

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.

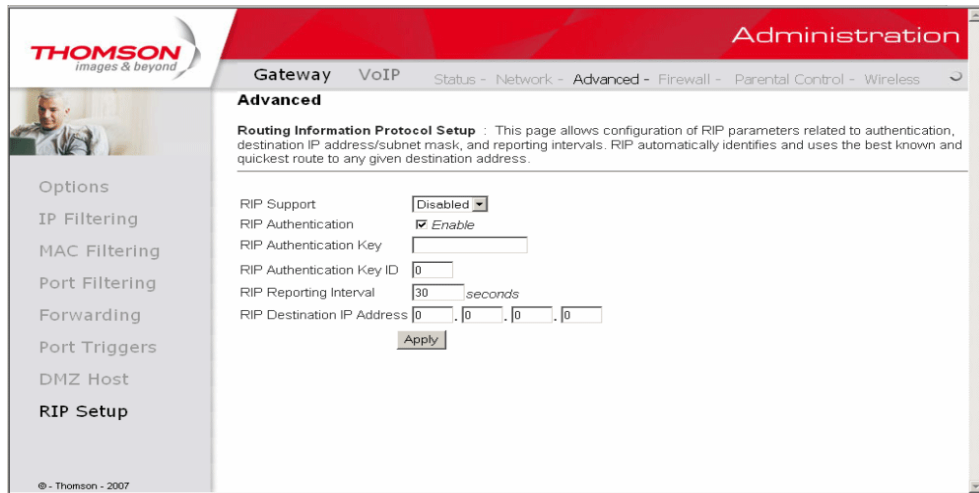


Fig. 26 Gateway\Advanced\RIP Setup

Chapter 2: WEB Configuration

Gateway – Firewall Web Page Group

1. Web Content Filtering

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

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

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

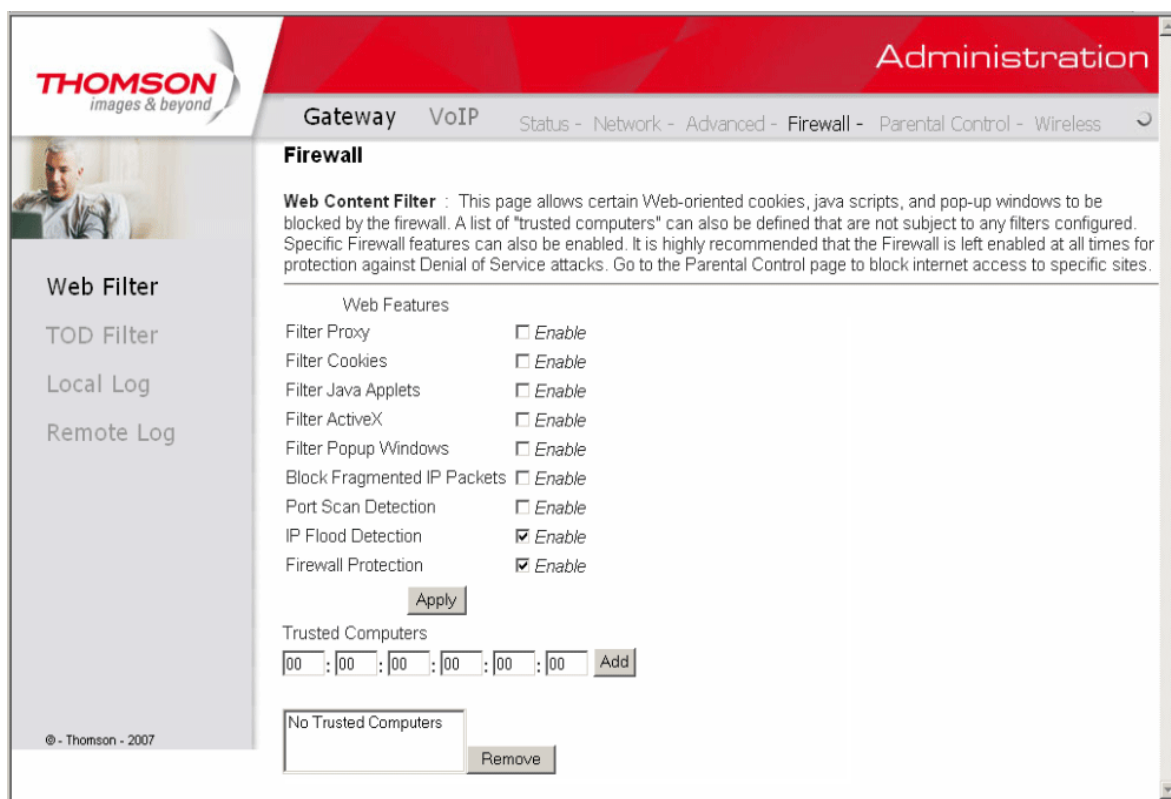


Fig. 27 Gateway\Firewall\Web Filter

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.

