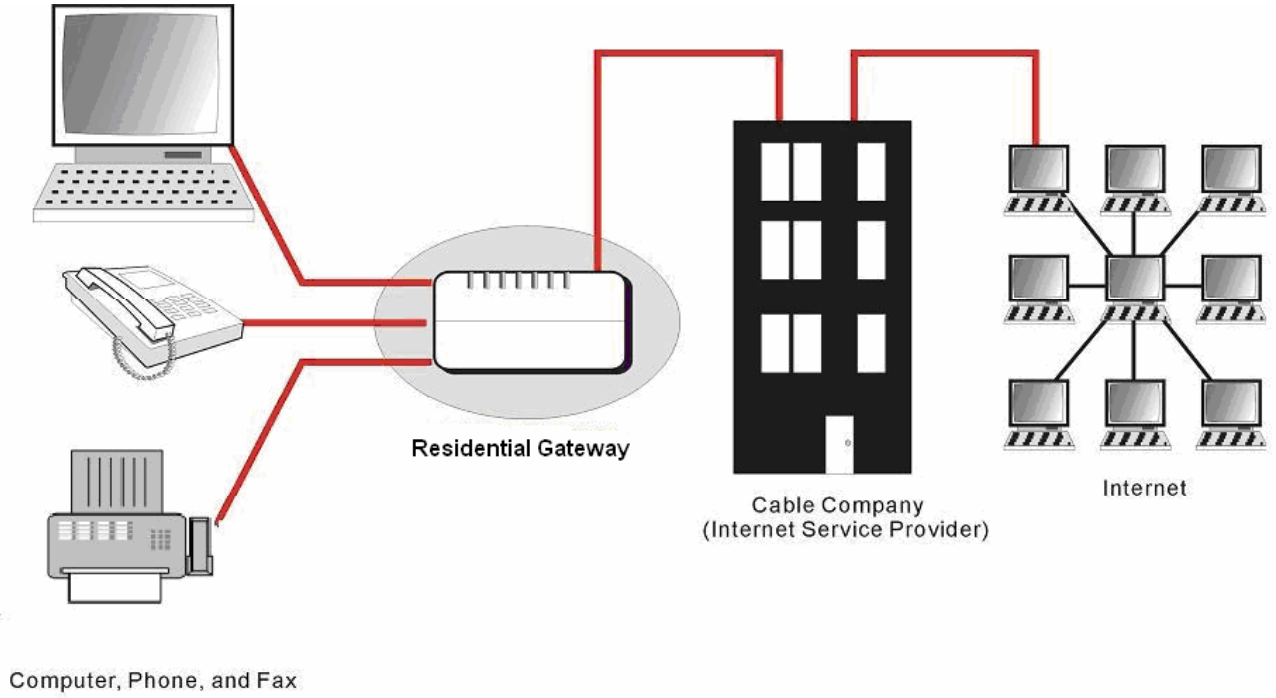
- WPS: WiFi Protected Setup

Illustrations contained in this document are for representation only.

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 wired and wireless 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 head end 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 DOCSIS-compliant and 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).

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

Please verify the following with the cable company

- The cable service to your home supports 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 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.

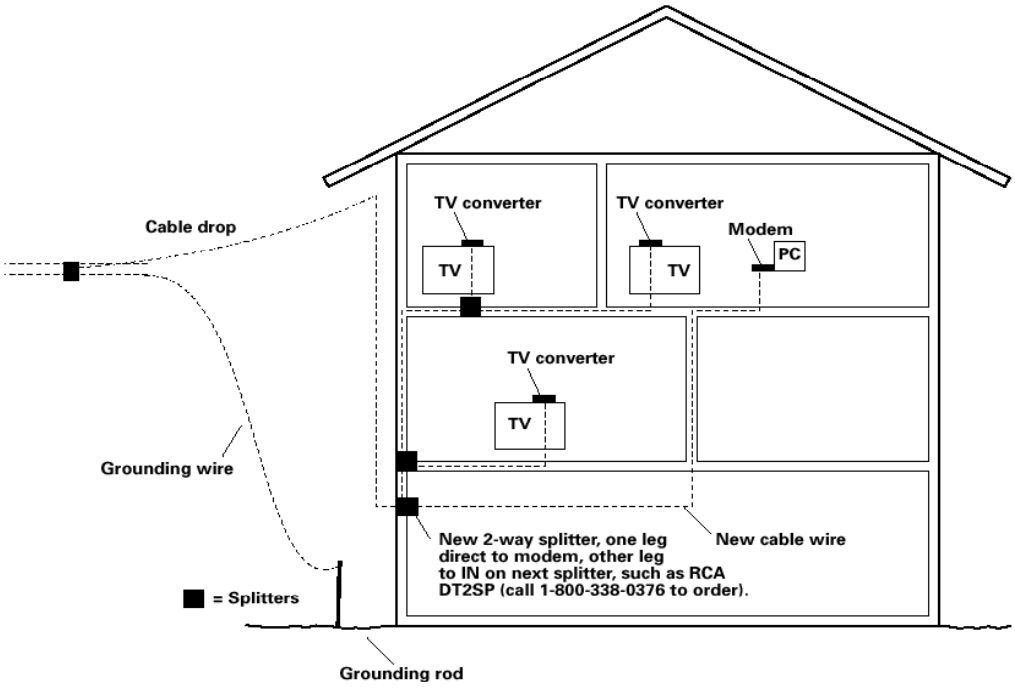


Fig. 1: Basic Home Wiring

Important Connection Information

The Residential Voice Gateway supports Telephone and Ethernet connections simultaneously.
Below are important points to remember before you connect the Residential Voice Gateway.

- For Ethernet connections, go to page 10.
- For telephone and fax connections, go to page 13.

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.

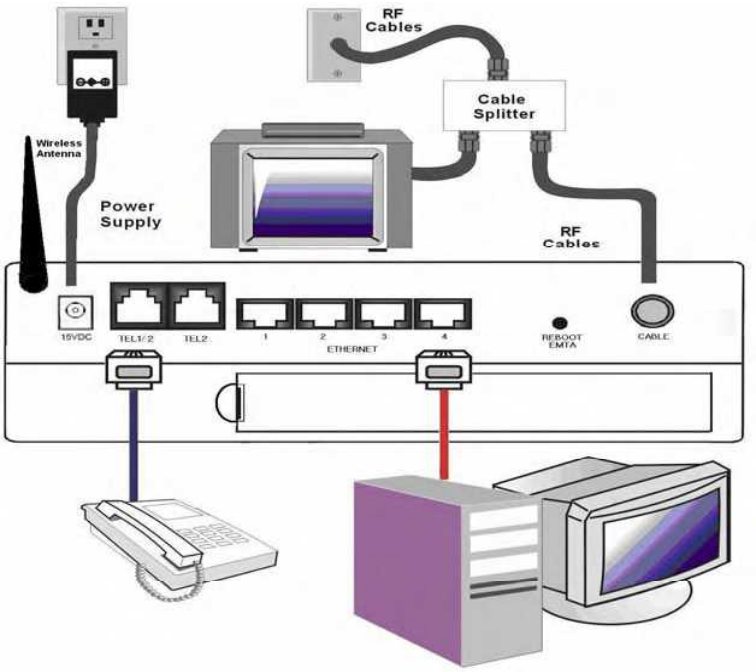


Fig.2: Ethernet Connection

Chapter 1: Connections and Setup

Connecting More Than Two Computers to the Residential Voice Gateway

If you need to connect more than two computers to DWG855, simply connect the computers to the Ethernet ports on the rear panel.

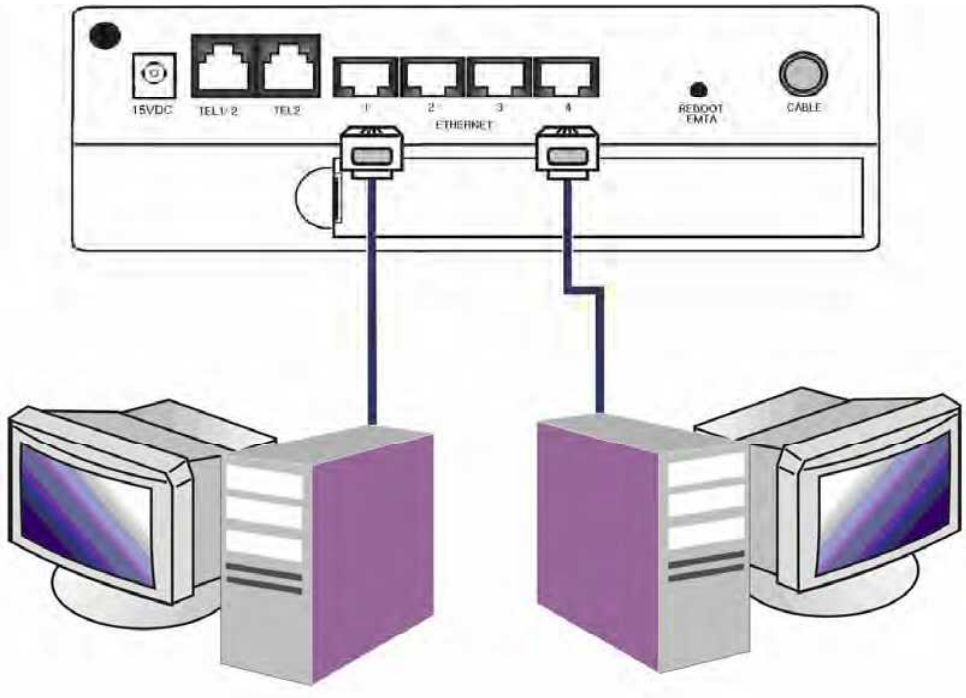


Fig.3: Multiple-PC Connection

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

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.

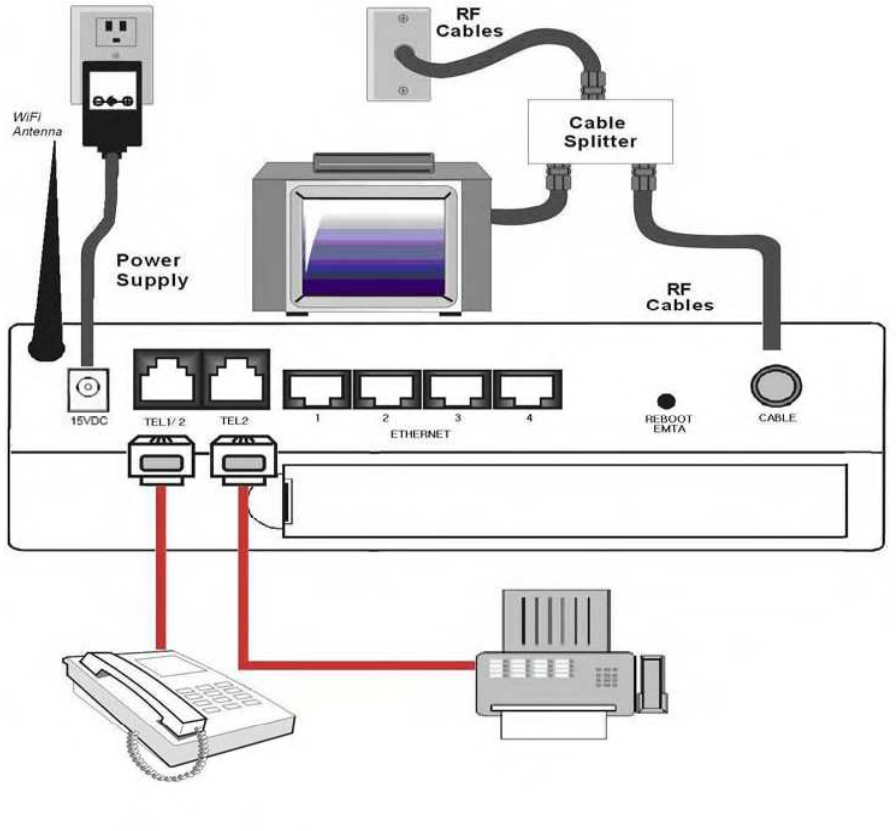


Fig. 4: Phone/Fax Connection

Illustrations contained in this document are for representation only.

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.

For a better wireless reception/connectivity, please make sure the supplied Wireless antenna is connected to the back of the unit.

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) 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: **192.168.100.1**
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. 5

If you login successfully, the main page will appear.

Outline of Web Manager

The main screen will be shown as below.

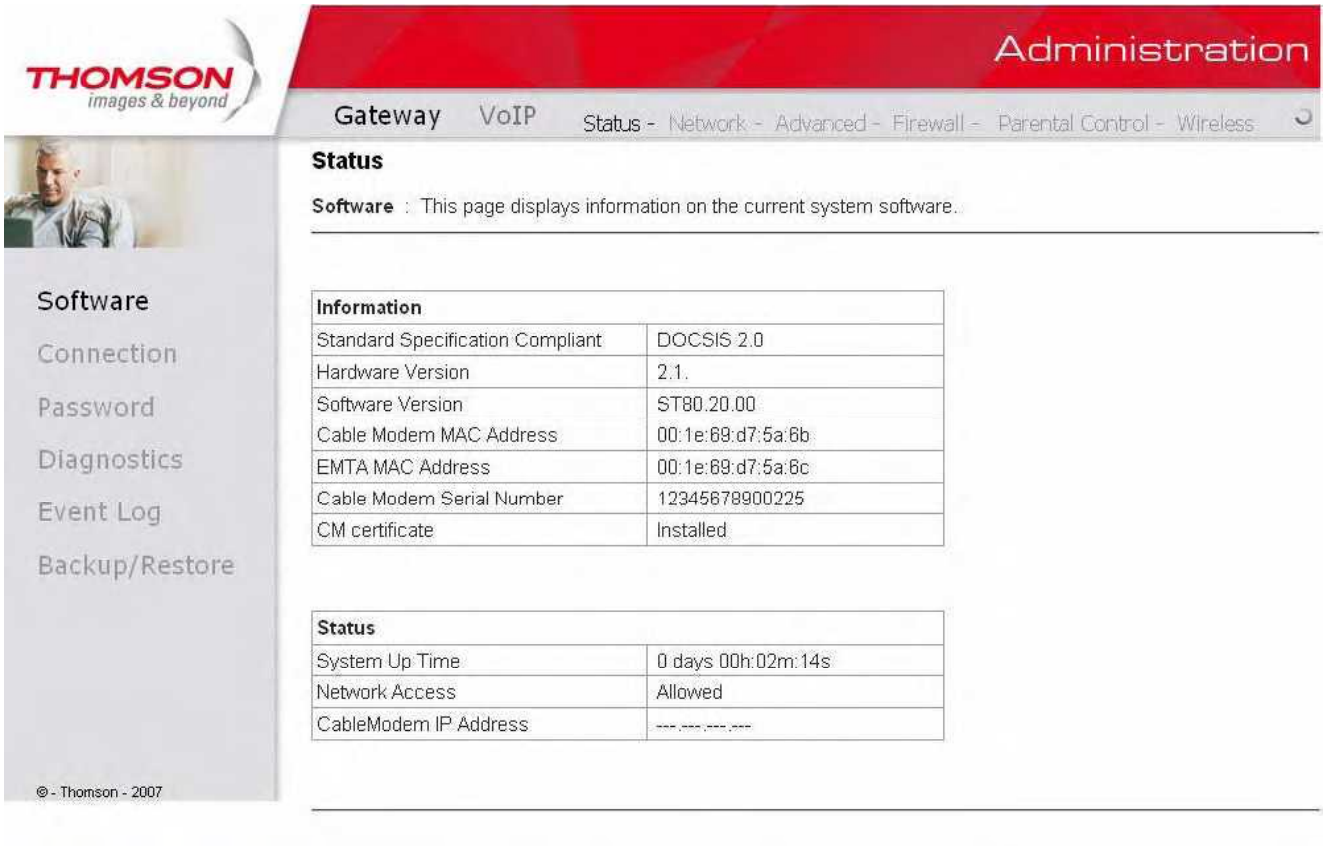


Fig. 6

- **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.

Please note, 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 or a little different than what is showing in the figures. This is normal.

Chapter 2: Web Configuration

Gateway – Status Web Page Group1. 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.

