



CABLE

SATELLITE

TELECOM

TERRESTRIAL

TCW770 – Wireless Gateway

User manual

THOMSON

Important Information

Safety Instructions

Using equipment safely

Your WIFI Cable Modem product has been manufactured to meet European and local safety standards, but you must take care if you want it to perform properly and safely.

It is important that you read this booklet completely, especially the safety instructions below.

Equipment connected to the protective earth of the building installation through the mains connection or through other equipment with a connection to protective earth and to a cable distribution system using coaxial cable, may in some circumstances create fire hazard. Connection to a cable distribution system has therefore to be provided through a device providing electrical isolation below a certain frequency range (galvanic isolator, see EN 60728-11).

If you have any doubts about the installation, operation or safety of the product, please contact your supplier.

To avoid the risk of electric shock

- Disconnect the WIFI Cable Modem product from the mains supply before you connect it to (or disconnect it from) any other equipments. Remember that contact with Mains can be lethal or causes severe electric shock.
- Never remove the product cover. Should the product fail, contact the Customer Service to arrange repair or service.
- Never allow anyone to push anything into holes, slots or any other opening in the case
- Do not block the ventilation slots; never stand it on soft furnishings or carpets
- Do not put anything on it which might spill or drip into it (e.g. Lighted candles or containers of liquids). Do not expose it to dripping or splashing. If an object or liquid enters inside the Cable Modem, unplug it immediately and contact the Customer Service.
- Do not store the WIFI Cable Modem product in excessively hot, cold or damp conditions. It is intended to operate at an ambient temperature of less than 35 degrees Celsius and a maximum humidity level of 70%. In case of a storm, it is recommended that you unplug the product from the mains and from the PC set or other equipment.
- Leave the mains socket accessible so that you can unplug the set quickly

Connecting to the mains supply

- This appliance is designed to operate in the rated voltage 100 ~ 240 VAC.
- If you are in any doubt about the mains lead, the plug or connection, please consult the Customer Service.
- Only the power adapter supplied with the product has to be used.

Important Information

Ensuring optimum performance

- Leave 7cm to 10cm around the appliance to ensure that proper ventilation gets to it.
- Do not store your appliance on its side (if not allowed)
- To clean the appliance, use a dry, clean soft cloth with no cleaning solvent or abrasive products. Clean the ventilation openings regularly.

Limiting the Human Body Exposure to the Electromagnetic Fields

Under normal use condition the user shall keep at least 20cm distance from the WIFI Cable Modem product.

Environmental considerations

This symbol means that your inoperative electronic appliance, and used battery when applicable, 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

Please help us protect the environment in which we live

Energy savings - You have a role to play...

Learn how you can use and explore ways for using your electronic equipment



The user manual detailed useful information on all the features of your product but also on energy consumption performances.

We strongly encourage you to carefully read the notice before putting your equipment in service to get the best service it can offer you.

- **By working together, we can reduce the impact we have on our earth!**

Important Information

Main technical specifications

General

Operating voltage	100 ~ 240 VAC
Typical Power consumption	18 W max
Dimensions (W x H x D)	220mm x 155mm x 38mm
Operating temperature range	0 – 40 °C
Storage temperature range	-20 – 70 °C
AC adapter (or plug-in adapter) type	ADAPTER 18W 12VDC/1.5A

Connections

DC input	12V/ 1.5A
Cable input	1xCoaxial cable connector
Ethernet plugs	4xRJ-45

Marking information



This symbol on your set guarantees that your product complies with the European Directive 1999/5/EC on Safety, Telecom, Electromagnetic Compatibility, with the 2009/125/EC Directive on Energy related Products and the Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment. This equipment is intended to be used indoor in a residential or office environment. This equipment may be operating in Europe

The CE Declaration of Conformity is available on the Website www.technicolor.com

Responsible Party: Technicolor R&D France
975, Avenue des Champs Blancs CS17616
35576 Cesson-Sévigné Cedex
France

Table of Contents

Chapter 1: Connections and Setup.....	1
Introduction	1
Wireless Gateway Features.....	1
What's on the CD-ROM.....	1
Computer Requirements	2
Wireless Gateway TCW770 Overview	4
Front Panel.....	4
Rear Panel.....	6
Side Panel	6
Relationship among the Devices	7
What the Modem Does	7
What the Modem Needs to Do Its Job.....	7
Contact Your Local Cable Company.....	7
Connecting the Wireless Gateway to a Single Computer	9
Attaching the Cable TV Wire to the Wireless Gateway.....	9
Important Connection Information	10
Ethernet Connection to a Computer	10
Connecting More Than One Computer to the Wireless Gateway.....	11
Turning on the Wireless Gateway	12
Chapter 2: WEB Configuration.....	13
Accessing the Web Configuration.....	13
Outline of Web Manager	14
Status	15
1. Software.....	15
2. Connection.....	16
3. Password.....	17

Table of Contents

4. Diagnostics	18
5. Event Log	19
6. Initial Scan	20
7. Backup/Restore.....	21
Network	22
1. LAN	22
2. WAN.....	23
3. Computers.....	24
4. DDNS	25
5. Time.....	26
6. FTP Diagnostics	27
7. Portbase Passthrough.....	28
Advanced	29
1. Options.....	29
2. IP Filtering.....	31
3. MAC Filtering	32
4. Port Filtering.....	33
5. Forwarding.....	34
6. Port Triggers	36
7. DMZ Host.....	38
8. RIP (Routing Information Protocol) Setup.....	39
Firewall.....	40
1. Web Filtering.....	40
2. TOD Filtering	41
3. Local Log and Remote Log	42

Table of Contents

Parental Control.....	44
1. Basic	44
2. Setup	45
Wireless.....	46
1. 802.11/ Radio.....	47
2. 802.11/ Primary Network	49
3. Access Control.....	57
4. 802.11/ Advanced.....	58
5. Bridging.....	60
6. 802.11 QoS (WMM) Settings.....	61
Chapter 3: Networking.....	63
Communications.....	63
Type of Communication	63
Cable Modem (CM) Section.....	64
Networking Section	64
Three Networking Modes	65
Cable Modem (CM) Mode	65
Residential Gateway (RG) Mode.....	67
CableHome (CH) Mode.....	68
MAC and IP Addresses Summary	70
Chapter 4: Additional Information	71
Frequently Asked Questions.....	71
General Troubleshooting	73
Service Information.....	74
Glossary	75

Chapter 1: Connections and Setup

Chapter 1: Connections and Setup

Introduction

Wireless Gateway Features

- CableLabs DOCSIS /EuroDOCSIS 1.0/1.1/2.0/3.0 Standard Compliant
- 4 x Standard RJ-45 connector for 10/100/1000 BaseT Ethernet with auto-negotiation and MDIX functions; Support maximum Ethernet cable length up to 100m (Category 5)
- WIFI interface 802.11n; 2,4GHz or 5 GHz with at least 2x2 antennas.
- Transparent bridging for IP traffic
- 1 x Master USB connector socket comply to USB2.0
- Transparent bridging between CPE and RF interface
- 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
- MPEG over IP encapsulation
- Power management
- Network Protocol: IP/TCP/UDP/ARP/ICMP/DHCP/FTP/TFTP/SNMP/HTTP
- Syslog (remote)
- Event Log (local)
- Clear LED display
- Reset switch in order to restore factory parameters
- Two detachable SMA antennas connectors (optional)

What's on the CD-ROM

Insert the Wireless 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
- Links to Thomson web site

Chapter 1: Connections and Setup

EURO-DOCSIS is trademarks of Cable Television Laboratories, Inc.

Computer Requirements

For the best possible performance from your Wireless 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/7, Linux	Mac OS** 7.6.1 or higher
Video	VGA or better (SVGA preferred)	VGA or better (SVGA built-in preferred)
Ethernet	10 /100 /1000 Base-T	10 /100 /1000 Base-T
	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 Wireless Gateway.	
Software	<ul style="list-style-type: none">• A TCP/IP network protocol for each machine• Microsoft Internet Explorer 4.0 or later or Netscape Navigator 4.0 or later.	

* Windows is a trademark of Microsoft Corporation.

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

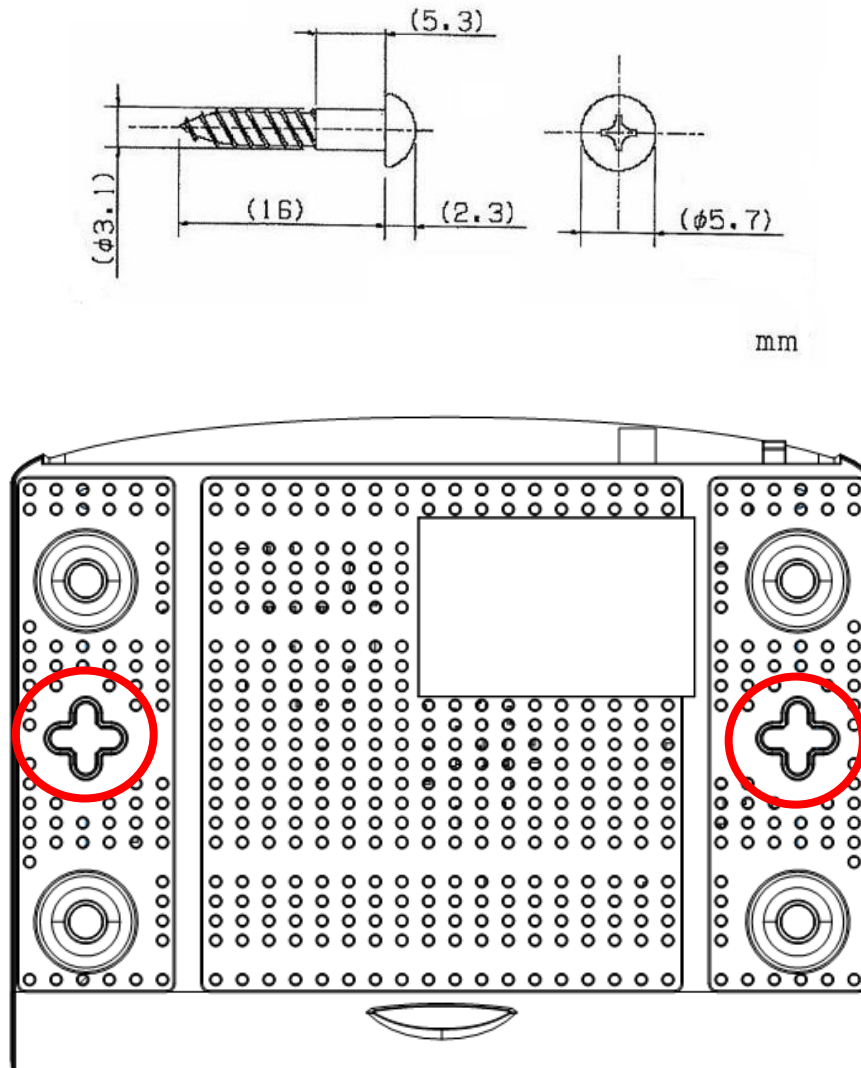
Chapter 1: Connections and Setup

Wall Mounting

This article will show the user through the process of wall-mounting the Wireless Gateway

The Adapter has two wall-mount slots on its back panel.

Two screws are needed to mount the Adapter.



To do this:

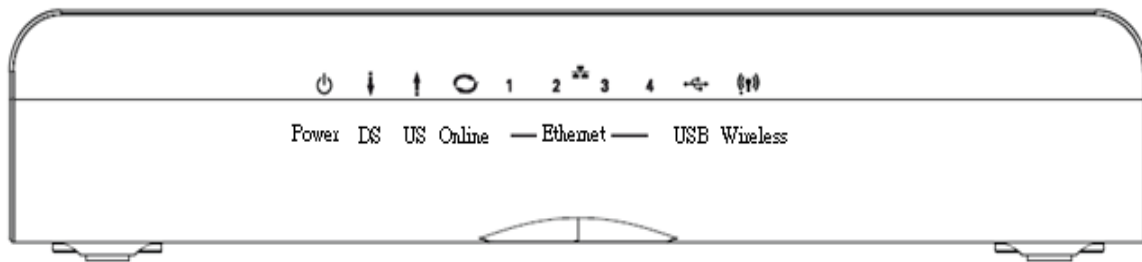
1. Ensure that the wall you use is smooth, flat, dry and sturdy and use the 2 screw holes which are 101.6 mm (4 inches) apart from each other.
2. Fix the screws into wall, leaving their heads 3 mm (0.12 inch) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw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

Chapter 1: Connections and Setup

Wireless Gateway TCW770 Overview

Front Panel

The following illustration shows the front panel of the TCW770 gateway:



Reset Button behavior

- a) Push and hold the button between 0 and 5 seconds → Reboot the device
- b) Between 6 and 10 seconds → Display the channel bonding status for DS and US
Note: This is the same as the above Channel Bonding display after the registration
- c) After 11 seconds → Perform the factory reset.

WPS LED is a backlight in WPS button

- a) When WiFi is on, the LED is blinking
- b) When WPS association is on, the LED is turned on

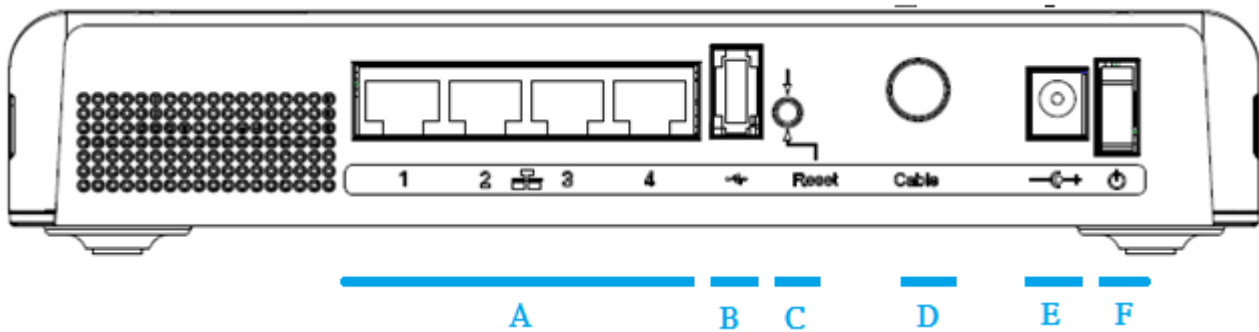
Chapter 1: Connections and Setup

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

TCW770	Power	Internet			Ethernet				USB	Wireless	Description
		DS	US	Online	1	2	3	4			
Boot-up Operation	ON	ON	ON	ON	ON	ON	ON	ON	X	X	Power on 0.25 sec
	X	FLASH	FLASH	FLASH	X	X	X	X	X	X	From power ON to system initialization complete
DOCSIS Start-up Operation	ON	FLASH	OFF	OFF	X	X	X	X	X	X	During DS scanning and acquiring SYNC
	ON	ON	FLASH	OFF	X	X	X	X	X	X	From SYNC completed, receiving UCD to ranging completed
	ON	ON	ON	FLASH	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	Operational (NACO=ON)
	ON	FLASH	FLASH	OFF	X	X	X	X	X	X	Operational (NACO=OFF)
Channel Bonding Operation	FLASH	FLASH	FLASH	FLASH	X	X	X	X	X	X	Wait registration with all DS and all US – Lights Flash sequentially from the right to left Minimum duration 3 seconds
	X	X	X	X	X	X	X	X	X	X	From 1 to 4 DS, from 1 to 4 LEDs are ON. From 5 to 8 DS, From 1 to 4 LEDs are flashing Duration 3 seconds
	OFF	X	X	OFF	X	X	X	X	X	X	From 1 to 2 US, from 2 to 3 LEDs are ON. From 3 to 4 US, From 2 to 3 LEDs are flashing Duration 3 seconds
	FLASH	FLASH	FLASH	FLASH	X	X	X	X	X	X	Wait registration with all DS and all US – Lights Flash sequentially from the left to right Minimum duration 3 seconds
CPE Operation	ON	X	X	X	OFF ON FLASH	OFF ON FLASH	OFF ON FLASH	OFF ON FLASH	X	X	No Ethernet Link Ethernet Link TX/RX Ethernet Traffic
	ON	X	X	X	X	X	X	X	X	OFF ON FLASH	Wireless is disable Wireless initiate success or enable TX/RX Wireless Traffic
USB Operation	ON	X	X	X	X	X	X	X	OFF ON FLASH	X	No USB Link USB Link TX/RX USB Traffic
SW Download Operation	ON	FLASH	FLASH	ON	X	X	X	X	X	X	Software Download (including FLASHING of Memory)