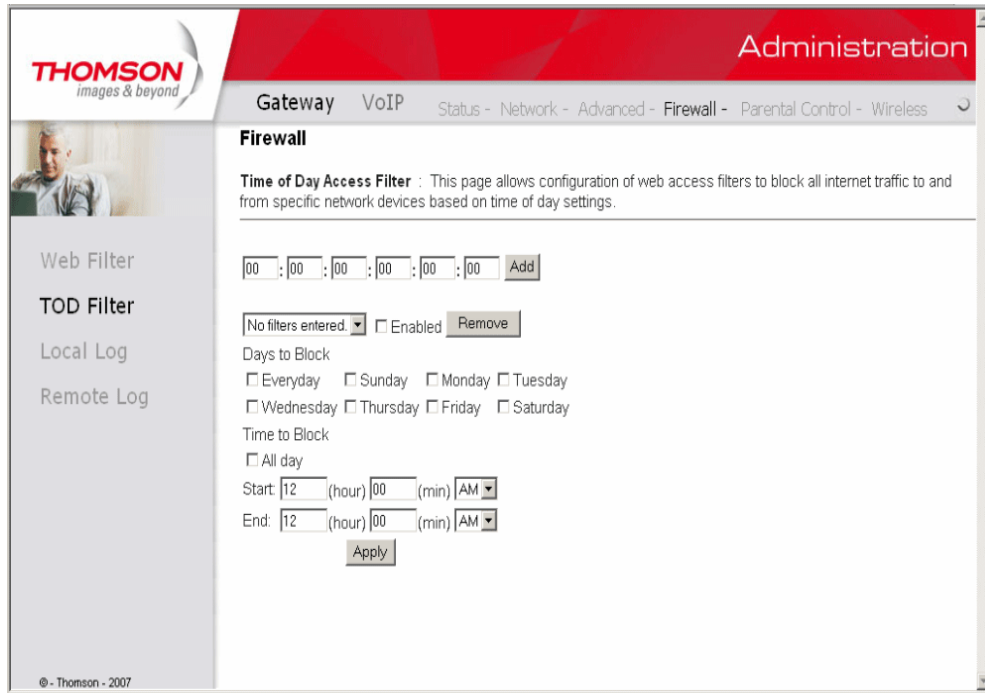


Fig. 28 Gateway\Firewall\TOD Filtering

Chapter 2: WEB Configuration

3. Local Log and Remote Log

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

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

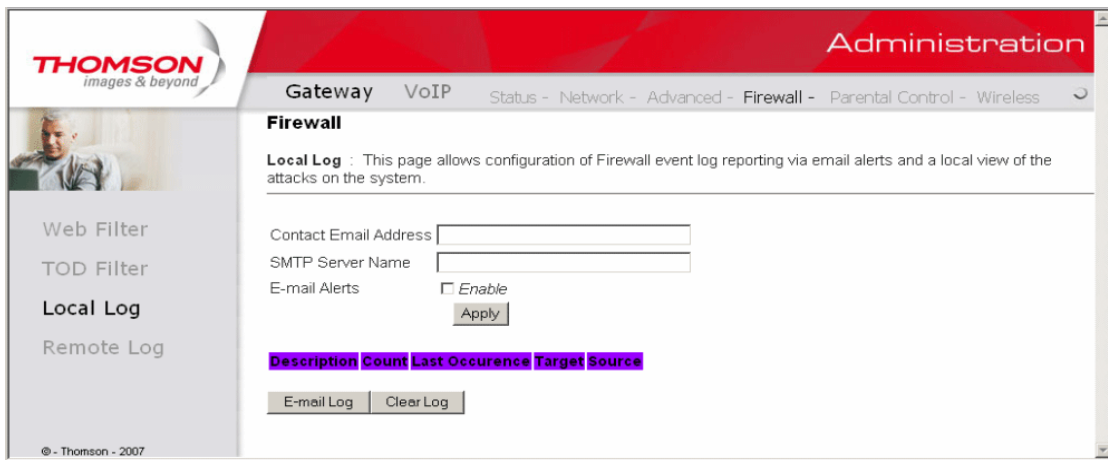


Fig. 29 Gateway\Firewall\Local Log

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

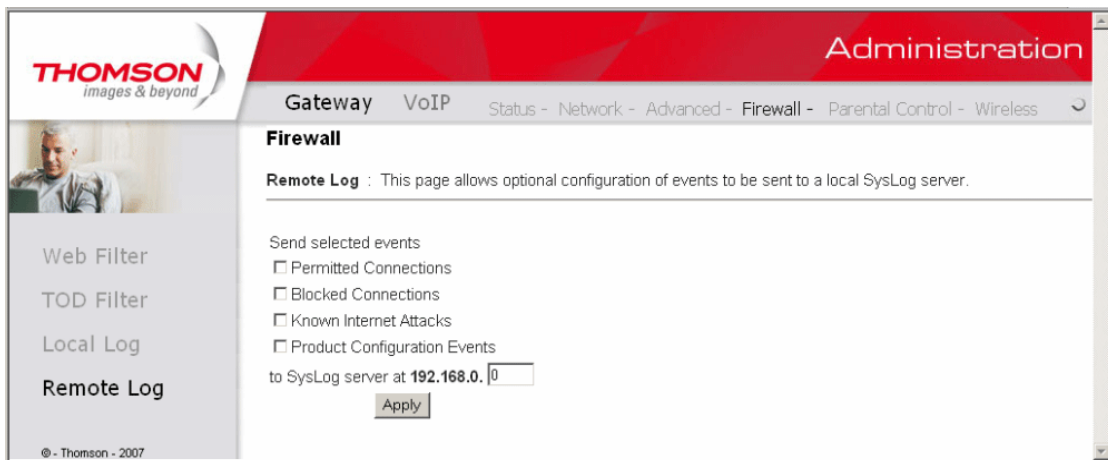


Fig. 30 Gateway\Firewall\Remote Log

Chapter 2: WEB Configuration

Gateway – Parental Control Web Page Group

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. disney.com) in the Domain List.