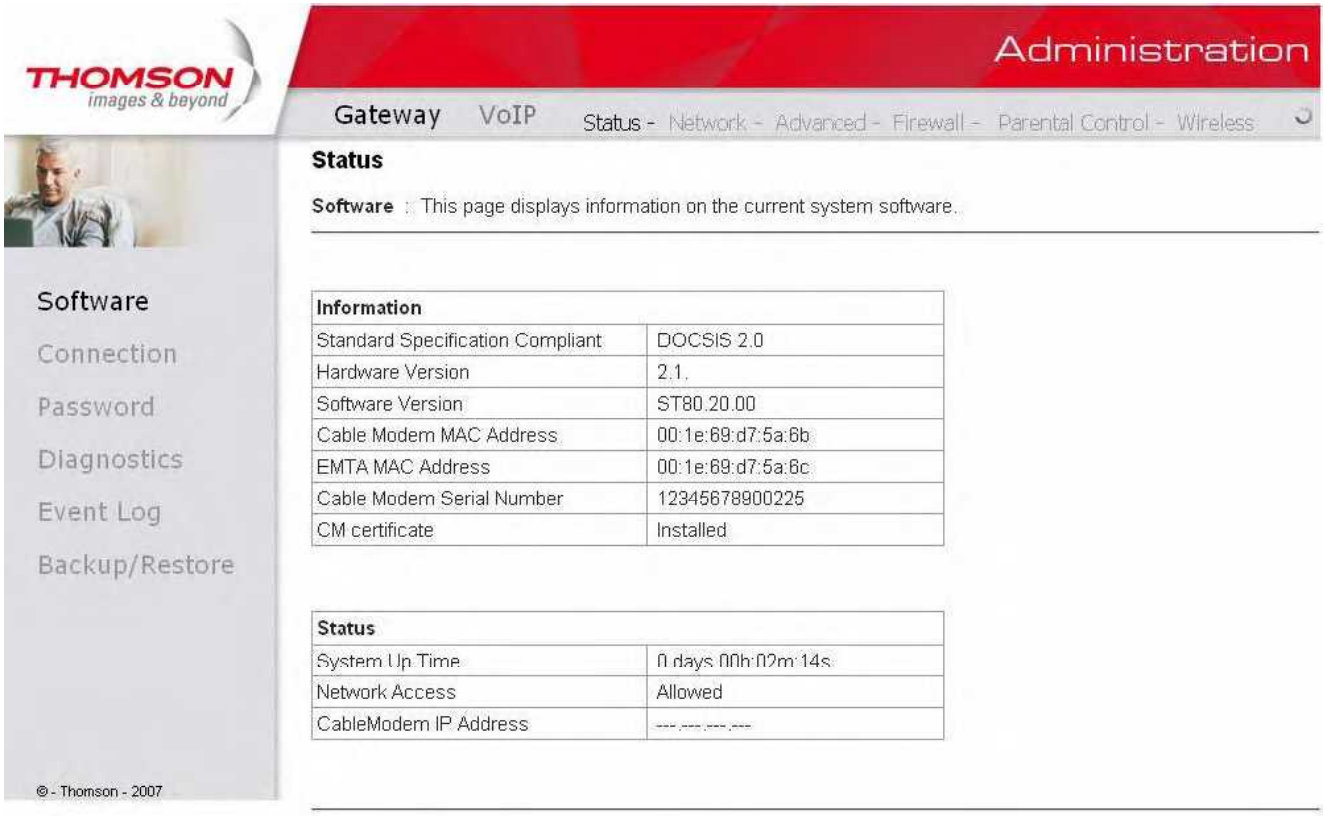


Fig. 7

Illustrations contained in this document are for representation only.

2. 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.

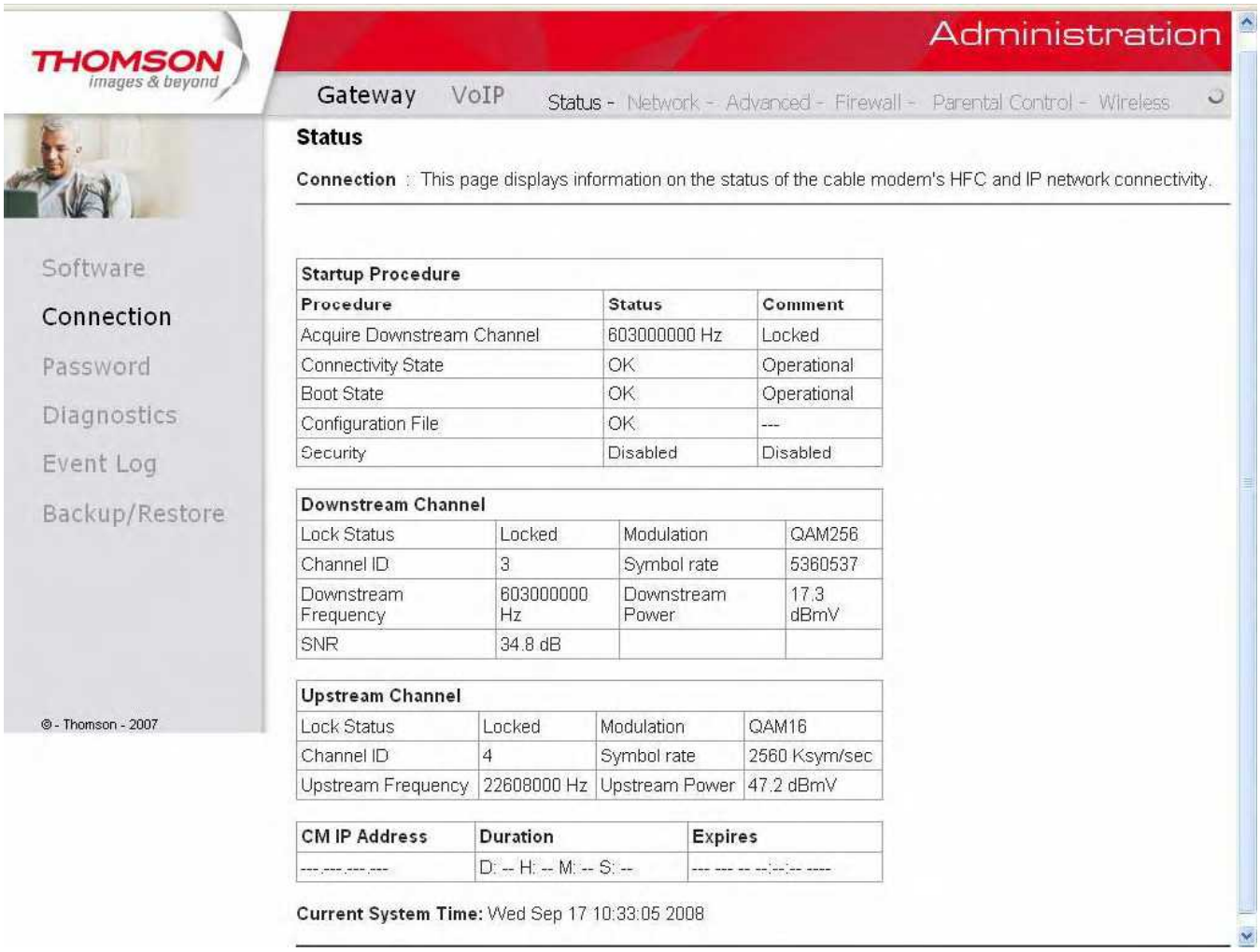


Fig. 8

Chapter 2: Web Configuration

3. 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.

Fig. 9

Illustrations contained in this document are for representation only.

4. 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.

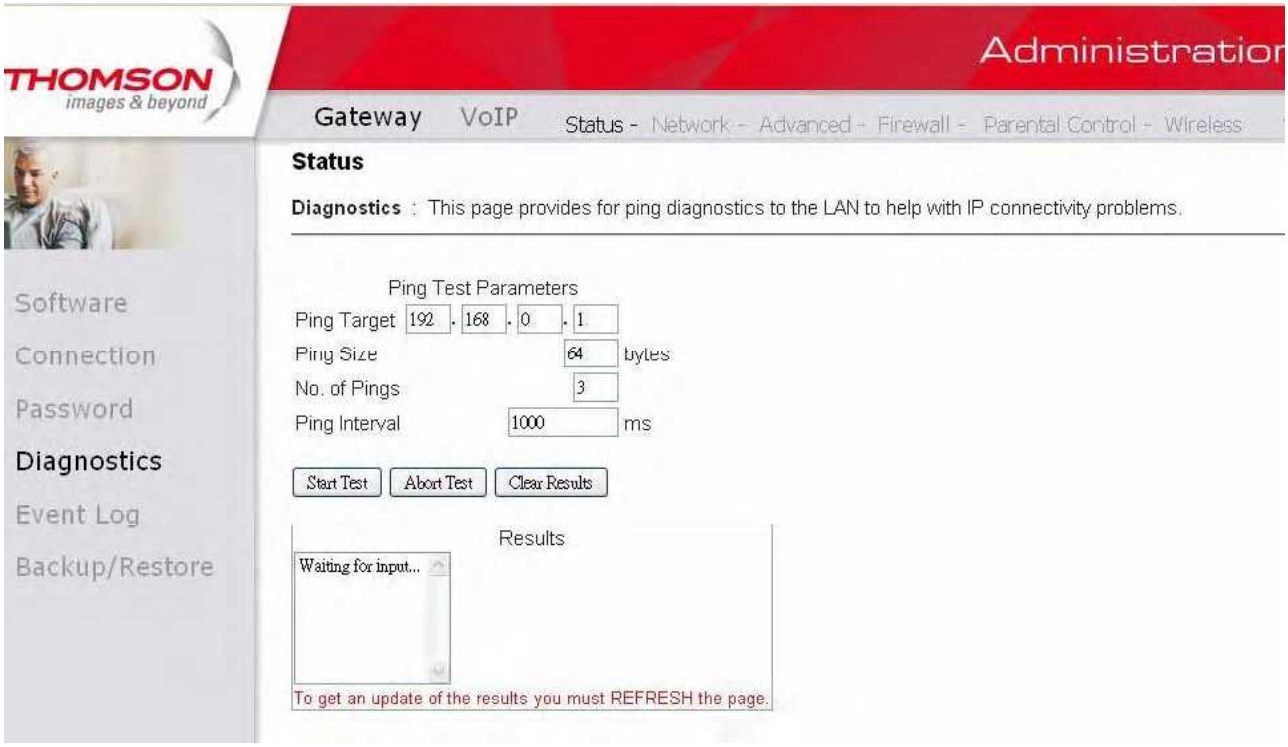


Fig. 10

Chapter 2: Web Configuration

5. Event Log

This page displays the content of the SNMP event log. Press "**Clear Log**" button to clear the logs.

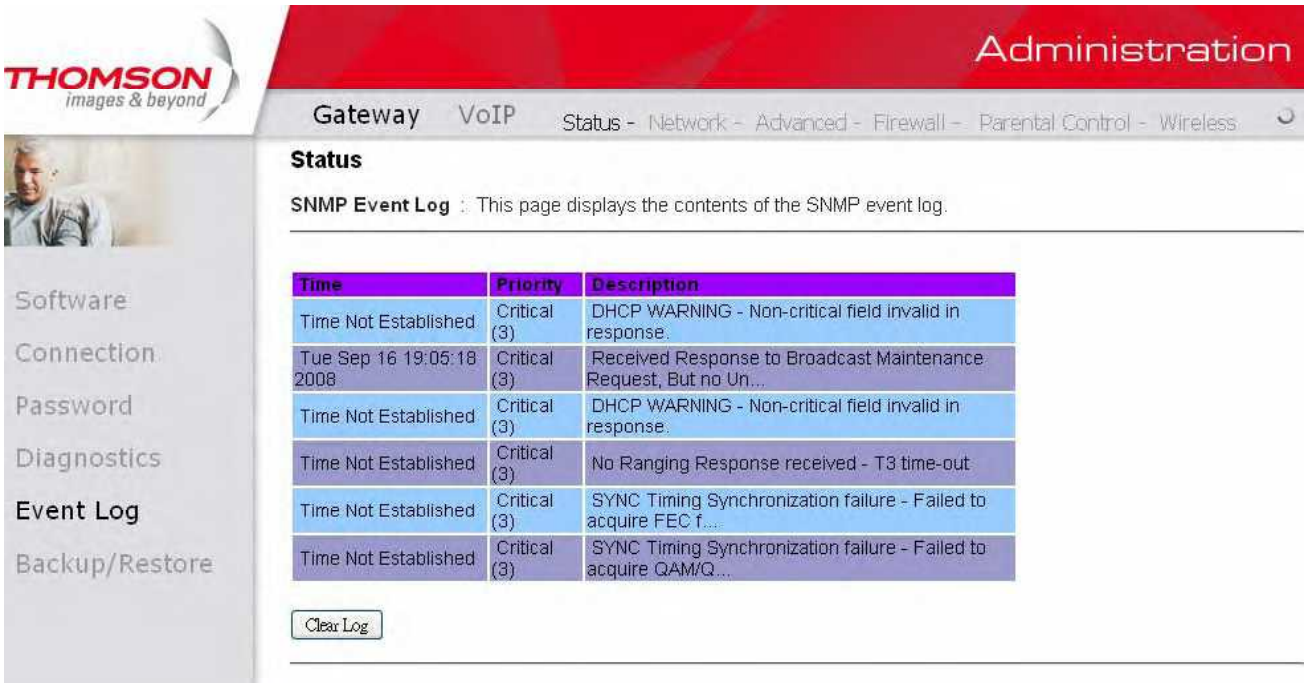


Fig. 11

6. Backup/Restore

This page allows you to save your current settings locally on your PC, or restored settings previously saved.

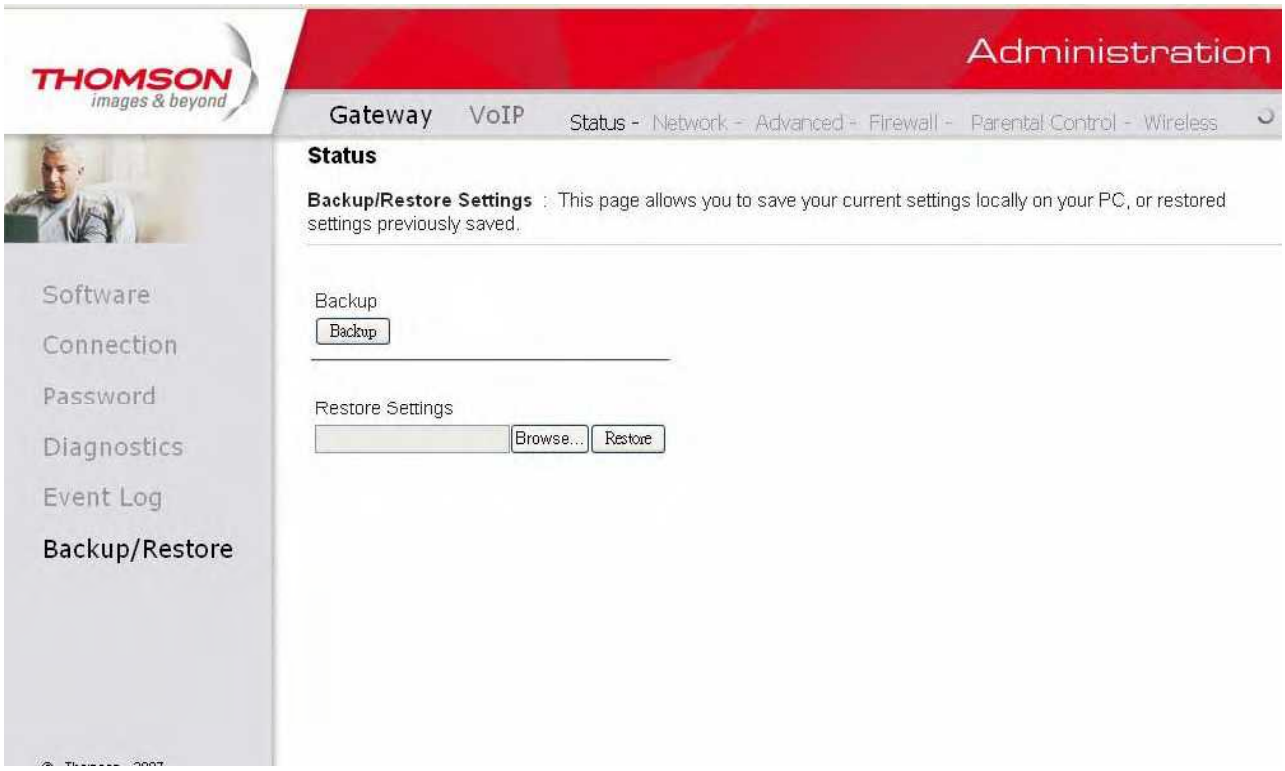


Fig. 12

To backup the current configuration, click "**Backup**" and follow the prompts.

To restore a previous configuration, click "**Browser**" and use the navigation window to locate the file. (UsuallyGatewaySettings.bin, unless you rename it before saving.) Once the file has been located, click "**Restore**" to restore the settings. Note that once the settings are restored, the device will reboot.

Chapter 2: Web Configuration

Gateway – Network Web Page Group

1. 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**.

