



CABLE

SATELLITE

TELECOM

TERRESTRIAL

DWG855 - Residential Voice Gateway

User manual

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.

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° to 40° C (32° to 104° F)

Storage Temperature: -30° to 65° C (-22° to 149° F)

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: _____

Chapter 1: Connections and Setup

Chapter 1: Connections and Setup	4
Introduction.....	4
Residential Voice Gateway Features	4
What's on the CD-ROM	4
Computer Requirements	5
Wall Mounting.....	6
Residential Voice Gateway DWG855 Overview	7
Front Panel	7
Rear Panel	9
Installing the Battery	9
Flank Panel	10
Relationship among the Devices	11
What the Modem Does.....	11
What the Modem Needs to Do Its Job	11
Contact Your Local Cable Company	12
Connecting the Residential Voice Gateway to a Single Computer	13
Attaching the Cable TV Wire to the Residential Voice Gateway	13
Important Connection Information	13
Ethernet Connection to One Computer	14
Connecting More Than Two Computers to the Residential Voice Gateway.....	15
Telephone or Fax Connection.....	16
Activating the Residential Voice Gateway	17
Chapter 2: Web Configuration	18
Accessing the Web Configuration.....	18
Outline of Web Manager.....	19
Gateway - Status Web Page Group	20

Chapter 1: Connections and Setup

1. Software	20
2. Connection	21
3. Password.....	22
4. Diagnostics.....	23
5. Event Log.....	24
6. Backup/Restore.....	25
Gateway – Network Web Page Group.....	26
1. LAN	26
2. WAN.....	27
3. Computers	28
4. DDNS	29
5. Time	30
Gateway – Advanced Web Page Group	31
1. Options.....	31
2. IP Filtering	32
3. MAC Filtering.....	33
4. Port Filtering.....	34
5. Forwarding	35
6. Port Triggers	36
7. DMZ Host	37
8. RIP (Routing Information Protocol) Setup.....	38
Gateway – Firewall Web Page Group	39
1. Web Content Filtering.....	39
2. TOD Access Filtering	40
3. Local Log and Remote Log	41
Gateway – Parental Control Web Page Group.....	42

Chapter 1: Connections and Setup

Basic Setup	42
Gateway – Wireless Web Page Group	43
1. Radio	44
2. Primary Network	45
3. Guest Networks	53
4. Access Control	54
5. Advanced	55
6. Bridging	57
7. WMM	58
VoIP – Basic Web Page Group	60
1. Basic LAN	60
2. Hardware Info	61
3. Event Log	62
4. CM State	63
5. Battery	64
Chapter 3: Additional Information	65
Frequently Asked Questions	65
General Troubleshooting	67
FCC Declaration of Conformity and Industry Canada Information	69
Service Information	70
Glossary	71

Chapter 1: Connections and Setup

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.

Chapter 1: Connections and Setup

Wall Mounting

The number of the screw: 2 pcs

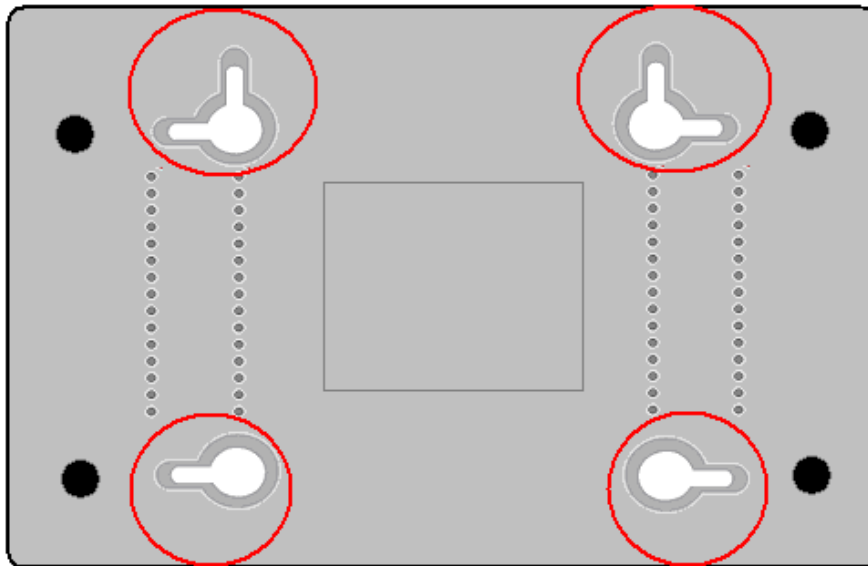
Direction for wall mounting: LED panel upward.

Dimension for the screw: 4.4 mm (0.17 inch)

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 (0.17 inch) 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:

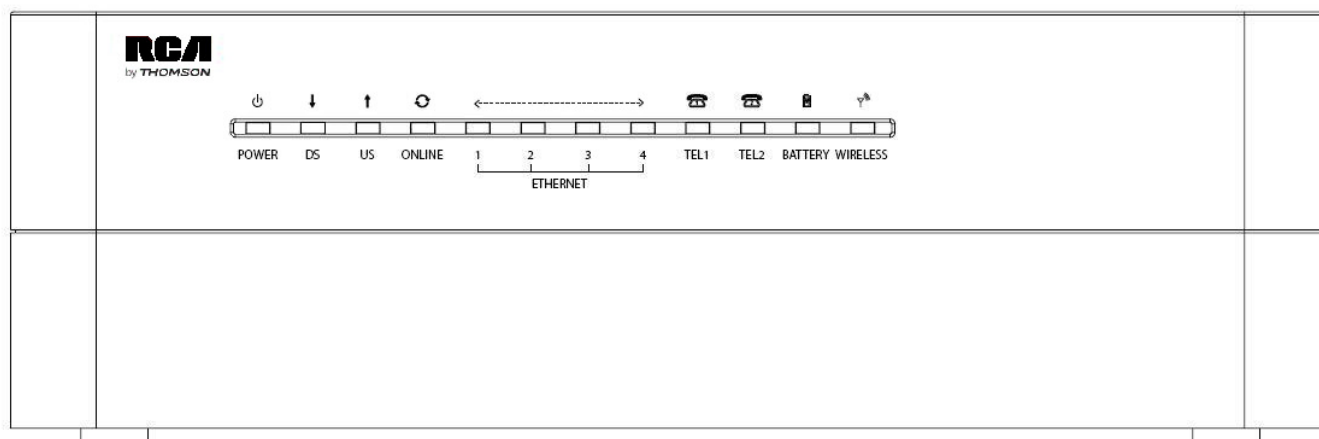
1. Ensure that the wall you use is smooth, flat, dry and sturdy and use the 4 screw holes which are 101.6 mm (4 inches) apart from each other.
2. Fix the screws into wall, leaving their heads 3 mm (0.12 inch) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw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

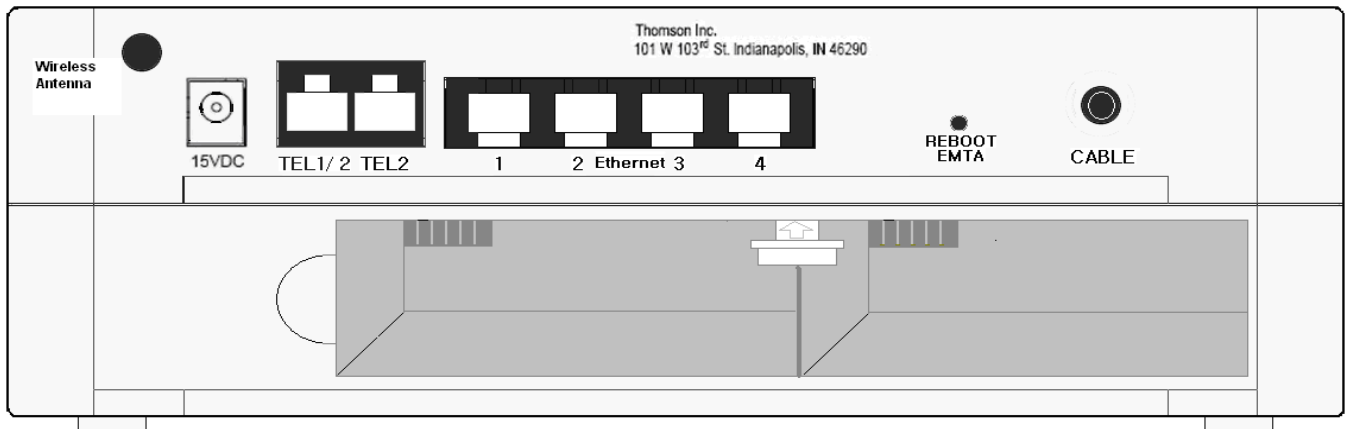
DWG855T/ DWG855CH	Power	Internet			Ethernet				Tel 1	Tel 2	Battery	Wireless	Description
		DS	US	Online	1	2	3	4					
Boot-up Operation	ON	ON	ON	ON	ON	ON	ON	ON	ON	ON	X	ON	Power on 0.25 sec
	ON	0.25 second			ON	ON	ON	ON	ON	ON	X	ON	From power ON to system initialization complete
	ON	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	Following system initialization complete to (before) DS scanning
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Following system initialization complete to (before) DS scanning
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)
	ON	ON	ON	ON	X	X	X	X	FLASH	OFF	OFF	X	MTA DHCP
MTA initialization	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
	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
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	ON	<CM Normal Operation>							ON	ON	ON	<CM Normal	Both Lines On-Hook

Chapter 1: Connections and Setup

DWG855T/ DWG855CH	Power	Internet			Ethernet				Tel 1	Tel 2	Battery	Wireless	Description								
		DS	US	Online	1	2	3	4													
Battery Good	ON								FLASH	ON		Operation>	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	ON		ON	ON	ON	ON	ON	FLASH	Both Lines On-Hook	Both Lines On-Hook	
	ON								ON	ON	ON		ON	ON	ON	ON	ON		Tel1 Off-hook, Tel2 On-hook	Tel1 Off-hook, Tel2 On-hook	
	ON								ON	ON	ON		ON	ON	ON	ON	ON		Tel1 On-hook, Tel2 Off-hook	Tel1 On-hook, Tel2 Off-hook	
	ON								ON	ON	ON		ON	ON	ON	ON	ON		Both Lines Off-Hook	Both Lines Off-Hook	
AC Good Battery Bad	ON								ON	ON	ON		ON	ON	ON	ON	ON	OFF	Both Lines On-Hook	Both Lines On-Hook	
	ON								ON	ON	ON		ON	ON	ON	ON	ON		Tel1 Off-hook, Tel2 On-hook	Tel1 Off-hook, Tel2 On-hook	
	ON								ON	ON	ON		ON	ON	ON	ON	ON		Tel1 On-hook, Tel2 Off-hook	Tel1 On-hook, Tel2 Off-hook	
	ON								ON	ON	ON		ON	ON	ON	ON	ON		Both Lines Off-Hook	Both Lines Off-Hook	
AC Fail Battery Good	FLASH								OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	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	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								
	< All LEDs may be unlit due to lack of battery power>											Tel1 Off-hook, Tel2 On-hook									
	< All LEDs may be unlit due to lack of battery power>											Tel1 On-hook, Tel2 Off-hook									
	< All LEDs may be unlit due to lack of battery power>											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

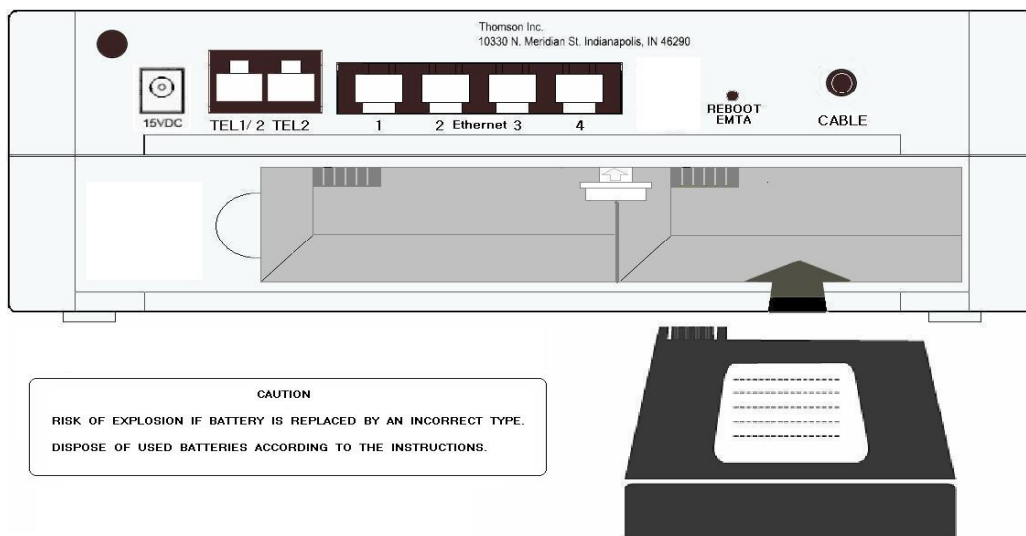
15VDC:

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.



Chapter 1: Connections and Setup

Flank Panel

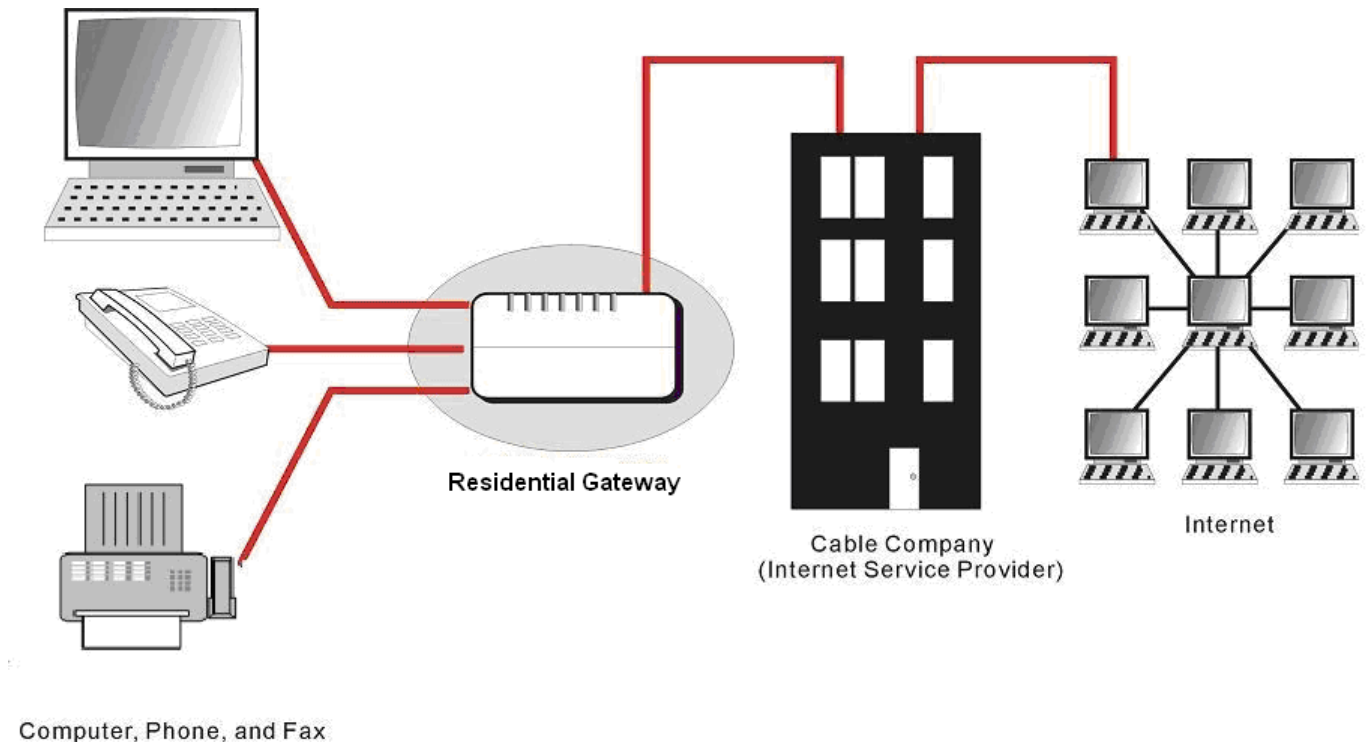


- WPS: WiFi Protected Setup

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

Chapter 1: Connections and Setup

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.

