

# 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.

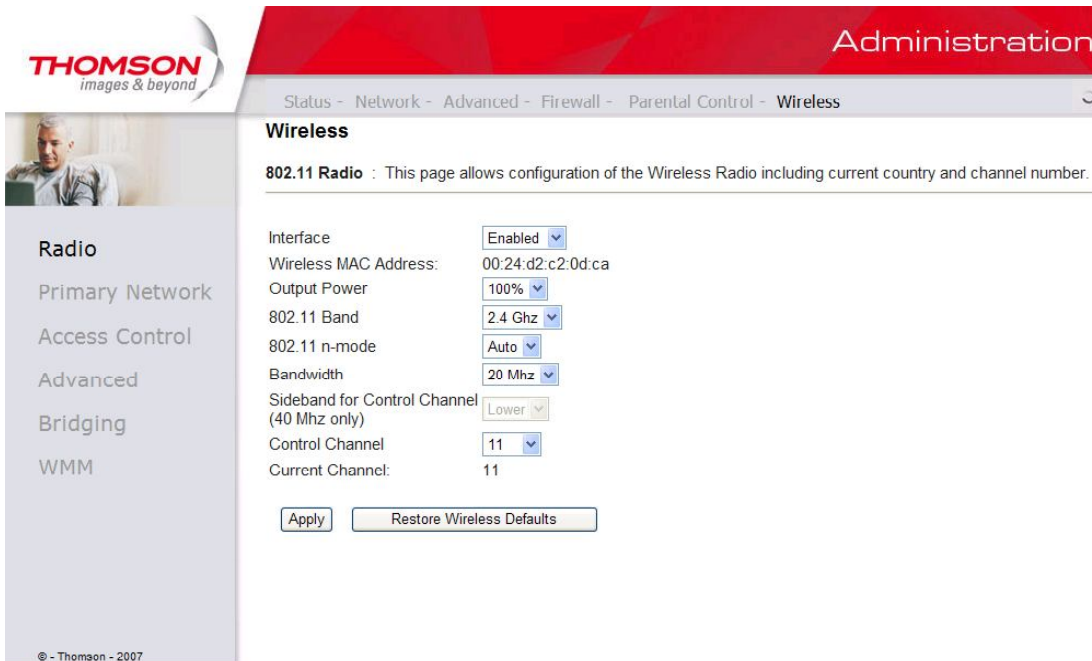


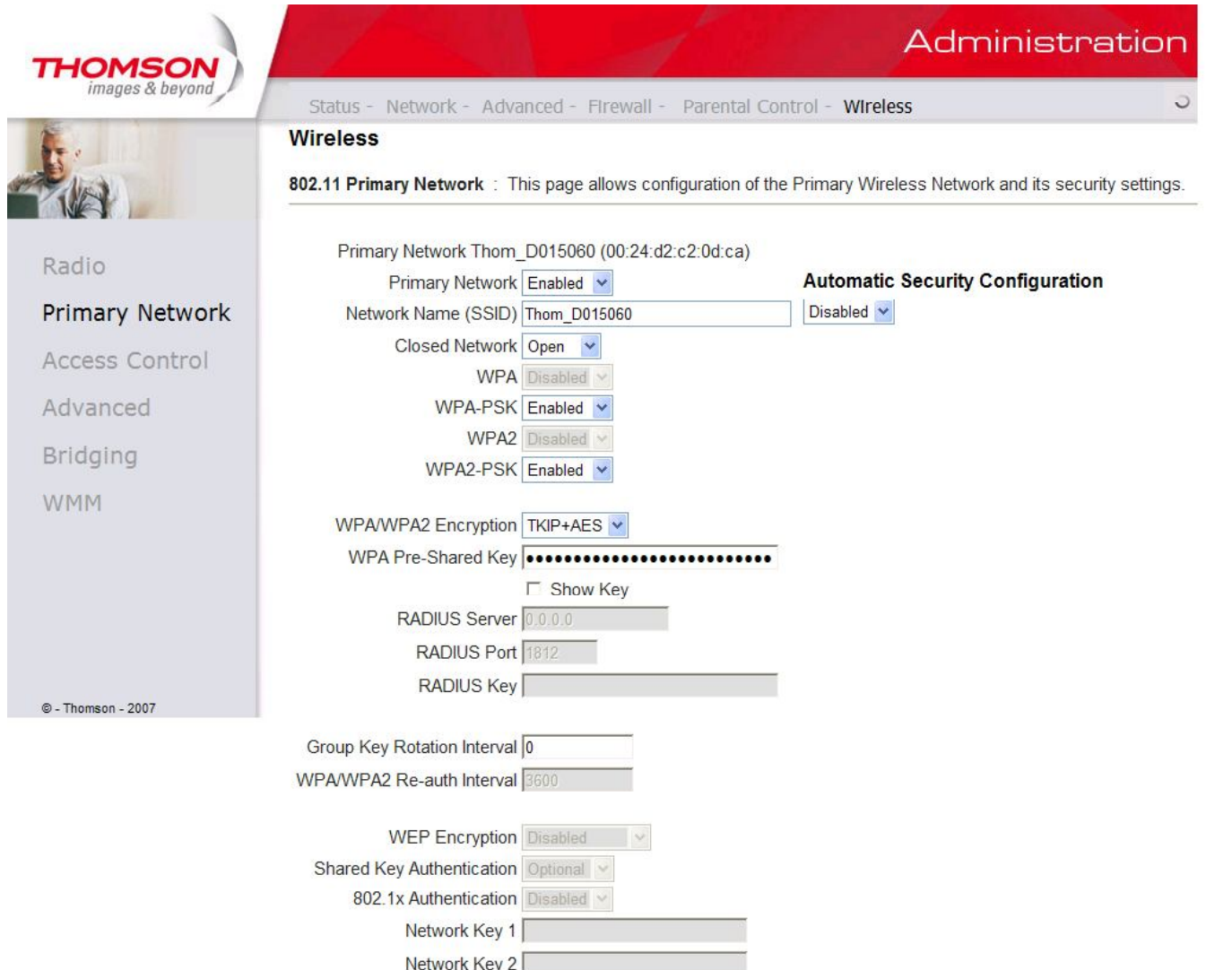
Fig. 30

- **Interface:** The wireless radio in your gateway can be completely de-activated by changing **Interface** to Disabled. Click the **Apply** button to save your settings. If you want to re-activate the disabled wireless radio in your gateway, need to contact cable operator.
- **Wireless MAC Address:** The MAC address for this wireless device will be displayed in this field automatically.
- **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 2.4G and 5G.
- **802.11n mode:** It will help you to **Enable** or **Disable** the 11N mode. To enable you need to select **Auto**, to disable you need to select **Off**
- **Bandwidth:** Select wireless channel width 20Mhz is for default value (bandwidth taken by wireless signals of this access point.)
- **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.

# 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.