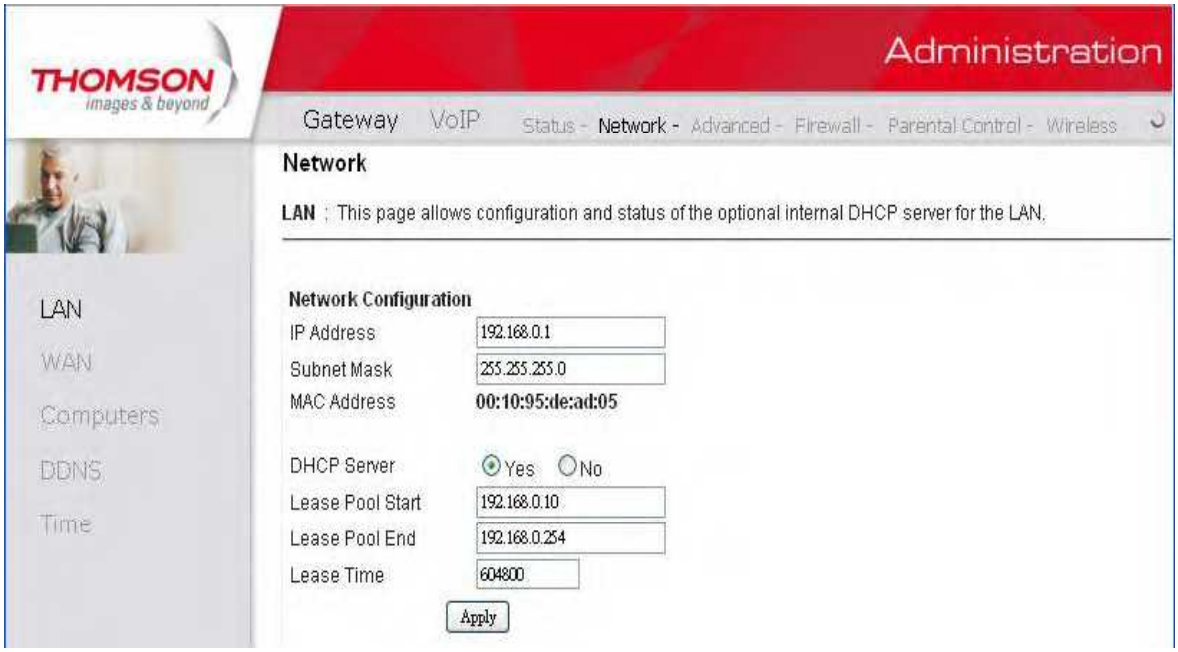


Fig. 13

2. 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.

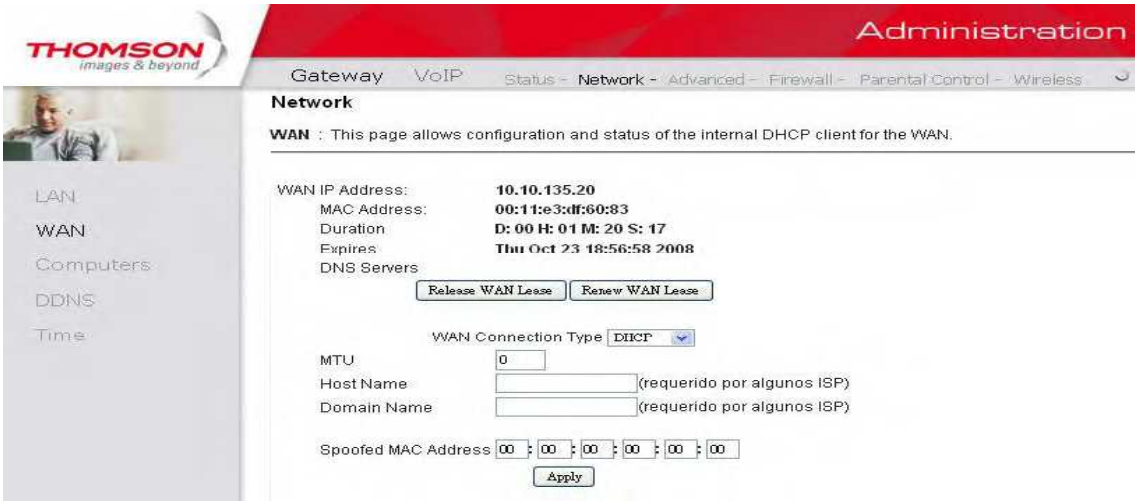


Fig. 14

3. 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.

Fig. 15

Chapter 2: Web Configuration

4. DDNS

Dynamic DNS (DDNS) allows a dynamic IP address to be aliased to a static, pre-defined host name so that the host can be easily contacted by other hosts on the internet even if its IP address changes. The CMRG supports a dynamic CNS client compatible with the Dynamic DNS service (http://www.dyndns.com/).

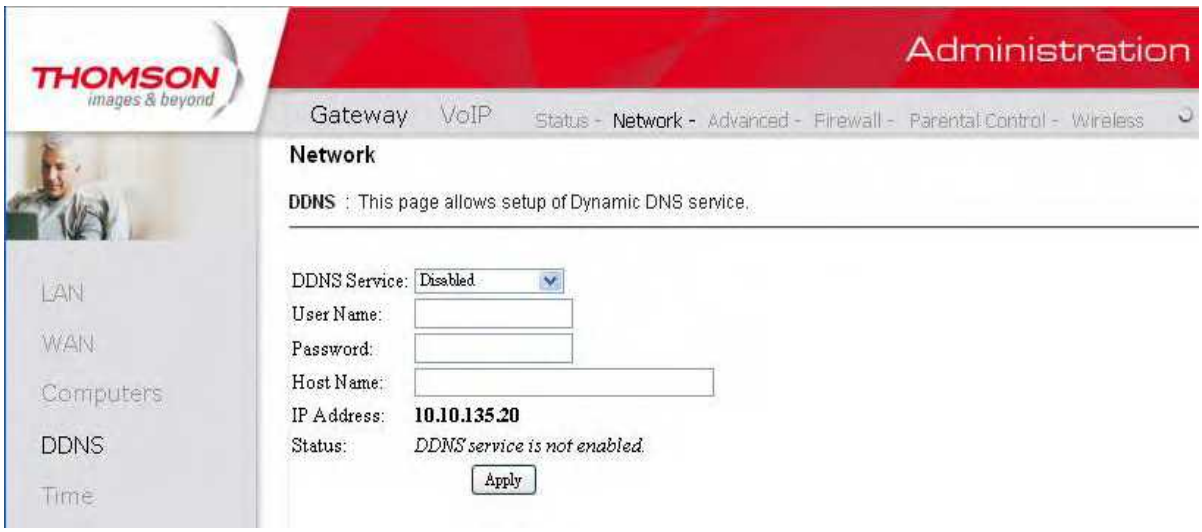


Fig. 16

To activate the DDNS client:

1. Go to the DynDNS website and create an account for the Dynamic DNS service. You will create a username and password, and be asked to choose a host name for your host's current IP address. This is the WAN IP address that has been assigned to your CMRG during provisioning.
2. Enter your account information on the DDNS web page, enable the service by selecting www.DynDNS.org from the DDNS Service drop-down list, and click "**Apply**".
3. The DDNS client will notify the DDNS service whenever the WAN IP address changes so that your chosen host name will be resolved properly by inquiring hosts. The current status of the service is shown at the bottom of the DDNS web page.

5. Time

This page allows configuration and display of the system time obtained from network servers via simple network protocol.

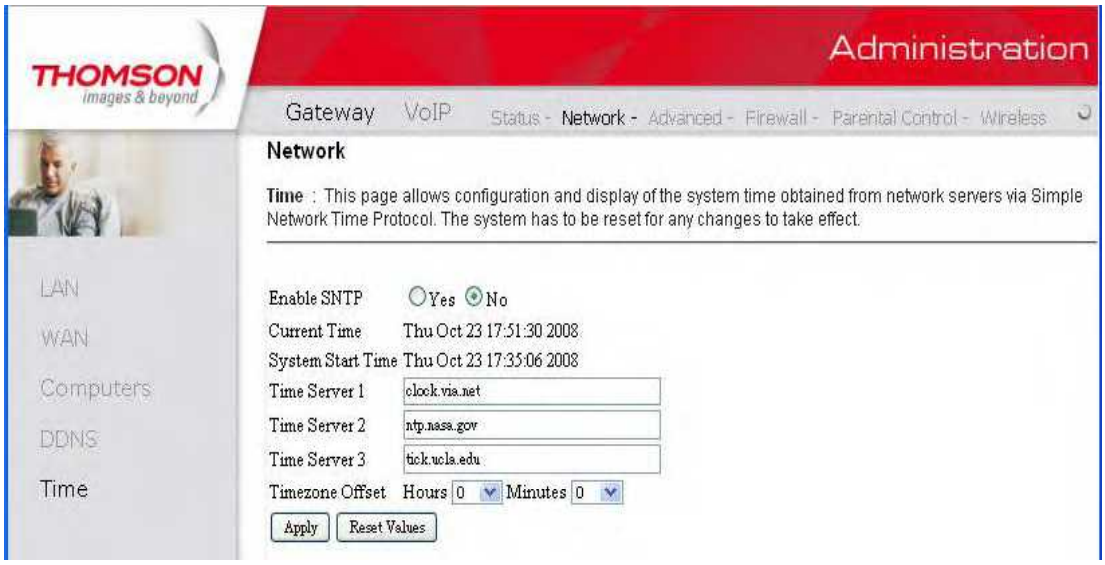


Fig. 17

Chapter 2: Web Configuration

Gateway – Advanced Web Page Group

1. Options

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

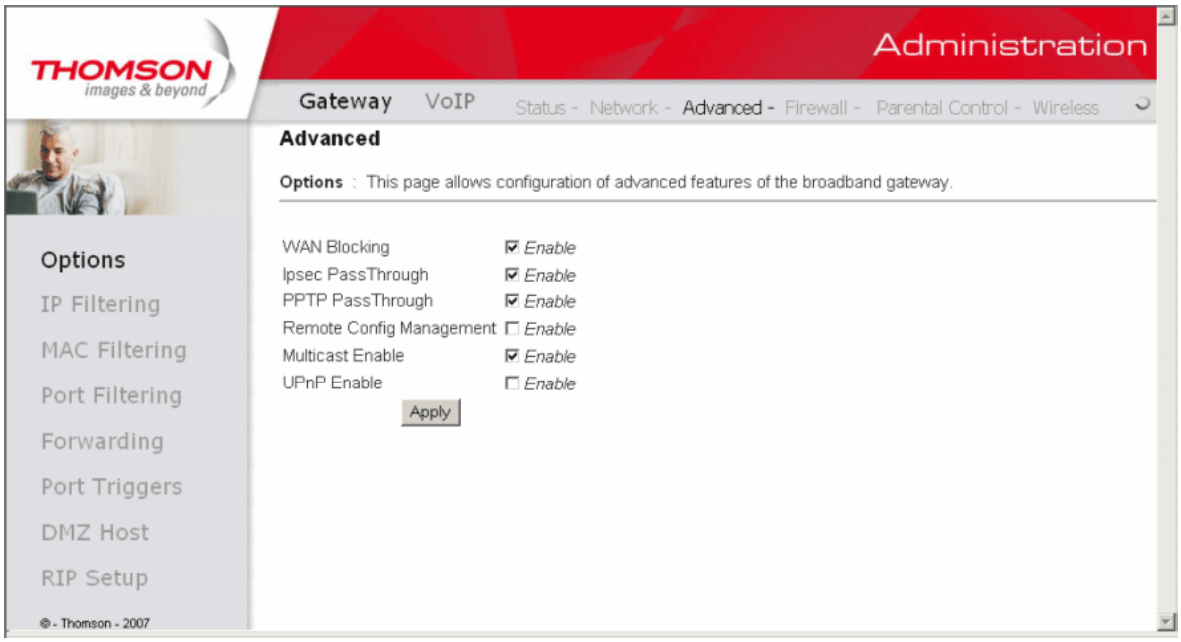


Fig. 18

- **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, your 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.

2. 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 (Internet). These PCs can still communicate with each other on your LAN, but traffic they originate to the WAN is blocked by the gateway.

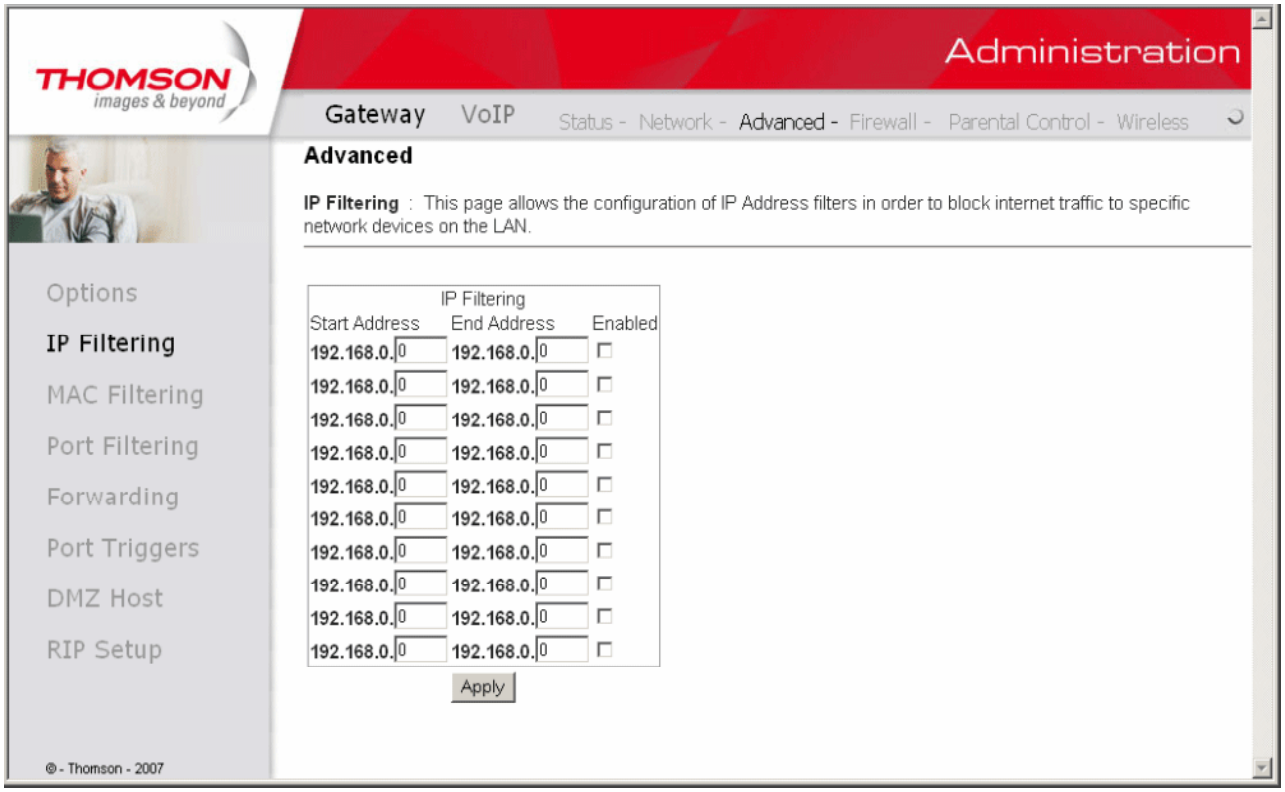


Fig. 19

Chapter 2: Web Configuration

3. 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.

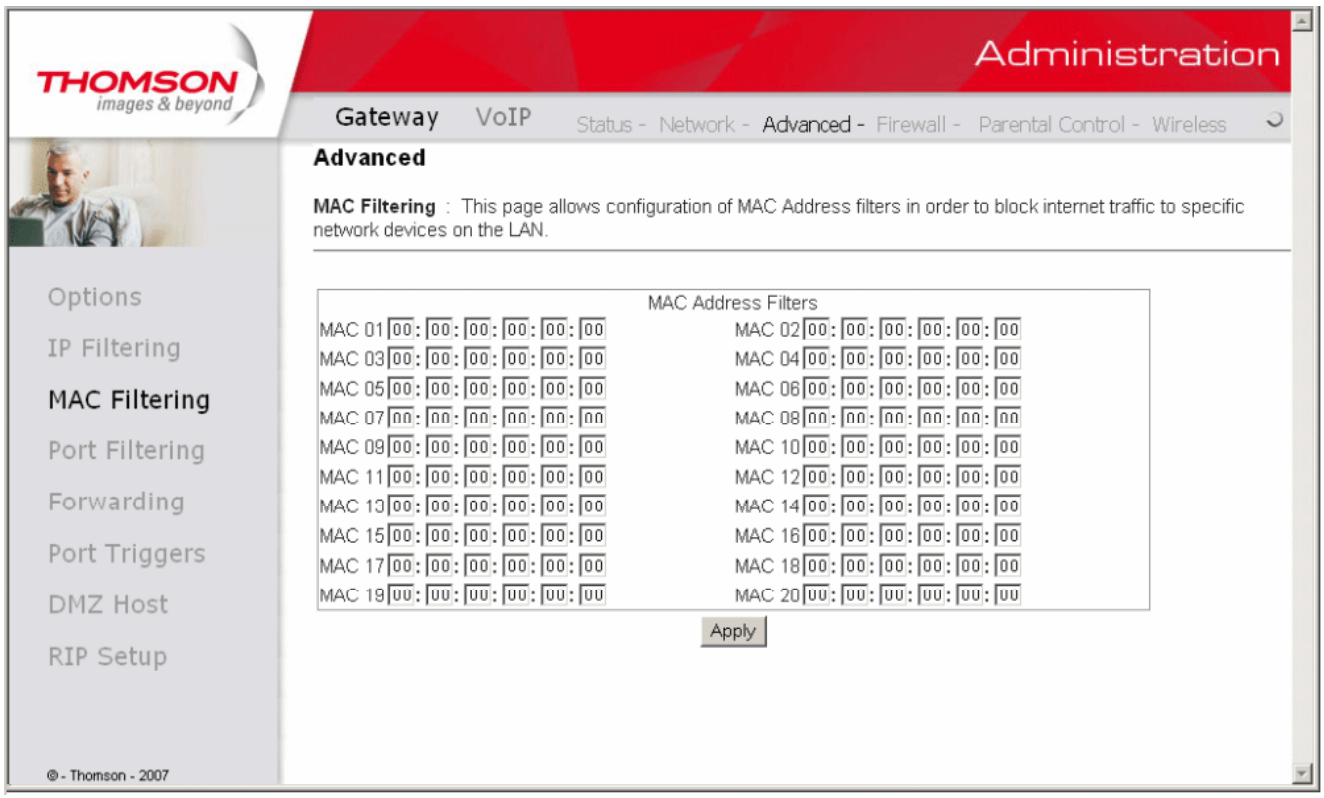


Fig. 20

Illustrations contained in this document are for representation only.