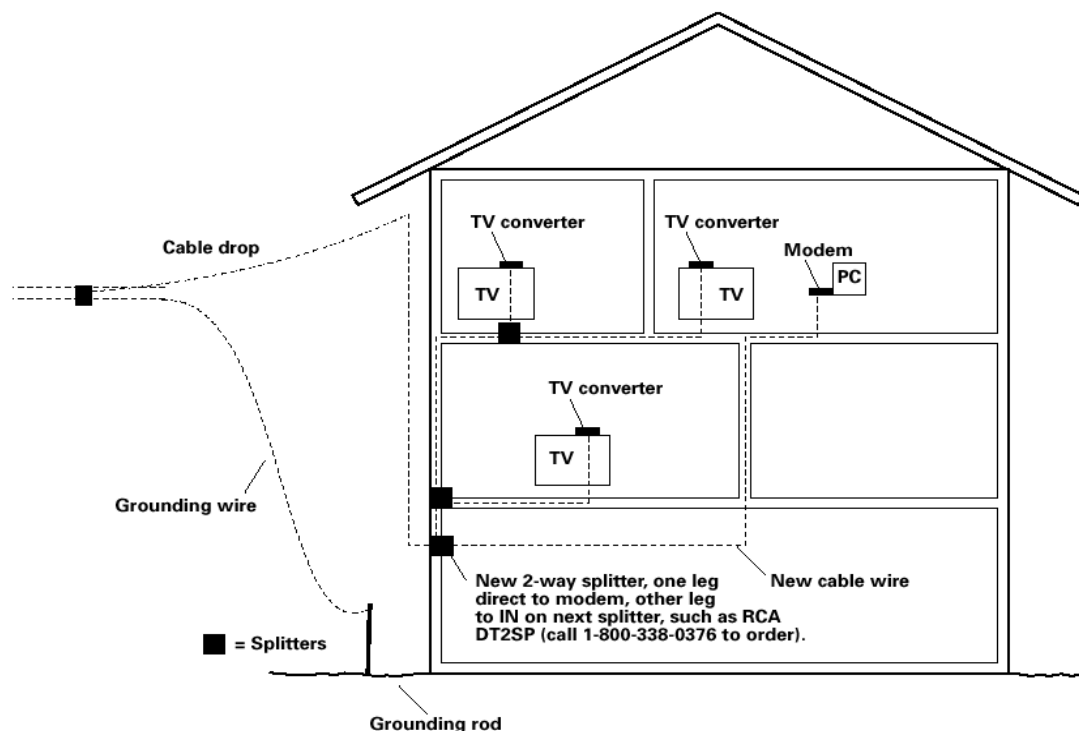


Fig. 1: Basic Home Wiring

Important Connection Information

The Residential Voice Gateway supports Telephone and Ethernet connections simultaneously.

Chapter 1: Connections and Setup

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

- For Ethernet connections, go to page 14.
- For telephone and fax connections, go to page 16.

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 DC jack on the Residential Voice Gateway, and plug the power supply into an AC outlet.
3. Note: Use only the power supply that accompanied this unit. Using other adapters may damage the unit. 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.

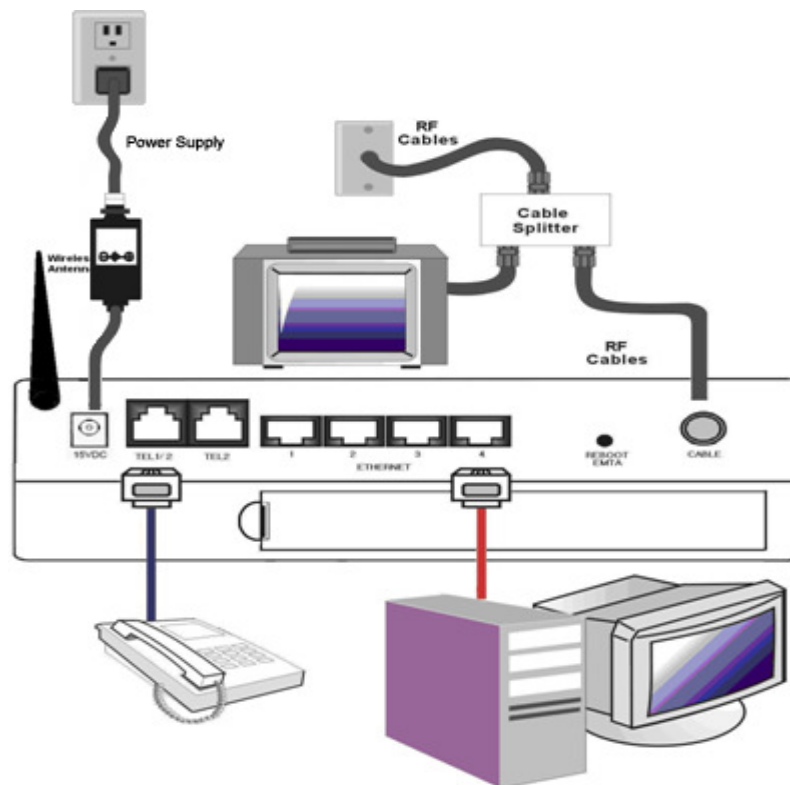


Fig.2 Ethernet Connection

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.

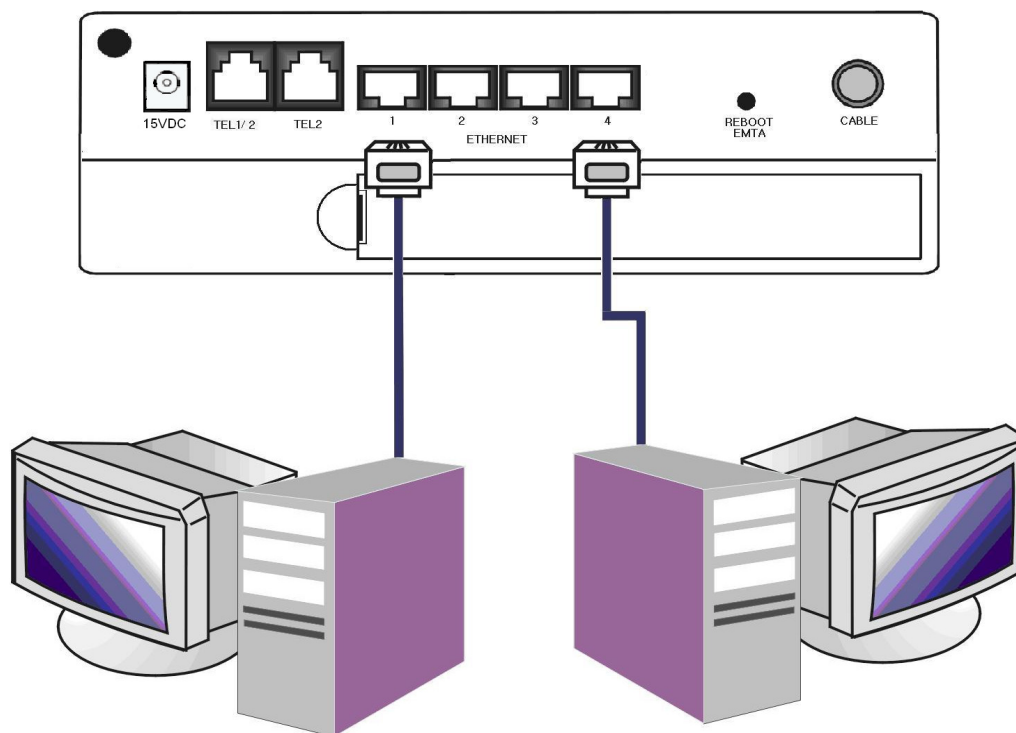


Fig.3: Multiple-PC Connection

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

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.

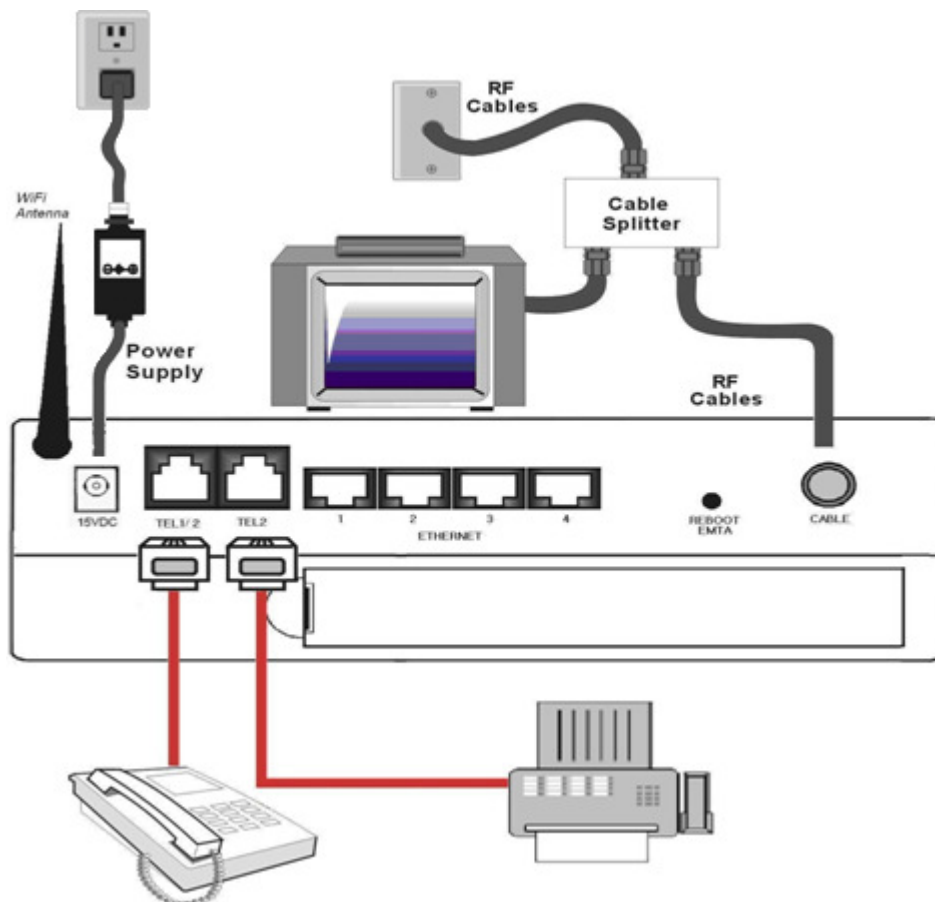


Fig. 4- Phone/Fax Connection

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.

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: **192.168.0.1**
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. 5 Dialogue for Login

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.

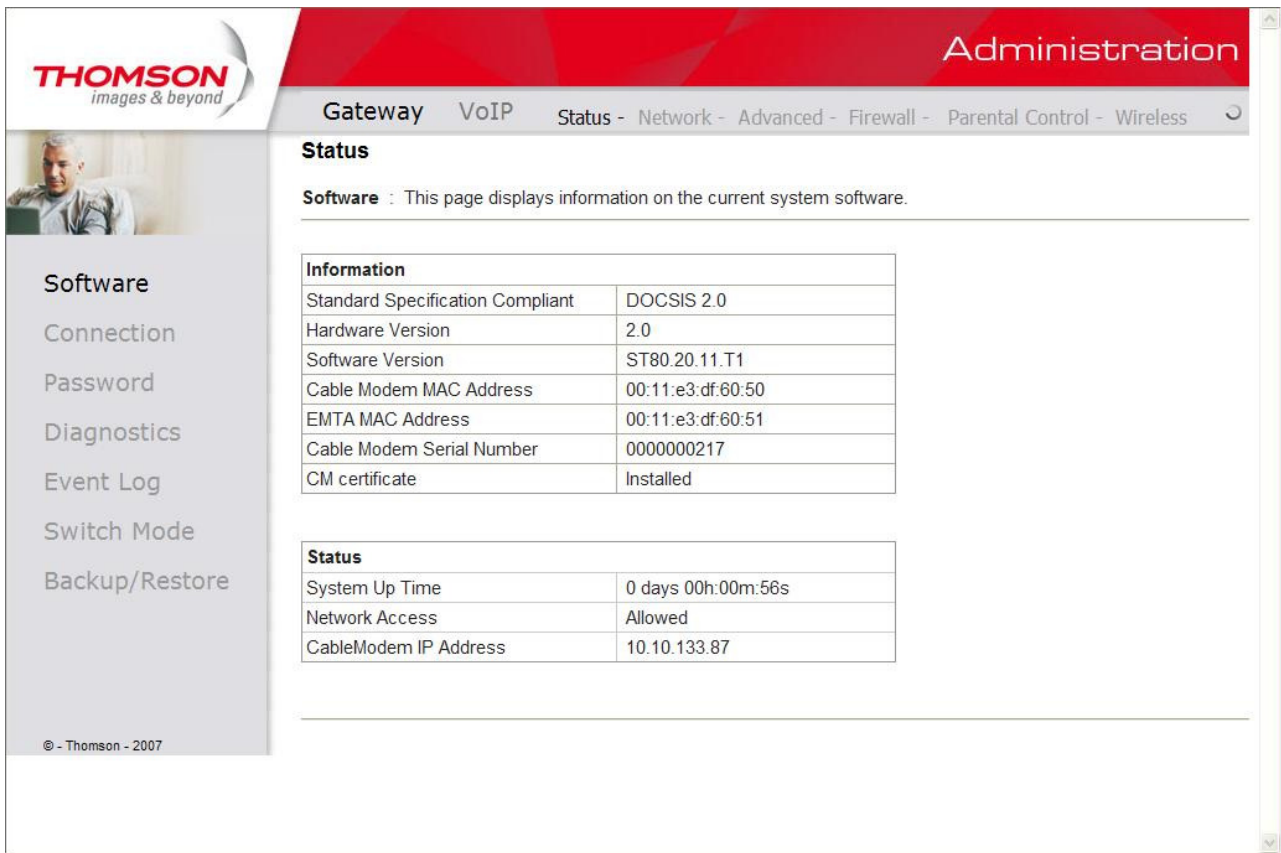


Fig. 6 Outline of Web Manager

- **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.