The screenshot shows the Thomson Administration interface. The top navigation bar includes 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Wireless' section is active, showing the '802.11 Primary Network' configuration page. The page title is 'Wireless'. Below the title, a description states: '802.11 Primary Network : This page allows configuration of the Primary Wireless Network and its security settings.' The configuration area is divided into two main sections: 'Primary Network' and 'Automatic Security Configuration'. The 'Primary Network' section includes fields for 'Primary Network' (Enabled), 'Network Name (SSID)' (Thom\_D015060), 'Closed Network' (Open), 'WPA' (Disabled), 'WPA-PSK' (Enabled), 'WPA2' (Disabled), and 'WPA2-PSK' (Enabled). The 'Automatic Security Configuration' section includes 'WPA/WPA2 Encryption' (TKIP+AES), 'WPA Pre-Shared Key' (masked), 'Show Key' (checkbox), 'RADIUS Server' (0.0.0.0), 'RADIUS Port' (1812), 'RADIUS Key' (masked), 'Group Key Rotation Interval' (0), and 'WPA/WPA2 Re-auth Interval' (3600). The bottom section includes 'WEP Encryption' (Disabled), 'Shared Key Authentication' (Optional), '802.1x Authentication' (Disabled), 'Network Key 1' (masked), and 'Network Key 2' (masked). The Thomson logo is visible in the top left corner, and the copyright notice '© - Thomson - 2007' is at the bottom left.