4. 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.

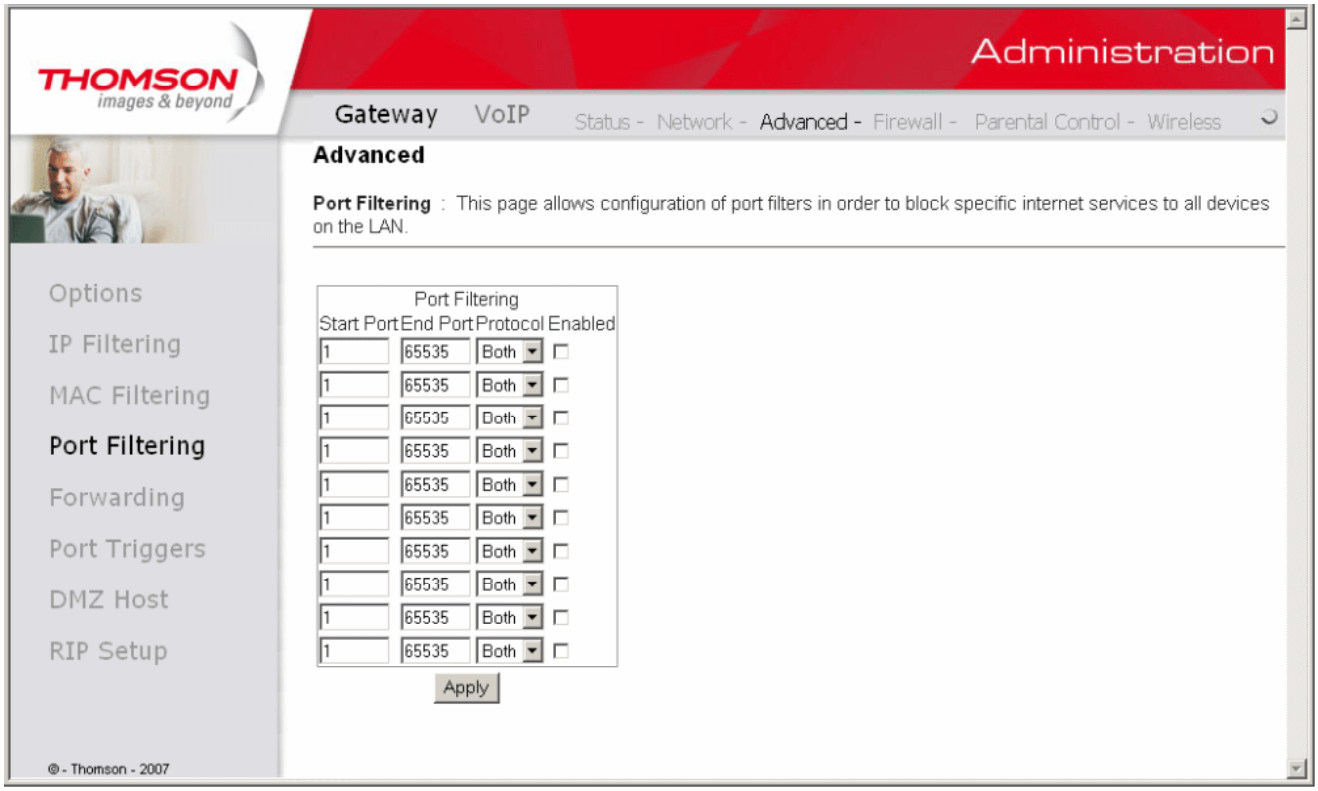


Fig. 21

Chapter 2: Web Configuration

5. 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.

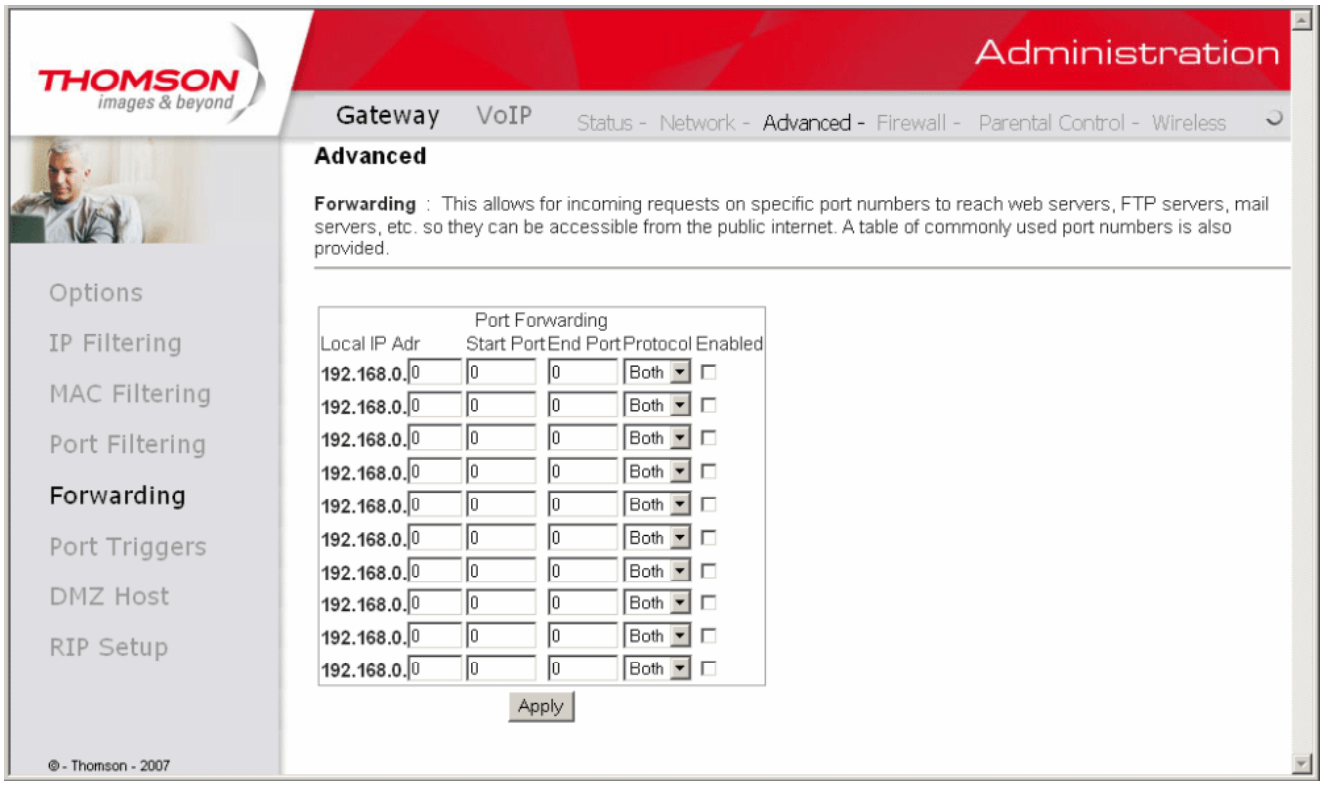


Fig. 22

Illustrations contained in this document are for representation only.

6. 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.

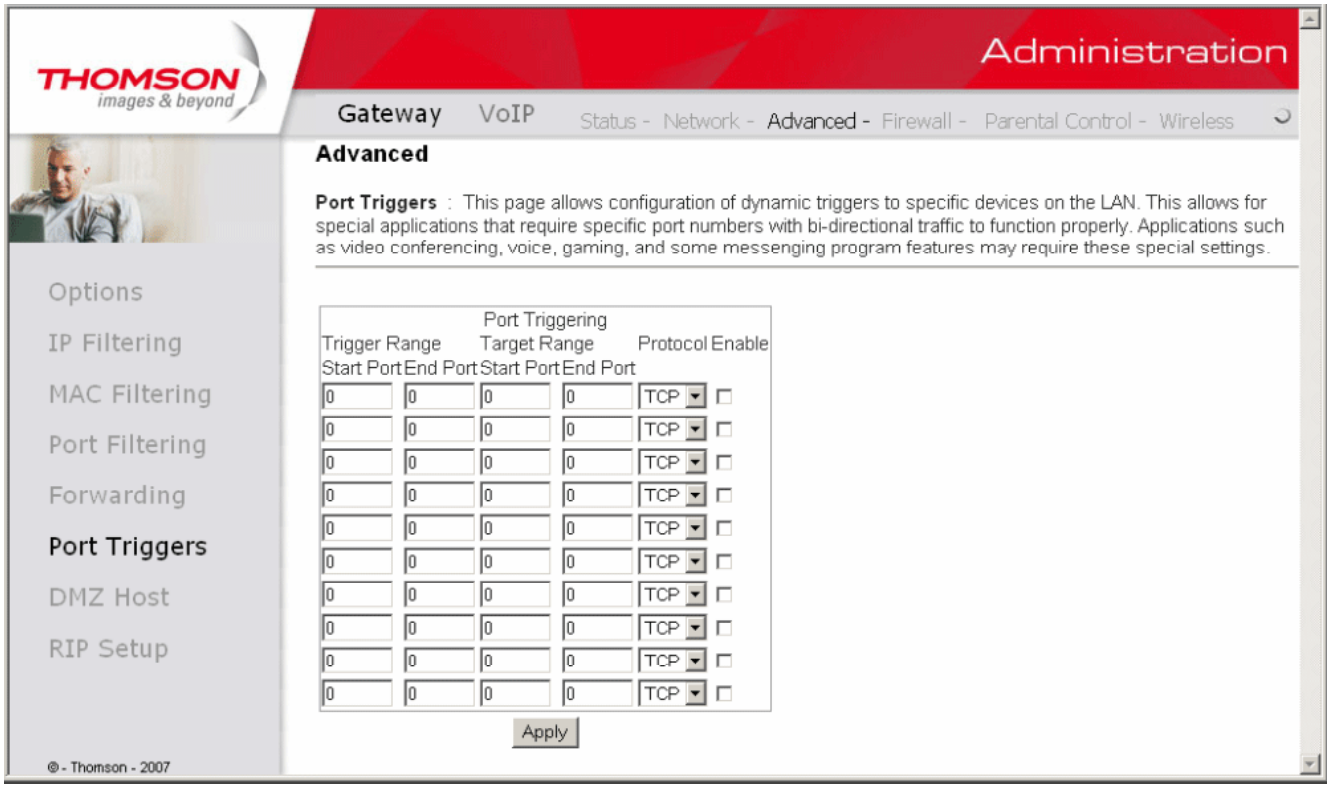


Fig. 23

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

7. 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.

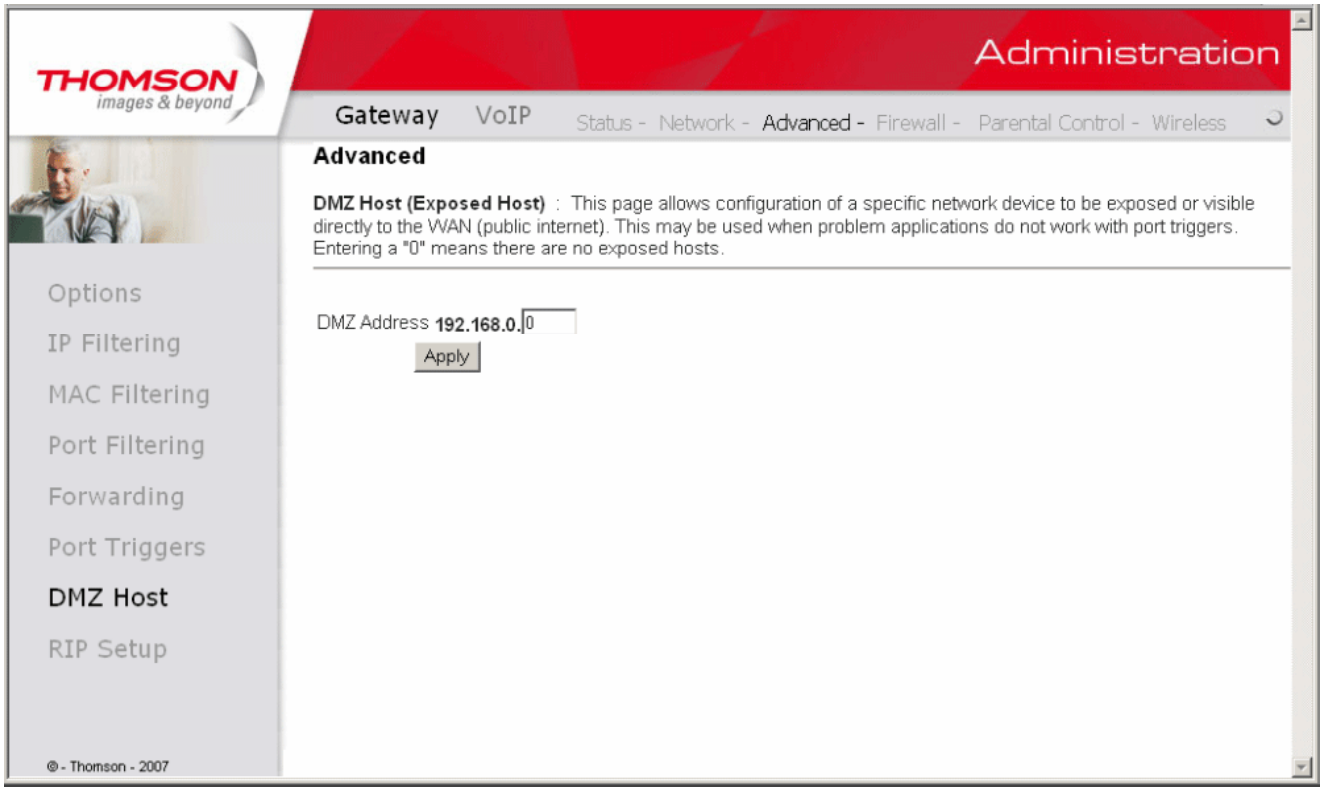


Fig. 24

Illustrations contained in this document are for representation only.

8. 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.

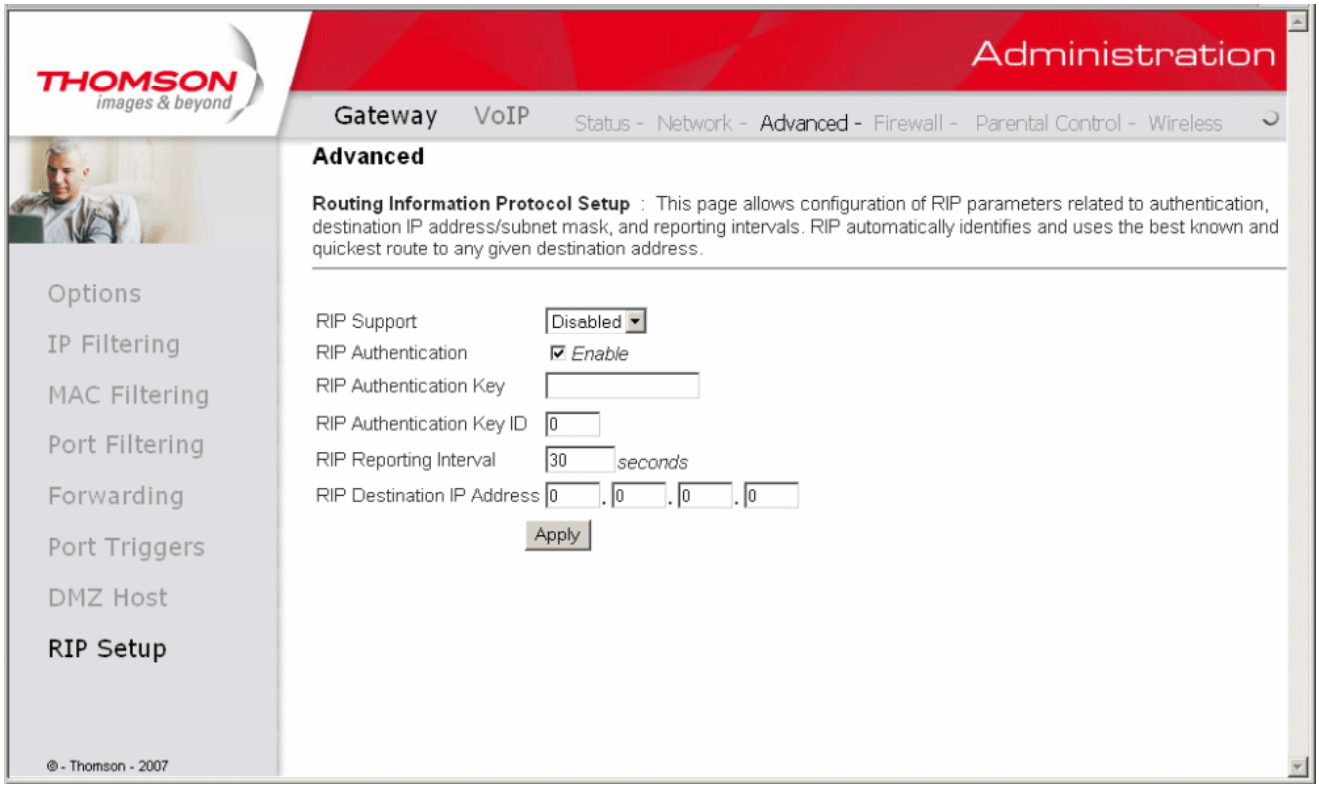


Fig. 25

Chapter 2: Web Configuration

Gateway – Firewall Web Page Group

1. 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.