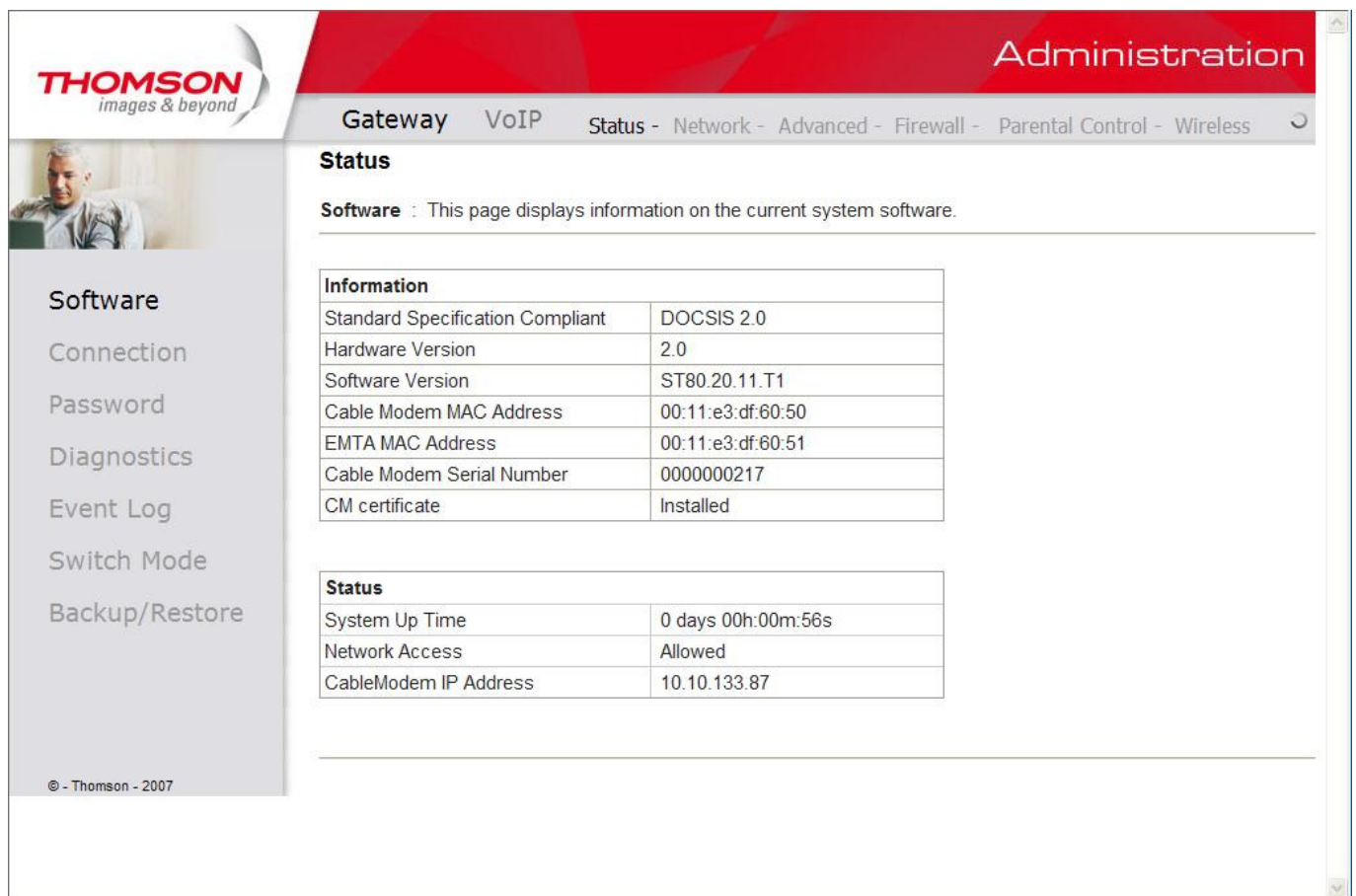
Chapter 2: Web Configuration

Gateway - Status Web Page Group

1. 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', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The left sidebar lists various configuration options: Software, Connection, Password, Diagnostics, Event Log, Switch Mode, and Backup/Restore. The main content area is titled 'Status' and contains a 'Software' section with a descriptive text and two tables of system information.

Information

Standard Specification Compliant	DOCSIS 2.0
Hardware Version	2.0
Software Version	ST80.20.11.T1
Cable Modem MAC Address	00:11:e3:df:60:50
EMTA MAC Address	00:11:e3:df:60:51
Cable Modem Serial Number	0000000217
CM certificate	Installed

Status

System Up Time	0 days 00h:00m:56s
Network Access	Allowed
CableModem IP Address	10.10.133.87

Fig. 7 Gateway\Status\Software

Chapter 2: Web Configuration

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.

THOMSON
images & beyond

Administration

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

Status

Connection : This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	453001000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	wayne-basic-D2.0.cfg
Security	Disabled	Disabled

Downstream Channel

Lock Status	Locked	Modulation	QAM256
Channel ID	4	Symbol rate	5360537
Downstream Frequency	453000000 Hz	Downstream Power	39.6 dBmV
SNR	32.6 dB		

Upstream Channel

Lock Status	Locked	Modulation	QPSK
Channel ID	1	Symbol rate	2560 Ksym/sec
Upstream Frequency	13008000 Hz	Upstream Power	33.0 dBmV

CM IP Address

CM IP Address	Duration	Expires
10.10.133.60	D: 06 H: 03 M: 20 S: 16	Mon Jul 05 14:43:10 2010

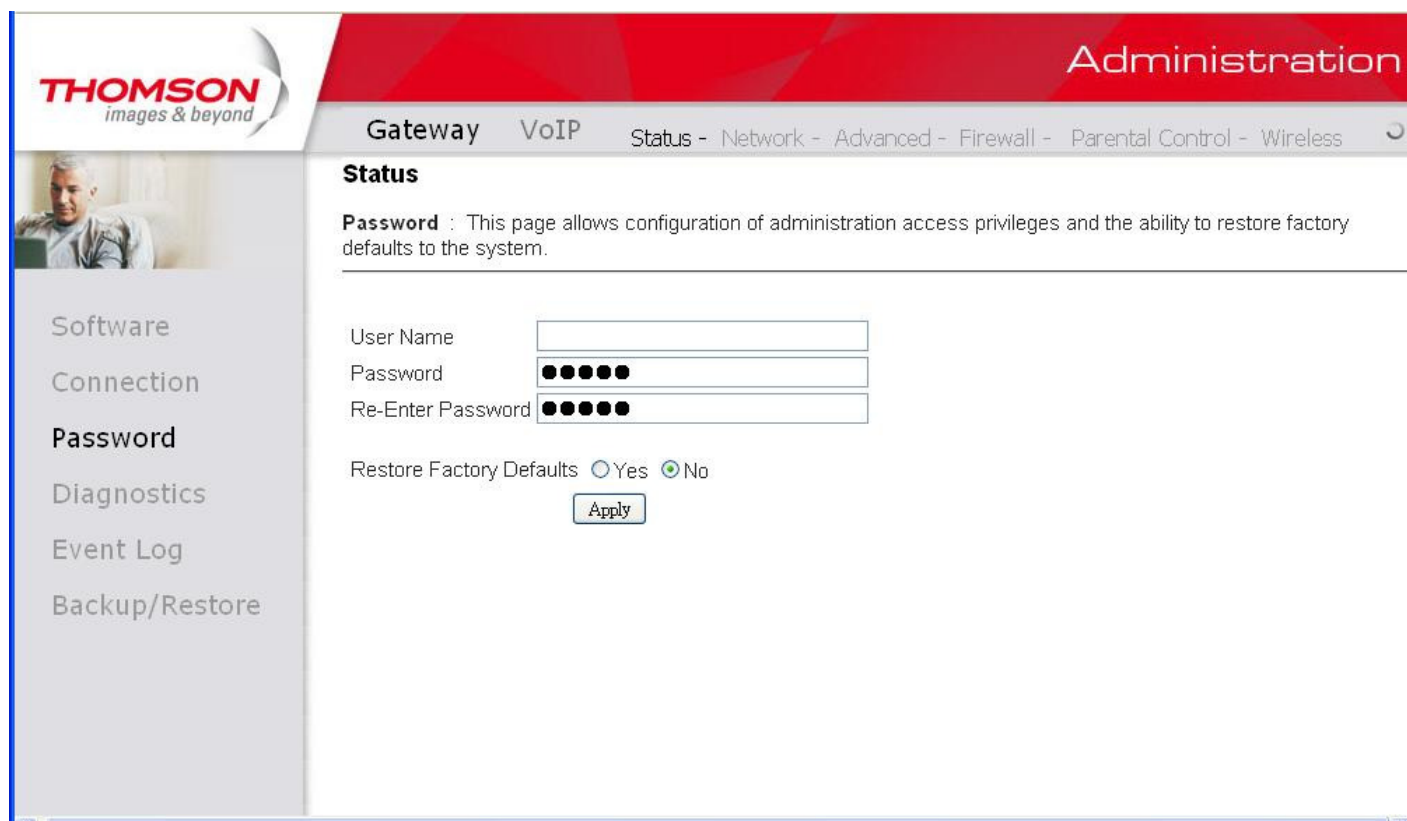
Current System Time: Tue Jun 29 10:33:05 2010

Fig. 8 Gateway\Status\Connection

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.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar is red with the Thomson logo on the left and the word "Administration" on the right. Below the navigation bar, there are tabs for "Gateway", "VoIP", "Status", "Network", "Advanced", "Firewall", "Parental Control", and "Wireless". The "Status" tab is selected. The main content area is titled "Status" and contains a description of the Password configuration page. Below the description, there are three input fields: "User Name", "Password", and "Re-Enter Password". The "Password" and "Re-Enter Password" fields are masked with black dots. Below the input fields, there is a "Restore Factory Defaults" section with two radio buttons: "Yes" and "No". The "No" radio button is selected. Below the radio buttons is an "Apply" button.

THOMSON
images & beyond

Administration

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

Status

Password : This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

User Name

Password

Re-Enter Password

Restore Factory Defaults ☐ Yes ☒ No

Fig. 9 Gateway\Status\Password

Chapter 2: Web Configuration

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.

THOMSON
images & beyond

Administration

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

Status

Diagnostics : This page provides for ping diagnostics to the LAN to help with IP connectivity problems.

Ping Test Parameters

Ping Target . . .

Ping Size bytes

No. of Pings

Ping Interval ms

Results

Pinging 192.168.100.1 with 64 bytes of data: [In progress]

To get an update of the results you must REFRESH the page.

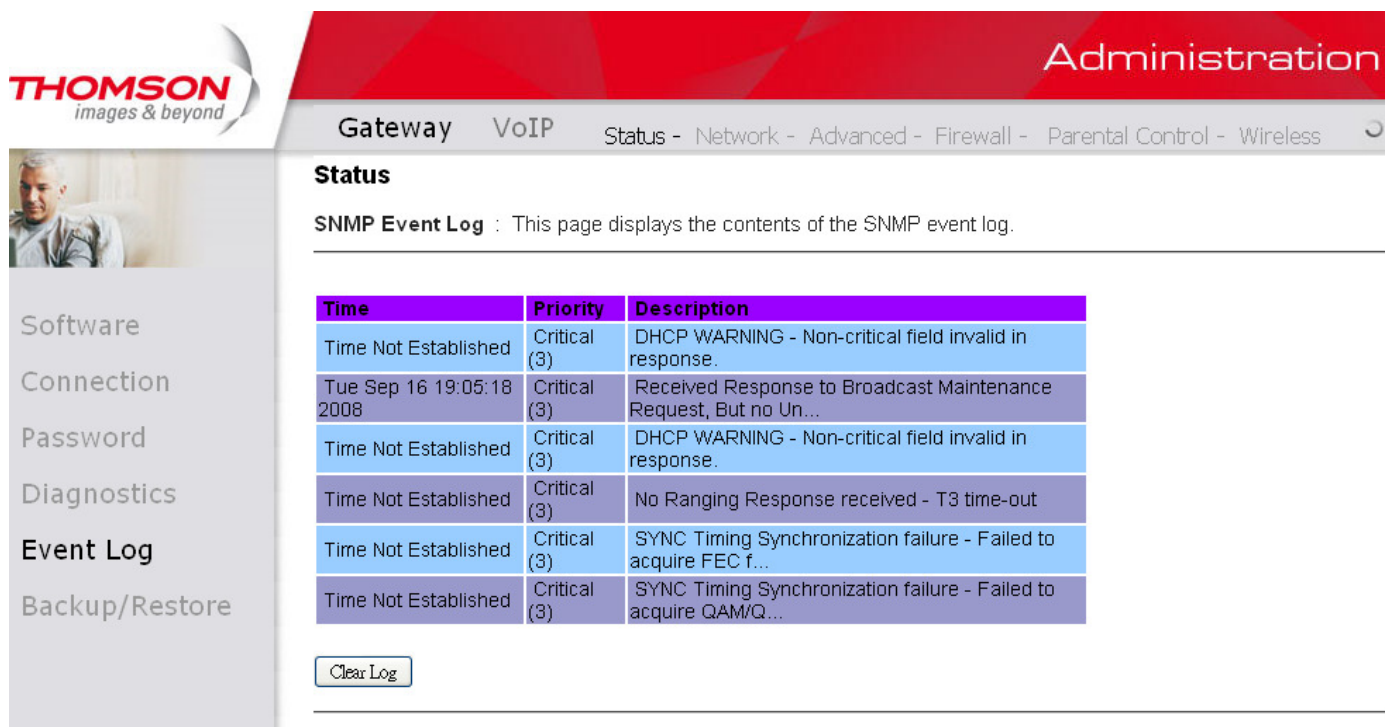
© - Thomson - 2007

Fig. 10 Gateway\Status\Diagnostics

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.



The screenshot shows the Thomson Gateway Administration web interface. The left sidebar contains navigation links: Software, Connection, Password, Diagnostics, **Event Log**, and Backup/Restore. The main content area has a red header with 'Administration' and a navigation bar with 'Gateway', 'VoIP', and a status menu (Status - Network - Advanced - Firewall - Parental Control - Wireless). Below the navigation bar, the 'Status' section is active, displaying the 'SNMP Event Log'. A text line states: 'SNMP Event Log : This page displays the contents of the SNMP event log.' Below this is a table with three columns: Time, Priority, and Description. The table contains six rows of event logs. At the bottom of the log section is a 'Clear Log' button.

Time	Priority	Description
Time Not Established	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Tue Sep 16 19:05:18 2008	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Time Not Established	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Time Not Established	Critical (3)	No Ranging Response received - T3 time-out
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire FEC f...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...