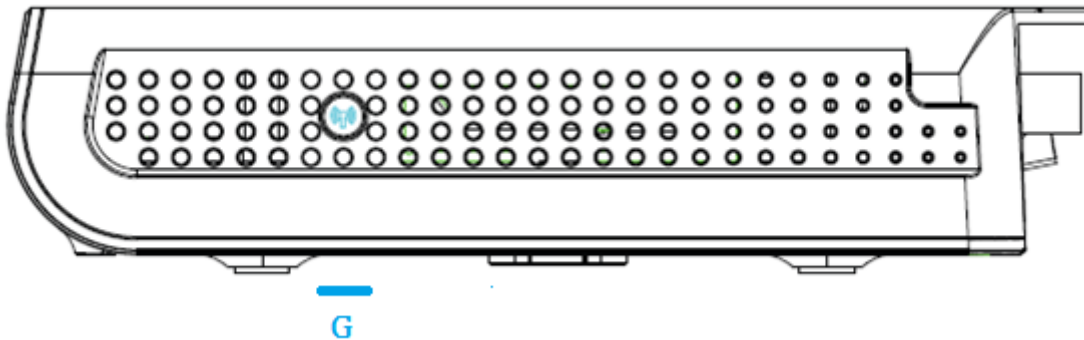
Chapter 1: Connections and Setup

Rear Panel



- | | | |
|---|-------------------|--|
| A | ETHERNET 1 2 3 4: | 4x Ethernet 10/100/1000 Mbps RJ-45 connectors |
| B | USB Host: | 1x USB 2.0 Connector |
| C | Reset: | 1x Reset or reset to factory default this Wireless Gateway |
| D | CABLE: | 1x F-Connector for the coax cable |
| E | 12VDC : | 1x Power connector to connect the DC power supply |
| F | Power switch: | 1x switch to power on/off this Wireless Gateway |

Side Panel



- | | | |
|---|---------------------------|--|
| G | WPS & WiFi on/off button: | 1x button with two features:
to activate/disable the WiFi, to execute a WPS association |
|---|---------------------------|--|

Chapter 1: Connections and Setup

Relationship among the Devices

What the Modem Does

The Wireless Gateway provides high-speed Internet access as well as cost-effective fax/modem services over residential, commercial, and education subscribers on public and private networks via an existing CATV infrastructure. The IP traffic can transfer between the Wireless Gateway and EURO-DOCSIS compliant head-end equipment. The data security secures upstream and downstream communications.

What the Modem Needs to Do Its Job

- **The Right Cable Company:** Make sure your local cable company provides data services that use cable TV industry-standard EURO-DOCSIS compliant technology.

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
- SSID, WEP/WPA-PSK information

Chapter 1: Connections and Setup

Please verify the following with the cable company

- The cable service to your home supports EURO-DOCSIS compliant two-way modem access.
- 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.

Please verify the following on the Wireless Gateway

The on/off button on the rear panel must be in the ON mode = on “1”

Chapter 1: Connections and Setup

Connecting the Wireless Gateway to a Single Computer

This section of the manual explains how to connect your Wireless 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 Wireless 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 Wireless Gateway to the first point the cable enters your home. The splitter must be rated for at least 1GHz.

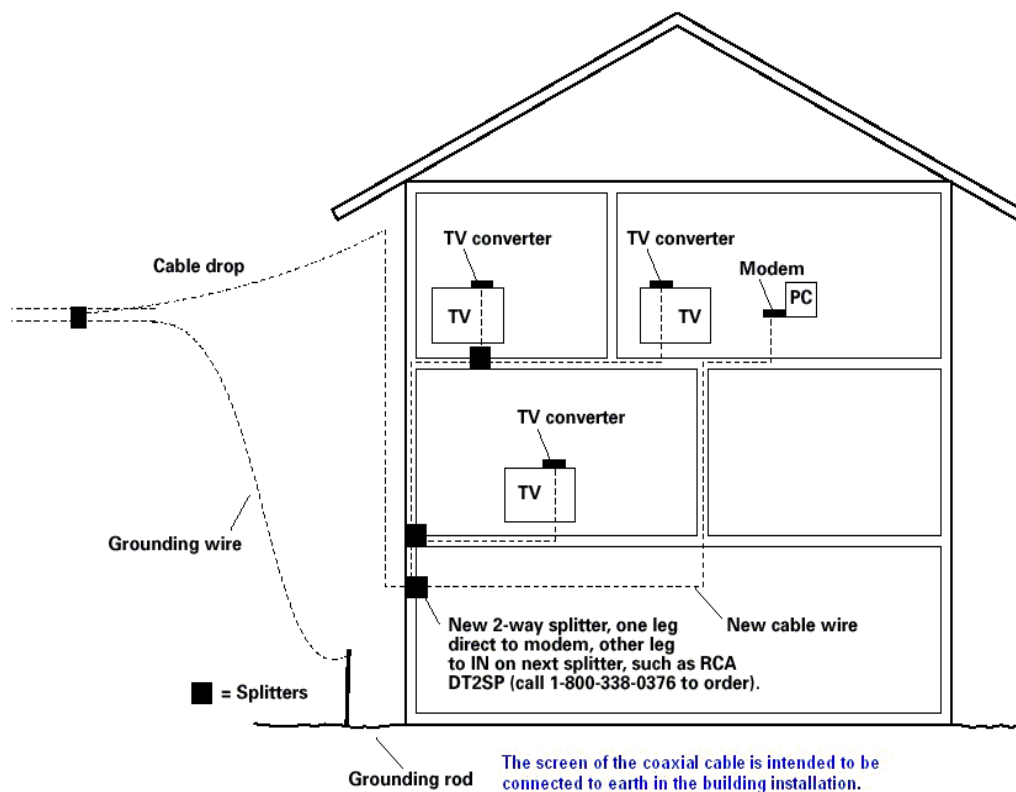


Fig. 1: Basic Home Wiring

Chapter 1: Connections and Setup

Important Connection Information

The Wireless Gateway supports 4 Ethernet connections simultaneously.

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

Ethernet Connection to a Computer

Make the connection 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 Wireless Gateway.
2. Connect the plug from the DC power supply into the POWER DC ADAPTER jack on the Cable Wireless Gateway, and plug the power supply into a DC outlet.

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

3. Connect one end of the Ethernet cable to the Ethernet port on the back of your computer, and the other end to the ETHERNET port on the Wireless 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.

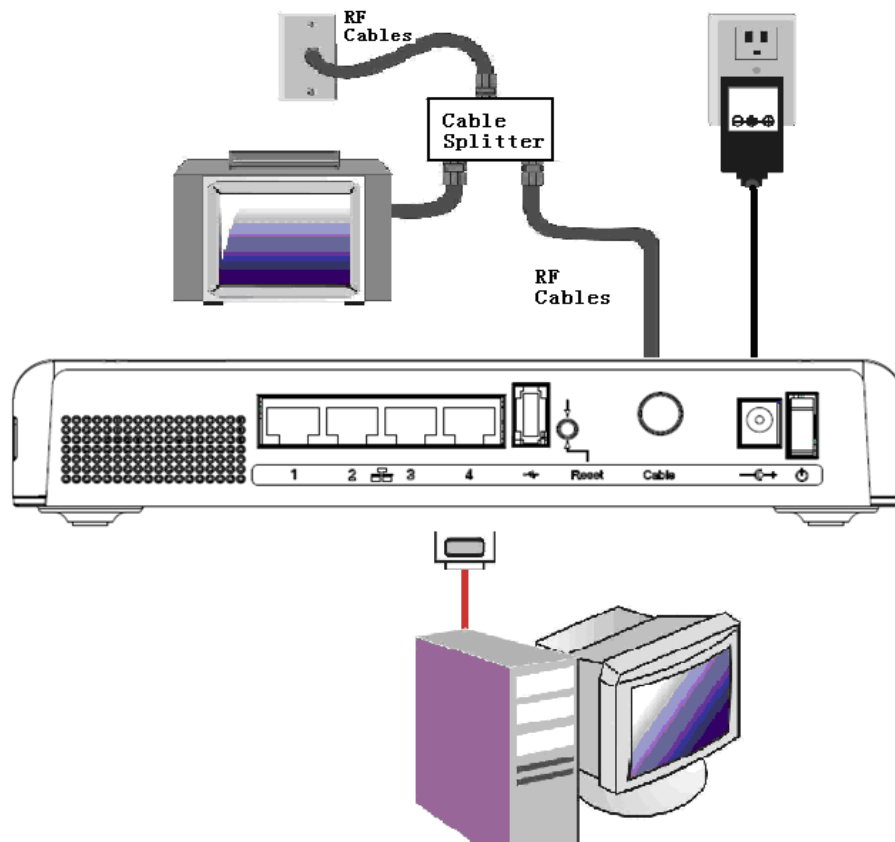


Fig.2: Ethernet Connection

Chapter 1: Connections and Setup

Connecting More Than One Computer to the Wireless Gateway

If you need to connect more than one computer to TCW770, simply connect the computers to the Ethernet ports on the rear panel.

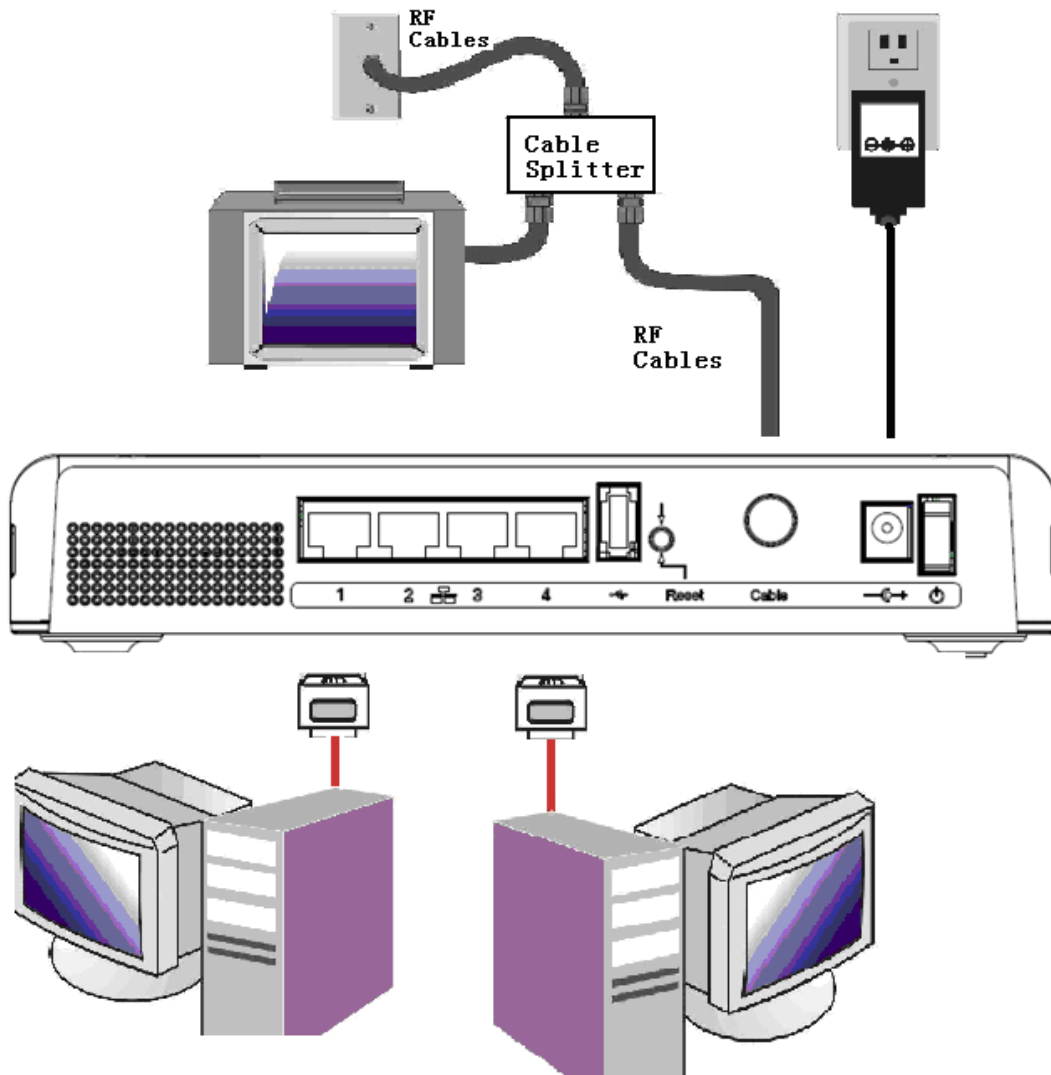


Fig.3: Multiple-PC Connection

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

Chapter 1: Connections and Setup

Turning on the Wireless Gateway

After installing the Wireless 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 Wireless Gateway is automatically updating its system software. Please wait for the lights to stop flashing. Do not remove the power supply or reset the Wireless Gateway during this process.

Chapter 2: WEB Configuration

Chapter 2: WEB Configuration

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

1. Make sure the Ethernet connection between the Wireless 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 **Wireless 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 web page 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 Wireless 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**”.
3. We strongly recommend to change the default password “admin” on the first connection :

Please define a username and password for administration .

This message will be displayed until the login and Password are changed.



Fig. 4 Login dialogue

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.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Software

Connection

Password

Diagnostics

Event Log

Initial Scan

Backup/Restore

© - Thomson - 2007

Fig. 5 Outline of Web Manager

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

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

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

Chapter 2: WEB Configuration

Status

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 shows the Thomson gateway Administration page. The top navigation bar is red with the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the navigation bar, there are tabs: Status - (selected), Network -, Advanced -, Firewall -, Parental Control -, and Wireless. The left sidebar contains a menu with options: Software (selected), Connection, Password, Diagnostics, Event Log, Initial Scan, and Backup/Restore. The main content area is titled "Status" and contains a "Software" section with the text: "This page displays information on the current system software." Below this text are two tables. The first table, titled "Information", lists system details. The second table, titled "Status", lists operational metrics.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.1
Software Version	STB6.01.60
Cable Modem MAC Address	00:10:95:de:ad:01
Cable Modem Serial Number	
CM certificate	Not Installed



Status	
System Up Time	0 days 00h:29m:23s
Network Access	Allowed
CableModem IP Address	---,---,---

Fig. 6 Status\Software

Chapter 2: WEB Configuration

2. Connection

This page reports current connection status containing connection 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.