Fig. 31

**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.

**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.

## Chapter 2: WEB Configuration

### **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.

WPA/WPA2 Encryption: TKIP+AES  
WPA Pre-Shared Key: [Redacted]  
RADIUS Server: 0.0.0.0  
RADIUS Port: 1812  
RADIUS Key: [Redacted]  
Group Key Rotation Interval: 0  
WPA/WPA2 Re-auth Interval: 3600  
WEP Encryption: Disabled  
Shared Key Authentication: Optional  
802.1x Authentication: Disabled  
Network Key 1: [Redacted]  
Network Key 2: [Redacted]  
Network Key 3: [Redacted]  
Network Key 4: [Redacted]  
Current Network Key: 1  
PassPhrase: [Redacted]  
Generate WEP Keys  
Apply

Fig. 32

### 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.

## Chapter 2: WEB Configuration

- **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 dropdown menus for WPA (Disabled), WPA-PSK (Enabled), WPA2 (Disabled), and WPA2-PSK (Enabled). Below these are fields for WPA/WPA2 Encryption (TKIP+AES), WPA Pre-Shared Key (a masked field), RADIUS Server (0.0.0.0), RADIUS Port (1812), and RADIUS Key (a masked field). At the bottom, there are input fields for Group Key Rotation Interval (0) and WPA/WPA2 Re-auth Interval (3600).

Fig. 33

### 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.

This screenshot is identical to Fig. 33, showing the WPA/WPA2 configuration interface with settings for WPA, WPA-PSK, WPA2, WPA2-PSK, encryption, pre-shared key, RADIUS server/port/key, and key rotation/re-auth intervals.

Fig. 34



## Chapter 2: WEB Configuration

### Automatic Security Configuration



WPS ▼

WPS Config State: Unconfigured

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

Device Name

**WPS Setup AP**

PIN:

**WPS Add Client**

Add a client: ☐ Push-Button ☒ PIN

PIN:

Fig. 35

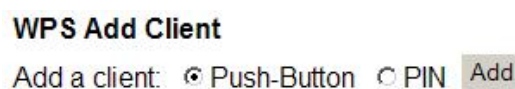
WiFi Protected Setup (WPS) is an easy and secure way of configuring and connecting your WiFi access point. In your case, the TCW770 is the Access Point (AP), and Your PC (or Wifi Device) is called the STA. When configuring your Wifi Network via WPS, Messages are exchanged between the STA and AP in order 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 “Push-Button” and “PIN”. Select the method you want. But, the default selection will be “PIN”.

If you select “Push-Button”, then the **WPS Add Client** option will appear as shown below.



**WPS Add Client**

Add a client: ☒ Push-Button ☐ PIN

Fig. 36

And then if you click “Add” button then **WPS Setup AP** page will appear as shown in Fig.37

## Chapter 2: WEB Configuration

### WPS Setup AP

Your AP is now waiting for the STA to connect.

PUSH

WPS Configure Status: InProgress

Fig. 37

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.

Continue

WPS Configure Status: Success!

Fig. 38

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: ☐ Push-Button ☒ PIN

PIN:

Fig. 39

- **PIN:** Use this option to set the PIN, enter 4-8 digits PIN of the device you wish to configure. After entering the pin click “Add” button, then the WPS Setup AP page will appear as shown in Fig.38

## Chapter 2: WEB Configuration

### WPS Setup AP

Your AP is now waiting for the STA to connect.

Abort

Entered PIN: 54461147

WPS Configure Status: InProgress

Fig. 40

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.

Continue

Entered PIN:

WPS Configure Status: Success!