Fig. 11 Gateway\Status\Event Log

Chapter 2: Web Configuration

6. Backup/Restore

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

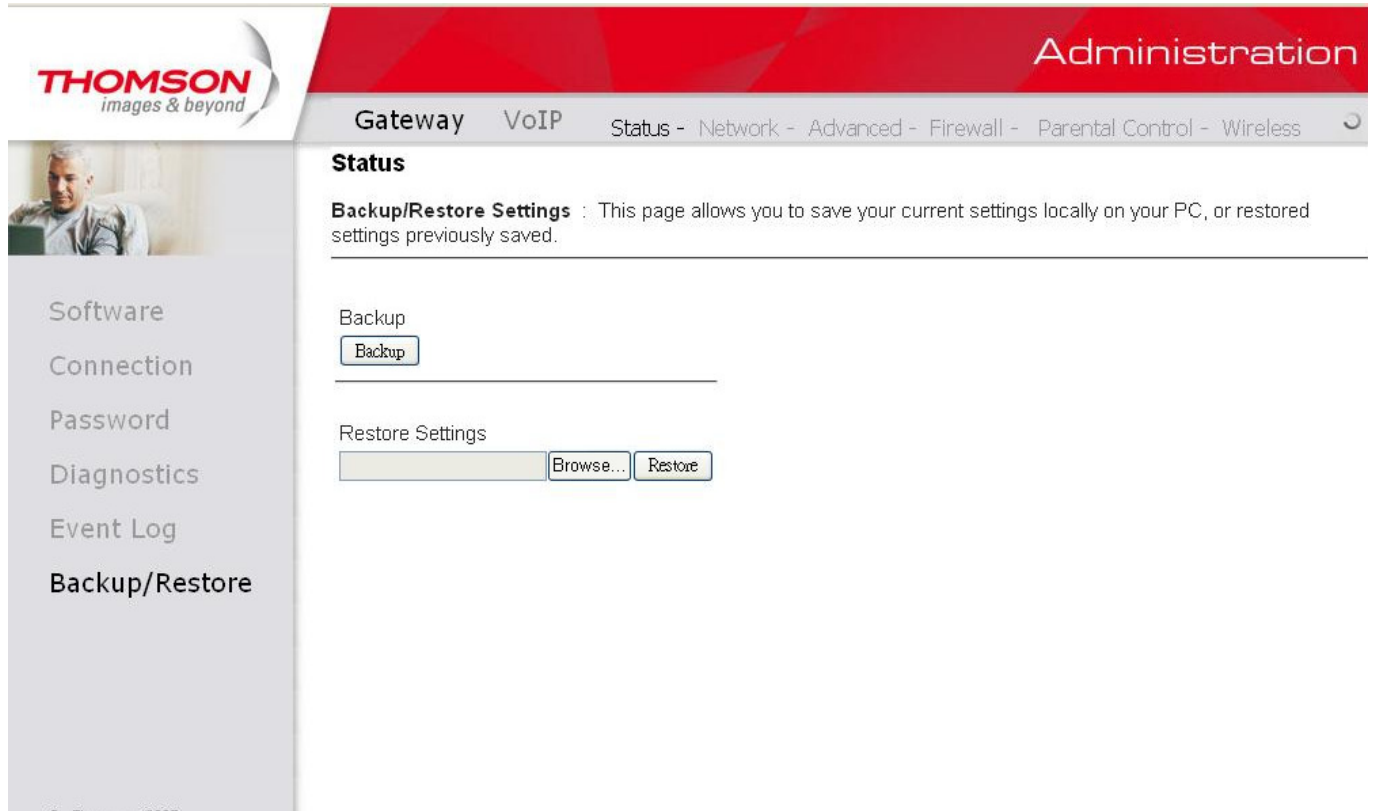


Fig. 12 Gateway\Status\Backup/Restore

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

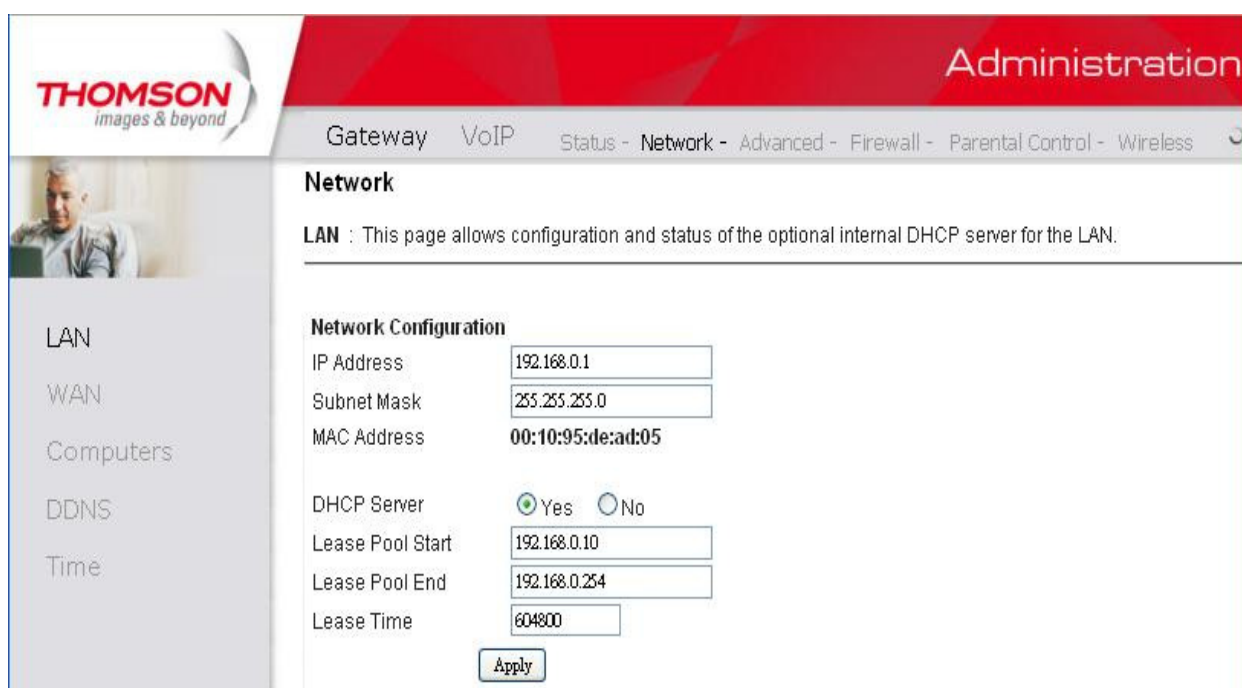
Gateway – Network Web Page Group

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**.



The screenshot displays the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Network' section is active, showing the 'LAN' configuration page. The page title is 'LAN : This page allows configuration and status of the optional internal DHCP server for the LAN.' The 'Network Configuration' section contains the following fields:

Field	Value
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	00:10:95:de:ad:05
DHCP Server	☒ Yes ☐ No
Lease Pool Start	192.168.0.10
Lease Pool End	192.168.0.254
Lease Time	604800

An 'Apply' button is located at the bottom of the configuration fields.

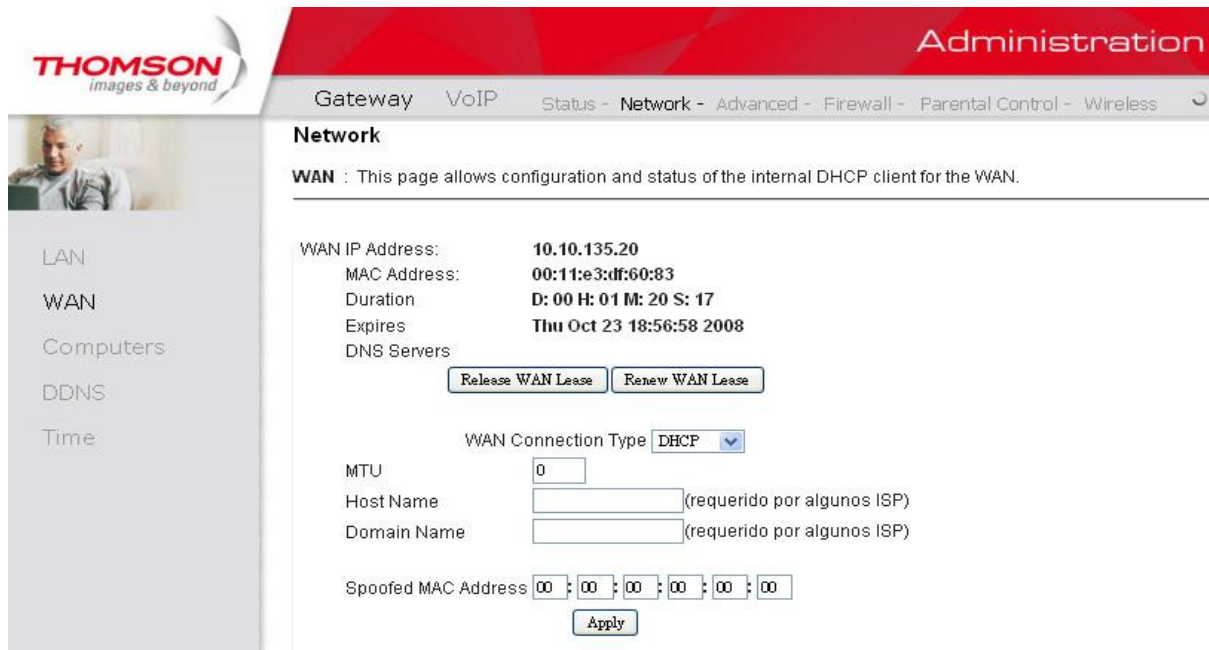
Fig. 13 Gateway\Network\LAN

Chapter 2: Web Configuration

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.



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' tab is selected. The left sidebar contains links for 'LAN', 'WAN', 'Computers', 'DDNS', and 'Time'. The main content area is titled 'WAN' and includes a description: 'This page allows configuration and status of the internal DHCP client for the WAN.' The configuration fields are as follows:

WAN IP Address:	10.10.135.20
MAC Address:	00:11:e3:df:60:83
Duration	D: 00 H: 01 M: 20 S: 17
Expires	Thu Oct 23 18:56:58 2008
DNS Servers	

Below the table are two buttons: 'Release WAN Lease' and 'Renew WAN Lease'. The 'WAN Connection Type' is set to 'DHCP' via a dropdown menu. Below this are input fields for 'MTU' (set to 0), 'Host Name', and 'Domain Name', each with a note '(requerido por algunos ISP)'. At the bottom, there is a 'Spoofed MAC Address' field with six input boxes for hexadecimal digits, followed by an 'Apply' button.

Fig. 14 Gateway\Network\WAN

Chapter 2: Web Configuration

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.

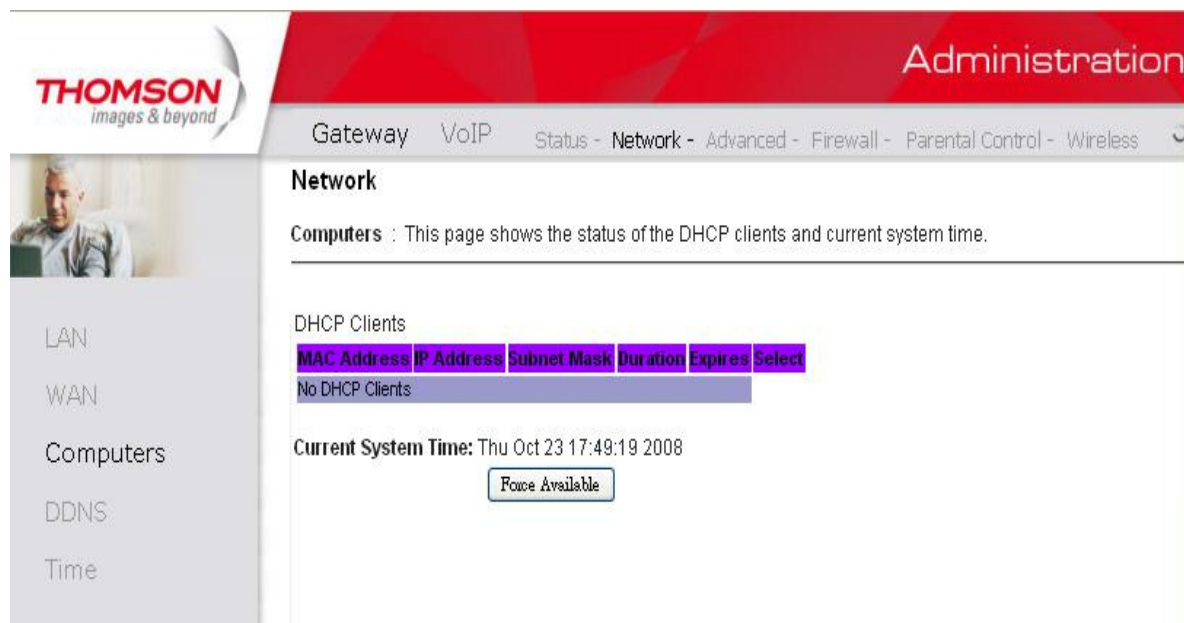


Fig. 15 Gateway\Network\Computers

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 DNS client compatible with the Dynamic DNS service (<http://www.dyndns.com/>).

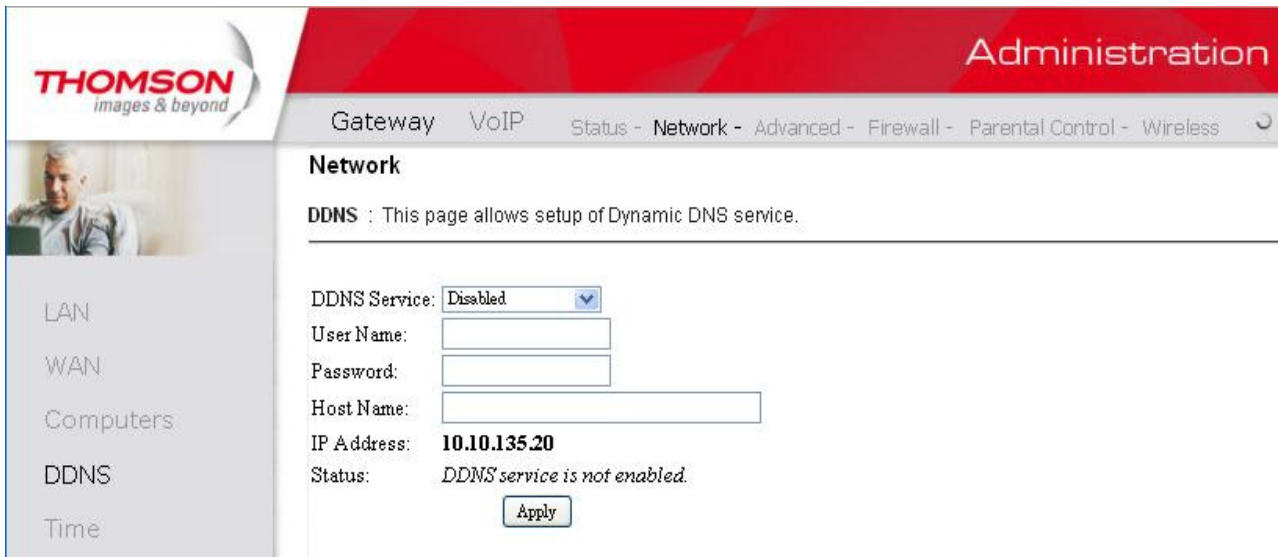


Fig. 16 Gateway\Network\DDNS

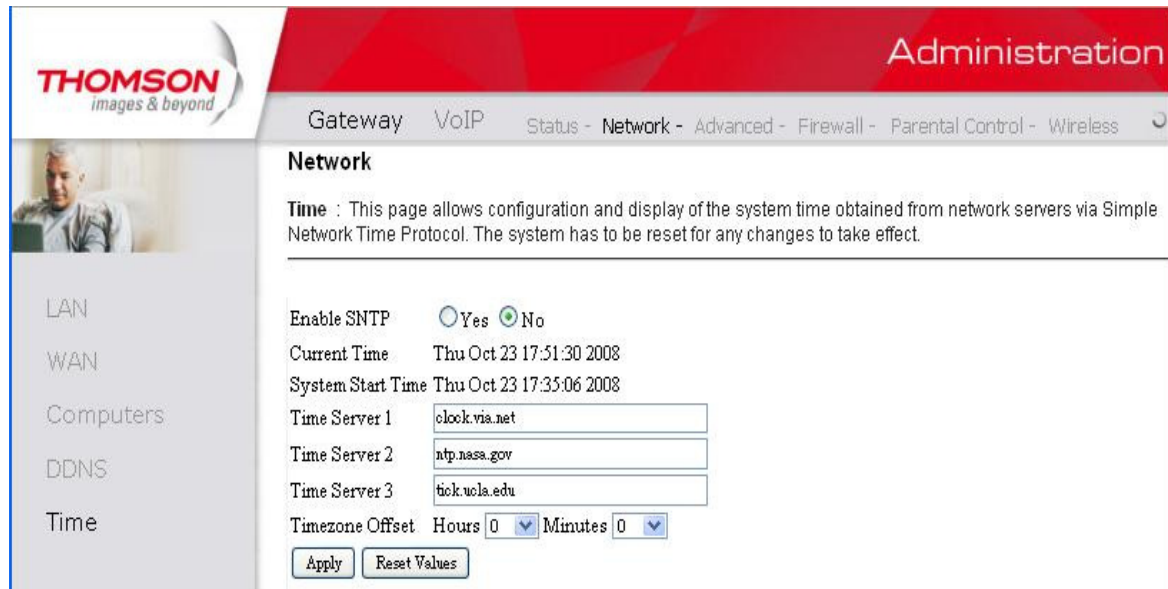
To activate the DDNS client:

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.

Chapter 2: Web Configuration

5. Time

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



The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes links for Gateway, VoIP, Status, Network (selected), Advanced, Firewall, Parental Control, and Wireless. The left sidebar contains links for LAN, WAN, Computers, DDNS, and Time (selected). The main content area is titled 'Network' and contains a 'Time' section. This section includes a description: 'Time : This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.' Below this, there are configuration options: 'Enable SNTP' with radio buttons for 'Yes' and 'No' (selected), 'Current Time' showing 'Thu Oct 23 17:51:30 2008', 'System Start Time' showing 'Thu Oct 23 17:35:06 2008', and three 'Time Server' fields with values 'clock.via.net', 'ntp.nasa.gov', and 'tick.ucla.edu'. At the bottom, there is a 'Timezone Offset' section with 'Hours' and 'Minutes' dropdown menus, both set to '0'. 'Apply' and 'Reset Values' buttons are located at the bottom of the configuration area.

Fig. 17 Gateway\Network\Time

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.