- Software
- Connection**
- Password
- Diagnostics
- Event Log
- Initial Scan
- Backup/Restore

© - Thomson - 2007

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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		Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	
Security	Disabled	Disabled

Downstream Channels							
Channel	Lock Status	Modulation	Channel ID	Symbol rate	Frequency	Power	SNR
1	Locked	QAM256	6	6952000		-2.2 dBmV	42.6 dB
2	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
3	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
4	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
5	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
6	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
7	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
8	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB

Upstream Channels						
Channel	Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power
1	Locked	QAM16	6	2560 Ksym/sec		49.9 dBmV
2	Not Locked	Unknown	0	0 Ksym/sec		0.0 dBmV
3	Not Locked	Unknown	0	0 Ksym/sec		0.0 dBmV
4	Not Locked	Unknown	0	0 Ksym/sec		0.0 dBmV

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

Current System Time: Tue Mar 12 10:00:18 2013

Fig. 7 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 on the switch for 15 seconds, then release it.

The screenshot shows the Thomson gateway's web administration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: "Status -", "Network -", "Advanced -", "Firewall -", "Parental Control -", and "Wireless". The "Status" tab is selected. On the left is a sidebar menu with options: "Software", "Connection", "Password" (highlighted), "Diagnostics", "Event Log", "Initial Scan", and "Backup/Restore". The main content area is titled "Status" and contains a "Password" section. This section includes a description: "This page allows configuration of administration access privileges and the ability to restore factory defaults to the system." Below this are three input fields: "User Name", "Password", and "Re-Enter Password", each with a text box and a masked password field (dots). At the bottom of the section is a "Restore Factory Defaults" option with radio buttons for "Yes" and "No" (the "No" option is selected), and an "Apply" button. The Thomson logo and "images & beyond" tagline are in the top left corner. A small image of a man is also visible in the sidebar. The copyright notice "© - Thomson - 2007" is at the bottom left of the sidebar.

Fig. 8 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

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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 192 . 168 . 0 . 1

Ping Size 64 bytes

No. of Pings 3

Ping Interval 1000 ms

Start Test Abort Test Clear Results

Results

Waiting for input...

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

© - Thomson - 2007

Fig. 9 Status\Diagnostics

Chapter 2: WEB Configuration

5. Event Log

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

The screenshot shows the Thomson Administration web interface. The top navigation bar is red with the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is displayed in white on the right. Below this, a grey bar contains tabs for "Status", "Network", "Advanced", "Firewall", "Parental Control", and "Wireless". The "Status" tab is selected. On the left, a vertical menu lists "Software", "Connection", "Password", "Diagnostics", "Event Log", "Initial Scan", and "Backup/Restore". The "Event Log" option is highlighted. The main content area is titled "Status" and contains the text "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 eight rows of log entries. At the bottom of the table is a "Clear Log" button. The Thomson logo and "© - Thomson - 2007" are visible in the bottom left corner.

Time	Priority	Description
Tue Mar 12 10:04:28 2013	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...
Tue Mar 12 09:30:45 2013	Error (4)	Configuration File CVC Validation Failure
Time Not Established	Warning (5)	DHCP WARNING - Non-critical field invalid in response ;CM-MAC...
Time Not Established	Critical (3)	No Ranging Response received - T3 time-out;CM-MAC=00:10:95:de...
Time Not Established	Warning (5)	Lost MDD Timeout;CM-MAC=00:10:95:de:ad:01;CMTS-MAC=00:e0:f7:f...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	WiFi Interface [wl0] set to Channel 1 (Side-Band Channel:N/A)...
Time Not Established	Critical (3)	Resetting the cable modem due to console command

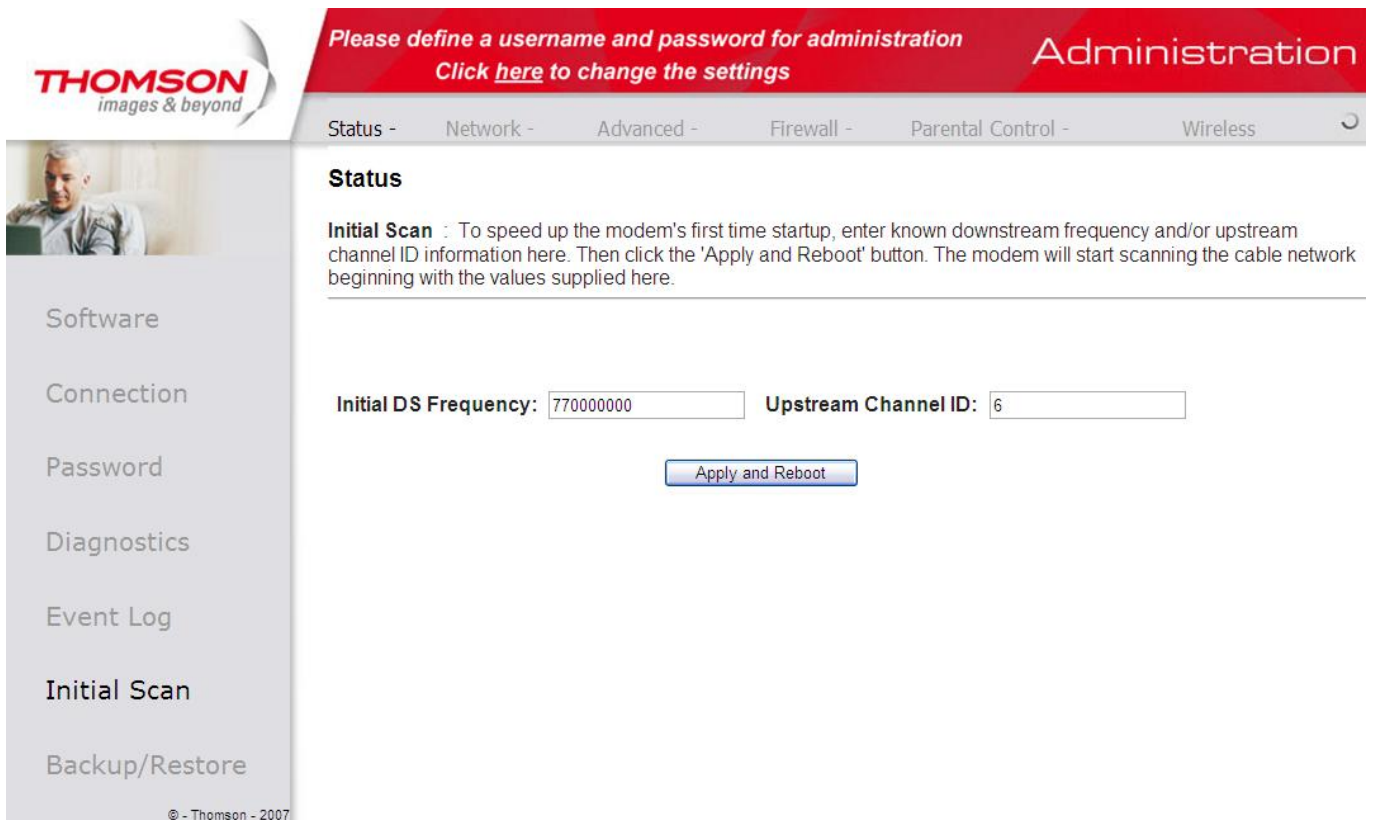
Clear Log

Fig. 10 Status\Event Log

Chapter 2: WEB Configuration

6. Initial Scan

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



The screenshot displays the Thomson Administration web interface. At the top, a red banner contains the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is also visible in the top right. Below the banner is a navigation bar with tabs: "Status -", "Network -", "Advanced -", "Firewall -", "Parental Control -", and "Wireless". The "Status" tab is selected. On the left side, there is a vertical menu with options: "Software", "Connection", "Password", "Diagnostics", "Event Log", "Initial Scan", and "Backup/Restore". The "Initial Scan" option is highlighted. The main content area is titled "Status" and contains a description of the "Initial Scan" process. Below this, there are two input fields: "Initial DS Frequency" with the value "770000000" and "Upstream Channel ID" with the value "6". An "Apply and Reboot" button is located below these fields. The Thomson logo is visible in the top left corner of the interface.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Status

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

Initial DS Frequency: Upstream Channel ID:

Software
Connection
Password
Diagnostics
Event Log
Initial Scan
Backup/Restore

© - Thomson - 2007

Fig. 11 Status\Initial Scan

Chapter 2: WEB Configuration

7. Backup/Restore

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

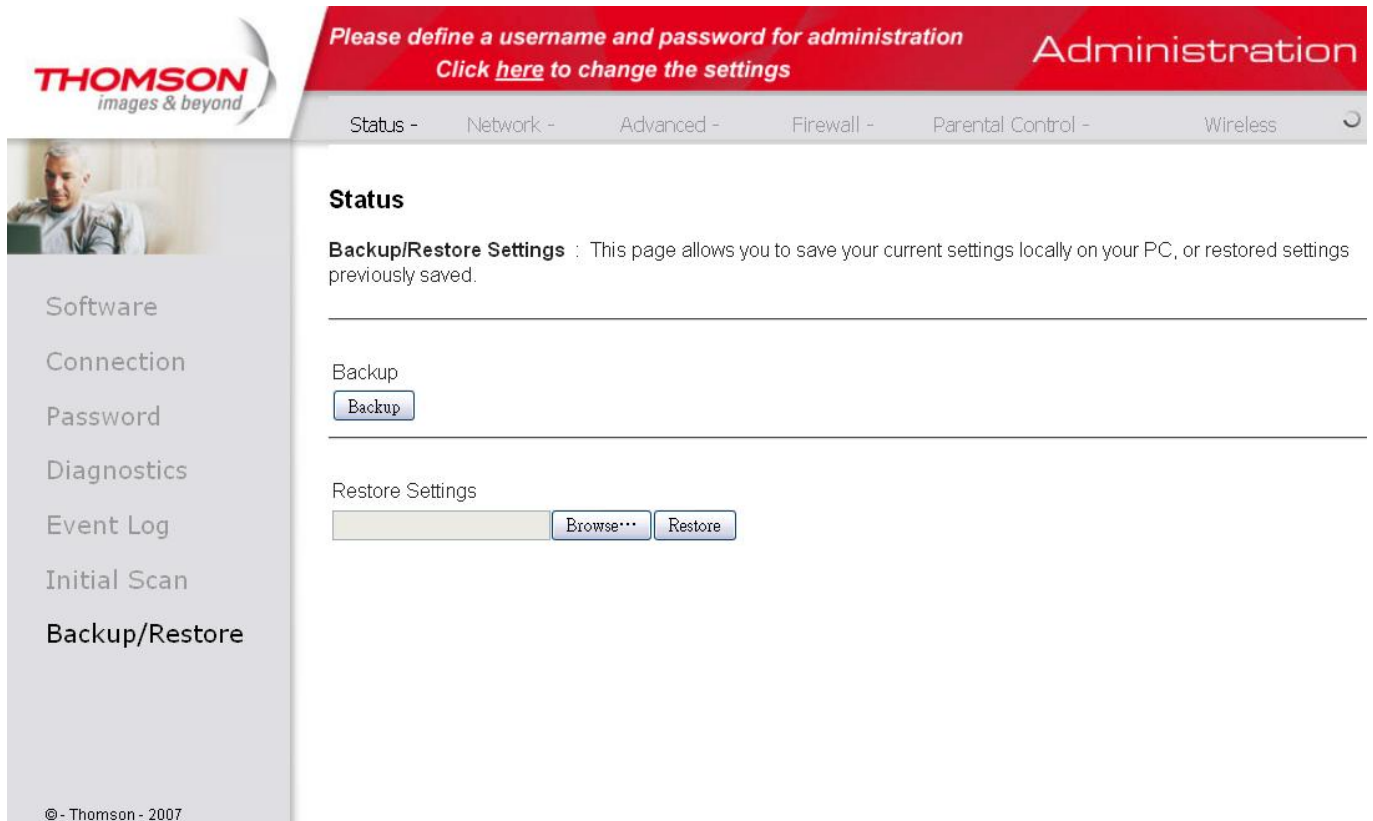


Fig. 12 Status\Backup/Restore

Chapter 2: WEB Configuration

Network

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 IP address that your gateway will use on the LAN side, enter it into the **IP Address box** and then click **Apply**.

The screenshot shows the Thomson Administration web interface. At the top, there is a red banner with the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Network" tab is selected. On the left is a sidebar with a list of menu items: LAN, WAN, Computers, DDNS, Time, FTP Diagnostics, Portbase, and PassThrough. The "LAN" item is highlighted. The main content area is titled "Network" and contains a description: "LAN : This page allows configuration and status of the optional internal DHCP server for the LAN." Below this is the "Network Configuration" section with the following fields and values:

IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
MAC Address	00:10:95:de:ad:05
DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
Lease Pool Start	192.168.0.10
Lease Pool End	192.168.0.254
Lease Time	604800

At the bottom of the configuration section is an "Apply" button. The footer of the page shows "© - Thomson - 2007".

Fig. 13 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.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Network

WAN : This page allows configuration and status of the internal DHCP client for the WAN.

WAN

IPv4 Address: ---:---:---:---:---:---
MAC Address: 00:10:95:de:ad:03
Duration D: -- H: -- M: -- S: --
Expires: ---:---:---:---:---:---

Release WAN Lease Renew WAN Lease

WAN Connection Type DHCP

Ipv4 MTU Size 0 (256-1500 octets, 0 = use default)

Spoofed MAC Address 00:00:00:00:00:00

Apply

© - Thomson - 2007

Fig. 14 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.

The screenshot shows the Thomson Administration web interface. The top navigation bar is red with the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is on the right. Below this is a grey navigation bar with links: Status -, Network -, Advanced -, Firewall -, Parental Control -, and Wireless. The "Network" link is selected. On the left is a vertical menu with options: LAN, WAN, Computers (highlighted), DDNS, Time, FTP Diagnostics, Portbase, and PassThrough. The main content area is titled "Network" and "Computers". It contains the text: "Computers : This page shows the status of the DHCP clients and current system time." Below this is a section for "DHCP Clients" with a table header: "MAC Address", "IP Address", "Subnet Mask", "Duration", "Expires", and "Select". The table body shows "No DHCP Clients". Below the table is the "Current System Time: Tue Mar 12 14:43:22 2013" and a "Force Available" button. At the bottom of the main content area is a "Stateless Auto Configuration" section with a table header: "IP Address", "MAC Address", and "Reachability State". The Thomson logo "THOMSON images & beyond" is in the top left corner, and "© - Thomson - 2007" is at the bottom left.

Fig. 15 Network\Computers

Chapter 2: WEB Configuration

4. DDNS

This page allows setup of Dynamic DNS service.

The screenshot shows the Thomson router's web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is displayed in large white text. Below the banner is a navigation bar with tabs: "Status -", "Network -", "Advanced -", "Firewall -", "Parental Control -", and "Wireless". The "Network" tab is selected. On the left side, there is a vertical menu with options: "LAN", "WAN", "Computers", "DDNS", "Time", "FTP Diagnostics", "Portbase", and "PassThrough". The "DDNS" option is highlighted. The main content area is titled "Network" and contains a sub-header "DDNS : This page allows setup of Dynamic DNS service." Below this, there are several fields: "DDNS Service:" with a dropdown menu set to "Disabled", "User Name:" with an empty text box, "Password:" with an empty text box, "Host Name:" with an empty text box, "IP Address:" with the value "10.10.136.63", and "Status:" with the text "DDNS service is not enabled." and an "Apply" button.

Fig. 16 Network\DDNS

- **DDNS Service-** Choose Enabled (www.DynDNS.org) to enable the basic setting. Choose Disabled to close the basic setting.
- **Username-** The username that you registered with your DDNS provider.
- **Password-** The password that you registered with your DDNS provider
- **Host Name-** The domain name or host name that is registered with your DDNS provider
- **Status-** It shows the DDNS service status whether it is enabled or disabled.

Click Apply to save the changes

Chapter 2: WEB Configuration

5. 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.