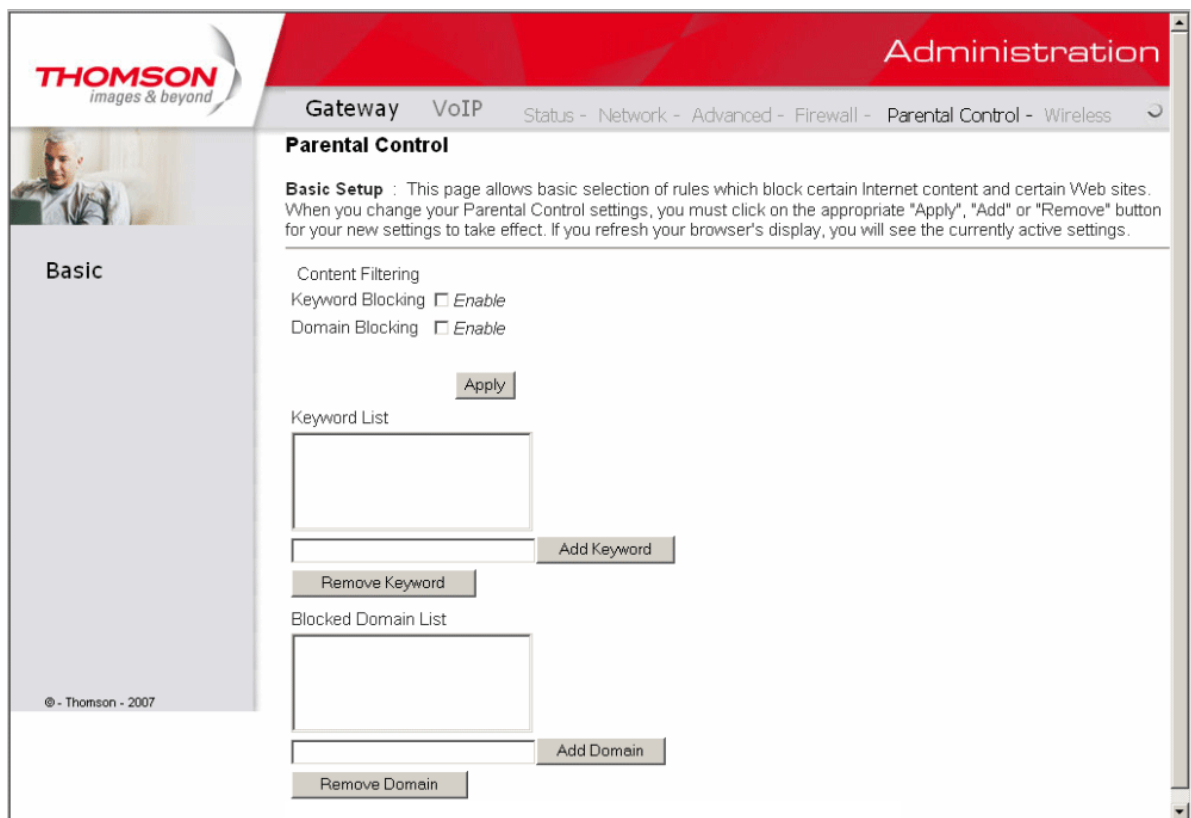


Fig. 31 Gateway\Parental Control\Basic

Chapter 2: WEB Configuration

Gateway – Wireless Web Page Group

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

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

Performance

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

Authentication

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

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

Network Type – Set to Open

Access Control List – Enter your wireless PCs' MAC addresses

Security

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

Data Encryption – Set to WEP (64-bit)