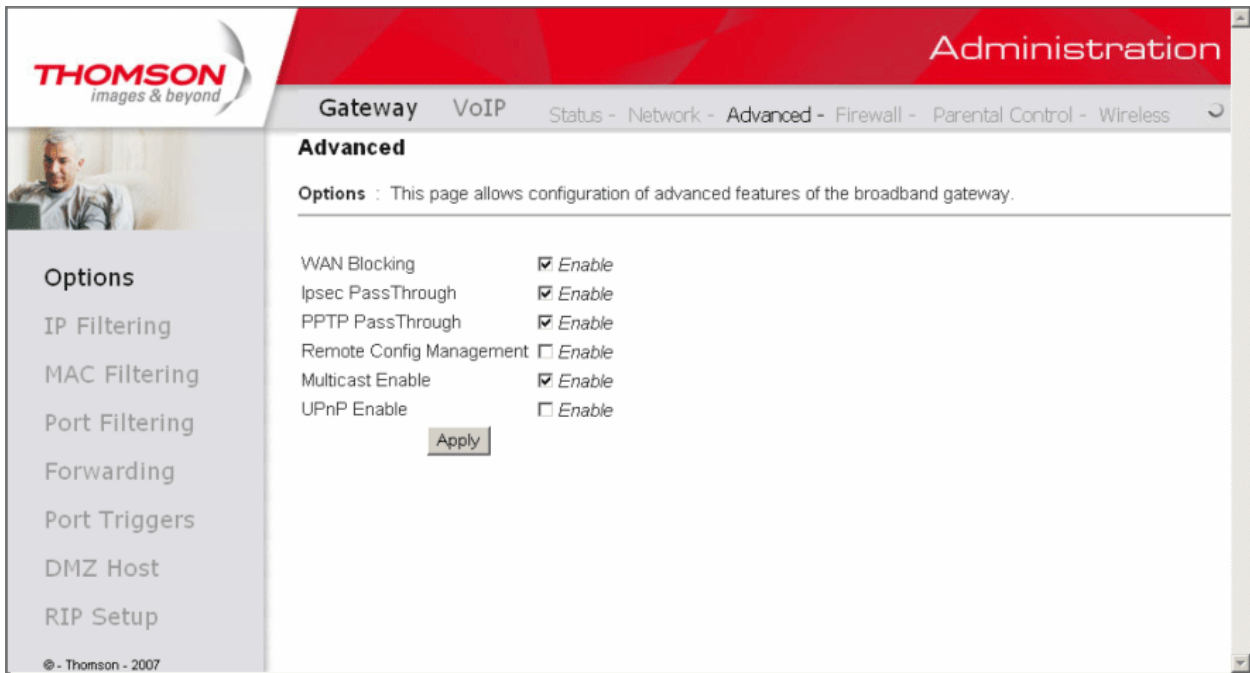


Fig. 18 Gateway\Advanced\Options

- **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.
- **Isec 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

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.

The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', and a series of tabs: 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Advanced' tab is selected. Below the navigation bar, the 'IP Filtering' section is active, displaying a table for configuring IP address filters. The table has three columns: 'Start Address', 'End Address', and 'Enabled'. There are ten rows, each with a text input field for the start address, a text input field for the end address, and a checkbox for the 'Enabled' status. All start and end addresses are currently set to '192.168.0.0'. An 'Apply' button is located below the table. On the left side of the interface, there is a sidebar with a list of options: 'Options', 'IP Filtering', 'MAC Filtering', 'Port Filtering', 'Forwarding', 'Port Triggers', 'DMZ Host', and 'RIP Setup'. The Thomson logo is visible in the top left corner, and the copyright notice '© - Thomson - 2007' is at the bottom left.

Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐

Apply

Fig. 19 Gateway\Advanced\IP Filtering

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.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', and a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Advanced' tab is selected. On the left, a sidebar lists options: 'Options', 'IP Filtering', 'MAC Filtering' (highlighted), 'Port Filtering', 'Forwarding', 'Port Triggers', 'DMZ Host', and 'RIP Setup'. The main content area is titled 'MAC Filtering' and contains the text: '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 for 'MAC Address Filters' with 20 rows, each containing a MAC address field (e.g., MAC 01, MAC 02, etc.) and a corresponding input field for the MAC address (format: 00:00:00:00:00:00). An 'Apply' button is located at the bottom right of the table.

MAC Address Filters	
MAC 01	00:00:00:00:00:00
MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00
MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00
MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00
MAC 08	00:00:00:00:00:00
MAC 09	00:00:00:00:00:00
MAC 10	00:00:00:00:00:00
MAC 11	00:00:00:00:00:00
MAC 12	00:00:00:00:00:00
MAC 13	00:00:00:00:00:00
MAC 14	00:00:00:00:00:00
MAC 15	00:00:00:00:00:00
MAC 16	00:00:00:00:00:00
MAC 17	00:00:00:00:00:00
MAC 18	00:00:00:00:00:00
MAC 19	00:00:00:00:00:00
MAC 20	00:00:00:00:00:00

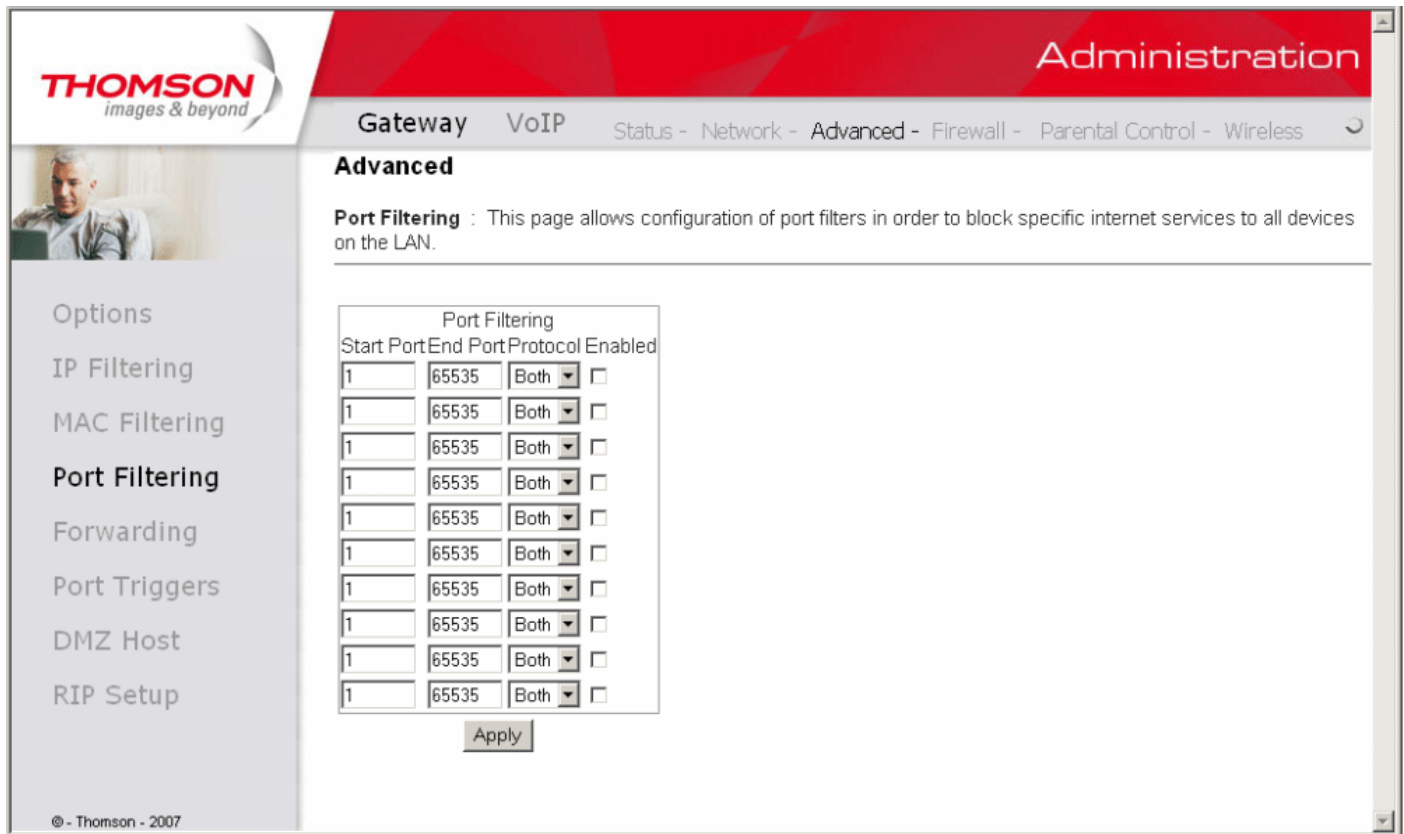
Apply

Fig. 20 Gateway\Advanced\MAC Filtering

Chapter 2: Web Configuration

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.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway' and 'VoIP' tabs, with a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Advanced' section is active, displaying the 'Port Filtering' configuration page. A sidebar on the left lists various configuration options, with 'Port Filtering' highlighted. The main content area contains a table for defining port filters, with columns for 'Start Port', 'End Port', 'Protocol', and 'Enabled'. The table is pre-filled with ten rows, each showing '1' for Start Port, '65535' for End Port, and 'Both' for Protocol. An 'Apply' button is located below the table. The Thomson logo and copyright notice '© - Thomson - 2007' are visible in the bottom left corner.

Start Port	End Port	Protocol	Enabled
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐
1	65535	Both	☐

Fig. 21 Gateway\Advanced\Port Filtering

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.

THOMSON
images & beyond

Administration

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

Advanced

Forwarding : This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Local IP Addr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐
192.168.0.0	0	0	Both	☐

Apply

Options
IP Filtering
MAC Filtering
Port Filtering
Forwarding
Port Triggers
DMZ Host
RIP Setup

© - Thomson - 2007

Fig. 22 Gateway\Advanced\Forwarding

Chapter 2: Web Configuration

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.

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 explains that this page allows configuration of dynamic triggers to specific devices on the LAN. Below the text is a table for configuring port triggers.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start	End	Start	End	Port	
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐
0	0	0	0	TCP	☐

An 'Apply' button is located at the bottom of the table.

Fig. 23 Gateway\Advanced\Port Triggers

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.

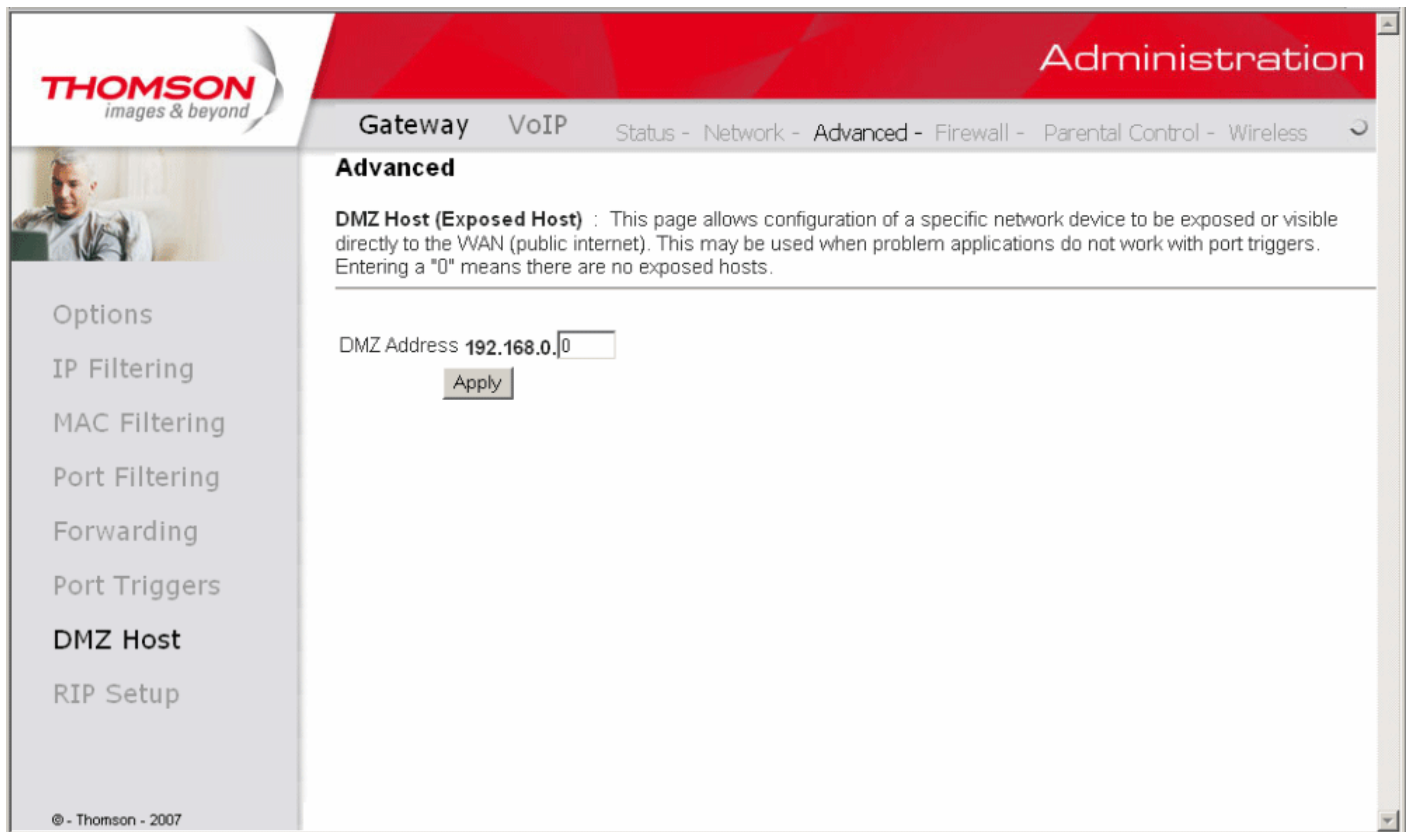


Fig. 24 Gateway\Advanced\DMZ Host

Chapter 2: Web Configuration

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.

The screenshot shows the Thomson Gateway web configuration interface. The top navigation bar includes 'Administration' and tabs for 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Advanced' tab is selected, and the 'RIP Setup' option is highlighted in the left sidebar. The main content area is titled 'Advanced' and contains the 'Routing Information Protocol Setup' section. This section includes a descriptive paragraph and several configuration fields: 'RIP Support' (set to 'Disabled'), 'RIP Authentication' (checked 'Enable'), 'RIP Authentication Key' (empty text box), 'RIP Authentication Key ID' (set to '0'), 'RIP Reporting Interval' (set to '30' seconds), and 'RIP Destination IP Address' (four empty boxes for IP octets). An 'Apply' button is located at the bottom of the configuration fields. The Thomson logo and copyright notice '© - Thomson - 2007' are visible in the bottom left corner.

THOMSON
images & beyond

Administration

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

Advanced

Routing Information Protocol Setup : This page allows configuration of RIP parameters related to authentication, destination IP address/subnet mask, and reporting intervals. RIP automatically identifies and uses the best known and quickest route to any given destination address.

RIP Support

RIP Authentication ☒ Enable

RIP Authentication Key

RIP Authentication Key ID

RIP Reporting Interval seconds

RIP Destination IP Address . . .

Apply

Options
IP Filtering
MAC Filtering
Port Filtering
Forwarding
Port Triggers
DMZ Host
RIP Setup

© - Thomson - 2007

Fig. 25 Gateway\Advanced\RIP Setup

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.

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, showing the 'Web Content Filter' page. The page title is 'Web Filter'. The left sidebar contains links for 'Web Filter', 'TOD Filter', 'Local Log', and 'Remote Log'. The main content area has a description of the Web Content Filter and a list of 'Web Features' with checkboxes for enabling or disabling them. The 'Trusted Computers' section includes a form for adding MAC addresses and a 'Remove' button for 'No Trusted Computers'.

Web Features	
Filter Proxy	☐ Enable
Filter Cookies	☐ Enable
Filter Java Applets	☐ Enable
Filter ActiveX	☐ Enable
Filter Popup Windows	☐ Enable
Block Fragmented IP Packets	☐ Enable
Port Scan Detection	☐ Enable
IP Flood Detection	☒ Enable
Firewall Protection	☒ Enable

Trusted Computers

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

No Trusted Computers Remove

Fig. 26 Gateway\Firewall\Web Filter

Chapter 2: Web Configuration

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.