The screenshot shows the Thomson router's web administration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is displayed in the top right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Network" tab is selected. On the left is a sidebar menu with options: LAN, WAN, Computers, DDNS, Time (highlighted), FTP Diagnostics, Portbase, and PassThrough. The main content area is titled "Network" and contains a description of the Time page. Below the description are configuration options for SNTP, current time, system start time, three time servers, and a timezone offset. At the bottom of the configuration section are "Apply" and "Reset Values" buttons.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Network

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.

Enable SNTP ☐ Yes ☒ No

Current Time Tue Mar 12 14:45:00 2013

System Start Time Tue Mar 12 14:37:47 2013

Time Server 1

Time Server 2

Time Server 3

Timezone Offset Hours Minutes

LAN

WAN

Computers

DDNS

Time

FTP Diagnostics

Portbase

PassThrough

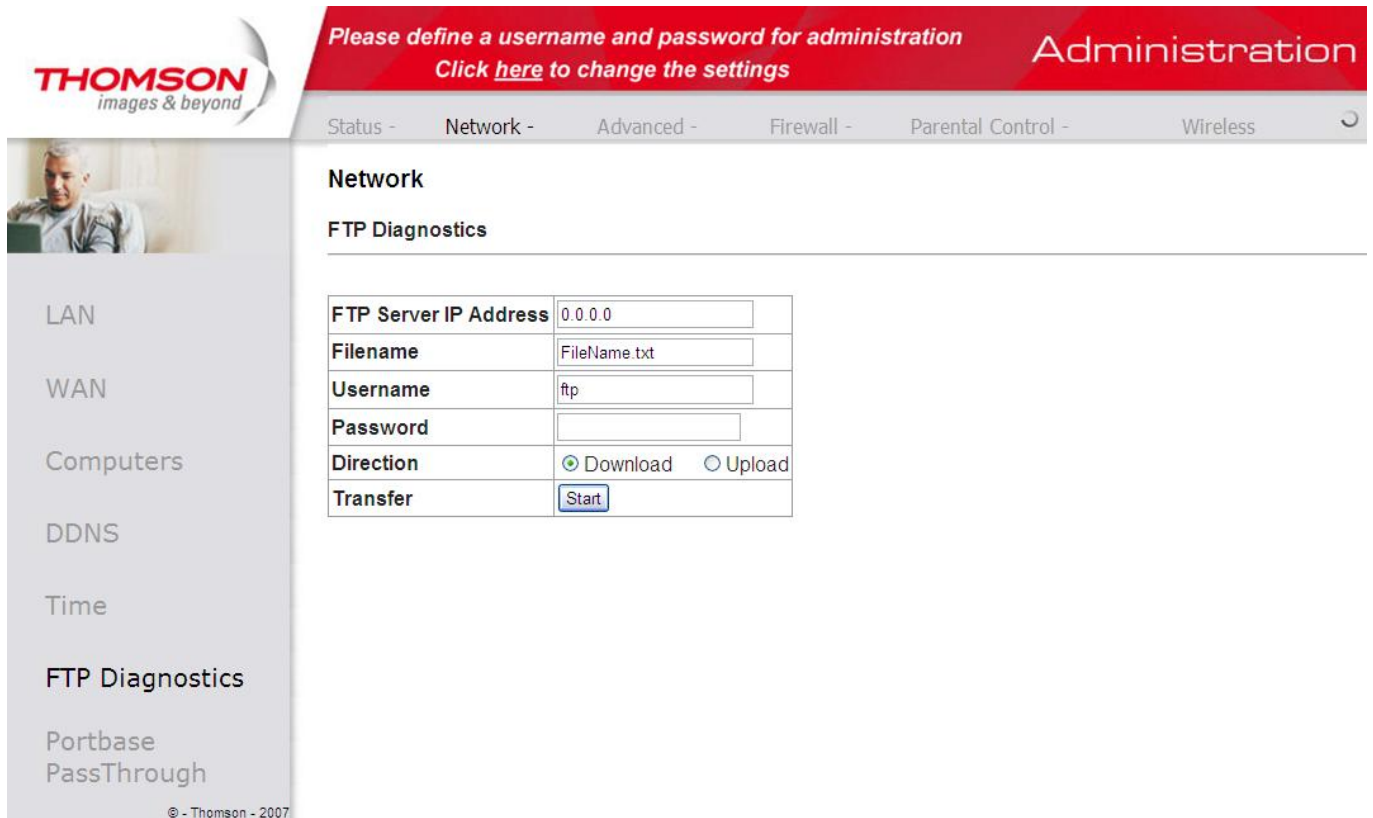
© - Thomson - 2007

Fig. 17 Network\Time

Chapter 2: WEB Configuration

6. FTP Diagnostics

This page allows to test download and upload transmit rate through FTP. Choose known FTP server and FileName with correct username and password then choose direction to Download or Upload. Press the 'Start' button to start.



The screenshot shows the Thomson Administration web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Network" tab is selected. On the left is a sidebar menu with options: LAN, WAN, Computers, DDNS, Time, FTP Diagnostics (highlighted), Portbase, and PassThrough. The main content area is titled "Network" and "FTP Diagnostics". It contains a form with the following fields:

FTP Server IP Address	0.0.0.0
Filename	FileName.txt
Username	ftp
Password	
Direction	<input checked="" type="radio"/> Download <input type="radio"/> Upload
Transfer	<input type="button" value="Start"/>

Fig. 18-1 Network\FTP Diagnostics

You will see the result on the page, when transmit done.

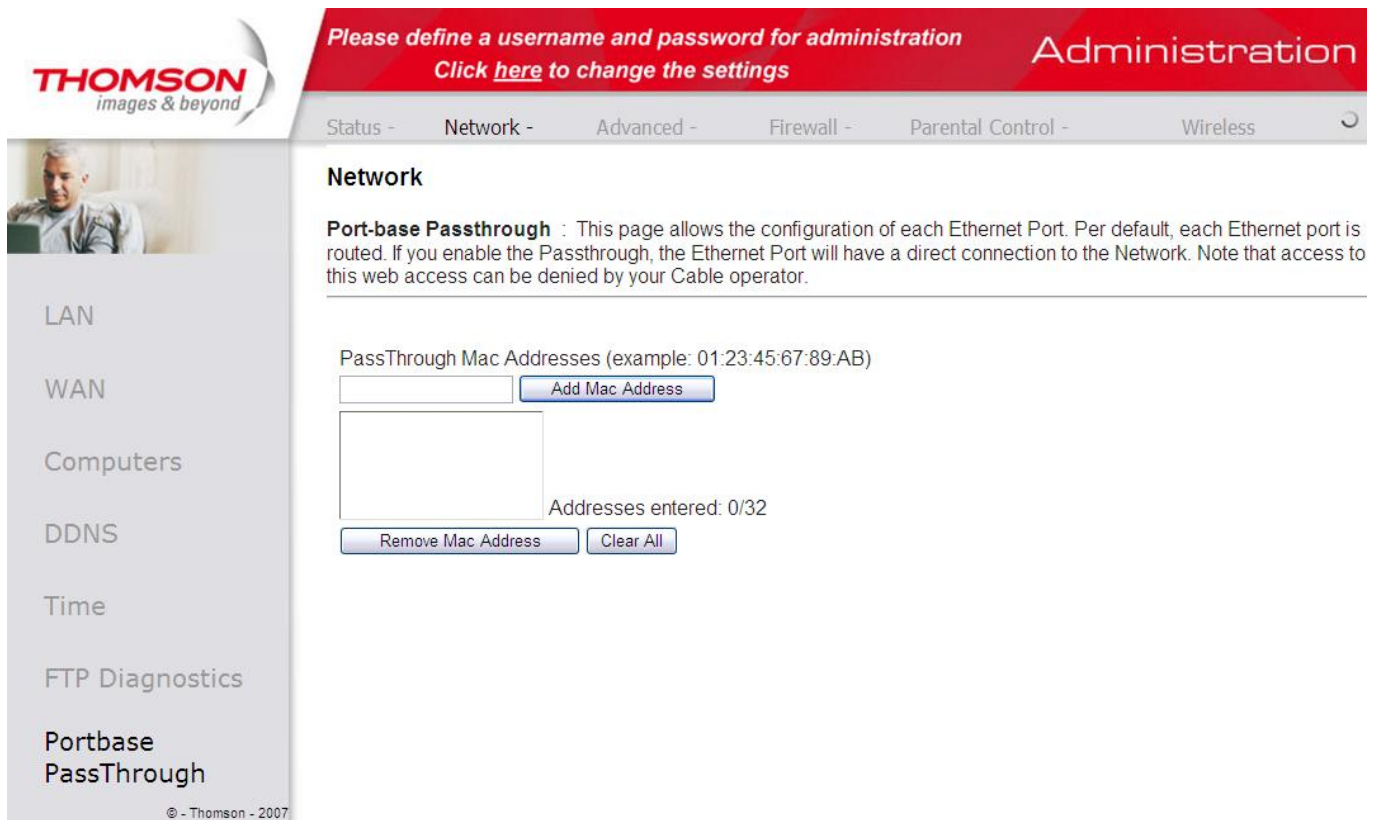
FTP Download	
Payload Data Bytes	6296 bytes
Total Packet Bytes	6752 bytes
Elapsed Time	0.027260 Secs
Payload Throughput	1.847689 Mbps
Packet Throughput	1.981511 Mbps

Fig. 18-2 Network\FTP Diagnostics

Chapter 2: WEB Configuration

7. Portbase Passthrough

This page allows the configuration of each Ethernet Port. Per default, each Ethernet port is routed. If you enable the Passthrough, the Ethernet Port will have a direct connection to the Network. Note that access to this web access can be denied by your Cable operator.



The screenshot shows the Thomson router's web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" tab is selected. Below the banner, a navigation bar shows "Status - Network - Advanced - Firewall - Parental Control - Wireless". The "Network" tab is active. The main content area is titled "Network" and contains the "Port-base Passthrough" section. This section explains that the page allows configuration of each Ethernet Port, which is routed by default. It notes that enabling Passthrough provides a direct connection to the Network, but access to the web interface may be denied by the cable operator. Below this text, there is a form for "PassThrough Mac Addresses (example: 01:23:45:67:89:AB)". The form includes a text input field, an "Add Mac Address" button, and a "Remove Mac Address" button. A "Clear All" button is also present. The status "Addresses entered: 0/32" is displayed. On the left side, a sidebar menu lists various configuration options: LAN, WAN, Computers, DDNS, Time, FTP Diagnostics, and Portbase PassThrough (which is highlighted). The Thomson logo and "images & beyond" tagline are visible in the top left corner. The copyright notice "© - Thomson - 2007" is at the bottom left.

Fig. 19 Network\Portbase PassThrough

Chapter 2: WEB Configuration

Advanced

1. Options

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

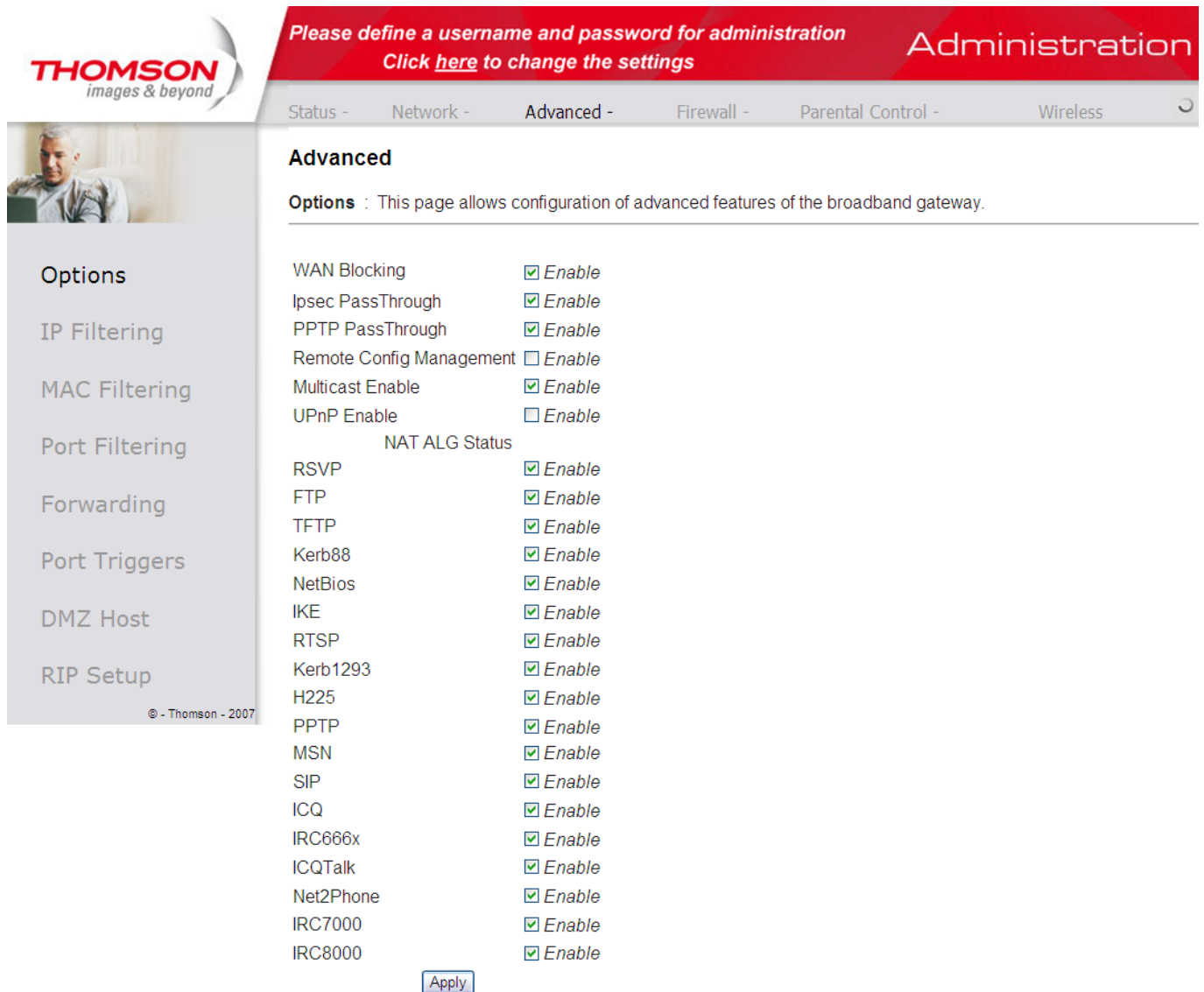


Fig. 20 Advanced\Options

- **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.
- **Ipssec 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.

Chapter 2: WEB Configuration

- **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.
- **UPnP** Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.
- **NAT ALG** enable NAT ALG (application layer gateways) allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as RSVP, FTP, TFTP, Kerb88, NetBios , IKE, RTSP, Kerb1293 , H225 , PPTP , MSN , SIP , ICQ , IRC666x , ICQTalk , Net2Phone , IRC7000 , IRC8000 file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

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. These PCs can still communicate with each other on your LAN, but packets they originate to WAN addresses are blocked by the gateway.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Advanced

IP Filtering : This page allows the configuration of IP Address filters in order to prevent local IP address from getting access to the Internet. By entering starting and ending IP address ranges, you can configure which local PCs are denied access to the WAN.

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

Apply

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

© - Thomson - 2007

Fig. 21 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 router's web configuration interface. The top navigation bar is red with the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" tab is selected. Below the navigation bar, the "Advanced" tab is active. The "MAC Filtering" section is highlighted in the left sidebar. The main content area shows the "MAC Address Filters" configuration. It contains two columns of MAC address input fields, each labeled from MAC 01 to MAC 20. Each field is a text box with a colon separator and six digits. An "Apply" button is located at the bottom right of the input fields. The Thomson logo is visible in the top left corner of the interface.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Advanced

MAC Filtering : This page allows configuration of MAC Address filters in order to prevent local MAC address from getting access to the Internet By entering MAC address , you can configure which local PCs are denied access to the WAN.