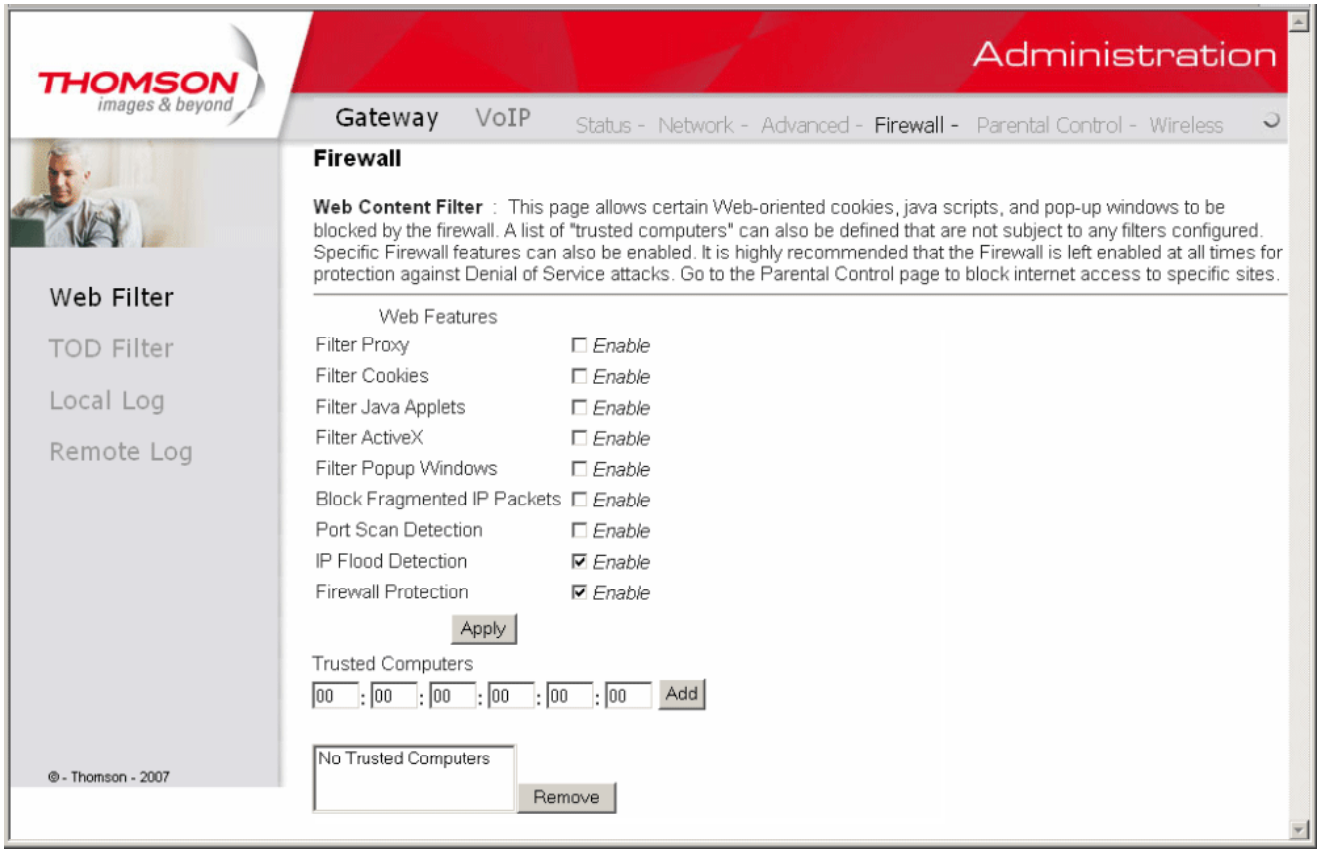


Fig. 26

Illustrations contained in this document are for representation only.

2. TOD Access 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.

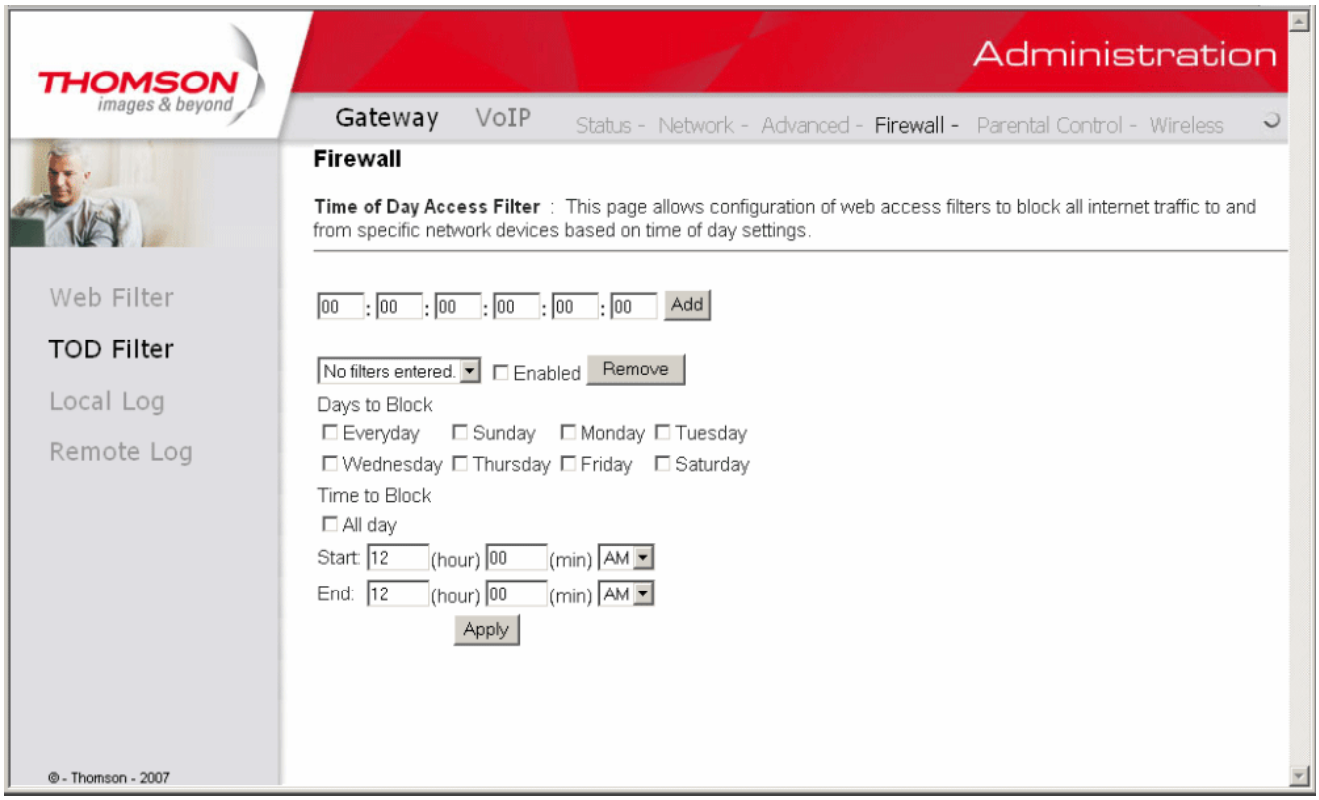


Fig. 27

Chapter 2: Web Configuration

3. 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.

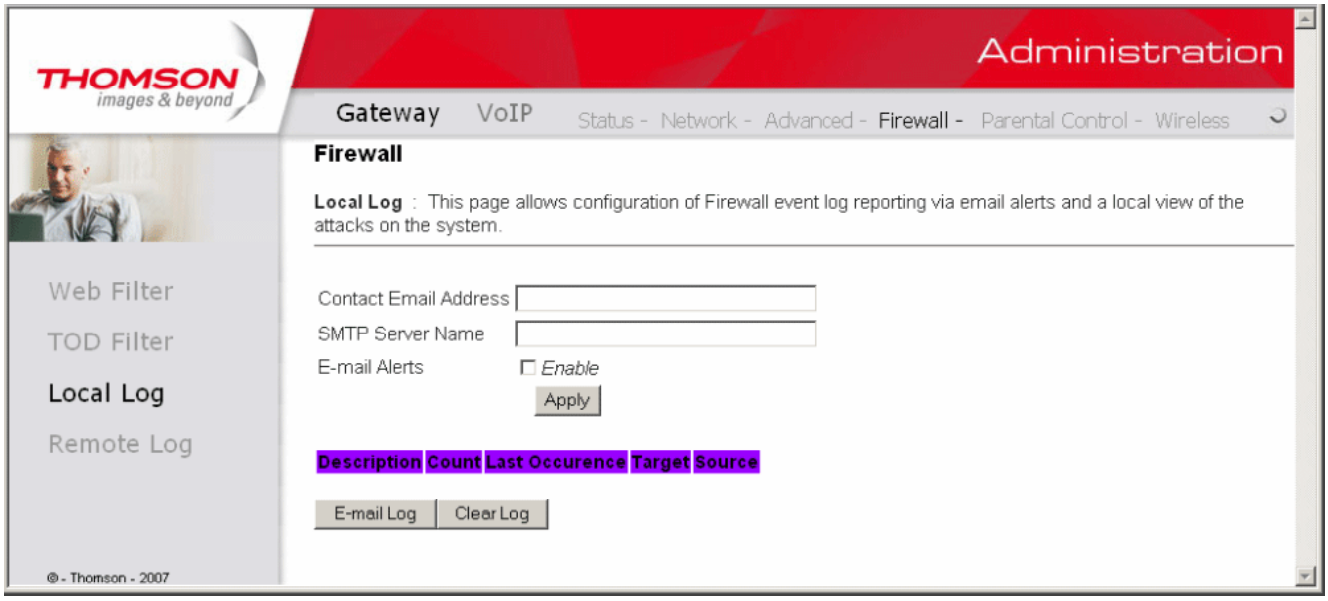


Fig. 28

Illustrations contained in this document are for representation only.

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.

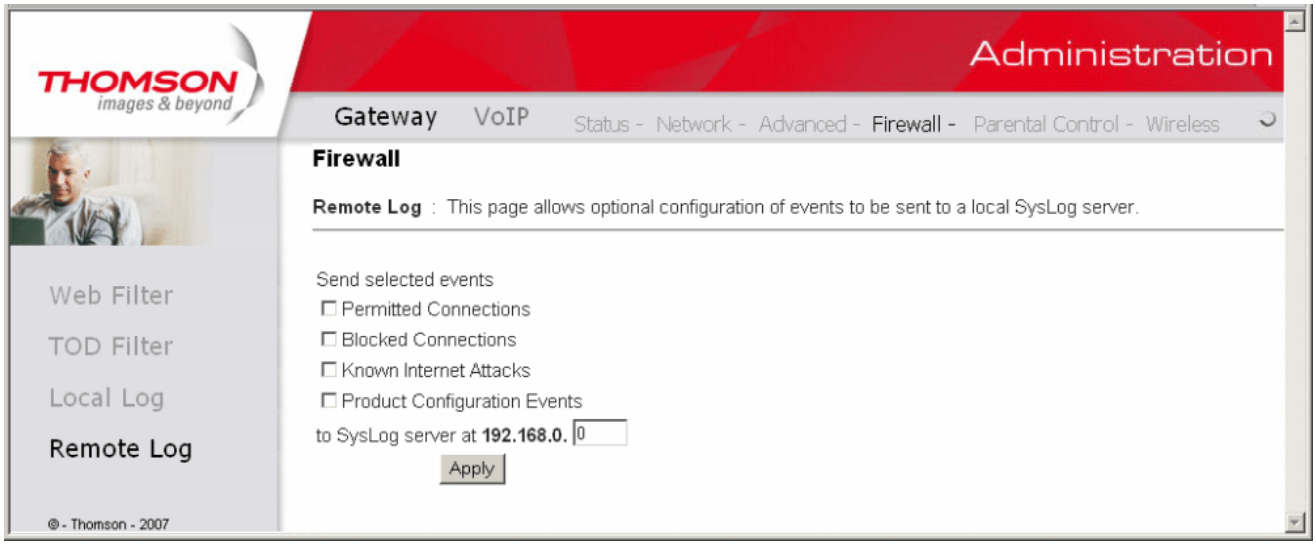


Fig. 29

Chapter 2: Web Configuration

Gateway – Parental Control Web Page Group

Basic Setup

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.

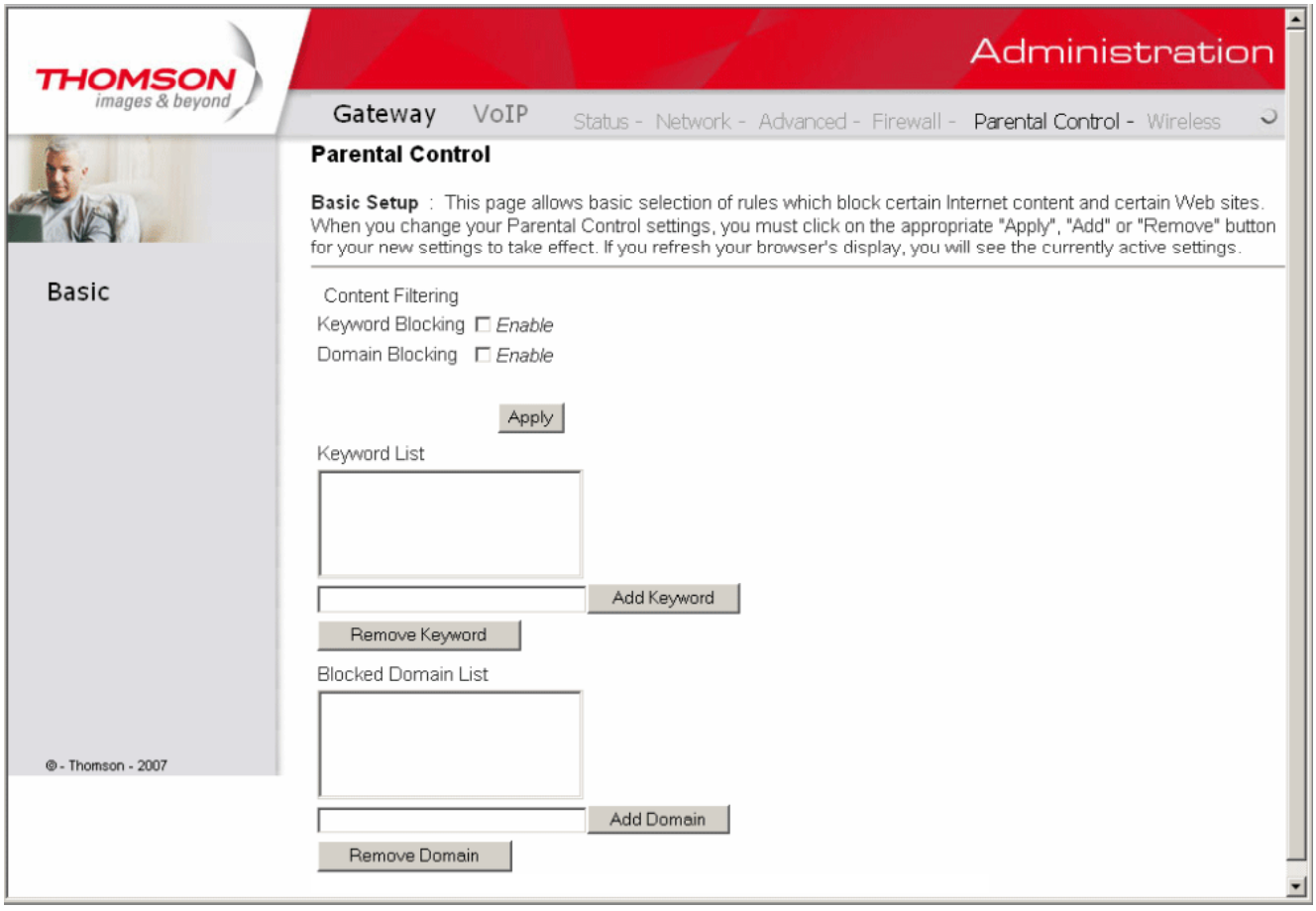


Fig. 30

Illustrations contained in this document are for representation only.