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 'Firewall' section is active, and the 'Time of Day Access Filter' page is displayed. The page title is 'Firewall'. The description states: '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.' The configuration area includes a MAC address input field (00:00:00:00:00:00) with an 'Add' button. Below this is a dropdown menu showing 'No filters entered.' and an 'Enabled' checkbox with a 'Remove' button. The 'Days to Block' section has checkboxes for 'Everyday', 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday'. The 'Time to Block' section has an 'All day' checkbox and 'Start' and 'End' time pickers. The 'Start' time is set to 12:00 AM and the 'End' time is set to 12:00 AM. An 'Apply' button is at the bottom. The Thomson logo is in the top left, and the copyright notice '© - Thomson - 2007' is in the bottom left.

Fig. 27 Gateway\Firewall\TOD Filter

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.

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. The configuration fields include 'Contact Email Address', 'SMTP Server Name', and 'E-mail Alerts' with an 'Enable' checkbox and an 'Apply' button. Below the configuration fields 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. 28 Gateway\Firewall\Local Log

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, Firewall section, Remote Log configuration page. The 'Remote Log' page allows optional configuration of events to be sent to a local SysLog server. The configuration fields include 'Send selected events' with checkboxes for 'Permitted Connections', 'Blocked Connections', 'Known Internet Attacks', and 'Product Configuration Events'. Below these is a text field for 'to SysLog server at 192.168.0.0' and an 'Apply' button.

Fig. 29 Gateway\Firewall\Remote Log

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.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Parental Control' section is active, showing the 'Basic Setup' tab. The page title is 'Parental Control'. The 'Basic Setup' section contains a description: 'This page allows basic selection of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.' Below this, there are two sections: 'Content Filtering' and 'Keyword List'. Under 'Content Filtering', there are checkboxes for 'Keyword Blocking' and 'Domain Blocking', both currently unchecked. An 'Apply' button is located below these checkboxes. The 'Keyword List' section has a text input field, an 'Add Keyword' button, and a 'Remove Keyword' button. The 'Blocked Domain List' section has a text input field, an 'Add Domain' button, and a 'Remove Domain' button. The Thomson logo is visible in the top left corner, and the copyright notice '© - Thomson - 2007' is at the bottom left.

Fig. 30 Gateway\Parental Control\Basic

Chapter 2: Web Configuration

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 Gateway\Wireless\Radio

- **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.

Chapter 2: Web Configuration

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.

The screenshot shows the Thomson Gateway Administration interface. The left sidebar contains a menu with options: Radio, Primary Network (selected), Access Control, Advanced, Bridging, and WMM. The main content area is titled 'Administration' and 'Wireless'. It displays the '802.11 Primary Network' configuration page. The page includes a description: 'This page allows configuration of the Primary Wireless Network and its security settings.' The configuration fields are as follows: Primary Network (angel29 (00:00:00:66:66:55)), Primary Network (Enabled), Network Name (SSID) (angel29), Closed Network (Open), WPA (Disabled), WPA-PSK (Disabled), WPA2 (Disabled), WPA2-PSK (Disabled), WPA/WPA2 Encryption (Disabled), WPA Pre-Shared Key (empty), RADIUS Server (0.0.0.0), RADIUS Port (1812), RADIUS Key (empty), Group Key Rotation Interval (0), WPA/WPA2 Re-auth Interval (3600), WEP Encryption (WEP (128-bit)), Shared Key Authentication (Optional), 802.1x Authentication (Disabled), Network Key 1 (00000000000000000000000000000001), Network Key 2 (00000000000000000000000000000000), Network Key 3 (00000000000000000000000000000000), Network Key 4 (00000000000000000000000000000000), Current Network Key (1), PassPhrase (empty), Generate WEP Keys button, and Apply button.

Fig. 32 Gateway\Wireless\Primary Network

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

Chapter 2: Web Configuration

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 the 128 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.

Chapter 2: Web Configuration

WEP Encryption

Shared Key Authentication

802.1x Authentication

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

Fig. 33 PassPhrase

- **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.

WPA/WPA2 Encryption

WPA Pre-Shared Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

WEP Encryption

Shared Key Authentication

802.1x Authentication

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

Fig. 34 802.1x Authentication

Chapter 2: Web Configuration

WPA/WPA2

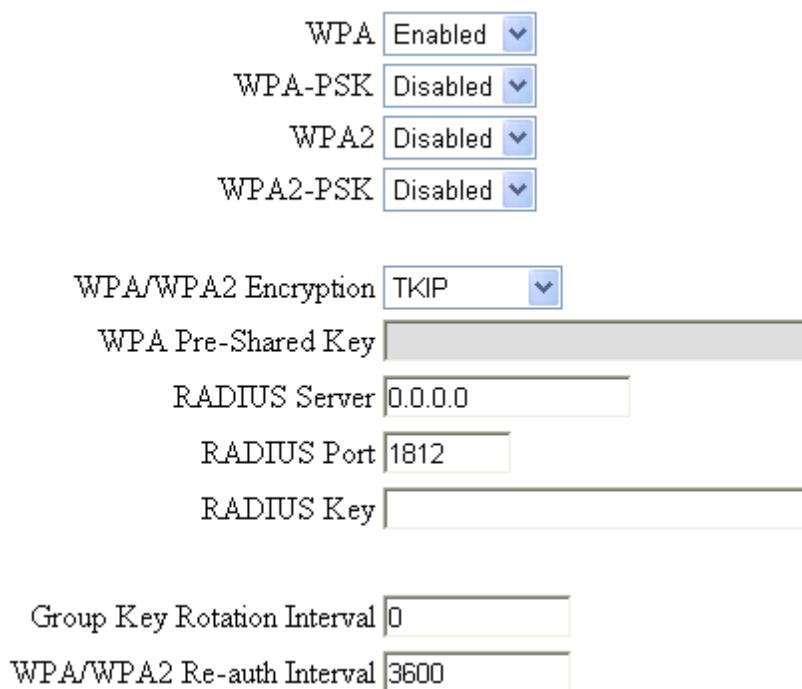
For the WPA/WPA2 network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, RADIUS Server, RADIUS Port, RADIUS Key, Group Key Rotation Interval, and WPA/WPA2 Re-auth Interval.

- **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.



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. 35 WPA/WPA2

Chapter 2: Web Configuration

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.**

The image shows a web configuration interface for WPA-PSK/WPA2-PSK. It contains several dropdown menus and text input fields. The settings are as follows:

Setting	Value
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. 36 WPA-PSK/WPA2-PSK

Chapter 2: Web Configuration

Automatic Security Configuration

The screenshot shows a web configuration page for WPS. At the top, there is a dropdown menu set to 'WPS'. Below it, a status box indicates 'WPS Config State: Unconfigured'. A text block explains that the physical button on the AP will provision wireless clients using WPS. The 'Device Name' field is set to 'ThomsonAP'. Under the 'WPS Setup AP' section, the 'PIN' field contains '12345670' and a 'Configure' button is visible. The 'WPS Add Client' section shows two radio buttons: 'Push-Button' (selected) and 'PIN'. An 'Add' button is next to the 'PIN' option. Below this, there is an empty 'PIN' input field.

Fig. 37 Automatic Security Configuration

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

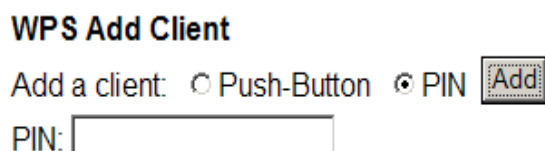
- **WPS Config:** It will help to **Enable** or **Disable** the WPS feature.
- **Device Name:** By using this you can change the factory default to a name of your choice up to 32 characters long as like **SSID**
- **WPS Setup AP:** Here we no need to do any configure. So, just skip this step.
- **WPS 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.

The screenshot shows the 'WPS Setup AP' page. The title 'WPS Setup AP' is prominently displayed. Below the title, a message states 'Your AP is now waiting for the STA to connect.' There is a large 'PUSH' button. At the bottom, a status box shows 'WPS Configure Status: InProgress'.

Chapter 2: Web Configuration

Fig. 38 WPS Setup AP/PUSH

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.



The image shows a web interface titled "WPS Add Client". Below the title, there is a label "Add a client:" followed by two radio buttons. The first radio button is labeled "Push-Button" and is unselected. The second radio button is labeled "PIN" and is selected. To the right of the "PIN" radio button is a button labeled "Add". Below the radio buttons, there is a label "PIN:" followed by a text input field.

Fig. 39 WPS/Push-Button

- **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!”.

WPS Setup AP

Your AP is now waiting for the STA to connect.



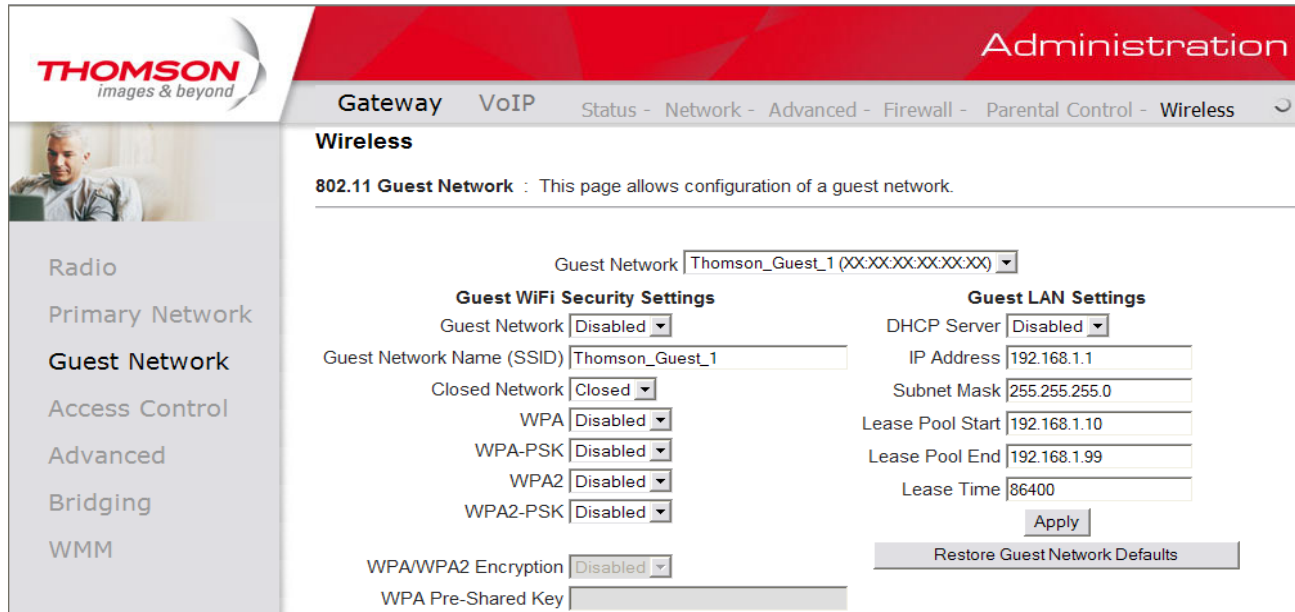
The image shows a web interface titled "WPS Setup AP". Below the title, there is a button labeled "Abort". Below the "Abort" button, there is a label "Entered PIN:" followed by a text input field. Below the text input field, there is a label "WPS Configure Status: InProgress".

Fig. 40 WPS Setup AP/PIN

Chapter 2: Web Configuration

3. Guest Networks

If enabled by the service provider, there are 3 additional Wireless Guest Networks can be configured and activated. The default guest network screen looks as follow:



THOMSON
images & beyond

Administration

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

Wireless

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

Guest Network Thomson_Guest_1 (XX:XX:XX:XX:XX:XX)

Guest WiFi Security Settings

Guest Network Disabled

Guest Network Name (SSID) Thomson_Guest_1

Closed Network Closed

WPA Disabled

WPA-PSK Disabled

WPA2 Disabled

WPA2-PSK Disabled

WPA/WPA2 Encryption Disabled

WPA Pre-Shared Key

Guest LAN Settings

DHCP Server Disabled

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Lease Pool Start 192.168.1.10

Lease Pool End 192.168.1.99

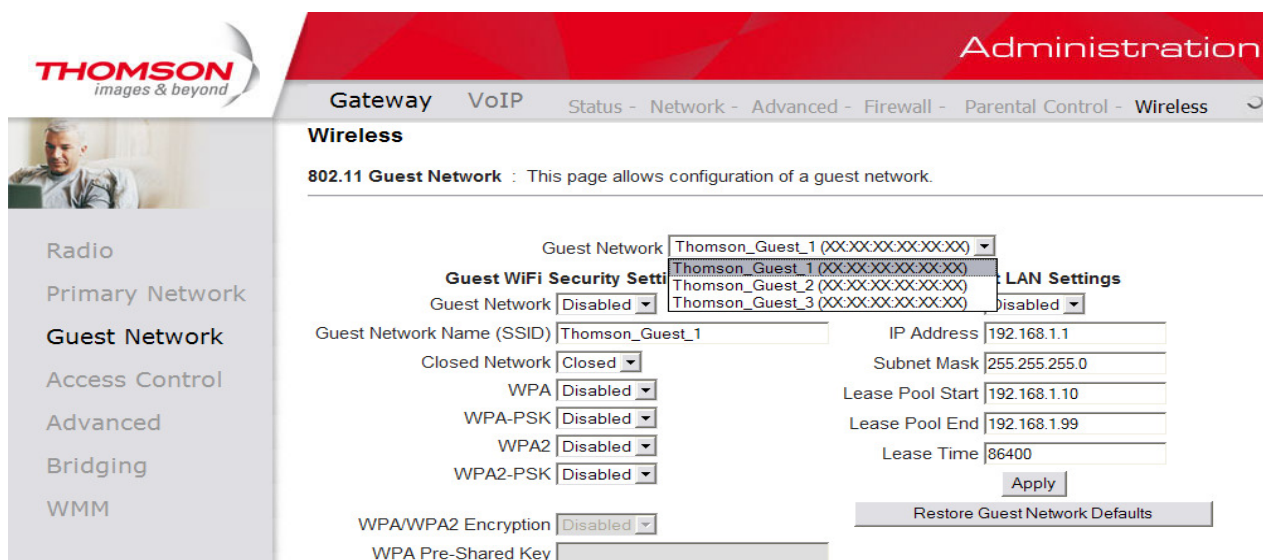
Lease Time 86400

Apply

Restore Guest Network Defaults

Fig 41 Gateway\Wireless\Guest Network

These networks are independent of each others. Each network is controlled and configured similar to the primary network (described in the previous section). You may select the appropriate network by clicking on the pull down bottom next to the “Thomson_Guest_1”.



THOMSON
images & beyond

Administration

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

Wireless

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

Guest Network Thomson_Guest_1 (XX:XX:XX:XX:XX:XX)

Guest WiFi Security Settings

Guest Network Disabled

Guest Network Name (SSID) Thomson_Guest_1

Closed Network Closed

WPA Disabled

WPA-PSK Disabled

WPA2 Disabled

WPA2-PSK Disabled

WPA/WPA2 Encryption Disabled

WPA Pre-Shared Key

Guest LAN Settings

DHCP Server Disabled

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Lease Pool Start 192.168.1.10

Lease Pool End 192.168.1.99

Lease Time 86400

Apply

Restore Guest Network Defaults

Fig 42 Gateway\Wireless\Guest Network

Chapter 2: Web Configuration

4. 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. 43 Gateway\Wireless\Access Control

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.