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

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

© - Thomson - 2007

Fig. 22 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 router's web configuration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is on the right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Advanced" tab is selected. On the left is a sidebar menu with options: Options, IP Filtering, MAC Filtering, Port Filtering (highlighted), Forwarding, Port Triggers, DMZ Host, and RIP Setup. The main content area is titled "Advanced" and "Port Filtering". It contains a description: "Port Filtering : This page allows configuration of port filters in order to prevent a range of TCP/UDP ports from accessing the Internet." Below this is a table for configuring port filters. The table has four columns: Start Port, End Port, Protocol, and Enabled. There are ten rows, each with a "1" in the Start Port column, "65535" in the End Port column, "Both" in the Protocol column, and an unchecked checkbox in the Enabled column. An "Apply" button is located below the table. The Thomson logo and "images & beyond" tagline are in the top left corner. The copyright notice "© - Thomson - 2007" is at the bottom left of the sidebar.

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

Apply

Fig. 23 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

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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.

Create IPv4

Port Forwarding									
Internal			External						
IP Address	Start Port	End Port	IP Address	Start Port	End Port	Prot	Description	Enabled	
									Remove All

UPnp Port Mapping

Protocol	Start Port	End Port	Description
----------	------------	----------	-------------

© - Thomson - 2007

Fig. 24-1 Advanced\Forwarding

Chapter 2: WEB Configuration

Press **'Create Ipv4'** button to specify rules. Choose **Service Name** or **Port** number range to set up. IP Address 0.0.0.0 means allow all IP address.

Known Rule Adder

Local IP Address:	<input type="text" value="0.0.0.0"/>
External IP Address:	<input type="text" value="0.0.0.0"/>
Service Name:	<input type="text" value="AIM Talk"/> ▼
	<input type="button" value="Add"/>

Local IP Address	<input type="text" value="0.0.0.0"/>
Local Start Port	<input type="text" value="0"/>
Local End Port	<input type="text" value="0"/>
External IP	<input type="text" value="0.0.0.0"/>
External Start Port	<input type="text" value="0"/>
External End Port	<input type="text" value="0"/>
Protocol	<input type="text" value="TCP"/> ▼
Description	<input type="text"/>
Enabled	<input type="text" value="Off"/> ▼
	<input type="button" value="Cancel"/> <input type="button" value="Apply"/>

Fig. 24-2 Advanced\Forwarding

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.

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 router's web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" tab is selected. Below the banner, a navigation bar shows "Status -", "Network -", "Advanced -", "Firewall -", "Parental Control -", and "Wireless". The "Advanced" section is active, displaying the "Port Triggers" configuration page. A "Create" button is visible. Below it, a table titled "Port Triggering" is shown with columns for "Trigger Range" (Start Port, End Port), "Target Range" (Start Port, End Port), "Protocol", "Description", "Enable", and a "Remove All" button. The left sidebar contains a menu with "Options", "IP Filtering", "MAC Filtering", "Port Filtering", "Forwarding", "Port Triggers", "DMZ Host", and "RIP Setup". The Thomson logo and "images & beyond" tagline are in the top left, and "© - Thomson - 2007" is at the bottom left.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Advanced

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

Create

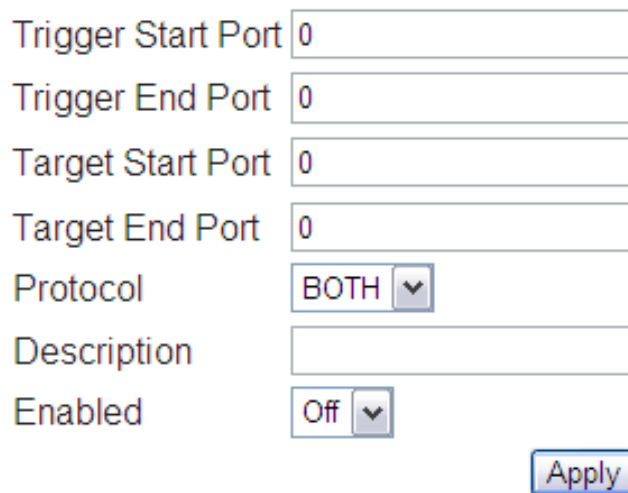
Port Triggering							
Trigger Range		Target Range		Protocol	Description	Enable	Remove All
Start Port	End Port	Start Port	End Port				

© - Thomson - 2007

Fig. 25-1 Advanced\Port Triggers

Chapter 2: WEB Configuration

Press **'Create'** button to specify rules.



Trigger Start Port	<input type="text" value="0"/>
Trigger End Port	<input type="text" value="0"/>
Target Start Port	<input type="text" value="0"/>
Target End Port	<input type="text" value="0"/>
Protocol	<input type="text" value="BOTH"/>
Description	<input type="text"/>
Enabled	<input type="text" value="Off"/>
<input type="button" value="Apply"/>	

Fig. 25-2 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.

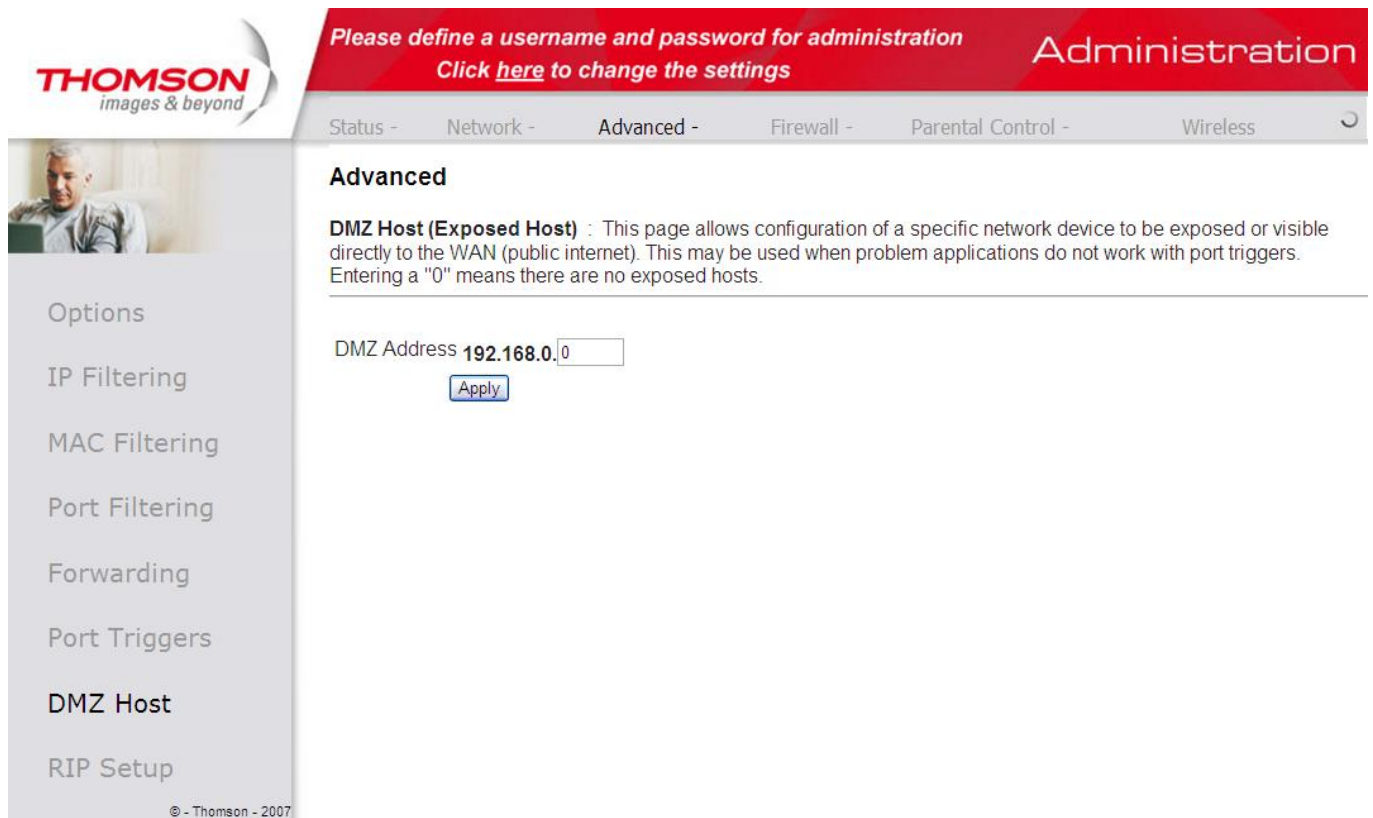


Fig. 26 Advanced\DMZ Host

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 router's web configuration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is displayed in the top right. Below the banner is a navigation bar with tabs: "Status -", "Network -", "Advanced -", "Firewall -", "Parental Control -", and "Wireless". The "Advanced" tab is selected. On the left side, there is a vertical menu with options: "Options", "IP Filtering", "MAC Filtering", "Port Filtering", "Forwarding", "Port Triggers", "DMZ Host", and "RIP Setup". The "RIP Setup" option is highlighted. The main content area is titled "Advanced" and contains the "Routing Information Protocol Setup" section. This section includes a description: "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." Below the description are the following settings: "RIP Support" (a dropdown menu set to "Disabled"), "RIP Authentication" (a checkbox labeled "Enable" which is checked), "RIP Authentication Key" (a text input field), "RIP Authentication Key ID" (a text input field set to "0"), "RIP Reporting Interval" (a text input field set to "30" followed by "seconds"), and "RIP Destination IP Address" (four text input fields set to "0", "0", "0", and "0" respectively). An "Apply" button is located at the bottom of the settings area. The Thomson logo and "images & beyond" tagline are in the top left corner. A small image of a man is also visible in the left sidebar. The copyright notice "© - Thomson - 2007" is at the bottom left of the sidebar.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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 . . .

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

© - Thomson - 2007

Fig. 27 Advanced\RIP Setup

Chapter 2: WEB Configuration

Firewall

1. Web 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.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Firewall

Web Content Filter : This page allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. A list of "trusted computers" can also be defined that are not subject to any filters configured. Specific Firewall features can also be enabled. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks. Go to the Parental Control page to block internet access to specific sites.

Web Features	Allowed Services
Filter Proxy <input type="checkbox"/> Enable	No Ports Restricted
Filter Cookies <input type="checkbox"/> Enable	
Filter Java Applets <input type="checkbox"/> Enable	
Filter ActiveX <input type="checkbox"/> Enable	
Filter Popup Windows <input type="checkbox"/> Enable	
Block Fragmented IP Packets <input type="checkbox"/> Enable	
Port Scan Detection <input type="checkbox"/> Enable	
IP Flood Detection <input checked="" type="checkbox"/> Enable	
Firewall Protection Low	

Apply

Trusted Computers

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

No Trusted Computers Remove

© - Thomson - 2007

Fig. 28 Firewall\Web Filter

Chapter 2: WEB Configuration

2. TOD Filtering

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

The screenshot shows the Thomson Administration web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Firewall" tab is selected. On the left is a sidebar with a Thomson logo and a list of menu items: Web Filter, TOD Filter (highlighted), Local Log, and Remote Log. The main content area is titled "Firewall" and contains the "Time of Day Access Filter" section. This section includes a text description, a time selection row (00:00:00:00:00:00) with an "Add" button, a "No filters entered" dropdown, an "Enabled" checkbox, and a "Remove" button. Below these are "Days to Block" (checkboxes for Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday) and "Time to Block" (checkbox for All day). The "Time to Block" section has "Start" and "End" time pickers, both set to 12:00 AM. An "Apply" button is at the bottom.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Firewall

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

00 : 00 : 00 : 00 : 00 : 00 [Add](#)

No filters entered. ☐ Enabled [Remove](#)

Days to Block

☐ Everyday ☐ Sunday ☐ Monday ☐ Tuesday
☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Time to Block

☐ All day

Start: 12 (hour) 00 (min) AM
End: 12 (hour) 00 (min) AM

[Apply](#)

© - Thomson - 2007

Fig. 29 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 Firewall Administration web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Status -, Network -, Advanced -, Firewall -, Parental Control -, and Wireless -. The "Firewall" tab is selected. On the left is a sidebar with a Thomson logo and a list of menu items: Web Filter, TOD Filter, Local Log (highlighted), and Remote Log. The main content area is titled "Firewall" and contains a description of the "Local Log" page. Below the description are input fields for "Contact Email Address", "SMTP Server Name", "SMTP Username", and "SMTP Password". There is also a checkbox for "E-mail Alerts" with an "Enable" label and an "Apply" button. At the bottom, there is a table with headers: Description, Count, Last Occurrence, Target, and Source. Below the table are two buttons: "E-mail Log" and "Clear Log".

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Firewall

Local Log : This page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system.

Contact Email Address

SMTP Server Name

SMTP Username

SMTP Password

E-mail Alerts ☐ Enable

Description	Count	Last Occurrence	Target	Source
-------------	-------	-----------------	--------	--------

© - Thomson - 2007

Fig. 30 Firewall\Local Log

Chapter 2: WEB Configuration

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

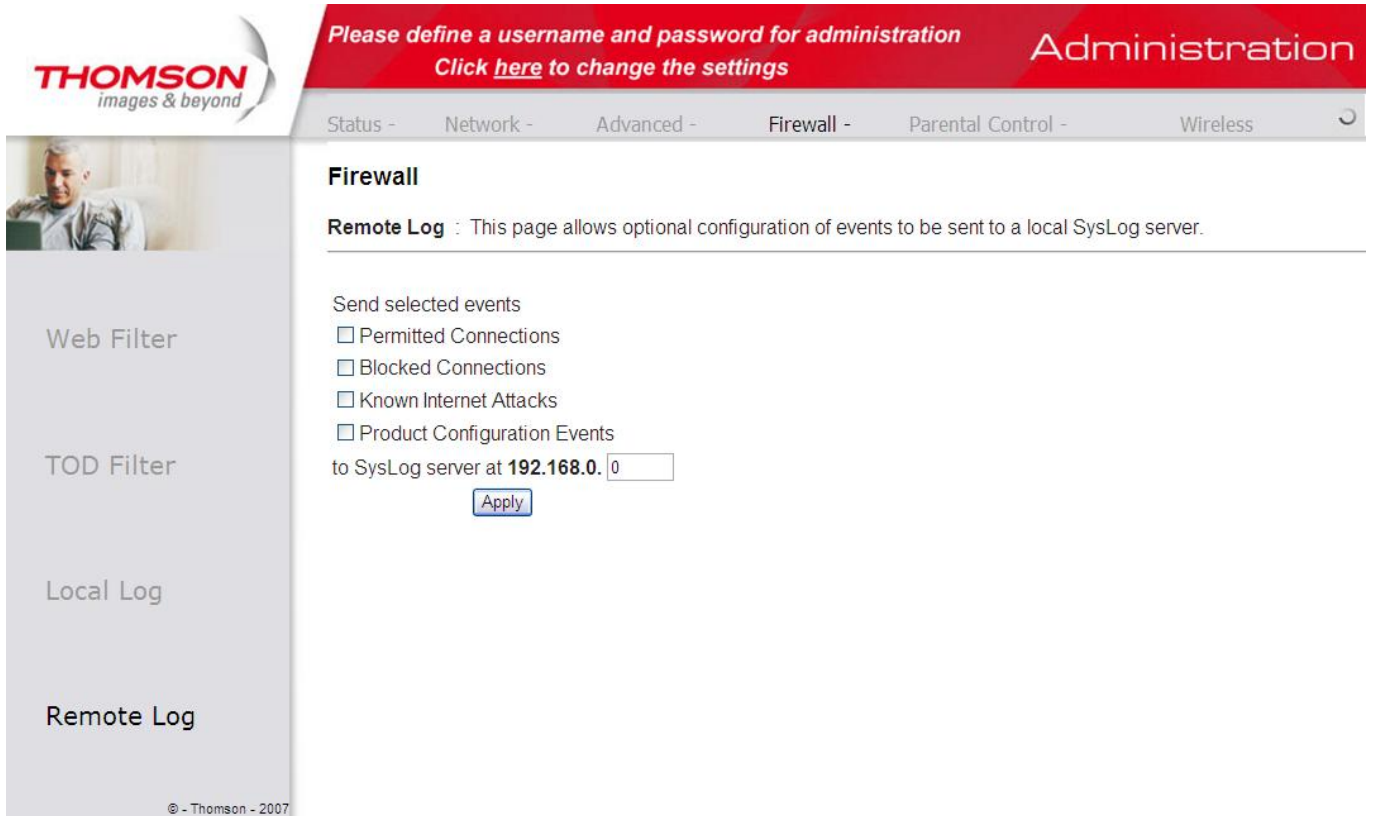


Fig. 31 Firewall\Remote Log

Chapter 2: WEB Configuration

Parental Control

1. Basic

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

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

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

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Parental Control

Basic Setup : 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.