Fig. 41



## 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 shows the Thomson Administration Web Page. The left sidebar contains a menu with options: Radio, Primary Network, Access Control (selected), Advanced, Bridging, and WMM. The main content area is titled 'Administration' and shows a breadcrumb trail: Status - Network - Advanced - Firewall - Parental Control - Wireless. The 'Wireless' section is active, displaying the '802.11 Access Control' configuration. It includes a description: 'This page allows the configuration of the Access Control to the AP as well as status on the connected clients.' Below this, there are two main settings: 'Administration Web Page Access' set to 'Allow' (with a note: '(Allow or Deny Access to Administration Web Page from PC connected over Wifi.)') and 'MAC Restrict Mode' set to 'Disabled'. A table for 'MAC Addresses' is provided with 8 rows and 2 columns. 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. 42

**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.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Wireless' section is active, displaying the '802.11 Advanced' settings. The left sidebar contains a menu with 'Radio', 'Primary Network', 'Access Control', 'Advanced' (selected), 'Bridging', and 'WMM'. The main content area lists various wireless settings with their current values: 54g™ Mode (54g Auto), Basic Rate Set (Default), 54g™ Protection (Auto), XPress™ Technology (Disabled), Afterburner™ Technology (Disabled), Rate (Auto), Beacon Interval (100), DTIM Interval (1), Fragmentation Threshold (2346), RTS Threshold (2347), NPHY Rate (Auto), 802.11n Protection (Auto), and Multicast Rate (Auto). An 'Apply' button is at the bottom of the settings list. The Thomson logo and '© - Thomson - 2007' are visible in the bottom left corner.

Fig. 43

#### 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.

## Chapter 2: WEB Configuration

### **Afterburner™ Technology:**

Afterburner technology is an enhancement for the 54g™ platform. Its 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.

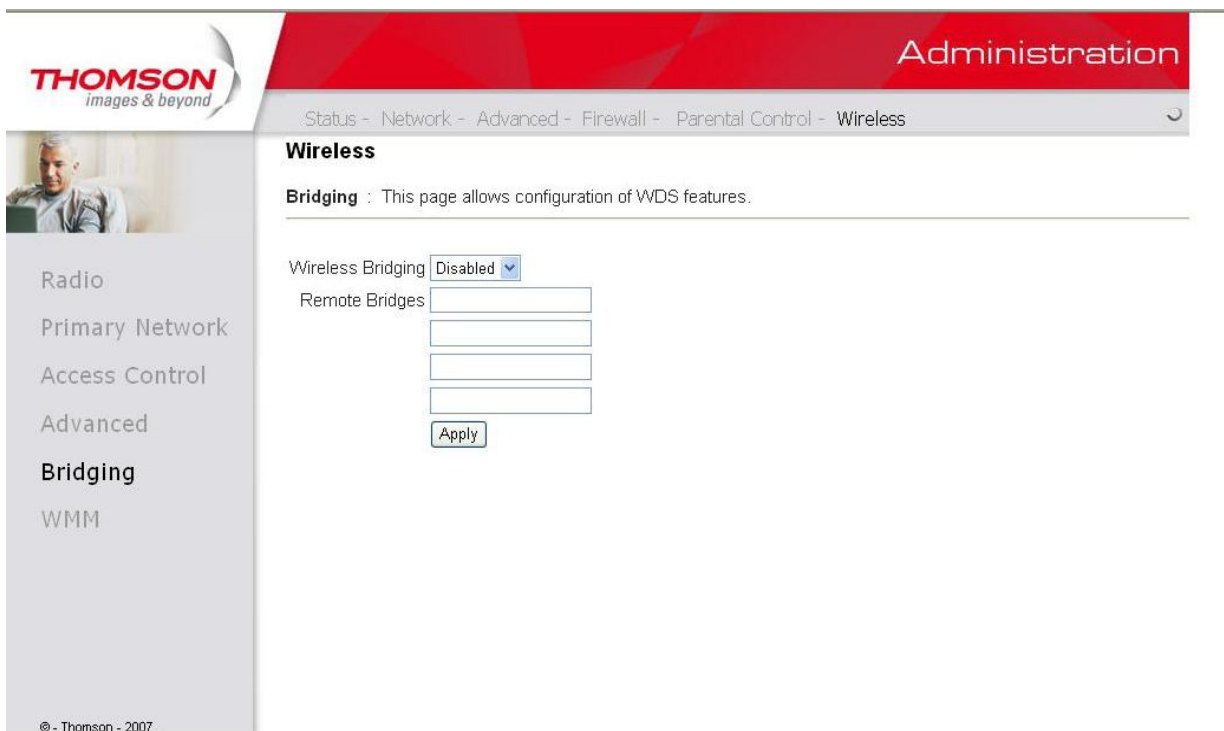


Fig. 44

- **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.