Gateway – Wireless Web Page Group

Important: Changes to the wireless web pages should be made from a PC that is directly connected 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 DWG855 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

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

Chapter 2: Web Configuration

1. Radio

This page allows configuration of the Wireless Radio including current country and channel number.

Press "**Apply**" button to enable the new setting that you have changed or press "**Restore Wireless Defaults**" button to restore to defaults setting.

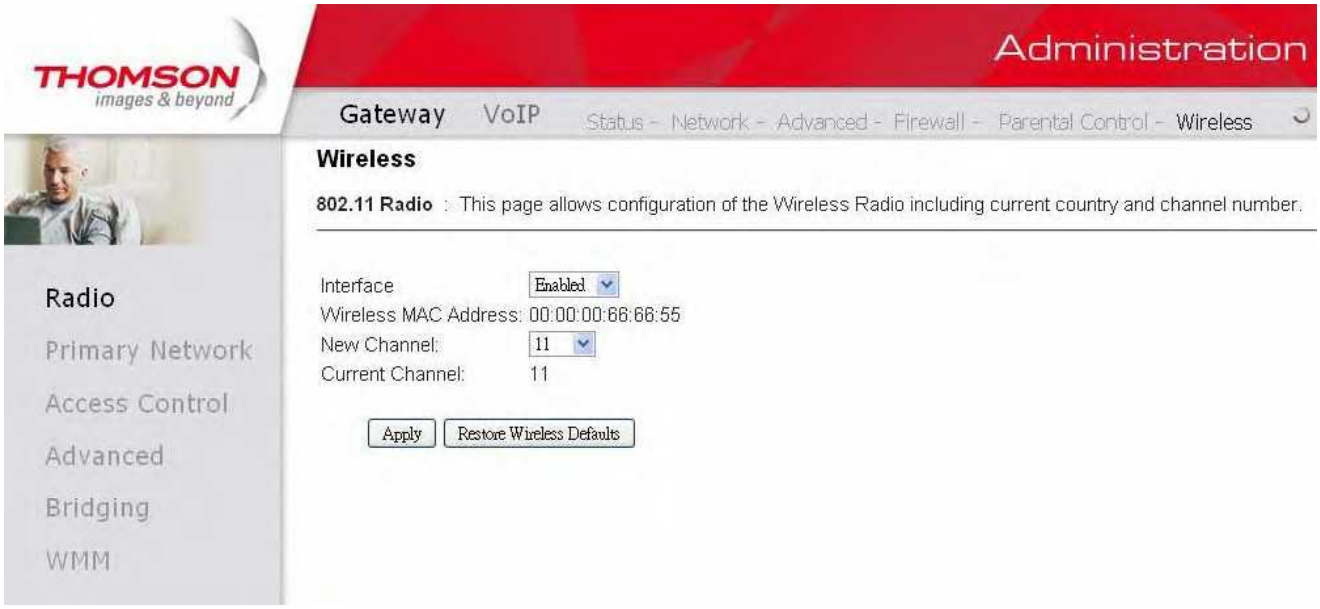


Fig. 31

- **Interface**: The wireless radio in your gateway can be completely de-activated by changing **Interface** to Disabled. Click the **Apply** button to save your settings. If you want to re-activate the disabled wireless radio in your gateway, need to contact cable operator.
- **Wireless MAC Address**: The MAC address for this wireless device will be displayed in this field automatically.
- **New Channel**: There are 13 channels that you can choose. Choose the one that is suitable for this device.
- **Current Channel**: The channel that you choose will be displayed in this field.

Restore Wireless defaults: To recover to the default settings, press this button to retrieve the settings and click Apply.

2. Primary Network

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.

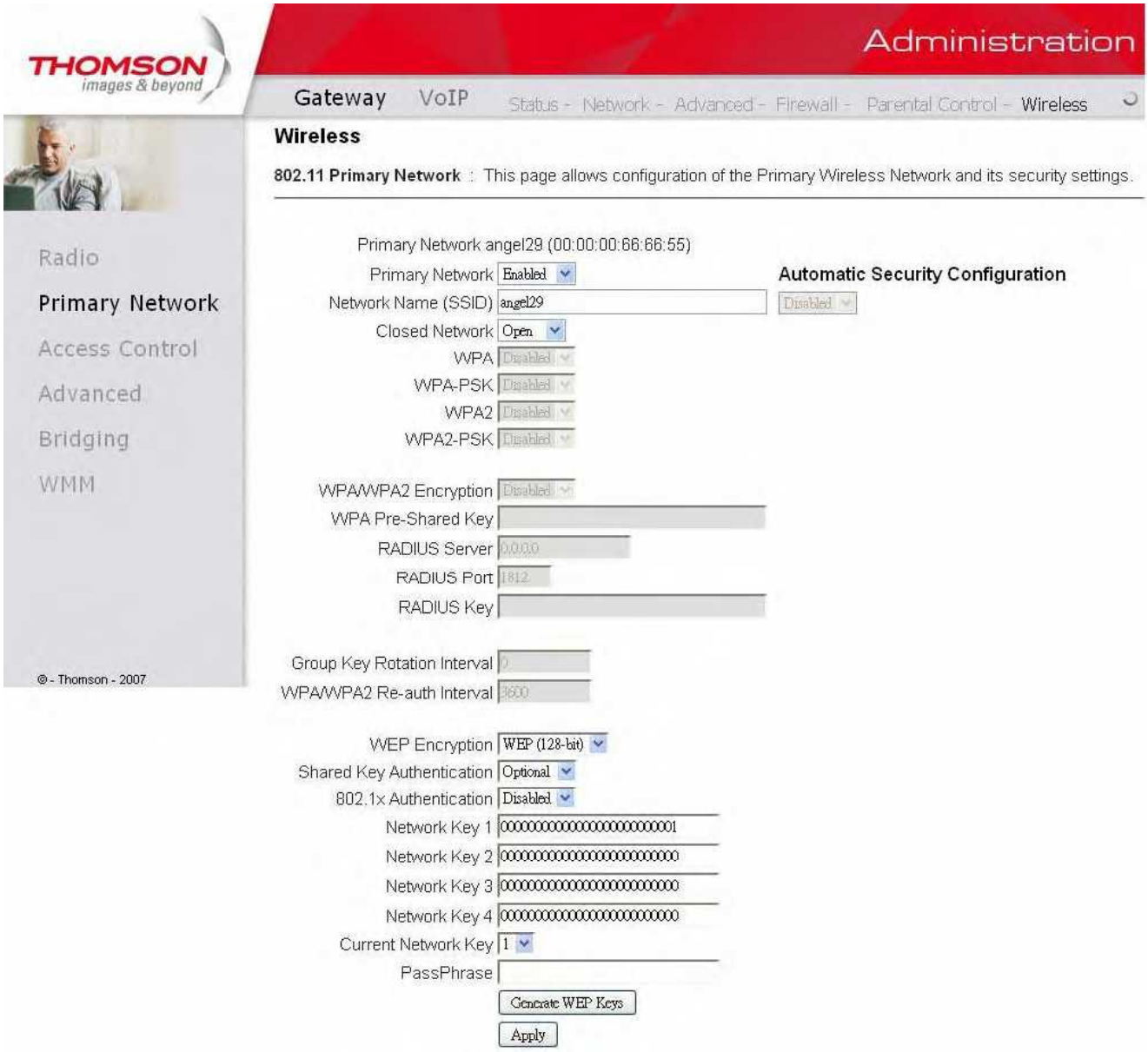


Fig. 32

Primary Network: It is used to Enable or Disable the whole Primary Network feature.

Network Name (SSID): By using this you can change the factory default to a name of your choice up to 32 characters long.

Closed Network: This control is used to hide or reveal your network name (SSID) 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 Closed Network to Enable, your SSID is included in that beacon, and is therefore detectable by any nearby wireless equipped PCs in the area. The benefit of using Enable is it can speed your WiFi setup on some PCs. If you set Closed Network to Disable, your SSID is not included in the beacon. This hides your network name (SSID), but as a result may require a bit more effort on your part to set up your wireless PCs. And when we Enable the **WPS Config** then the **Closed Network** will be Disabled automatically.

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 the128 Bit Encryption, and have the same Key value too. Otherwise, it will not be able to decrypt the data.
(*Note: You need to connect one end of the Ethernet cable to the Ethernet port on the back of your computer, and the other end to the ETHERNET port on the Residential Voice Gateway.*)

- 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.

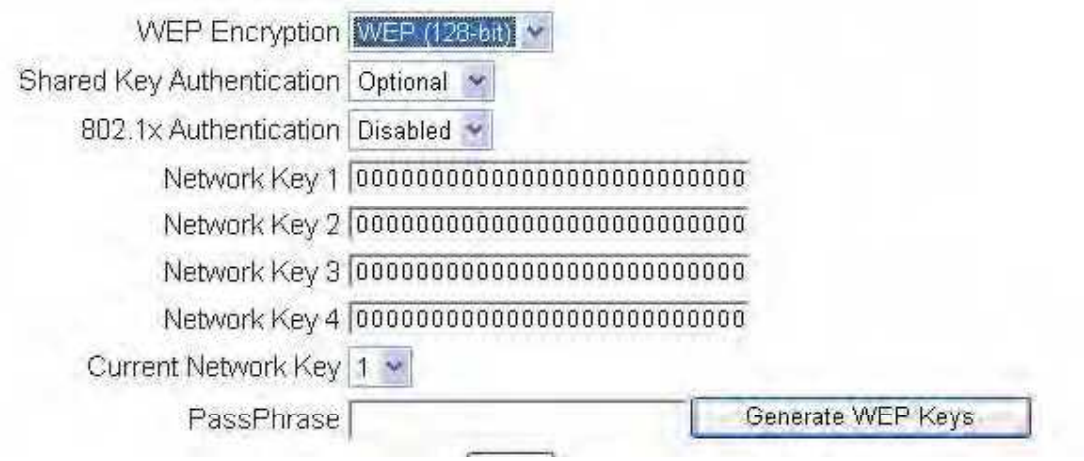


Fig. 33

- **Apply:** After proper configuration, click Apply to invoke the settings.

Chapter 2: Web Configuration

802.1x Authentication

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.

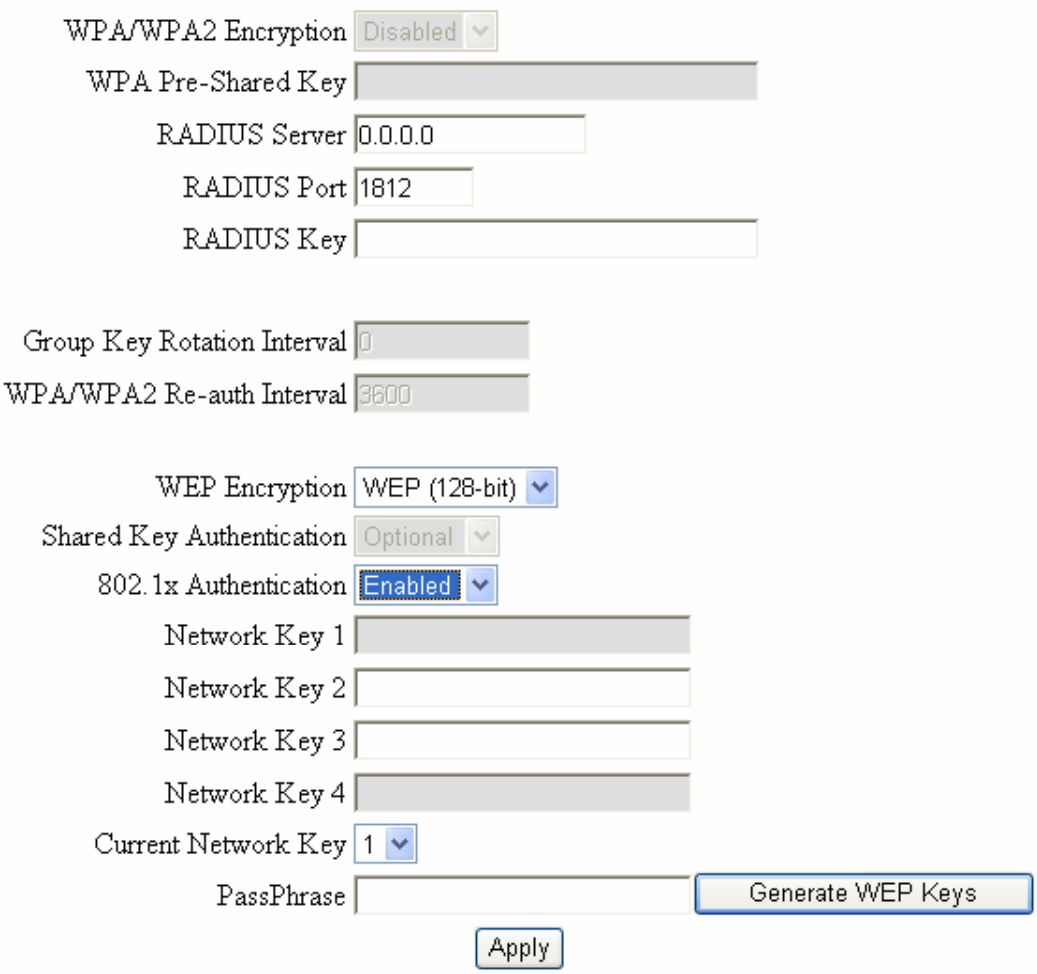


Fig. 34

WPA/WPA2

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 mater 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.

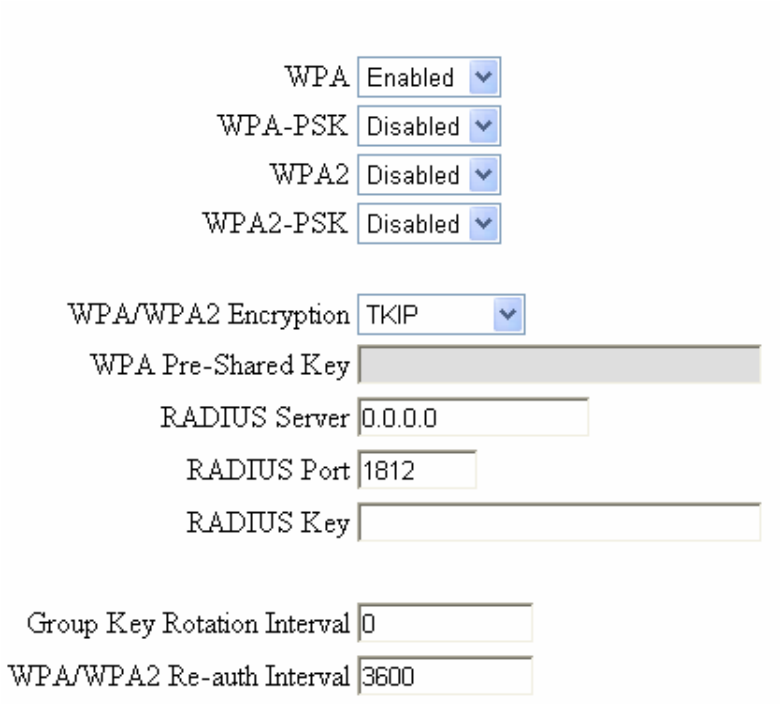


Fig. 35

WPA-PSK/ WPA2-PSK

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.**

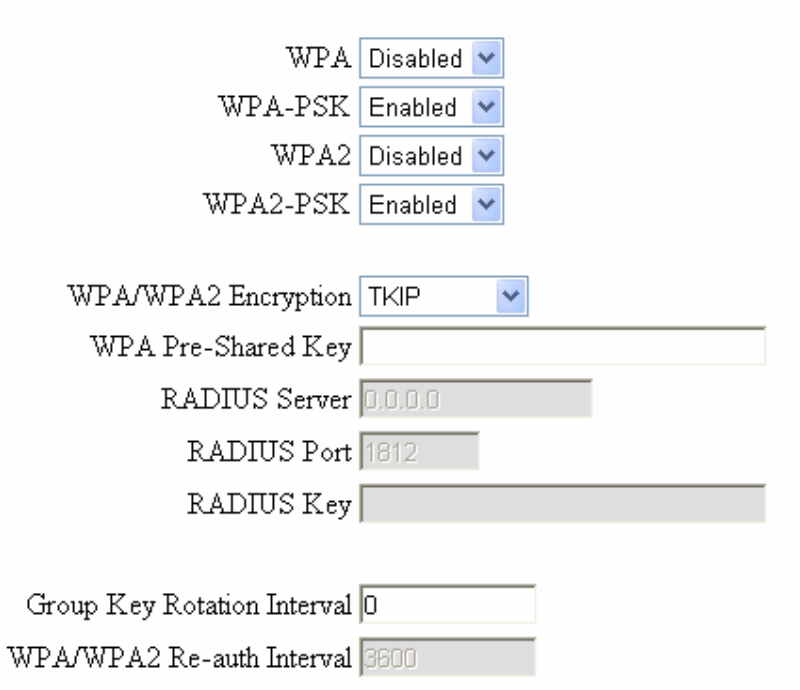


Fig. 36

Automatic Security Configuration

Fig. 37

WiFi Protected Setup (WPS): It is a secure way of configuring and connecting your WiFi access point.