Content Filtering

Keyword Blocking ☐ Enable

Domain Blocking ☐ Enable

Apply

Keyword List

Add Keyword

Remove Keyword

Blocked Domain List

Add Domain

Remove Domain

© - Thomson - 2007

Fig. 32 Parental Control\Basic

Chapter 2: WEB Configuration

2. Setup

This page allows configuration of users, if you encounter a blocked website, you can override the block by entering the following user name and password.

The screenshot shows the Thomson router's web configuration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is displayed in the top right. Below the banner is a navigation bar with tabs: "Status -", "Network -", "Advanced -", "Firewall -", "Parental Control -", and "Wireless". The "Parental Control" tab is selected. On the left side, there is a sidebar with a "THOMSON images & beyond" logo, a photo of a man, and two main menu items: "Basic" and "Setup". The "Setup" item is currently selected. The main content area is titled "Parental Control" and contains a sub-header "User Setup : This page allows configuration of users." Below this is a form with the following fields: "User Name" (with a text box containing "Default"), "Password" (with a masked input box showing five dots), "Re-Enter Password" (with a masked input box showing five dots), and "Inactivity time" (with a text box containing "30" and a label "min"). An "Apply" button is located at the bottom of the form. At the bottom left of the sidebar, the copyright notice "© - Thomson - 2007" is visible.

User Name	Default
Password
Re-Enter Password
Inactivity time	30 min
<input type="button" value="Apply"/>	

Fig. 33 Parental Control\Setup

Chapter 2: WEB Configuration

Wireless

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 TCW770 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.

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 Radio 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 Radio 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 Primary Network Web Page discussion below for details.

Data Encryption – Set to WPA (64-bit)

PassPhrase – Use this feature to generate security keys

Chapter 2: WEB Configuration

1. 802.11/ Radio

To set the basic configuration for the wireless features, please click **Radio** item from the **Wireless** menu.

The screenshot shows the Thomson Administration web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Wireless" tab is selected. On the left is a sidebar menu with options: Radio, Primary Network, Access Control, Advanced, Bridging, and WMM. The "Radio" option is highlighted. The main content area is titled "Wireless" and contains the "802.11 Radio" configuration section. A description states: "802.11 Radio : This page allows configuration of the Wireless Radio including current country and channel number." The configuration fields are as follows: Interface (Enabled), Wireless MAC Address (00:26:24:78:C2:22), Output Power (100%), 802.11 Band (2.4 Ghz, Current: 2.4 GHz), 802.11 n-mode (Auto), 802.11 N Support Required (Off), Bandwidth (20 Mhz, Current: 20MHz), Sideband for Control Channel (40 Mhz only) (None, Current: None), Control Channel (1), Current Channel: 1, Interference Level: Acceptable, Regulatory Mode (Off), TPC Mitigation (db) (0 (Off)), OBSS Coexistence (1 (Enabled)), and STBC Tx (Auto). At the bottom are three buttons: Apply, Restore Wireless Defaults, and Scan Wireless APs.

Fig. 34 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. Activated by changing interface to enabled.
- **Wireless MAC Address:** The MAC address for this wireless device will be displayed in this field automatically.
- **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. Control the range of the AP by adjusting the radio output power.
- **802.11 Band:** It can Support 2.4 GHz and 5 GHz exclusively.
- **802.11n mode:** It may help you to **Enable** or **Disable** the 11N mode. To enable you need to select **Auto**, to disable you need to select **Off**, and so force the AP to operate in **802.11g mode**.
- **Bandwidth:** Select wireless channel width 20Mhz is for default value (bandwidth taken by wireless signals of this access point.)

Chapter 2: WEB Configuration

- **Sideband for Control Channel (40Mhz only):** There are “Lower” and “Upper” can be selected if Bandwidth 40Mhz is Enabled.
- **Control 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.

Setting	Description	Value List or Range	Default
Network Name (SSID)	Set the Network Name (also known as SSID) of this network.	Up to 32-character string containing ASCII characters only	THOM_Dxxxxxxx
Network Type	Select Closed to hide the network from active scans. Select Open to reveal the network to active scans.	Open, Closed	Open
New Channel	Select a particular channel on which to operate.	1-13	1, 6 or 11
Interface	Enable or disable the wireless interface.	Enabled, Disabled	Enabled

● Table1. Basic Settings Definitions

Chapter 2: WEB Configuration

2. 802.11/ Primary Network

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

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Wireless

802.11 Primary Network : This page allows configuration of the Primary Wireless Network and its security settings.

Primary Network Thom_D1892775 (00:26:24:78:c2:22)

Primary Network ☐ Enabled

Network Name (SSID)

Closed Network ☐ Open

AP Isolate ☐ Disabled

WPA ☐ Disabled

WPA-PSK ☐ Enabled

WPA2 ☐ Disabled

WPA2-PSK ☐ Enabled

WPA/WPA2 Encryption

WPA Pre-Shared Key

☐ Show 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

Automatic Security Configuration

WPS

WPS Config State: Configured

The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)

Device Name

WPS Setup AP

UUID: 36f764d0e3940d3a630044d6f9180495

PIN:

WPS Add Client

Add a client:

Client PIN:

Authorized Client MAC:

Fig. 35 Wireless\Primary Network

- **Primary Network:** 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.

Chapter 2: WEB Configuration

- **Closed Network:** This control is used to hide or reveal your network name (SSID) to any remote, wireless equipped PC in the area that may be scanning WiFi channels to find available WiFi networks. The gateway WiFi radio frequently transmits a beacon signal which can contain this network name (SSID). If you set Closed Network to Enable, your SSID is included in that beacon, and is therefore detectable by any nearby wireless equipped PCs in the area. The benefit of using Enable is it can speed your WiFi setup on some PCs. If you set Closed Network to Disable, your SSID is not included in the beacon. This hides your network name (SSID), but as a result may require a bit more effort on your part to set up your wireless PCs. And when we Enable the **WPS Config** then the **Closed Network** will be Disabled automatically.
- **WPA (Wi-Fi Protected Access)/WPA2:**
It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than none WPA modes. **WPA2** is the second generation of **WPA** security
- **WPA-PSK (WPA-Pre-Shared Key) /WPA2-PSK (WPA2-Pre-Shared Key):**
It is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.
- **WEP Encryption:**
You can choose **64-bit** or **128-bit** according to your needs. If you choose **Disabled**, the Network Keys will not be shown on this page. If selected, the data is encrypted using the key before being transmitted. For example, if you set 128-bit in this field, then the receiving station must be set to use 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 Wireless Gateway.)
- If you select WEP (**64-bit** or **128-bit**), you can adjust the following settings. And by selecting **Disable** you can disable WEP Encryption.
- **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.
- **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.

The screenshot displays a web configuration page for 802.1x Authentication. The interface includes several input fields and dropdown menus. At the top, 'WPA/WPA2 Encryption' is set to 'TKIP+AES'. Below it, 'WPA Pre-Shared Key' is a masked field. The 'RADIUS Server' field contains '0.0.0.0', 'RADIUS Port' is '1812', and 'RADIUS Key' is a masked field. Further down, 'Group Key Rotation Interval' is '0' and 'WPA/WPA2 Re-auth Interval' is '3600'. The 'WEP Encryption' dropdown is set to 'Disabled'. 'Shared Key Authentication' is set to 'Optional', and '802.1x Authentication' is set to 'Disabled'. There are four 'Network Key' fields (1-4), all of which are masked. The 'Current Network Key' dropdown is set to '1'. A 'PassPhrase' field is also present and masked. At the bottom, there is a 'Generate WEP Keys' button and an 'Apply' button.

Fig. 36 802.1x 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 Wireless 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.

The screenshot displays a web configuration interface for WPA/WPA2 settings. It includes several dropdown menus and text input fields. The 'WPA' dropdown is set to 'Disabled', 'WPA-PSK' to 'Enabled', 'WPA2' to 'Disabled', and 'WPA2-PSK' to 'Enabled'. The 'WPA/WPA2 Encryption' dropdown is set to 'TKIP+AES'. The 'WPA Pre-Shared Key' field is a long text box filled with dots. The 'RADIUS Server' field contains '0.0.0.0', 'RADIUS Port' contains '1812', and 'RADIUS Key' is an empty text box. The 'Group Key Rotation Interval' field contains '0', and the 'WPA/WPA2 Re-auth Interval' field contains '3600'.

WPA	Disabled
WPA-PSK	Enabled
WPA2	Disabled
WPA2-PSK	Enabled
WPA/WPA2 Encryption	TKIP+AES
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

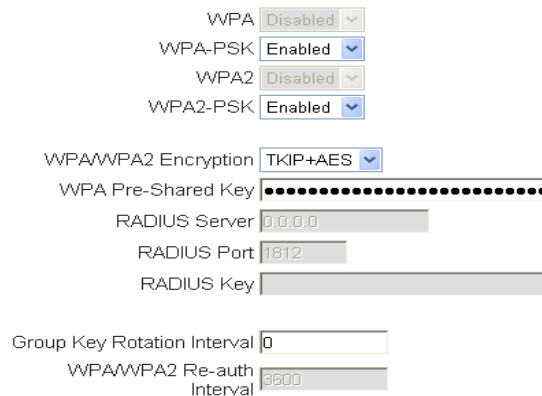
Fig. 37 WPA/WPA2

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 screenshot displays a web configuration interface for WPA-PSK/WPA2-PSK. It features several settings: WPA is set to 'Disabled', WPA-PSK is 'Enabled', WPA2 is 'Disabled', and WPA2-PSK is 'Enabled'. The WPA/WPA2 Encryption is set to 'TKIP+AES'. The WPA Pre-Shared Key field is filled with 64 dots. The RADIUS Server is '0.0.0.0', RADIUS Port is '1812', and RADIUS Key is empty. The Group Key Rotation Interval is '0', and the WPA/WPA2 Re-auth Interval is '3600'.

WPA	Disabled
WPA-PSK	Enabled
WPA2	Disabled
WPA2-PSK	Enabled
WPA/WPA2 Encryption	TKIP+AES
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. 38 WPA-PSK/WPA2-PSK

Chapter 2: WEB Configuration

Automatic Security Configuration

The screenshot shows a web configuration page titled "Automatic Security Configuration". At the top, there is a dropdown menu set to "WPS". Below it, a box displays "WPS Config State: Configured". A text label states: "The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)". Further down, a "Device Name" field contains the text "ThomsonAP". The next section is "WPS Setup AP", showing a "UUID: 36f764d0e3940d3a630044d6f9180495" and a "PIN: 46819406" field with a "Configure" button. The final section is "WPS Add Client", featuring an "Add a client:" label with an "Add" button, a "Client PIN:" field, and an "Authorized Client MAC:" field.

Fig. 39 Automatic Security Configuration

WiFi Protected Setup (WPS) is an easy and secure way of configuring and connecting your WiFi access point. In your case, the TCW770 is the Access Point (AP), and Your PC (or Wifi Device) is called the STA. When configuring your Wifi Network via WPS, Messages are exchanged between the STA and AP in order to configure the Security Settings on both devices.

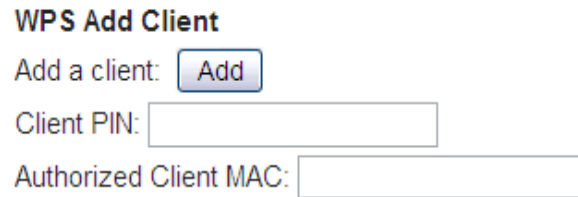
- **WPS Config:** It will help you to **Enable** or **Disable** the WPS feature. To enable you need to select **WPS**, to disable you need to select **Disabled**.

Note: After you **Enabled** the WPS you will get the options as show in Fig.35 and the WPS Config State box will show its configuration status.

- **Device Name:** By using this you can change the factory default to a name of your choice which is up to 32 characters long as like **SSID**.
- **WPS Setup AP:** Here you do not need to change anything, just skip this step.
- **WPS Add Client:** There are two methods “Add a client” and “Client PIN”. Select the method you want.

Chapter 2: WEB Configuration

If you select “Add a client”, then the **WPS Add Client** option will appear as shown below.



The image shows a web form titled "WPS Add Client". It contains three input fields: "Add a client:" with a blue "Add" button, "Client PIN:" with a text box, and "Authorized Client MAC:" with a text box.

Fig. 40 WPS/Add a client

And then if you click “Add” button then **WPS Setup AP** page will appear as shown in Fig.38

WPS Setup AP

Your AP is now waiting for the STA to connect.

Abort

PUSH

WPS Configure Status: InProgress

Fig. 41 WPS Add AP/PUSH

And **WPS Configure Status** will be “In progress”, after establishing the connection the **WPS Configure Status** will be “Success!” as shown below. After successful connection the client will get IP address from AP and then internet will be accessible.

WPS Setup AP SUCCESSFUL

Configuration is complete. Click 'Continue' to return to the previous page.

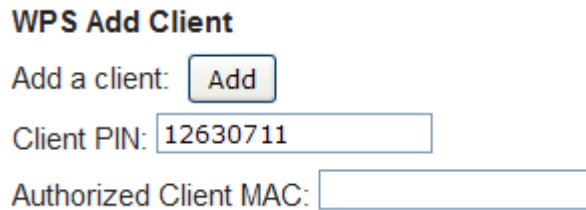
Continue

WPS Configure Status: Success!

Fig. 42 WPS Add AP successful/PUSH

Chapter 2: WEB Configuration

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 PIN to establish the connection. You can get the PIN from your connected Wi-Fi client.



WPS Add Client

Add a client:

Client PIN:

Authorized Client MAC:

Fig. 43 WPS/PIN

- **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 in Fig.41.

WPS Setup AP

Your AP is now waiting for the STA to connect.

Entered PIN: 54461147

WPS Configure Status: InProgress

Fig. 44 WPS Add AP/PIN

And **WPS Configure Status** will be “In progress”, after establishing the connection the **WPS Configure Status** will be “Success!” as shown below. After successful connection the client will get IP address from AP and then internet will be accessible.

WPS Setup AP SUCCESSFUL

AP Configuration is complete. Click 'Continue' to return to the previous page.

Entered PIN:

WPS Configure Status: Success!