**Administration**

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

**Wireless**

**802.11 Wi-Fi Multimedia** : This page allows configuration of the Wi-Fi Multimedia QoS.

WMM Support    
No-Acknowledgement    
Power Save Support

EDCA AP Parameters:

	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Limit (usec) Oldest First
AC_BE	15	63	3	0	0	<input type="button" value="Off"/> <input type="button" value="v"/>
AC_BK	15	1023	7	0	0	<input type="button" value="Off"/> <input type="button" value="v"/>
AC_VI	7	15	1	6016	3008	<input type="button" value="Off"/> <input type="button" value="v"/>
AC_VO	3	7	1	3264	1504	<input type="button" value="Off"/> <input type="button" value="v"/>

EDCA STA Parameters:

AC_BE	15	1023	3	0	0
AC_BK	15	1023	7	0	0
AC_VI	7	15	2	6016	3008
AC_VO	3	7	2	3264	1504

Fig. 45

#### 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

## Chapter 2: WEB Configuration

for a particular AC for generating a random number for the backoff.

### **CW<sub>max</sub>:**

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

## 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

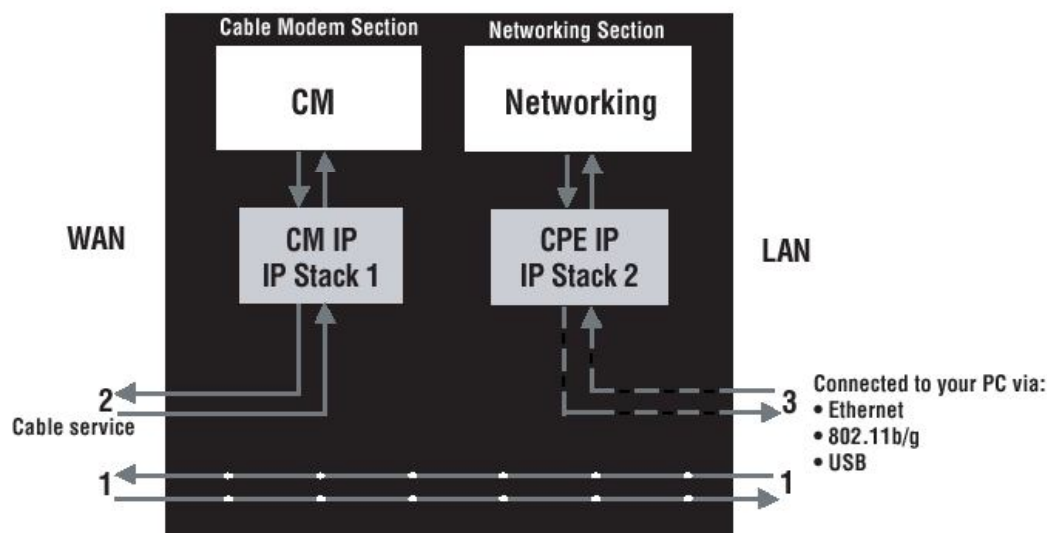


Fig.46

## 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 down-stream 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