- **WPS Config:** It will help to **Enable** or **Disable** the WPS feature.
- **Device Name:** By using this you can change the factory default to a name of your choice up to 32 characters long as like **SSID**
- **WPS Setup AP:** Here we no need to do any configure. So, just skip this step.
- **WPS Add Client:** There are two methods "Push-Button" and "PIN". Select the method you want.
  If you select "Push-Button", then the **WPS Setup AP** page will appear as shown below.

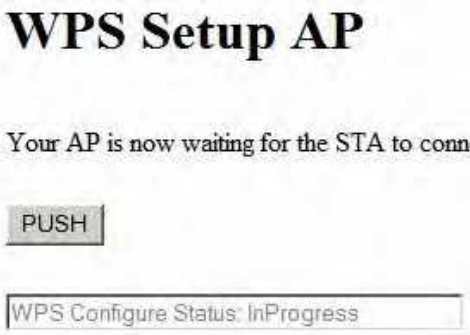


Fig. 38

And **WPS Configure Status** will be "In progress", after establishing the connection the **WPS Configure Status** will be "Success!". If you select **WPS Method** to PIN then It will ask for PIN while configuring the WiFi AP by showing a text box so, you need to enter that PIN to establish the connection. You can get the PIN from client.

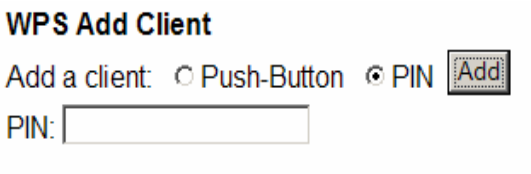


Fig. 39

- **PIN:** Use this option to set the PIN, enter 4-8 digits PIN of the device you wish to configure. After entering the pin click "Add" button, then the WPS Setup AP page will appear as shown below and the status will be "In progress", after establishing the connection the WPS Configure Status will be "Success!".

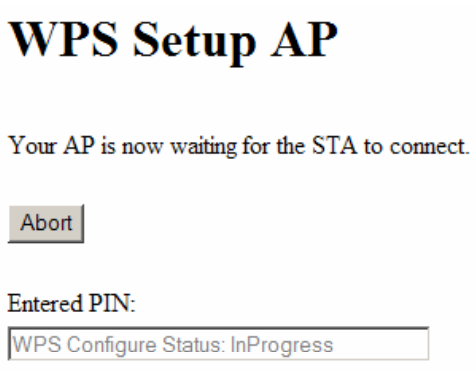


Fig. 40

3. Access Control

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

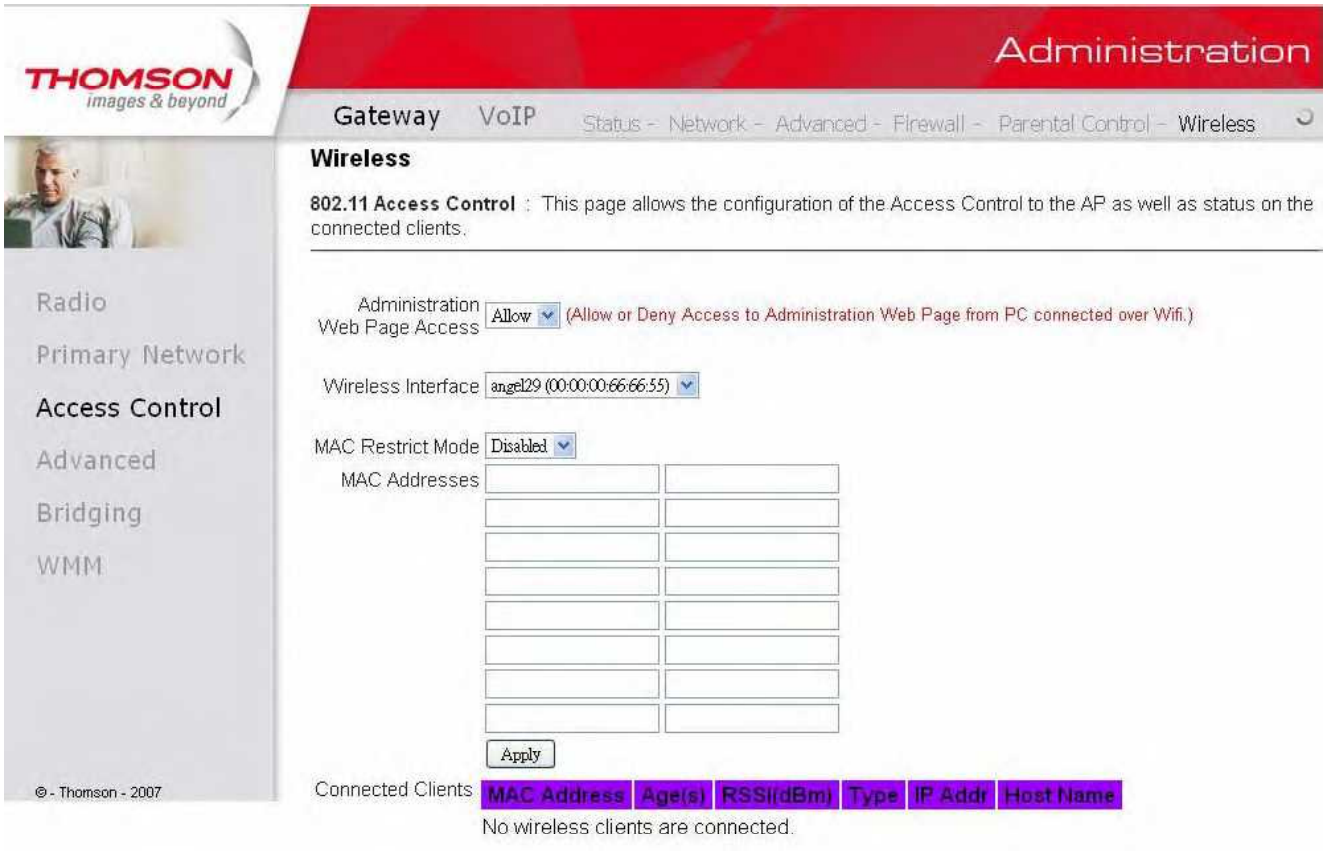


Fig. 41

Administration Web page Access: It Allow or Deny access to Administration Web Page from PC connected over WiFi.

Wireless Interface: By default it will be having two interfaces, "Primary Network interface" and "Guest Network Interface". The "Primary Network interface" will be available for all users. If you want to access the "Guest Network Interface" then you need to contact cable operator.

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.

4. 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.

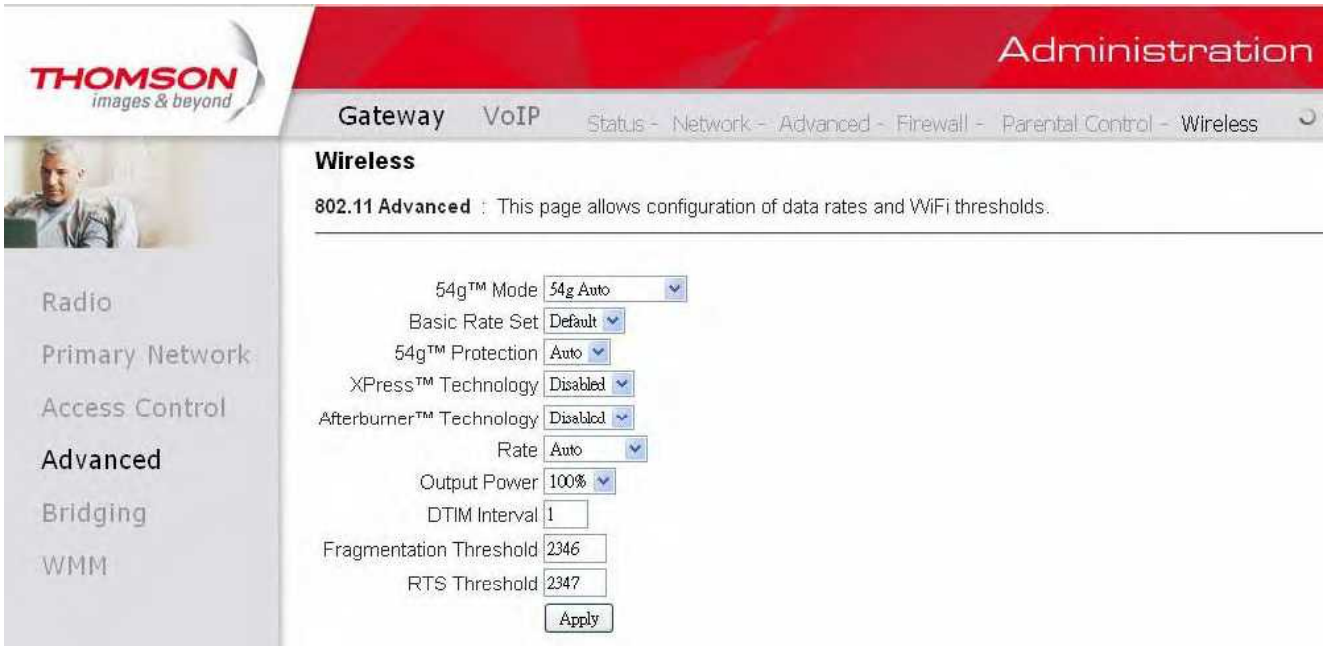


Fig. 42

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 Wireless 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)

54gTM Network Mode:
There are three modes for you to choose, please check the specification of your wireless card and choose a proper setting.

54gTM Protection:
Select Auto to turn on the 54gTM protection; select Off to turn down the protection.

XpressTM 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.

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

5. 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.

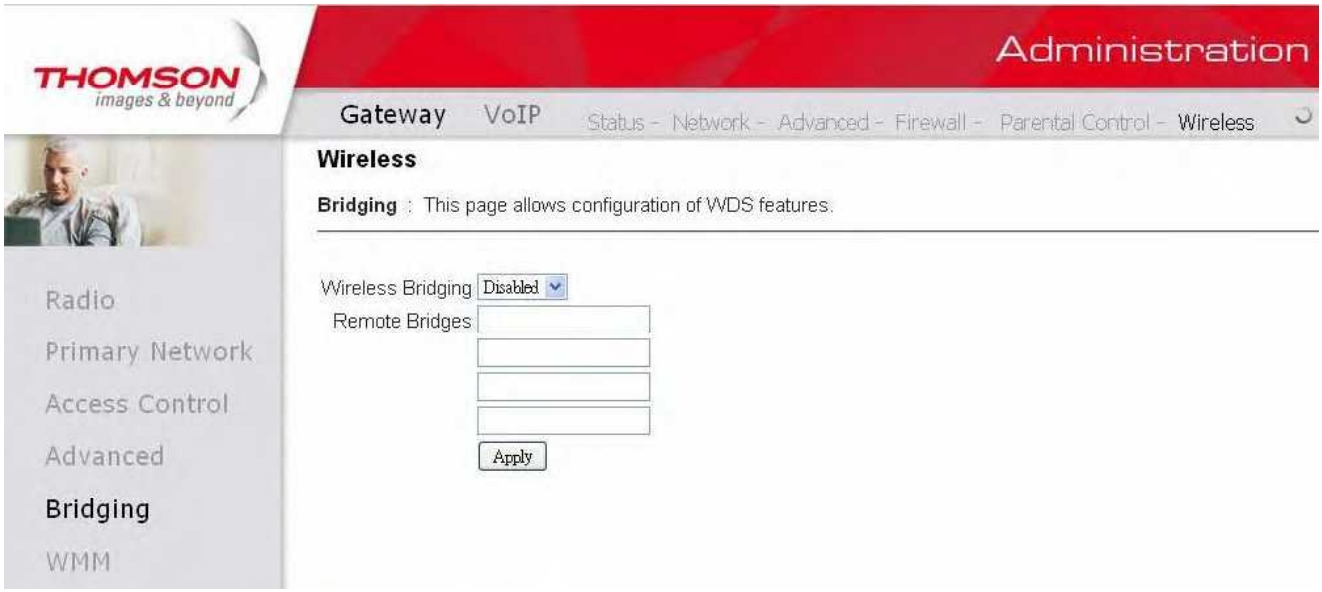


Fig. 43

- **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.

6. WMM

This page allows you to configure Wi-Fi Multi-Media (WMM). WMM is an implementation of Quality of Service (QoS) which is defined by the IEEE standard 802.11e.

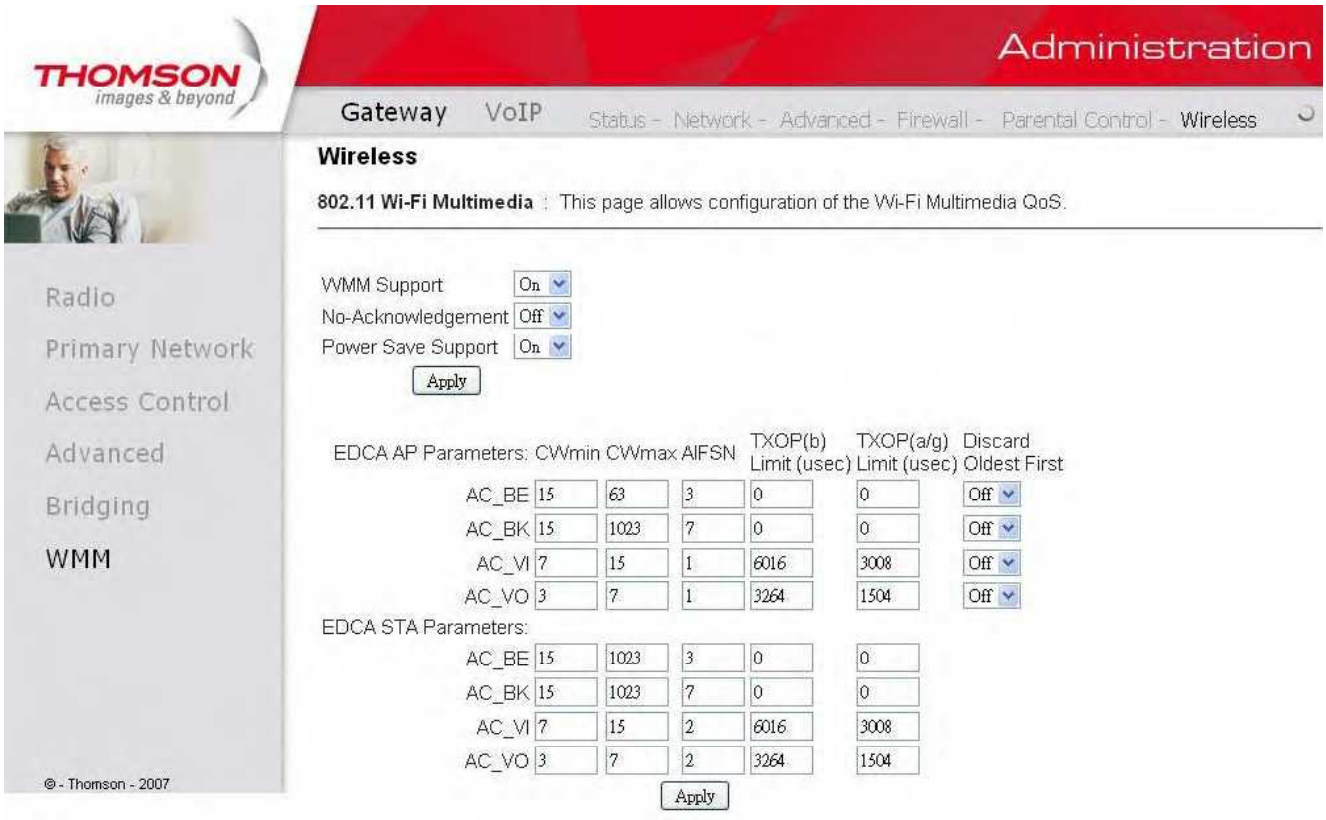


Fig. 44

WMM Support:

Sets WMM support. Choices are Auto, On or Off. If enabled (Auto or On), the WMM information Element is included in beacon frame.