Fig. 45 WPS Add AP successful/PIN

Chapter 2: WEB Configuration

3. Access Control

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

The screenshot displays the Thomson Administration Web Page. The top navigation bar includes links for Status, Network, Advanced, Firewall, Parental Control, and Wireless. The 'Wireless' section is active, showing the 'Access Control' configuration page. The page title is '802.11 Access Control'. The description states: 'This page allows the configuration of the Access Control to the AP as well as status on the connected clients.' The configuration options include: 'Administration Web Page Access' set to 'Allow' (with a note: '(Allow or Deny Access to Administration Web Page from PC connected over Wifi.)'), 'MAC Restrict Mode' set to 'Disabled', and a table for 'MAC Addresses' with 8 empty rows. An 'Apply' button is located below the table. At the bottom, the 'Connected Clients' section shows a table with headers: MAC Address, Age(s), RSSI(dBm), Type, IP Addr, and Host Name. The table is currently empty, with the text 'No wireless clients are connected.' displayed below it.

Fig. 46 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

4. 802.11/ 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.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

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

Wireless

802.11 Advanced : This page allows configuration of data rates and WiFi thresholds.

54g™ Mode 54g Auto

XPress™ Technology Disabled

802.11n Protection Auto

Short Guard Interval Auto

Basic Rate Set Default

Multicast Rate Auto

NPHY Rate Auto

Rate Auto

Beacon Interval 100

DTIM Interval 1

Fragmentation Threshold 2346

RTS Threshold 2347

Apply

© - Thomson - 2007

Fig. 47 Wireless\Advanced

- **54g™ Mode:**

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

- **Basic Rate Set:**

Select **default** or **All** basic rate.

- **54g™ Protection:**

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

- **Xpress™ Technology:**

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

- **Afterburner™ Technology:**

Chapter 2: WEB Configuration

- Afterburner technology is an enhancement for the 54g™ platform, It maximum performance implementation of the IEEE 802.11g standard. Products with this new technology provide up to 40 percent greater throughput than typical standard 802.11g systems without impacting the performance of neighboring wireless LANs.
- **Rate:**
This determines the speed of the 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.
- **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)
- **NPHY Rate:**
This determines the speed of the 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.
- **802.11n Protection:**
Select **Auto** to turn on the 802.11n protection; select **Off** to turn down the protection.
- **Multicast Rate:**
The Multicast Rate option sets the threshold throughput level a wireless client must obtain in order to be "accepted" by the base station. The lower this value, theoretically, the greater number of clients that can connect, especially those at greater distances from the base station. At the opposite end, the higher this number, only those wireless clients that can achieve the higher throughput value will be able to connect.

Chapter 2: WEB Configuration

5. Bridging

The Bridging page provides a location where settings can be adjusted related to the 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.

The screenshot shows the Thomson Administration web interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Status - Network - Advanced - Firewall - Parental Control - Wireless. The "Wireless" tab is selected. On the left is a sidebar with the Thomson logo and a list of menu items: Radio, Primary Network, Access Control, Advanced, Bridging (highlighted), and WMM. The main content area is titled "Wireless" and contains a section "Bridging" with the text "This page allows configuration of WDS features." Below this, there is a "Wireless Bridging" dropdown menu set to "Disabled", followed by four empty text boxes for "Remote Bridges". An "Apply" button is at the bottom of the form. A copyright notice "© - Thomson - 2007" is at the bottom left of the sidebar.

Fig. 48 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 to each other.
- **Apply:**
After proper configuration, click Apply to invoke the settings.

Chapter 2: WEB Configuration

6. 802.11 QoS (WMM) Settings

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). The QoS assigns priority to the selected network traffic and prevents packet collisions and delays thus improving VoIP calls and watching video over WLANs.

- **WMM Support:**

This field allows you to enable WMM to improve multimedia transmission.

- **No-Acknowledgement:**

This field allows you to enable WMM No-Acknowledgement.

- **Power Save Support:**

This field allows you to enable WMM Power-Save-Support.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes links for Status, Network, Advanced, Firewall, Parental Control, and Wireless. The 'Wireless' section is active, displaying the '802.11 Wi-Fi Multimedia' configuration page. On the left, a sidebar menu lists 'Radio', 'Primary Network', 'Access Control', 'Advanced', 'Bridging', and 'WMM'. The main content area contains three toggle switches: 'WMM Support' (On), 'No-Acknowledgement' (Off), and 'Power Save Support' (On), followed by an 'Apply' button. Below these are two tables of EDCA parameters. The first table, 'EDCA AP Parameters', has columns for CWmin, CWmax, AIFSN, TXOP(b) Limit (usec), TXOP(a/g) Limit (usec), and Discard Oldest First. The second table, 'EDCA STA Parameters', has the same columns. Both tables have four rows for AC_BE, AC_BK, AC_VI, and AC_VO. The third table, 'WMM TXOP Short Retry Parameters', has columns for Short Retry Limit, Short Fallbk Limit, Long Retry Limit, Long Fallbk Limit, and Max Rate in 500kbps, with four rows for AC_BE, AC_BK, AC_VI, and AC_VO. An 'Apply' button is at the bottom of the parameters section.

EDCA AP Parameters:	CWmin	CWmax	AIFSN	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	AIFSN	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

WMM TXOP Short Retry Parameters:	Short Retry Limit	Short Fallbk Limit	Long Retry Limit	Long Fallbk Limit	Max Rate in 500kbps
AC_BE	7	3	4	2	0
AC_BK	7	3	4	2	0
AC_VI	7	3	4	2	0
AC_VO	7	3	4	2	0

Fig. 49 Wireless\WMM

Chapter 2: WEB Configuration

EDCA AP Parameters:

The parameters for Access Point (AP) of EDCA (enhanced distributed channel access).

EDCA STA Parameters:

The parameters for WIFI station of EDCA.

CWmin: This attribute shall specify the value of the minimum size of the window that shall be used by a QAP for a particular AC for generating a random number for the backoff.

CWmax: This attribute shall specify the value of the maximum size of the window that shall be used by a QAP for a particular AC for generating a random number for the backoff.

AIFSN: This attribute shall specify the number of slots, after a SIFS duration, that the QAP, for a particular AC, shall sense the medium idle either before transmitting or executing a backoff.

TXOP (b) Limit (usec)/ TXOP (a/g) Limit (usec):

This attribute shall specify the maximum number of microseconds of an EDCA TXOP for a given AC at the QAP.

If buffer full and parameter is TRUE then discard oldest first.

4 AC's (Access Category) are defined:

AC_BK (background)

AC_BE (best-effort)

AC_VI (Video)

AC_VO (Voice)

Chapter 3: Networking

Communications

Data communication involves the flow of packets of data from one device to another. These devices include personal computers, Ethernet, cable modems, digital routers and switches, and highly integrated devices that combine functions, like the Wireless Cable Gateway.

The gateway integrates the functionality often found in two separate devices into one. It's both a cable modem and an intelligent wireless gateway networking device that can provide a host of networking features, such as NAT and firewall. Figure 2 illustrates this concept, with the cable modem (CM) functionality on the left, and networking functionality on the right. In this figure, the numbered arrows represent communication based on source and destination, as follows:

Type of Communication

1. Communication between the Internet and your PCs

Example: The packets created by your request for a page stored at a web site, and the contents of that page sent to your PC.

2. Communication between your cable company and the cable modem side

Example: When your cable modem starts up, it must initialize with the cable company, which requires the cable company to communicate directly with the cable modem itself.

3. Communication between your PCs and the networking side

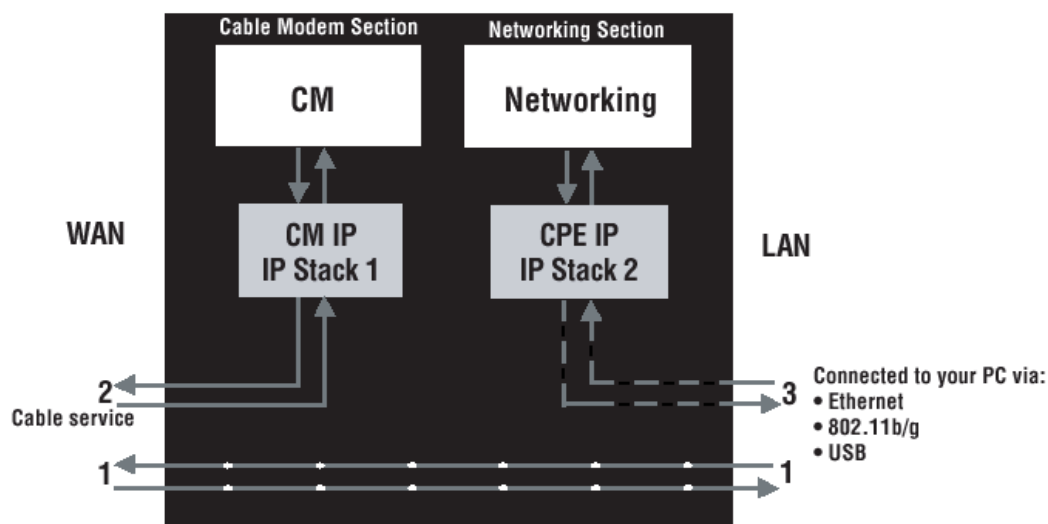


Fig.50 Communication between your PCs and the network side

Chapter 3: Networking

Example: The Wireless Cable Gateway offers a number of built-in web pages which you can use to configure its networking side; when you communicate with the networking side, your communication is following this path.

Each packet on the Internet addressed to a PC in your home travels from the Internet downstream on the cable company's system to the WAN side of your Wireless Cable Gateway. There it enters the Cable Modem section, which inspects the packet, and, based on the rules, proceeds to either forward or block the packet from proceeding on to the Networking section. Similarly, the Networking section then decides whether to forward or block the packet from proceeding on to your PC. Communication from your home device to an Internet device works similarly, but in reverse, with the packet traveling upstream on the cable system.

Cable Modem (CM) Section

The cable modem (or CM) section of your gateway uses EURO-DOCSIS Standard cable modem technology. EURO-DOCSIS specifies that TCP/IP over Ethernet style data communication be used between the WAN interface of your cable modem and your cable company.

A EURO-DOCSIS modem, when connected to a Cable System equipped to support such modems, performs a fully automated initialization process that requires no user intervention. Part of this initialization configures the cable modem with a CM IP (Cable Modem Internet Protocol) address, as shown in Figure 3, so the cable company can communicate directly with the CM itself.

Networking Section

The Networking section of your gateway also uses TCP/IP (Transmission Control Protocol/ Internet Protocol) for the PCs you connected on the LAN side. TCP/IP is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TCP/IP requires that each communicating device be configured with one or more TCP/IP stacks, as illustrated by Figure 4. On a PC, you often use software that came with the PC or its network interface (if you purchased a network interface card separately) to perform this configuration. To communicate with the Internet, the stack must also be assigned an IP (Internet Protocol) address. 192.168.100.1 is an example of an IP address. A TCP/IP stack can be configured to get this IP address by various means, including a DHCP server, by you directly entering it, or sometimes by a PC generating one of its own.

Ethernet requires that each TCP/IP stack on the Wireless Cable Gateway also have associated with it an Ethernet MAC (Media Access Control) address. MAC addresses are permanently fixed into network devices at the time of their manufacture. 00:90:64:12:B1:91 is an example of a MAC address.

Data packets enter and exit a device through one of its network interfaces. The gateway offers Ethernet and 802.11b/g wireless network interfaces on the LAN side and the EURO-DOCSIS network interface on the WAN side.

Chapter 3: Networking

When a packet enters a network interface, it is offered to all the TCP/IP stacks associated with the device side from which it entered. But only one stack can accept it — a stack whose configured Ethernet address matches the Ethernet destination address inside the packet. Furthermore, at a packet's final destination, its destination IP address must also match the IP address of the stack.

Each packet that enters a device contains source MAC and IP addresses telling where it came from, and destination MAC and IP addresses telling where it is going to. In addition, the packet contains all or part of a message destined for some application that is running on the destination device. IRC used in an Internet instant messaging program, HTTP used by a web browser, and FTP used by a file transfer program are all examples of applications. Inside the packet, these applications are designated by their port number. Port 80, the standard HTTP port, is an example of a port number.

The Networking section of the router performs many elegant functions by recognizing different packet types based upon their contents, such as source and destination MAC address, IP address, and ports.

Three Networking Modes

Your gateway can be configured to provide connectivity between your cable company and your home LAN in any one of three Networking Modes: CM, RG, and CH. This mode setting is under the control of your cable company, who can select the mode to match the level of home networking support for which you have subscribed. By default, all units are set for the RG mode, however; your cable company may change these defaults during device initialization.

Cable Modem (CM) Mode

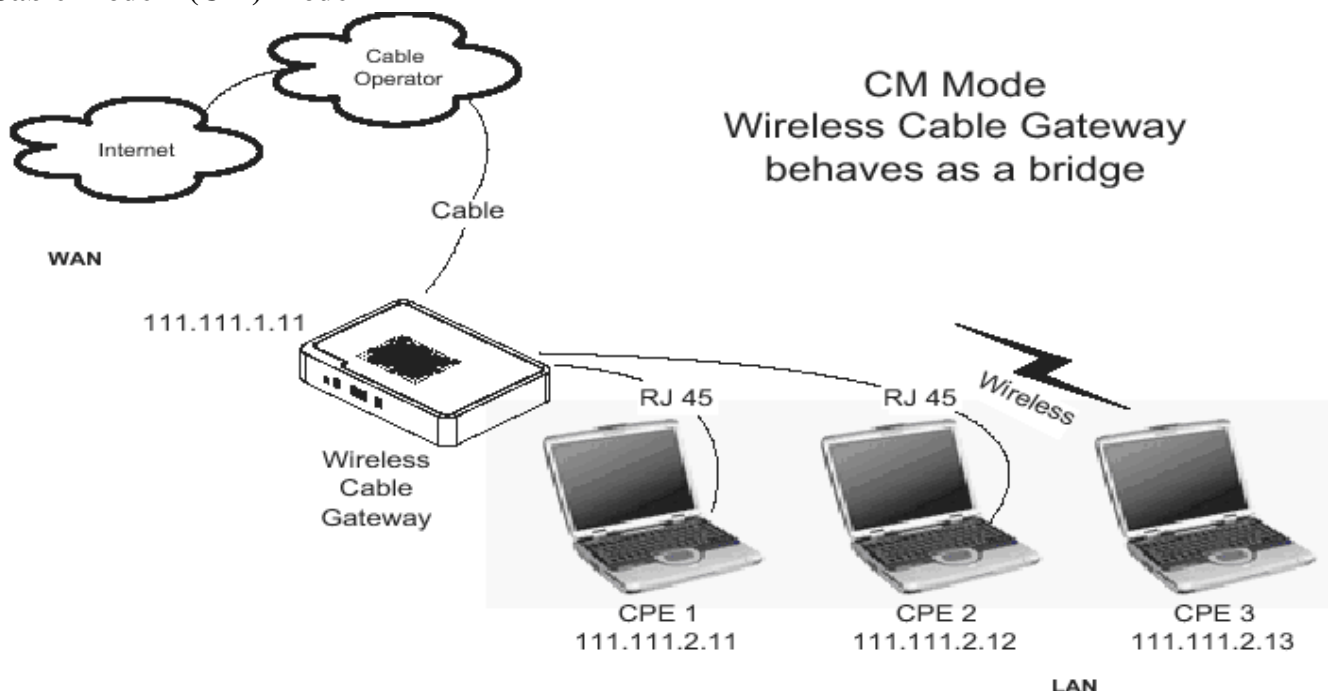


Fig.51 Cable Modem Mode

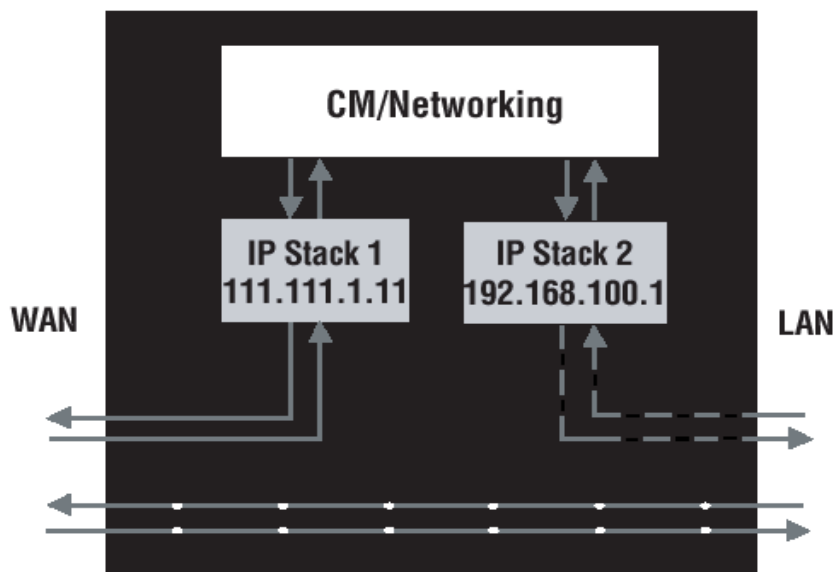


Fig. 52 Two IP stacks are activated in cable modem mode

CM (Cable Modem) Mode provides basic home networking. In this mode, two IP stacks are active:

- IP Stack 1 - for use by the cable company to communicate with the cable modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable gateway.
- IP Stack 2 - for use by you, the end user, to communicate with the cable modem and Networking sections, to access the internal web page diagnostics and configuration. This stack uses a fixed IP address: 192.168.100.1. It uses a MAC address of MAC label + 1 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:92.