PassPhrase – Use this feature to generate security keys

Chapter 2: WEB Configuration

1. 802.11b/g/n Radio

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

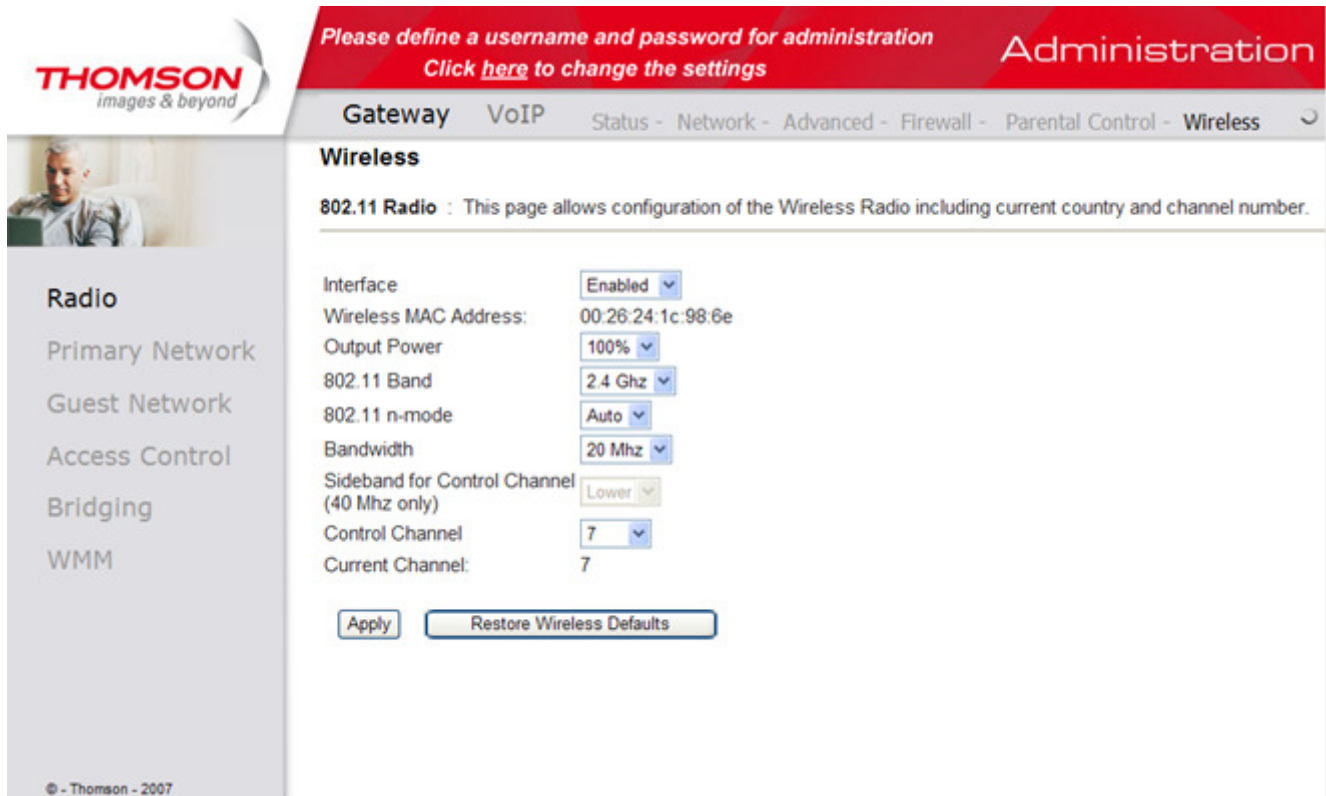


Fig. 32 Gateway\Wireless\Radio

- **Interface:** The wireless radio in your gateway can be completely de-activated by changing **Interface** to Disabled. Click the **Apply** button to save your settings. 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 will 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

Your service provider might enforce different default settings, please check with your provider to insure proper setup

Chapter 2: WEB Configuration

2. 802.11b/g/n 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.