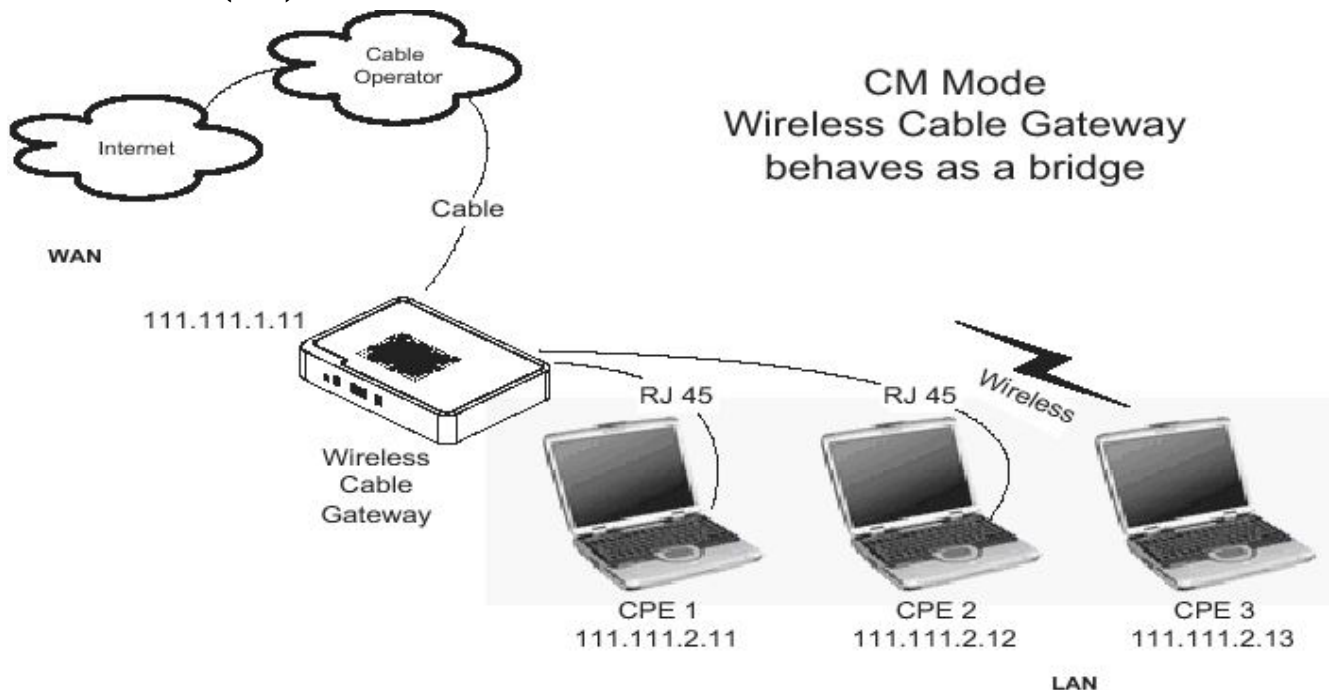


Fig.47

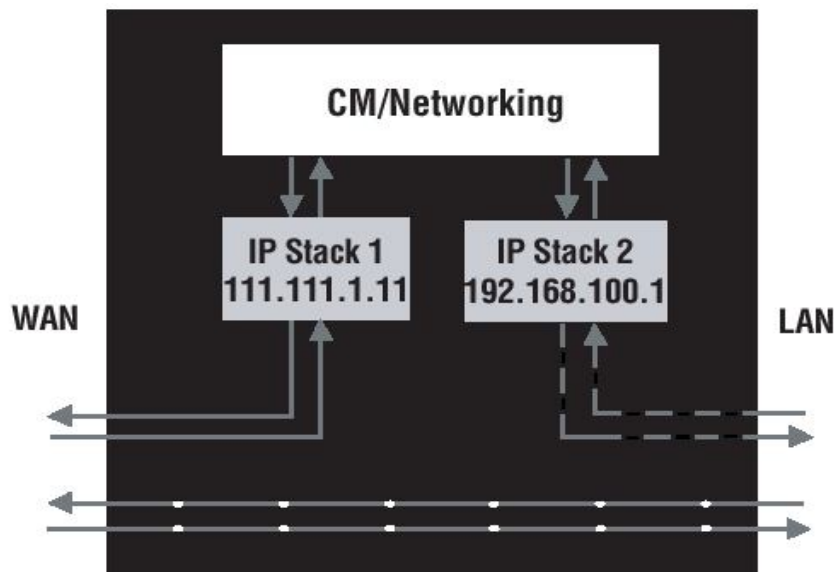


Fig. 48

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

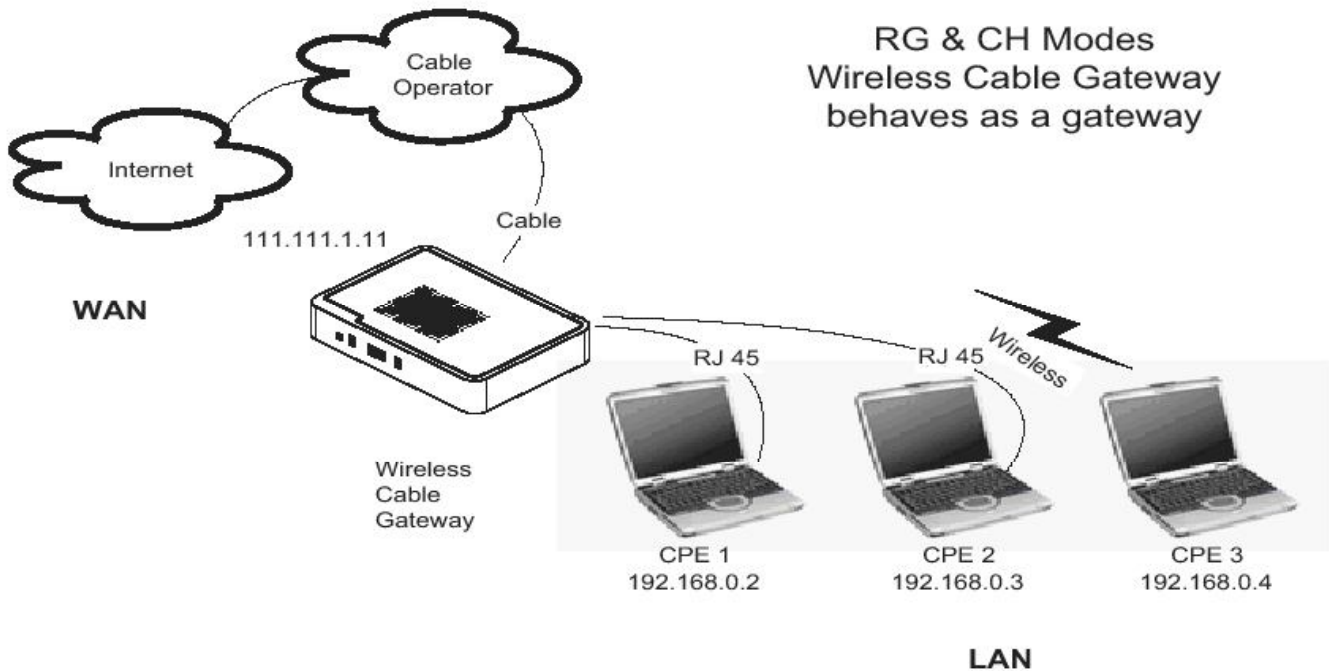


Fig. 49

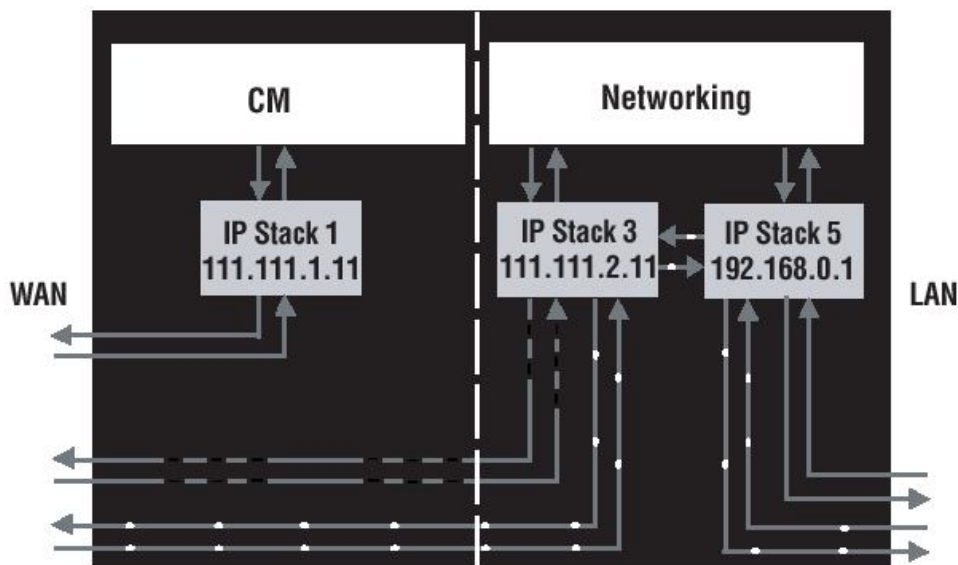


Fig. 50

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. 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

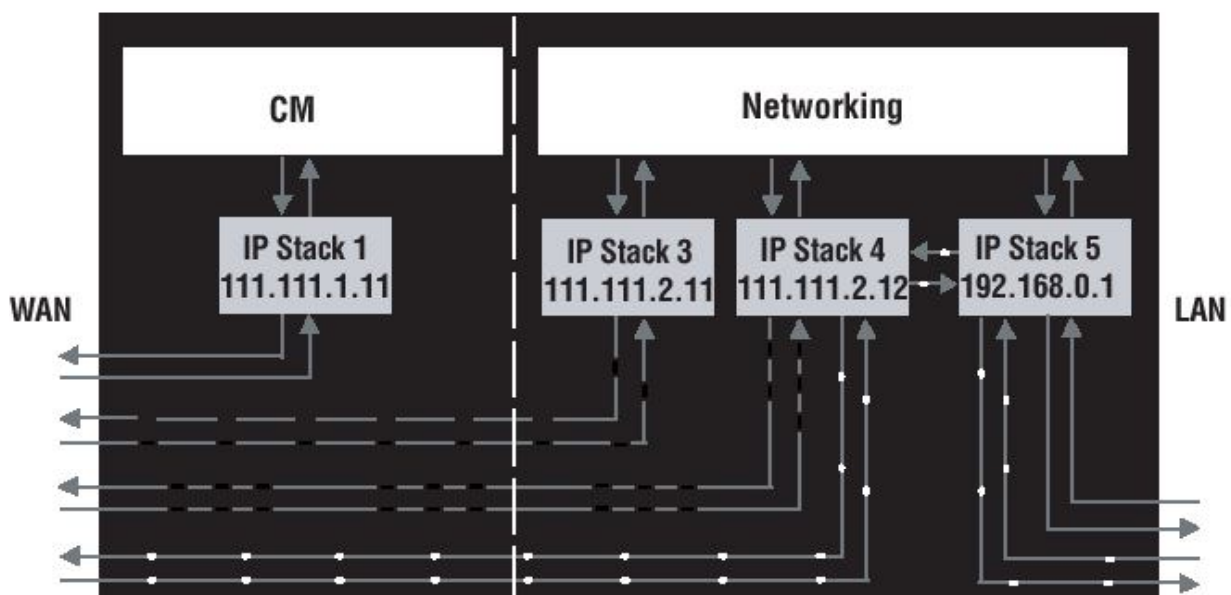


Fig. 51



## 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	CM label + 5	
	LAN gateway		

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

## Chapter 4: Additional information

throughput speeds of each client on the network) can improve by **up to** 27% in 802.11g-only networks, and **up to** 75% in mixed networks comprised of 802.11g and 802.11b standard equipment. The technology achieves higher throughput by re-packaging data, reducing the number of overhead control packets, so that more useful data can be sent during a given amount of time.

\* Monthly subscription fee applies.

\*\* 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 connections to your Wireless 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 by calling your cable provider.

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

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

## Chapter 4: Additional information

### FCC Declaration of Conformity and Industry Canada Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Trade Name:	Model: TCW770
Equipment Classification:	Computing Device Accessory
Responsible Party:	Thomson Inc. 101 W 103rd Street Indianapolis, IN 46290 Telephone 317-415-4151

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect this equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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



# Chapter 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 subscriber’s property and the service provider’s property.

## Chapter 4: Additional Information

**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

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](http://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**