With CM Mode, your cable company must provide one IP address for the CM section, plus one for each PC you connect from their pool of available addresses. Your cable company may have you or your installer manually enter these assigned addresses into your PC, or use a DHCP Server to communicate them to your PCs, or use a method that involves you entering host names into your PCs.

Note that in CM Mode, packets passing to the Internet to/from your PCs do not travel through any of the IP stacks; instead they are directly bridged between the WAN and LAN sides.

Chapter 3: Networking

Residential Gateway (RG) Mode

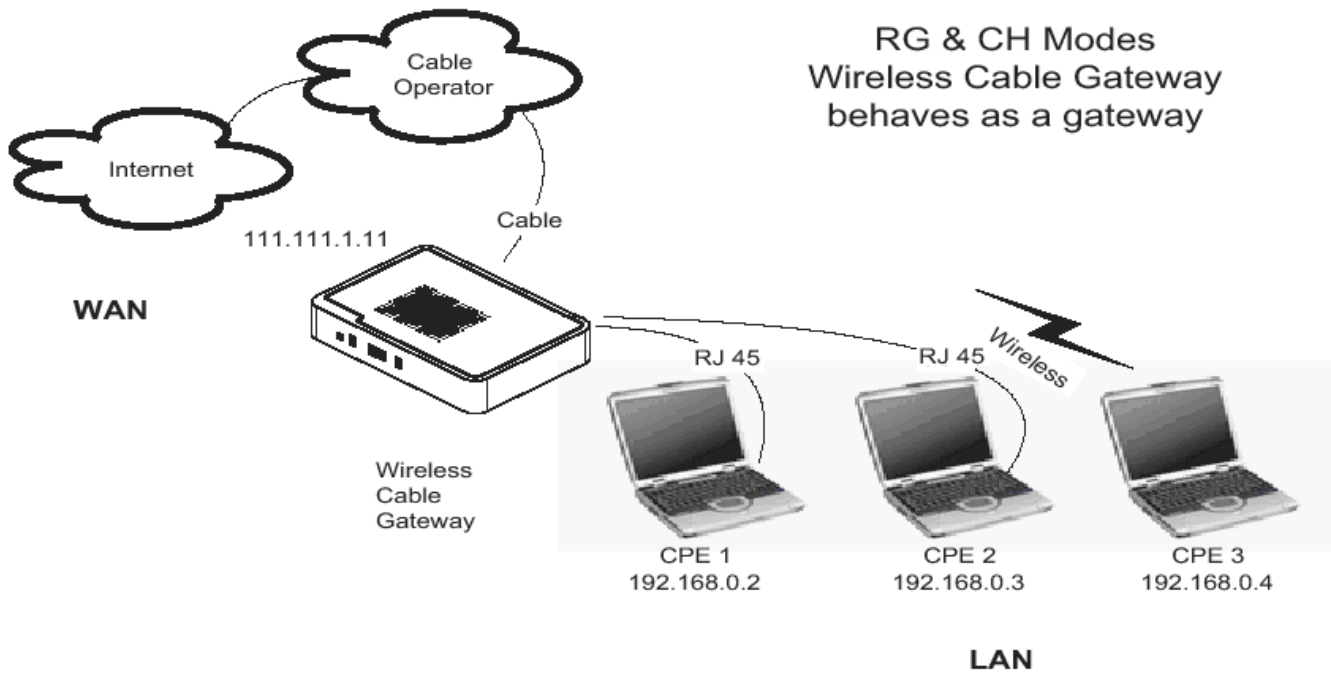


Fig. 53 Residential Gateway Mode

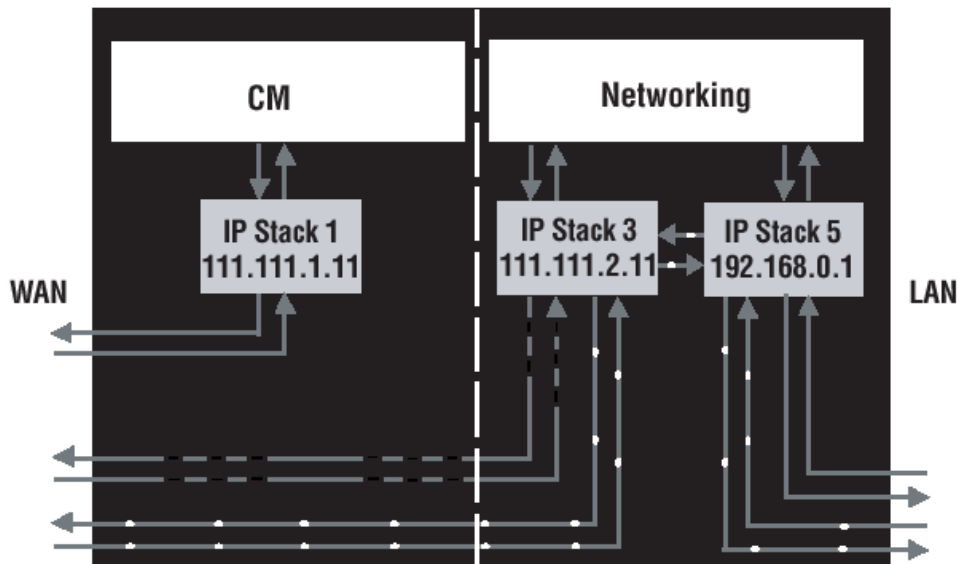


Fig. 54 Three IP stacks are activated in Residential mode

RG (Residential Gateway) Mode provides basic home networking plus NAT (Network Address Translation). In this mode, three IP stacks are active:

- IP Stack 1 - for use by the cable company to communicate with the Cable Modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable Gateway.

Chapter 3: Networking

- IP Stack 3 - for use by you to remotely (i.e. from somewhere on the WAN side, such as at your remote workplace) communicate with the Cable Modem and Networking sections, to remotely access the internal web page diagnostics and configuration. This stack is also used by your cable company to deliver packets between the Internet and the gateway's networking section so they can be routed to/from your PCs. This stack requires an IP address assigned by the cable company from their pool of available addresses. Your cable company may have you or your installer manually enter assigned addresses into your gateway, or use a DHCP Server to communicate them, or use a method that involves you entering host names. This stack uses a MAC address of MAC label + 2 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:93.
- IP Stack 5 - for use by you to locally (i.e. from somewhere on the LAN side in your home) communicate with the Cable Modem and Networking sections, to access the internal web page diagnostics and configuration. This stack is also used by the gateway's networking section to route packets between the gateway's Networking section and your PCs. This stack uses a fixed IP address: 192.168.0.1. It uses a MAC address of MAC label + 4 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:95.

With RG Mode, your cable company must provide one IP address for the CM section, plus one for the Networking section, from their pool of available addresses. With RG Mode, each PC you connect gets an IP address from a DHCP Server that is part of the Networking section of the gateway.

CableHome (CH) Mode

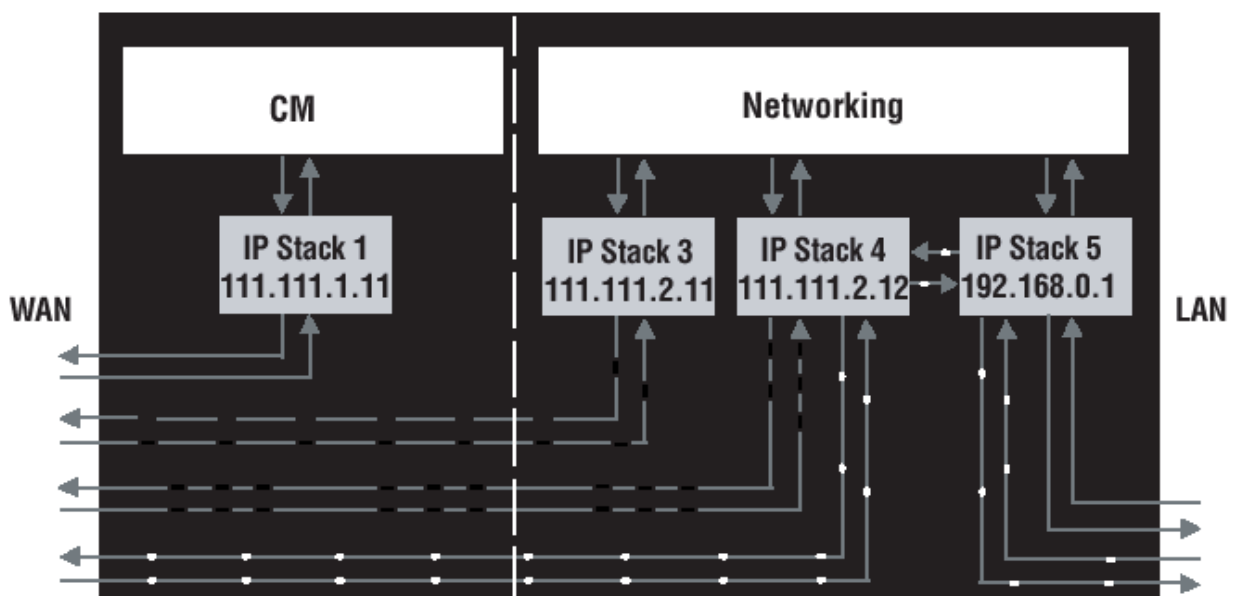


Fig. 55 Four IP stacks are activated in CableHome Mode

Chapter 3: Networking

CH (CableHome) Mode provides all the functionality of RG mode and adds the ability of the cable company to control the home networking configuration of your Wireless Cable Gateway for you, so you don't need to perform the configuration yourself. In this mode, four IP stacks are active:

- IP Stack 1 - for use by the cable company to communicate with the Cable Modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable Gateway.
- IP Stack 3 - for use by your cable company to communicate with the Networking section to help you configure and manage your home networking. This stack requires an IP address assigned by the cable company from their pool of available addresses. Your cable company may have you or your installer manually enter assigned addresses into your gateway, or use a DHCP Server to communicate them, or use a method that involves you entering host names. This stack uses a MAC address of MAC label + 2 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12: B1:93.
- IP Stack 4 - for use by you to remotely (i.e. from somewhere on the WAN side, such as at your remote workplace) communicate with the Cable Modem and Networking sections, to remotely access the internal web page diagnostics and configuration. This stack is also used by your cable company to deliver packets between the Internet and the Wireless Cable Gateway's Networking section so they can be routed to/from your PCs. This stack requires an IP address assigned by the cable company from their pool of available addresses. Your cable company may have you or your installer manually enter these assigned addresses into your gateway, or use a DHCP Server to communicate them, or use a method that involves you entering host names. This stack uses a MAC address of MAC label + 3 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90: 64:12:B1:94.
- IP Stack 5 - for use by you to locally (i.e. from somewhere on the LAN side in your home) communicate with the Cable Modem and Networking sections, to access the internal web page diagnostics and configuration. This stack is also used by the Wireless Cable Gateway Networking section to route packets between the Wireless Cable Gateway's Networking section and your PCs. This stack uses a fixed IP address: 192.168.0.1. It uses a MAC address of MAC label+ 4 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:95.

With CH Mode, your cable company must provide one IP address for the CM section, plus two for the Networking section, from their pool of available addresses. Each PC you connect gets an IP address from a DHCP Server that is part of the Networking section of the gateway.

Chapter 3: Networking

MAC and IP Addresses Summary

This table summarizes all the MAC and IP addresses that may be associated with the TCP/IP communication stacks in your Wireless Cable Gateway. The ones actually used depend upon your gateway Operating Mode, as explained above. At minimum, your cable company will need to know the MAC address associated with IP Stack 1, which is the MAC address shown on the modem label.

Stack Name	Purpose - Mode	MAC Address	IP Address
IP Stack 1	CM WAN access - all Modes	per label on CM	assigned by cable company
IP Stack 2	local management - CM Mode		during initialization
IP Stack 3	only	CM label + 1	fixed at 192.168.100.1
IP Stack 4			
IP Stack 5	CableHome remote management	CM label + 2	assigned by cable company
---	- CH Mode only	CM label + 3	assigned by cable company
	end-user remote management, LAN WAN access - RG Mode only		
	WAN data access - CH Mode only	CM label + 4	fixed at 192.168.0.1
	local management - RG, CH Modes only LAN gateway	CM label + 5	

MAC and IP Addresses

Chapter 4: Additional information

Chapter 4: 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. My modem is connected to the power sector but does not work

A. Check the ON/OFF button on the rear panel of your modem. Should be set to "1"

Q. Once my Wireless 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 Wireless Gateway at the same time?

A. Absolutely!

Q. What do you mean by "Broadband?"

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

Q. What is EURO-DOCSIS 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 Wireless Gateway will work with all upgraded cable systems that are EURO-DOCSIS-compliant.

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

A. It is one of the popular performance-enhancing WiFi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks. When Xpress is turned on, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by **up to 27%** in 802.11g-only networks,

Chapter 4: Additional information

and **up to** 75% in mixed networks comprised of 802.11g and 802.11b standard equipment. The technology achieves higher throughput by re-packaging data, reducing the number of overhead control packets, so that more useful data can be sent during a given amount of time.

* Monthly subscription fee applies.

** Additional equipment required. Contact your cable company and ISP for any restrictions or additional fees.

Chapter 4: 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 Wireless 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.

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

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

<http://www.Technicolor.com>

Chapter 4: Additional information

Service Information

If you purchased or leased your Wireless 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 Wireless Gateway from a retailer, see the enclosed warranty card.

Chapter 4: Additional information

Glossary

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

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

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

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

EURO-DOCSIS (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 Wireless Gateway, that connects the modem to the cable system.

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

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

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

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

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

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

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

Chapter 4: Additional information

subscriber's property and the service provider's property.

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.

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

USA

For more information

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

© 2007 Thomson Inc.- Trademark(s) ® Registered\ -Marca(s) Registrada(s)

Photos and features subject to change without notice.

Illustration of product finish may vary from actual color.

THOMSON