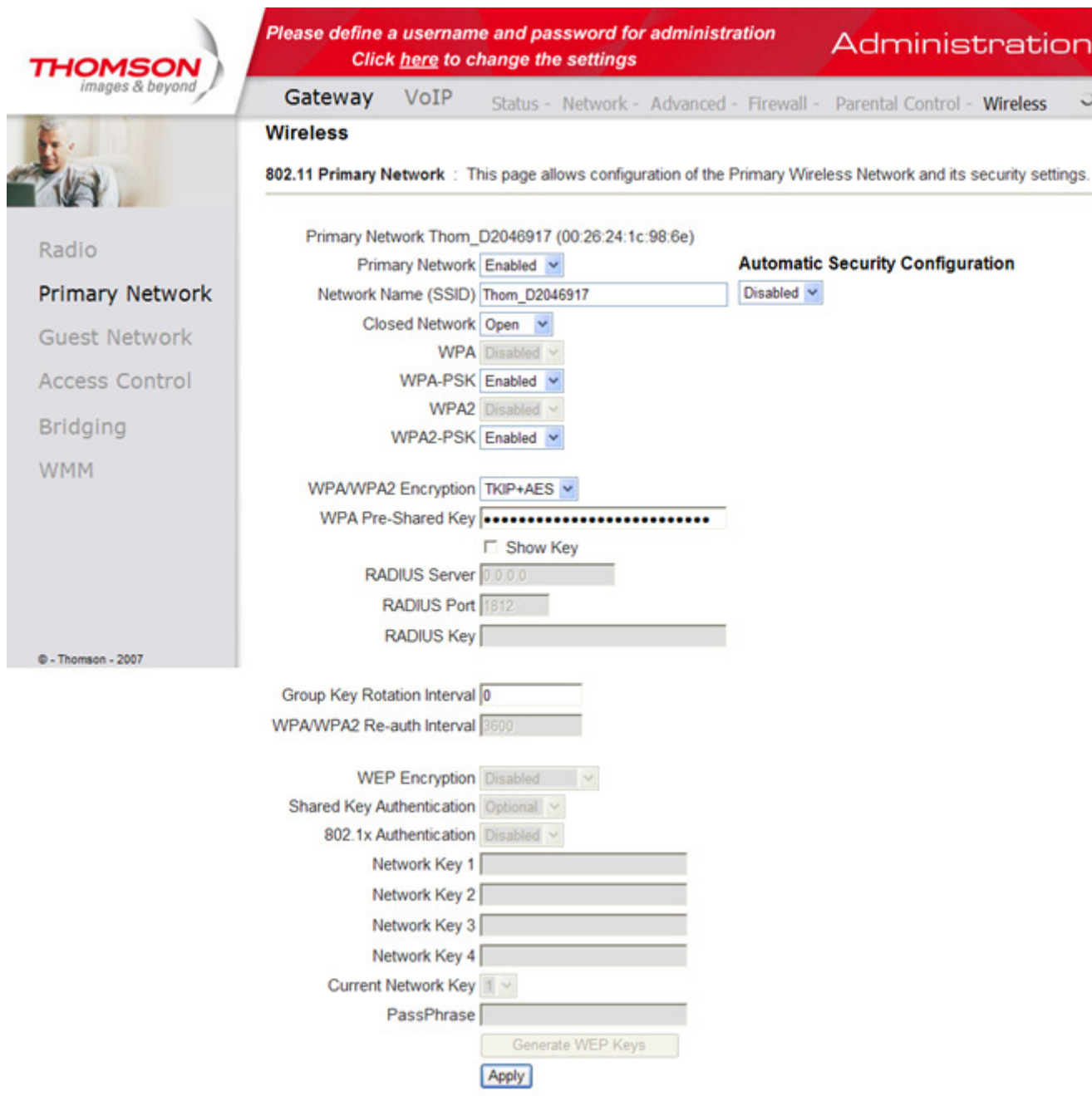


Fig. 33 Gateway\Primary Network

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

Chapter 2: WEB Configuration

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 Voice Gateway.*)

- If you select WEP (**64-bit** or **128-bit**), you can adjust the following settings-
- **Shared Key Authentication:** Decide whether to set the shared key **Optional** or **Required** by selecting from the drop-down menu.
- **Network Key 1 to 4:** The system allows you to enter four sets of the WEP key. For **64-bit** WEP mode, the key length is 5 characters or 10 hexadecimal digits. As for **128-bit** WEP mode, the key length is 13 characters or 26 hexadecimal digits.
- **Current Network Key:** Select one set of the network key (from 1 to 4) as the default one.
- **PassPhrase:** You can enter ASCII codes into this field. The range is from 8 characters to 64 characters. For **ASCII characters**, you can key in **63** characters in this field. If you want to key in **64** characters, only **hexadecimal characters** can be used.
- **Generate WEP Keys:** Click this button to generate the PassPhrase.

The screenshot shows a configuration page for WEP encryption. At the top, 'WEP Encryption' is set to 'WEP (128-bit)'. Below it, 'Shared Key Authentication' is set to 'Optional' and '802.1x Authentication' is set to 'Disabled'. There are four 'Network Key' fields, each with a text input area containing 26 empty hexadecimal characters. Below these is a 'Current Network Key' dropdown menu set to '1'. At the bottom, there is a 'PassPhrase' text input field and a 'Generate WEP Keys' button.

Fig. 34 PassPhrase

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

Chapter 2: WEB Configuration

802.1x Authentication

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

- **RADIUS Server:** RADIUS Server is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. Please key in the IP Address for the RADIUS Server.
- **RADIUS Port:** Besides the IP address of the RADIUS Server, you have to enter the port number for the server. Port 1812 is the reserved RADIUS-authentication port described in RFC 2138. Earlier AP (RADIUS clients) use port 1945. The default value will be shown on this box. You can keep and use it.
- **RADIUS Key:** A RADIUS Key is like a password, which is used between IAS and the specific RADIUS client to verify identity. Both IAS and the RADIUS client must be use the same RADIUS Key for successful communication to occur. Enter the RADIUS Key.

WPA/WPA2 Encryption

WPA Pre-Shared Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

WEP Encryption

Shared Key Authentication

802.1x Authentication

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

Fig. 35 802.1x 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 Voice Gateway for a period of time longer than the setting here, it would be disconnected and the authentication will be executed again. The default value is 3600, you may modify it.

The screenshot shows a configuration interface for WPA/WPA2. It includes several dropdown menus and text input fields. The WPA status is set to 'Enabled', while WPA-PSK, WPA2, and WPA2-PSK are all 'Disabled'. The encryption type is set to 'TKIP'. The WPA Pre-Shared Key field is currently empty. The RADIUS Server is set to '0.0.0.0', the RADIUS Port is '1812', and the RADIUS Key field is empty. The Group Key Rotation Interval is set to '0', and the WPA/WPA2 Re-auth Interval is set to '3600'.