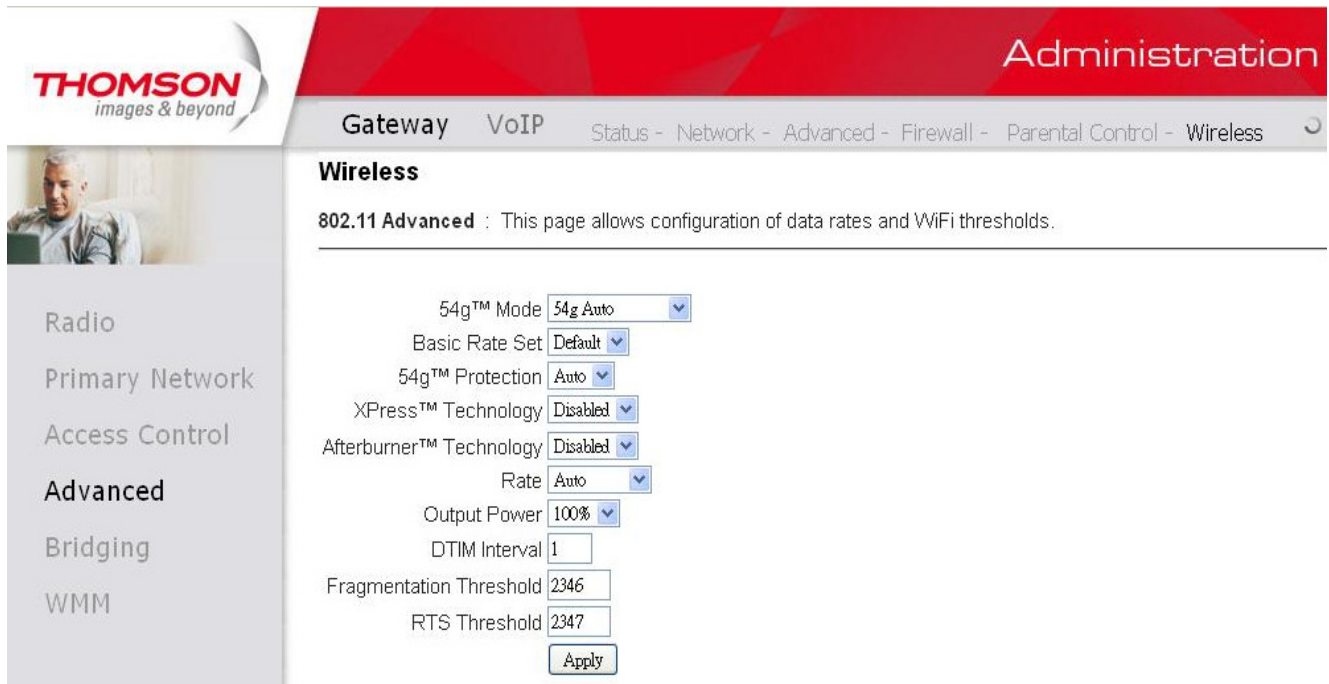
Connected Clients: The information of currently connected clients will be displayed here.

Chapter 2: Web Configuration

5. 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.



The screenshot shows the Thomson Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', and a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Wireless' section is active. On the left, a sidebar menu lists 'Radio', 'Primary Network', 'Access Control', 'Advanced' (selected), 'Bridging', and 'WMM'. The main content area is titled 'Wireless' and contains a description: '802.11 Advanced : This page allows configuration of data rates and WiFi thresholds.' Below this, several settings are listed with dropdown menus or text boxes: '54g™ Mode' (54g Auto), 'Basic Rate Set' (Default), '54g™ Protection' (Auto), 'XPress™ Technology' (Disabled), 'Afterburner™ Technology' (Disabled), 'Rate' (Auto), 'Output Power' (100%), 'DTIM Interval' (1), 'Fragmentation Threshold' (2346), and 'RTS Threshold' (2347). An 'Apply' button is at the bottom.

Fig. 44 Gateway\Wireless\Advanced

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

Chapter 2: Web Configuration

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

6. 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.

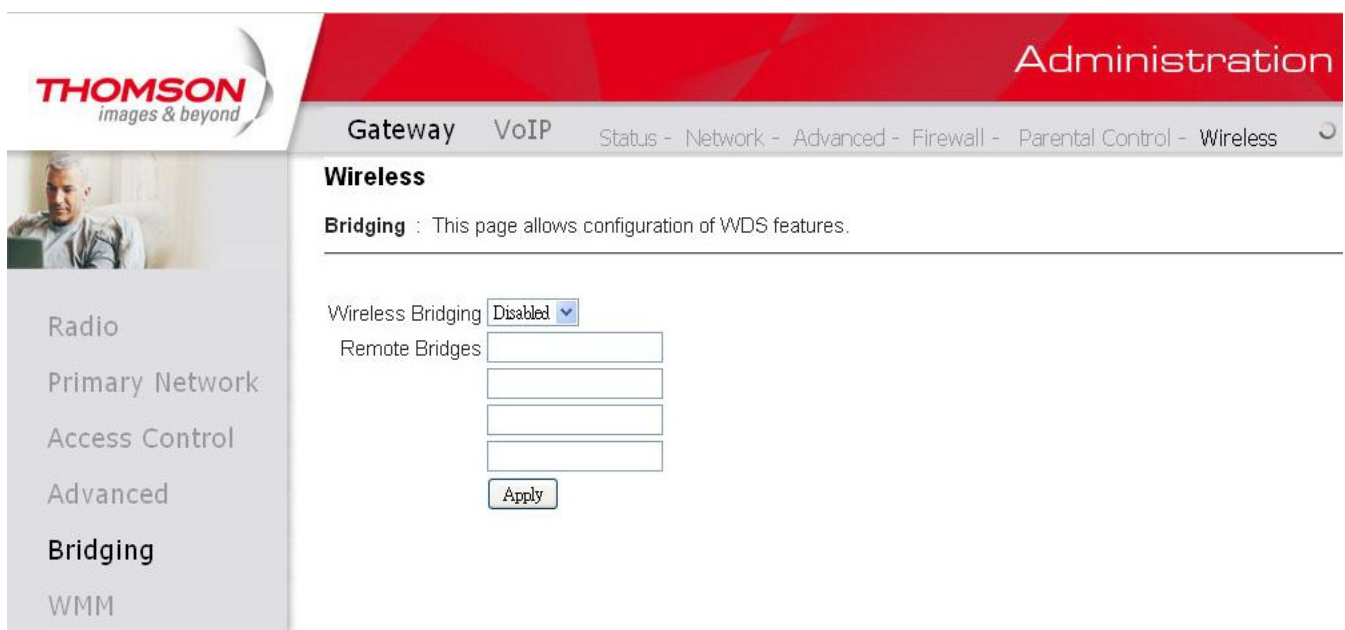


Fig. 45 Gateway\Wireless\Bridging

- **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

7. 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.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', and a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The left sidebar lists configuration categories: 'Radio', 'Primary Network', 'Access Control', 'Advanced', 'Bridging', and 'WMM' (which is highlighted). The main content area is titled 'Wireless' and contains the '802.11 Wi-Fi Multimedia' section. This section includes three toggle switches: 'WMM Support' (set to 'On'), 'No-Acknowledgement' (set to 'Off'), and 'Power Save Support' (set to 'On'). Below these is an 'Apply' button. The 'EDCA AP Parameters' section contains a table for configuring four Access Categories (AC_BE, AC_BK, AC_VI, AC_VO) with columns for CWmin, CWmax, AIFS, TXOP(b) Limit (usec), TXOP(a/g) Limit (usec), and Discard Oldest First. The 'EDCA STA Parameters' section contains a similar table for the same four categories. Both tables have an 'Apply' button at the bottom.

EDCA AP Parameters:				CWmin	CWmax	AIFS	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
AC_BE	15	63	3	0	0	Off			
AC_BK	15	1023	7	0	0	Off			
AC_VI	7	15	1	6016	3008	Off			
AC_VO	3	7	1	3264	1504	Off			

EDCA STA Parameters:				CWmin	CWmax	AIFS	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)
AC_BE	15	1023	3	0	0			
AC_BK	15	1023	7	0	0			
AC_VI	7	15	2	6016	3008			
AC_VO	3	7	2	3264	1504			

Fig. 46 Gateway\Wireless\WMM

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).

Chapter 2: Web Configuration

Transmit parameters include Contention Window (CW_{min} and CW_{max}), 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).

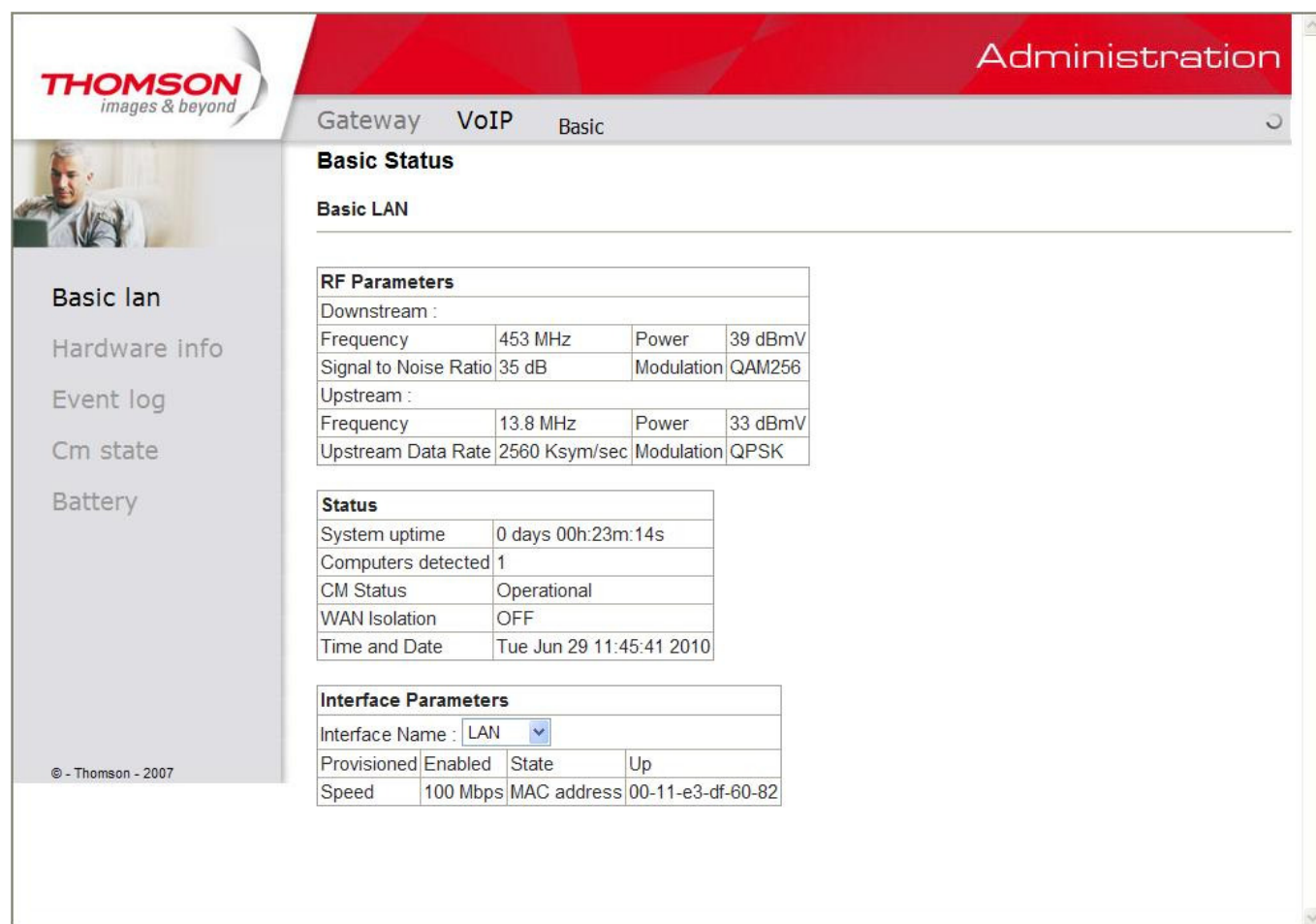
Transmit parameters include Contention Window (CW_{min} and CW_{max}), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

Chapter 2: Web Configuration

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.



The screenshot displays the Thomson VoIP Basic LAN configuration page. The page has a red header with the Thomson logo and the word "Administration". Below the header, there are tabs for "Gateway", "VoIP", and "Basic". The "Basic" tab is selected. The page is divided into a left sidebar and a main content area. The sidebar contains links for "Basic lan", "Hardware info", "Event log", "Cm state", and "Battery". The main content area is titled "Basic Status" and "Basic LAN". It contains three sections: "RF Parameters", "Status", and "Interface Parameters".

RF Parameters

Downstream :			
Frequency	453 MHz	Power	39 dBmV
Signal to Noise Ratio	35 dB	Modulation	QAM256
Upstream :			
Frequency	13.8 MHz	Power	33 dBmV
Upstream Data Rate	2560 Ksym/sec	Modulation	QPSK

Status

System uptime	0 days 00h:23m:14s
Computers detected	1
CM Status	Operational
WAN Isolation	OFF
Time and Date	Tue Jun 29 11:45:41 2010

Interface Parameters

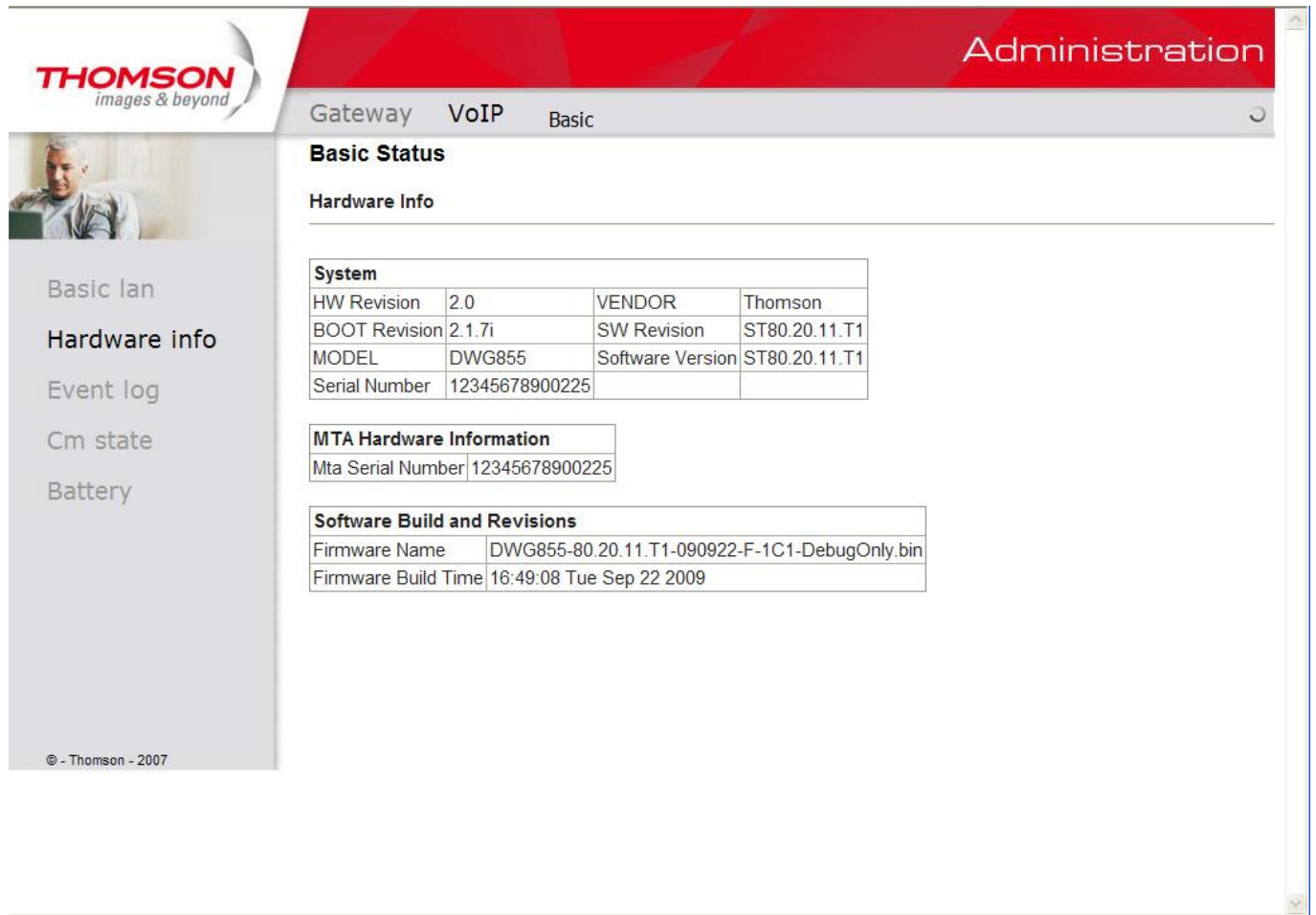
Interface Name : LAN			
Provisioned	Enabled	State	Up
Speed	100 Mbps	MAC address	00-11-e3-df-60-82

Fig.47 VoIP\Basic\Basic LAN

Chapter 2: Web Configuration

2. Hardware Info

The hardware Info is displayed on this page.