No-Acknowledgement:

Sets No-Acknowledgement support. Choices are On or Off. When enabled, acknowledgments for data are not transmitted.

Power Save Support:

Sets Power Save Support. Choices are On or Off. When Power Save is enabled, the AP queues packets for STAs that are in power-save mode. Queued packets are transmitted when the STA notifies AP that it has left power-save mode.

EDCA AP Parameters:

Specifies the transmit parameters for traffic transmitted from the AP to the STA for the four Access Categories: Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO).

Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).
There are also two AP-specific settings: Admission Control and Discard Oldest First. Admission control specifies if admission control is enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. On discards the oldest first; Off discards the newest first.

EDCA STA Parameters:
Specifies the transmit parameters for traffic transmitted from the STA to the AP for the four Access Categories: Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

VoIP – Basic Web Page Group

1. 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.

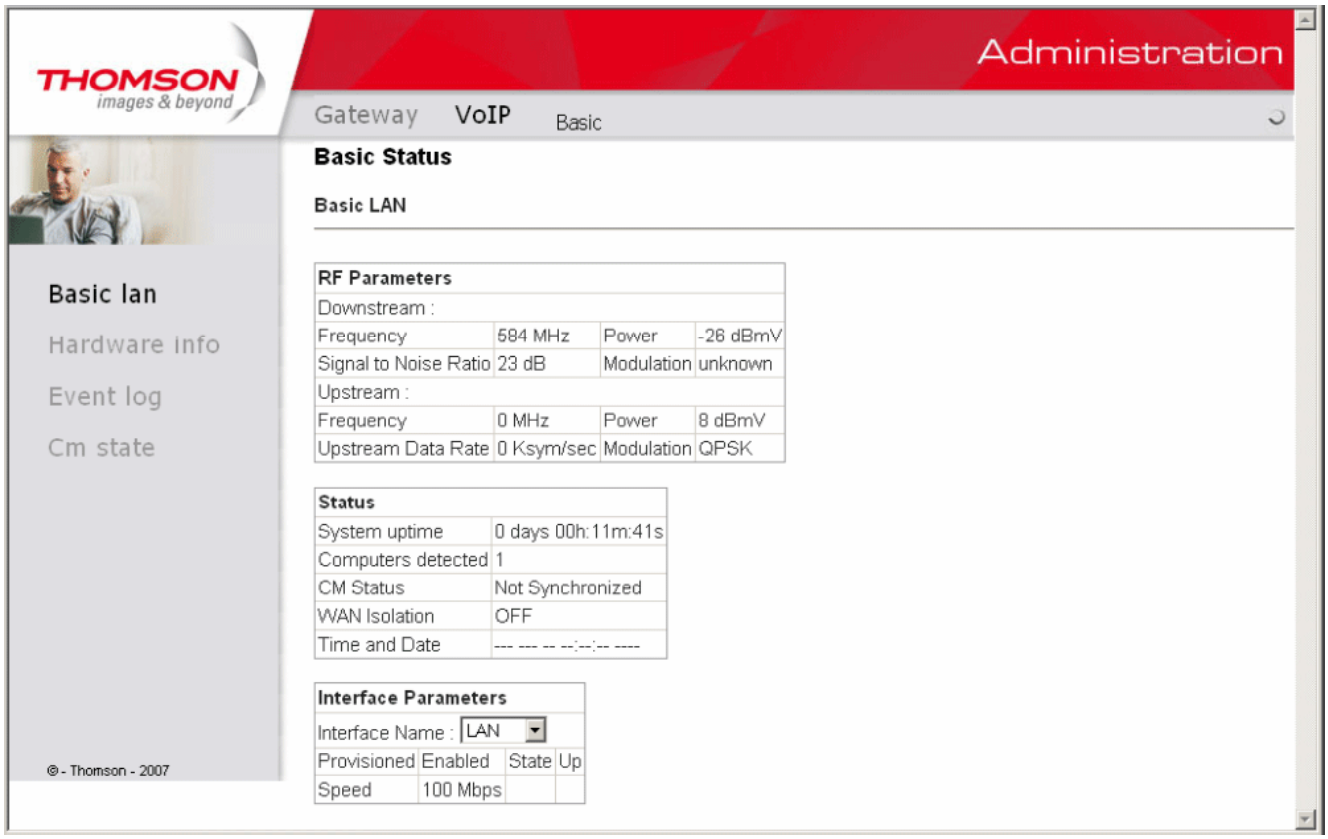


Fig.45

Chapter 2: Web Configuration

2. Hardware Info

The hardware Info is displayed on this page.

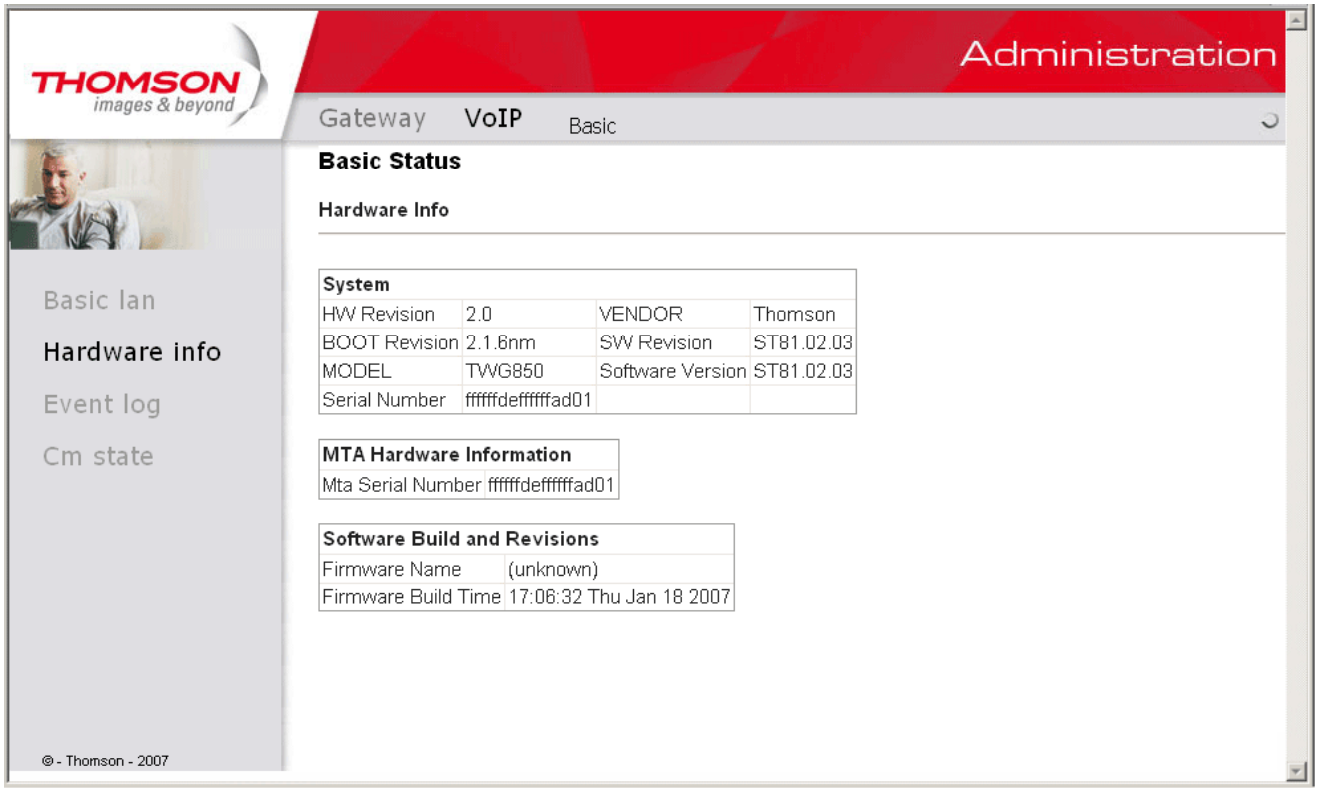
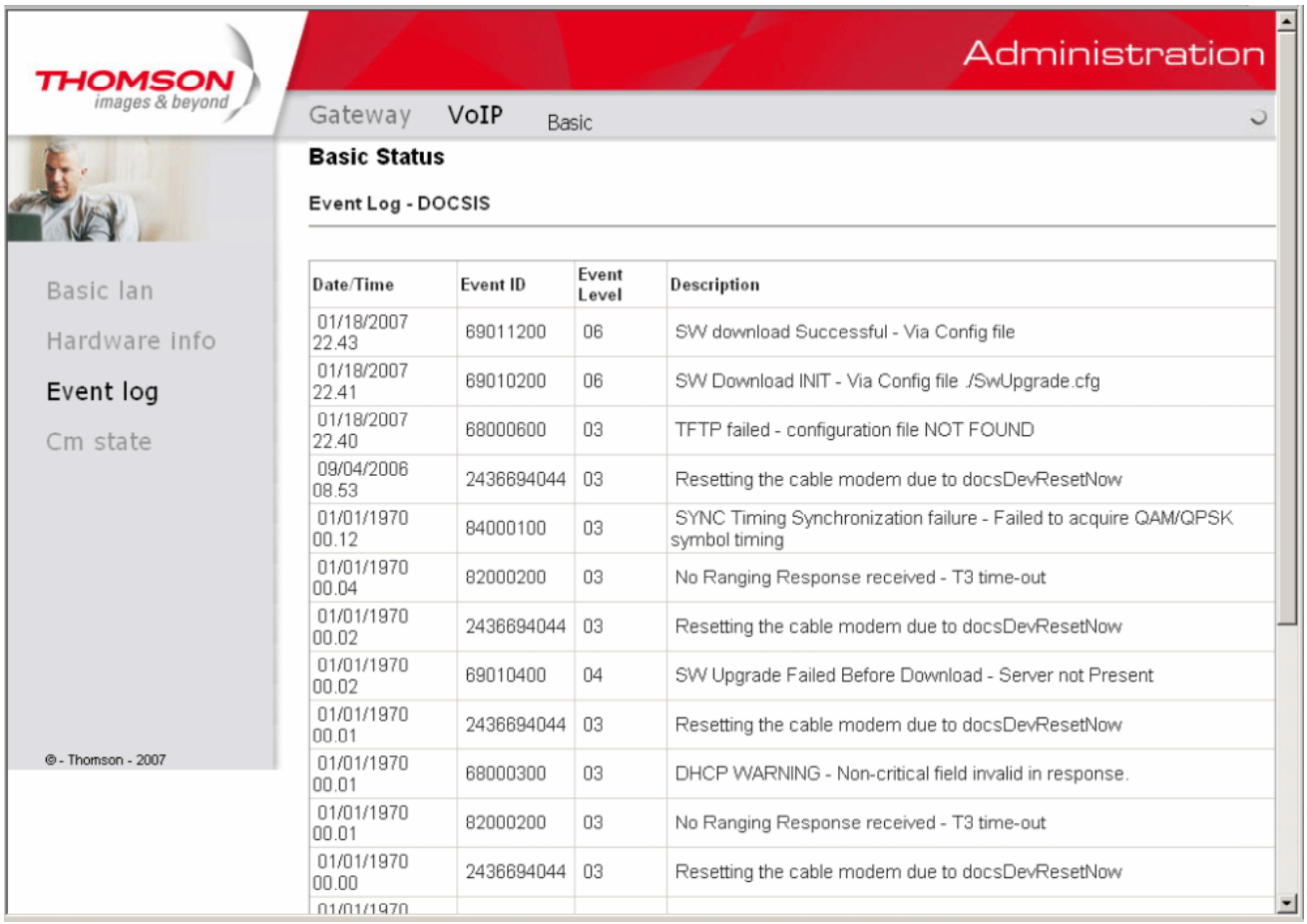


Fig. 46

3. Event Log

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



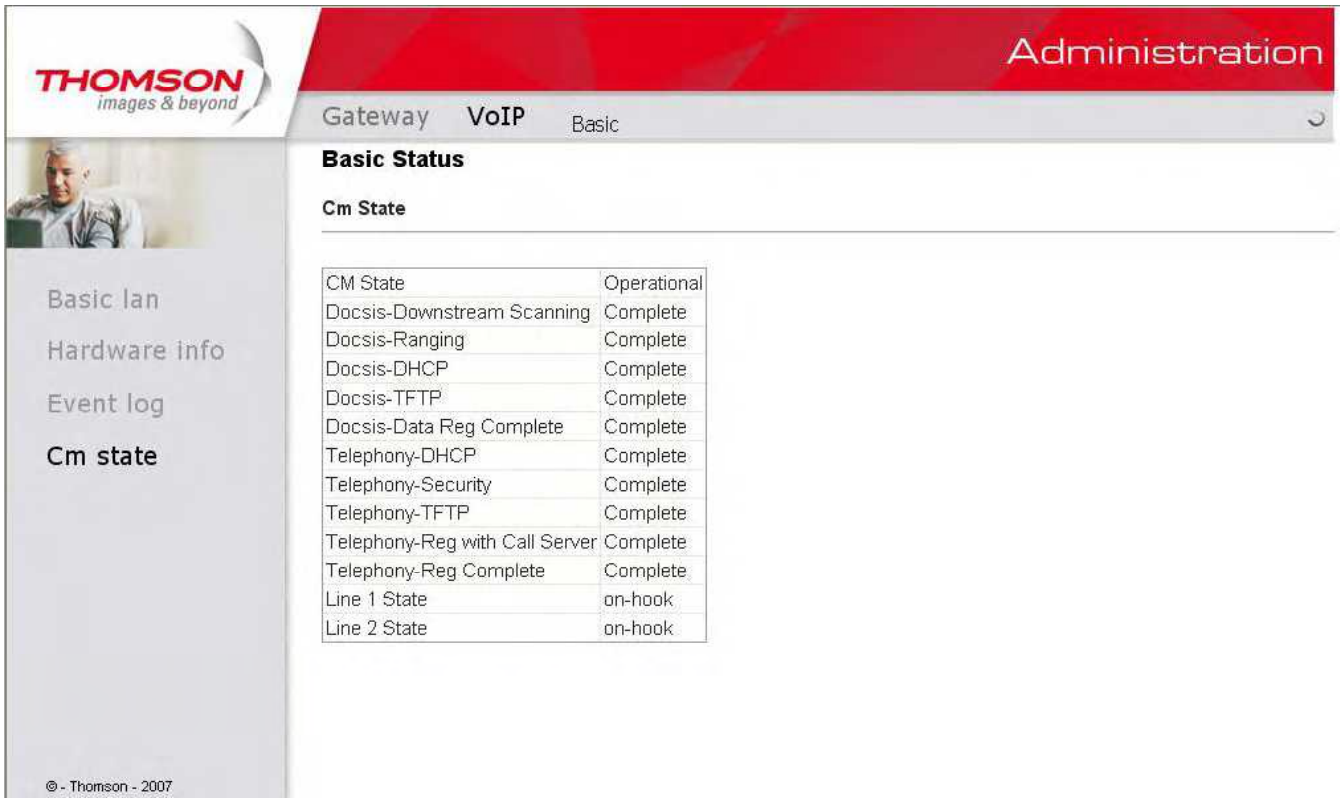
Date/Time	Event ID	Event Level	Description
01/18/2007 22.43	69011200	06	SW download Successful - Via Config file
01/18/2007 22.41	69010200	06	SW Download INIT - Via Config file ./SwUpgrade.cfg
01/18/2007 22.40	68000600	03	TFTP failed - configuration file NOT FOUND
09/04/2006 08.53	2436694044	03	Resetting 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

Fig. 47

Chapter 2: Web Configuration

4. CM State

This page shows the current state of the cable modem.



CM State	Operational
Docsis-Downstream Scanning	Complete
Docsis-Ranging	Complete
Docsis-DHCP	Complete
Docsis-TFTP	Complete
Docsis-Data Reg Complete	Complete
Telephony-DHCP	Complete
Telephony-Security	Complete
Telephony-TFTP	Complete
Telephony-Reg with Call Server	Complete
Telephony-Reg Complete	Complete
Line 1 State	on-hook
Line 2 State	on-hook

Fig. 48

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 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 Residential Voice Gateway will work with all upgraded cable systems that are DOCSIS-compliant.

Q. What is PacketCable and what does it mean?

A. Like DOCSIS, 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 PacketCable-compliant.

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 may apply.

** Additional equipment required. Contact your Cable Company and ISP for any restrictions or additional fees.

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 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 or some 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 22 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, be sure to connect to port TEL1/2.

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

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:	Model: DWG855
Equipment Classification:	Computing Device Accessory
Responsible Party:	Thomson Inc.
	101 West 103rd Street
	Indianapolis, IN 46290
	Telephone: 317-574-0496

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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Chapter 3: Additional Information

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

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 (Hyper Text 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.

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.

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.

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.

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.

101 W 103rd Street

Indianapolis, IN 46290

Fore more information
Thomson 46, quai Alphonse Le Gallo 92100 Boulogne-Billancourt France
Fax : 33 (0) 141 86 56 59 www.thomson-broadband.com

RCA by THOMSON