WPA	Enabled
WPA-PSK	Disabled
WPA2	Disabled
WPA2-PSK	Disabled
WPA/WPA2 Encryption	TKIP
WPA Pre-Shared Key	
RADIUS Server	0.0.0.0
RADIUS Port	1812
RADIUS Key	
Group Key Rotation Interval	0
WPA/WPA2 Re-auth Interval	3600

Fig. 36 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.**

WPA	Disabled	▼
WPA-PSK	Enabled	▼
WPA2	Disabled	▼
WPA2-PSK	Enabled	▼
WPA/WPA2 Encryption	TKIP	▼
WPA Pre-Shared Key	<input type="text"/>	
RADIUS Server	<input type="text" value="0.0.0.0"/>	
RADIUS Port	<input type="text" value="1812"/>	
RADIUS Key	<input type="text"/>	
Group Key Rotation Interval	<input type="text" value="0"/>	
WPA/WPA2 Re-auth Interval	<input type="text" value="3600"/>	

Fig. 37 WPA-PSK/WPA2-PSK

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. 38 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 DWG875/DWG875T 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”.

Chapter 2: WEB Configuration

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

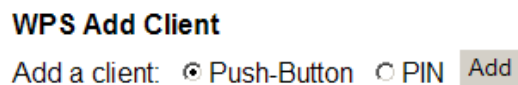


Fig. 39 WPS/Push-Button

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

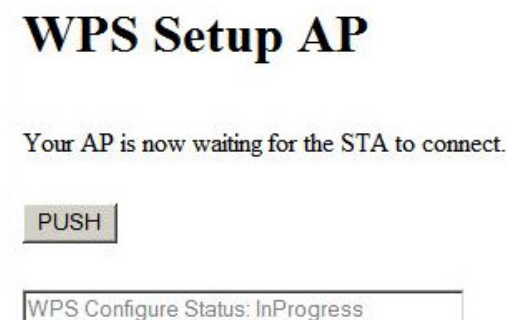


Fig. 40 WPS Setup AP/PUSH

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


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



Fig. 41 WPS Setup 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.



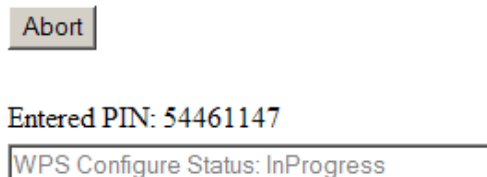
WPS Add Client
Add a client: Push-Button PIN
PIN:

Fig. 42 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

Fig. 43 WPS Setup 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.

Chapter 2: WEB Configuration

WPS Setup AP SUCCESSFUL

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

Continue

Entered PIN:

WPS Configure Status: Success!

Fig. 44 WPS Setup AP successful/PIN

Chapter 2: WEB Configuration

3. Guest Network

This page allows you to configure a guest network.