The screenshot shows the Thomson VoIP Basic configuration interface. The top navigation bar includes 'Gateway', 'VoIP', and 'Basic'. The left sidebar contains links for 'Basic lan', 'Hardware info', 'Event log', 'Cm state', and 'Battery'. The main content area is titled 'Basic Status' and 'Hardware Info'. It displays three tables: 'System', 'MTA Hardware Information', and 'Software Build and Revisions'.

System			
HW Revision	2.0	VENDOR	Thomson
BOOT Revision	2.1.7i	SW Revision	ST80.20.11.T1
MODEL	DWG855	Software Version	ST80.20.11.T1
Serial Number	12345678900225		

MTA Hardware Information	
Mta Serial Number	12345678900225

Software Build and Revisions	
Firmware Name	DWG855-80.20.11.T1-090922-F-1C1-DebugOnly.bin
Firmware Build Time	16:49:08 Tue Sep 22 2009

Fig. 48 VoIP\Basic\Hardware Info

Chapter 2: Web Configuration

3. Event Log

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

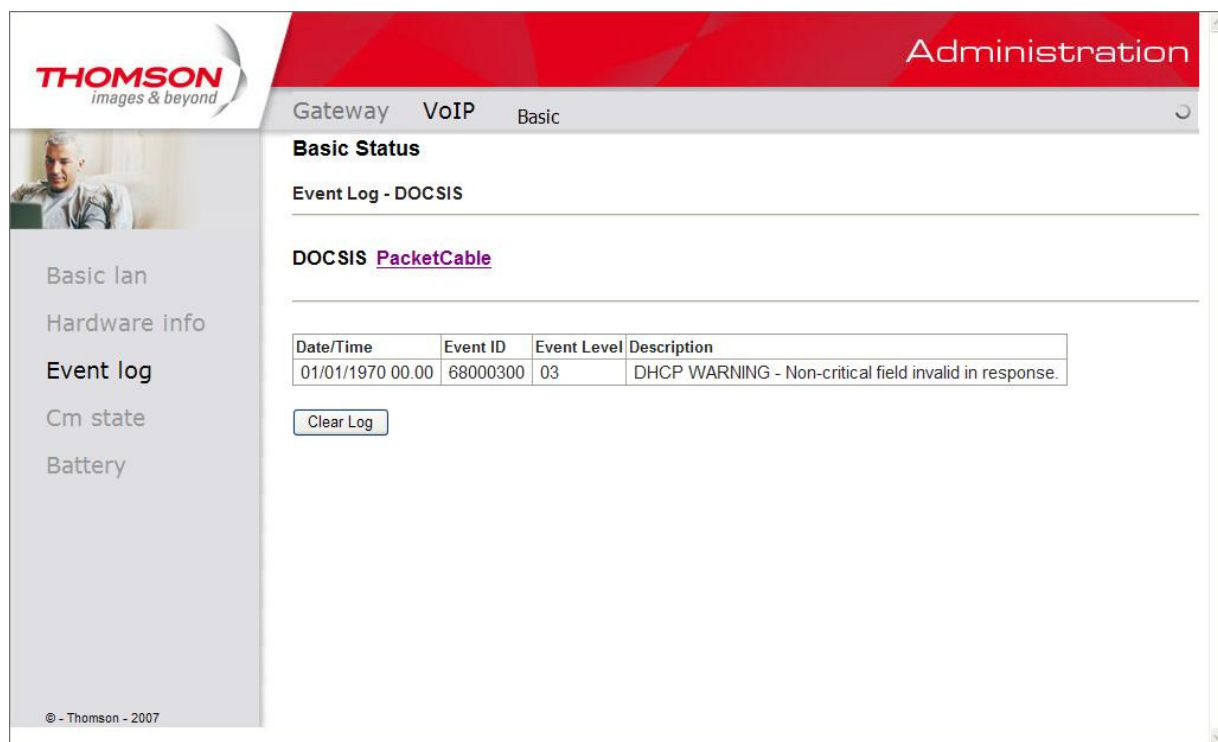


Fig. 49 VoIP\Basic\Event Log\DOCSIS

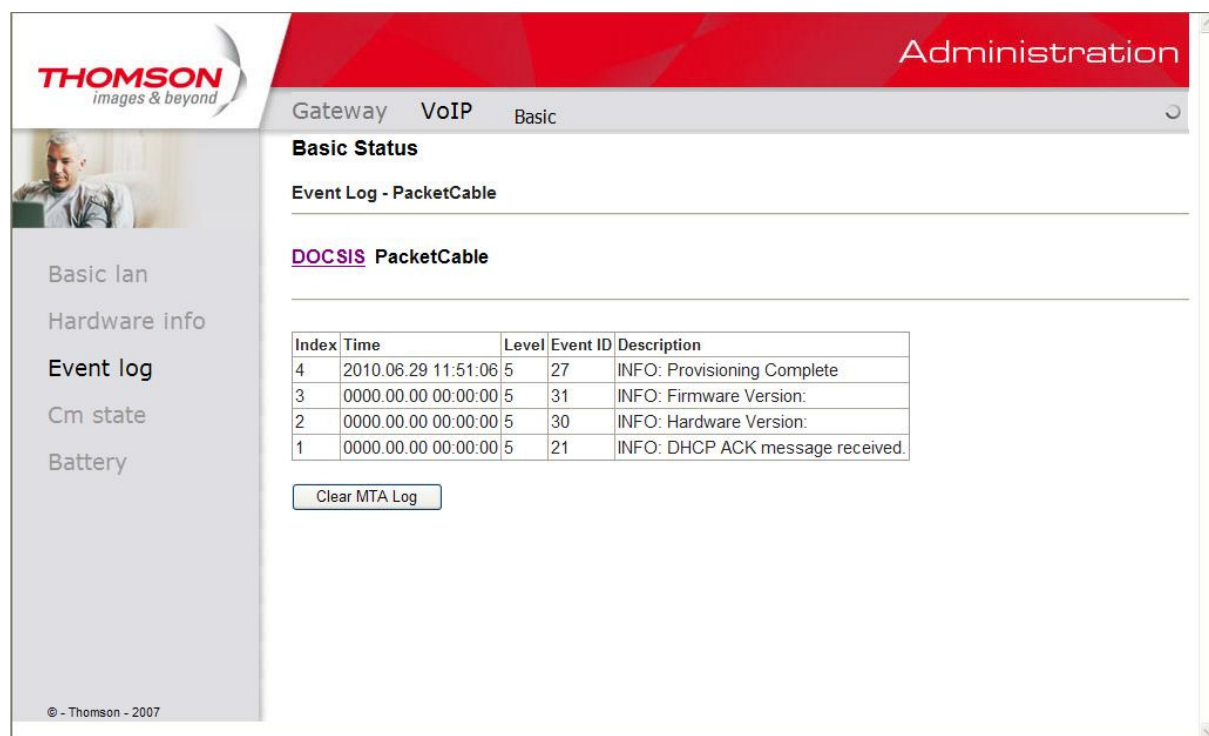
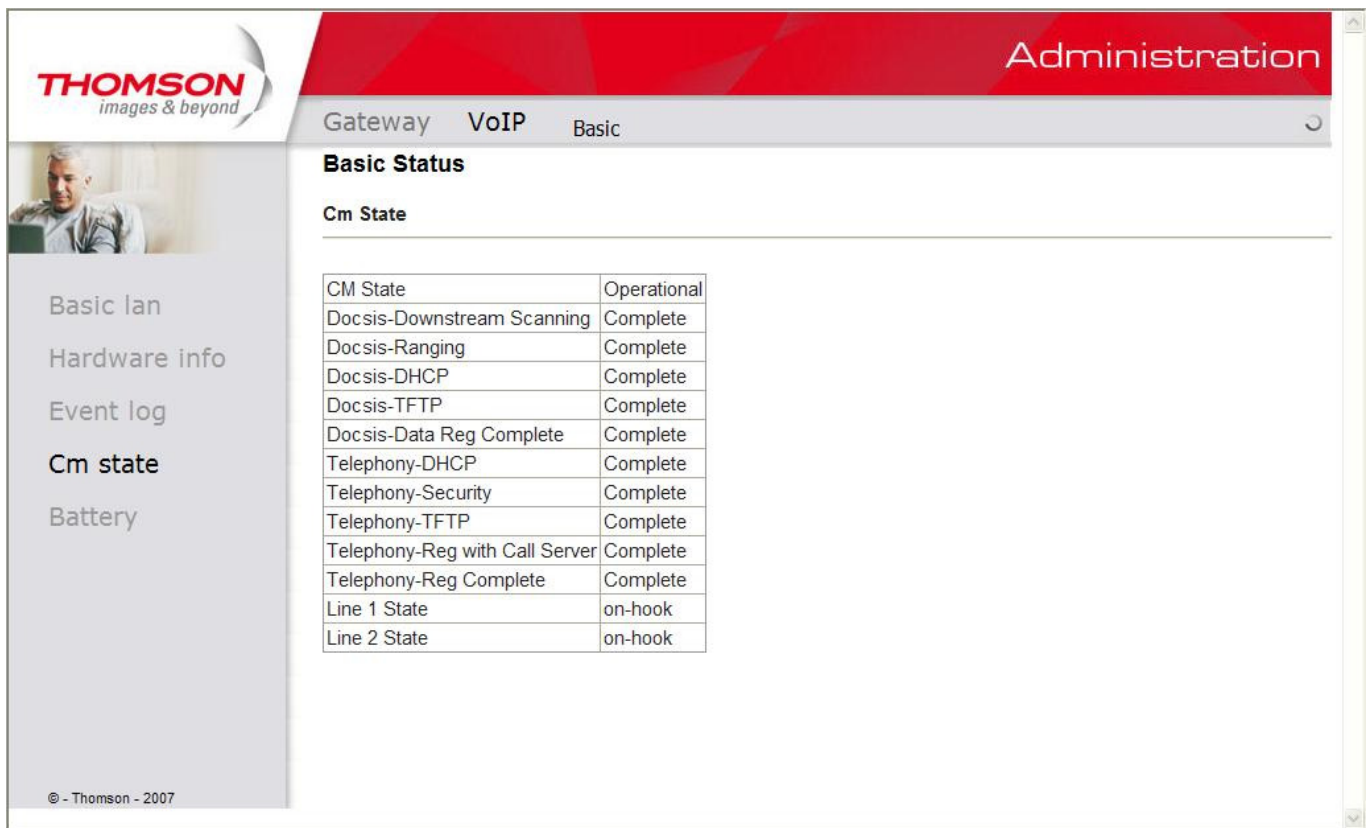


Fig. 50 VoIP\Basic\Event Log\PacketCable

Chapter 2: Web Configuration

4. CM State

This page shows the current state of the cable modem.



The screenshot displays the Thomson web configuration interface. The top navigation bar is red with the 'Administration' title. Below it, a grey bar contains the tabs 'Gateway', 'VoIP', and 'Basic'. The left sidebar features the Thomson logo and a list of menu items: 'Basic lan', 'Hardware info', 'Event log', 'Cm state' (highlighted), and 'Battery'. The main content area is titled 'Basic Status' and 'Cm State'. It contains a table with the following data:

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

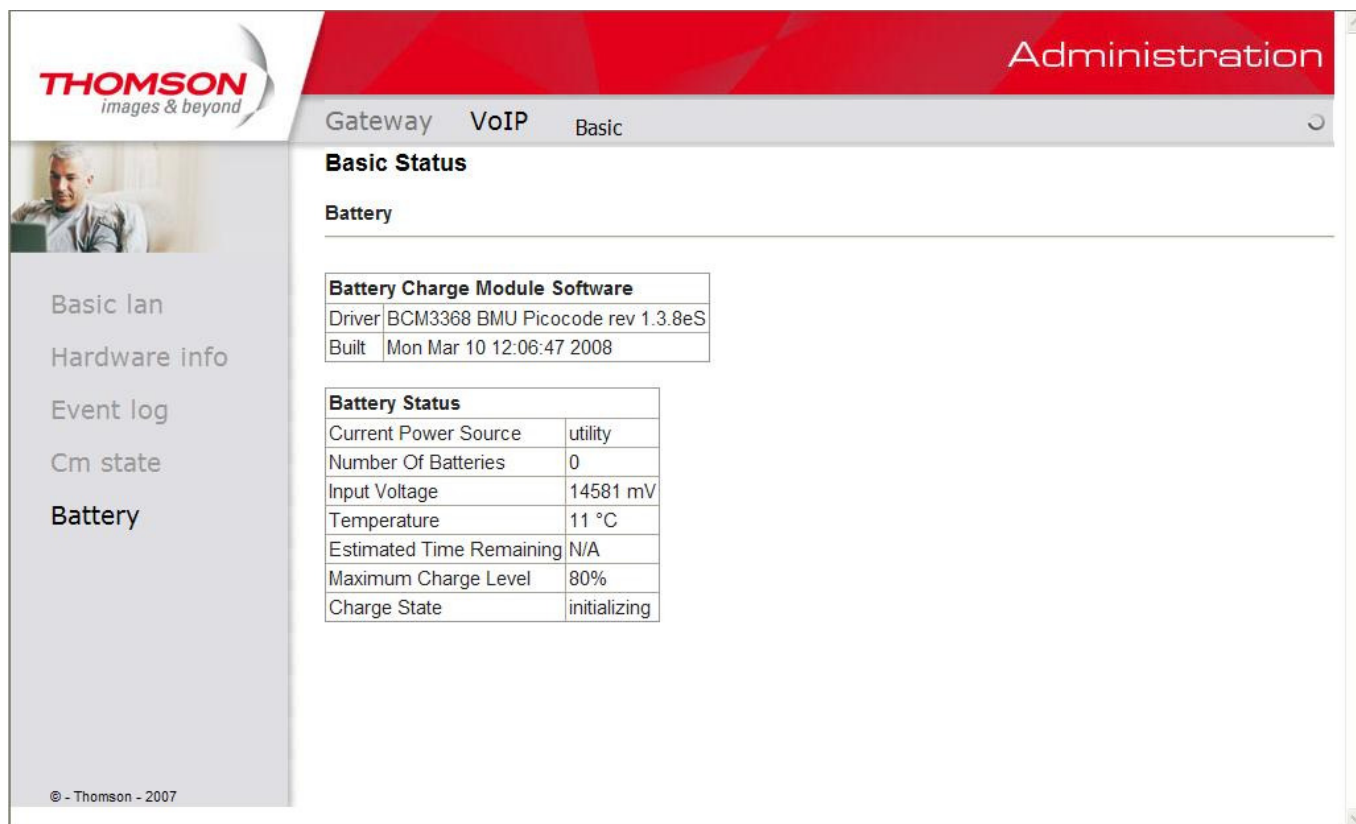
At the bottom left of the sidebar, the copyright notice '© - Thomson - 2007' is visible.

Fig. 51 VoIP\Basic\CM state

Chapter 2: Web Configuration

5. Battery

This page shows the current state of battery.



THOMSON
images & beyond

Administration

Gateway VoIP Basic

Basic Status

Battery

Battery Charge Module Software	
Driver	BCM3368 BMU Picocode rev 1.3.8eS
Built	Mon Mar 10 12:06:47 2008

Battery Status	
Current Power Source	utility
Number Of Batteries	0
Input Voltage	14581 mV
Temperature	11 °C
Estimated Time Remaining	N/A
Maximum Charge Level	80%
Charge State	initializing

© - Thomson - 2007

Fig. 52 VoIP\Basic\Battery

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 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?

Chapter 3: Additional Information

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 103 rd 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.

IMPORTANT NOTE:

Chapter 3: Additional Information

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.

Chapter 3: Additional Information

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

For more information

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

© 2006 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.