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

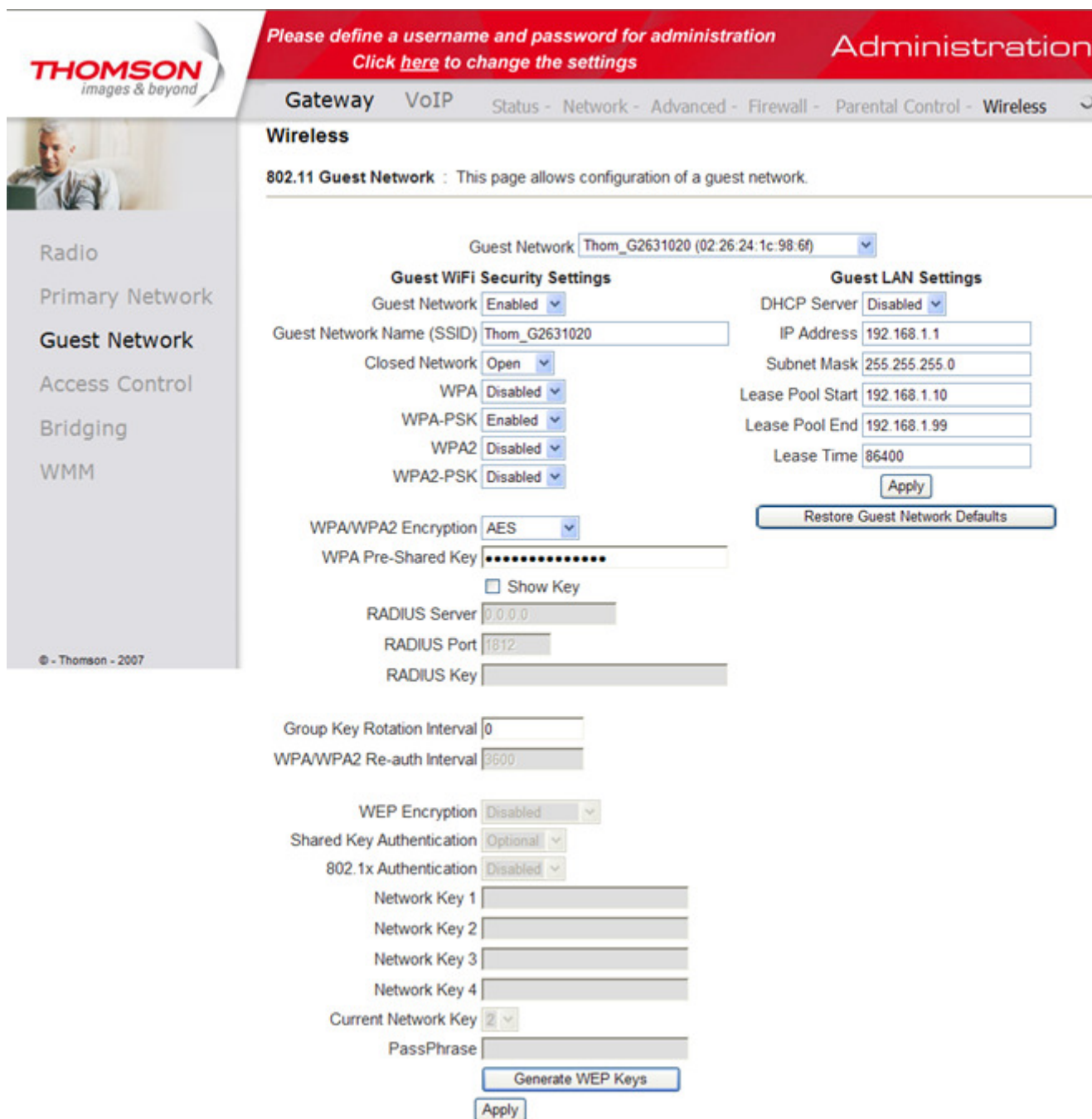


Fig. 45 Gateway\Wireless\Guest Network

Chapter 2: WEB Configuration

4. Access Control

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

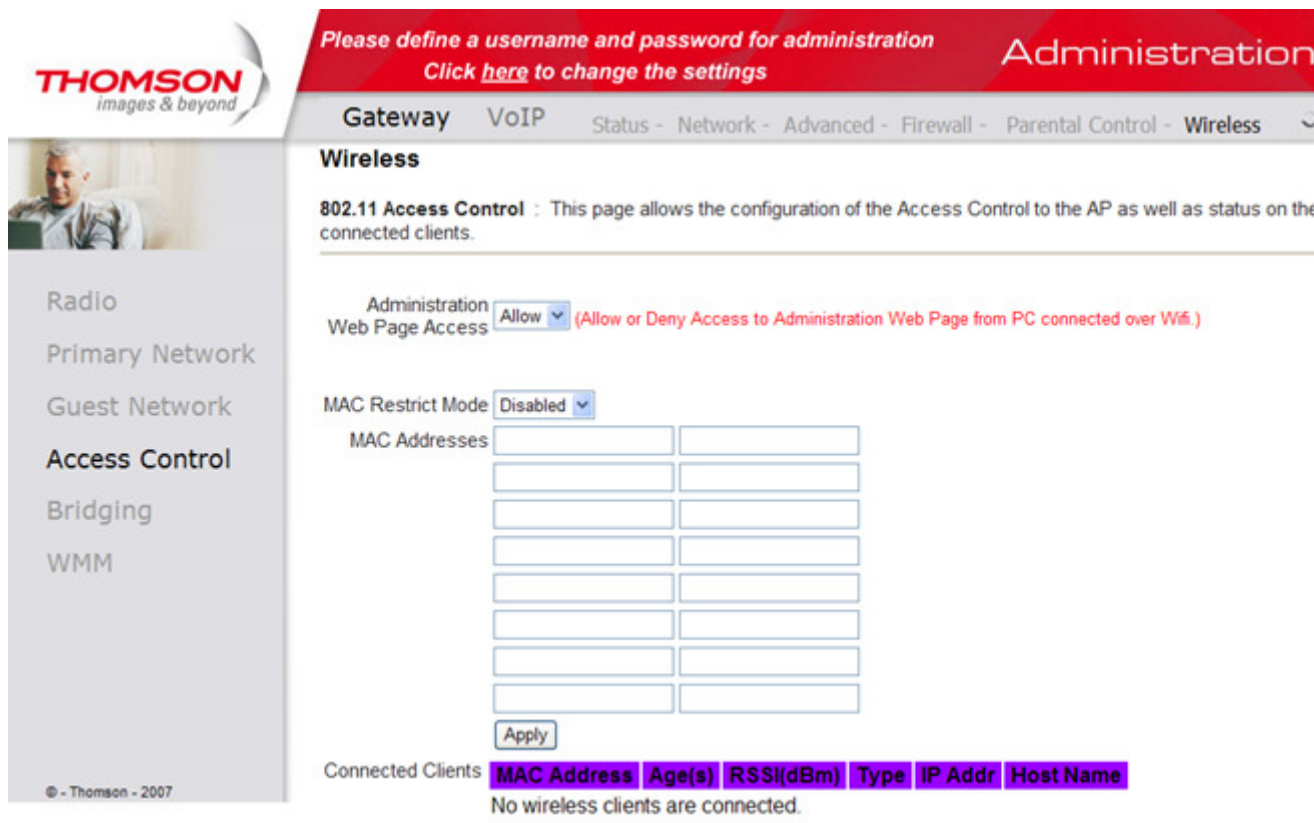


Fig. 46 Gateway\Wireless\Access Control

Administration Web Page Access : Select **Allow** to permit access to Administration Web Page from PC connected over Wifi; or choose **Deny** to prevent the clients connected over Wifi from access to Administration Web Page.

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

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

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

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

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

Chapter 2: WEB Configuration

5. 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.

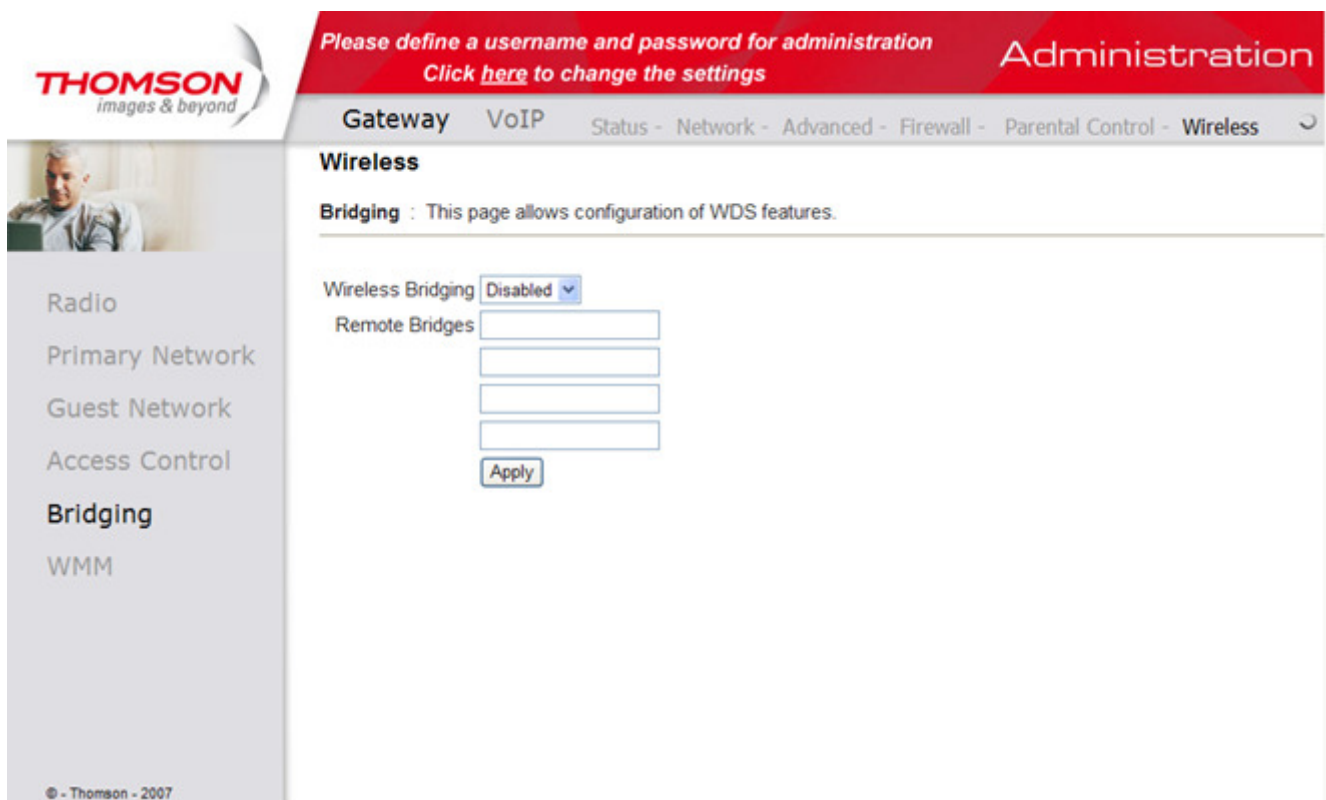


Fig. 47 Gateway\Wireless\Bridging

- **Wireless Bridging:**
Choose **Disabled** to shutdown this function; select **Enabled** to turn on the function of WDS.
- **Remote Bridges:**
Enter the MAC Addresses of the remote Bridges to relay the signals for each other.
- **Apply:**
After proper configuration, click Apply to invoke the settings.

Chapter 2: WEB Configuration

6. 802.11e 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.

- **Enable WMM:**
This field allows you to enable WMM to improve multimedia transmission.
- **Enable WMM No-Acknowledgement:**
This field allows you to enable WMM No-Acknowledgement.
- **Power Save Support:**
This field allows you to enable WMM Power-Save-Support.

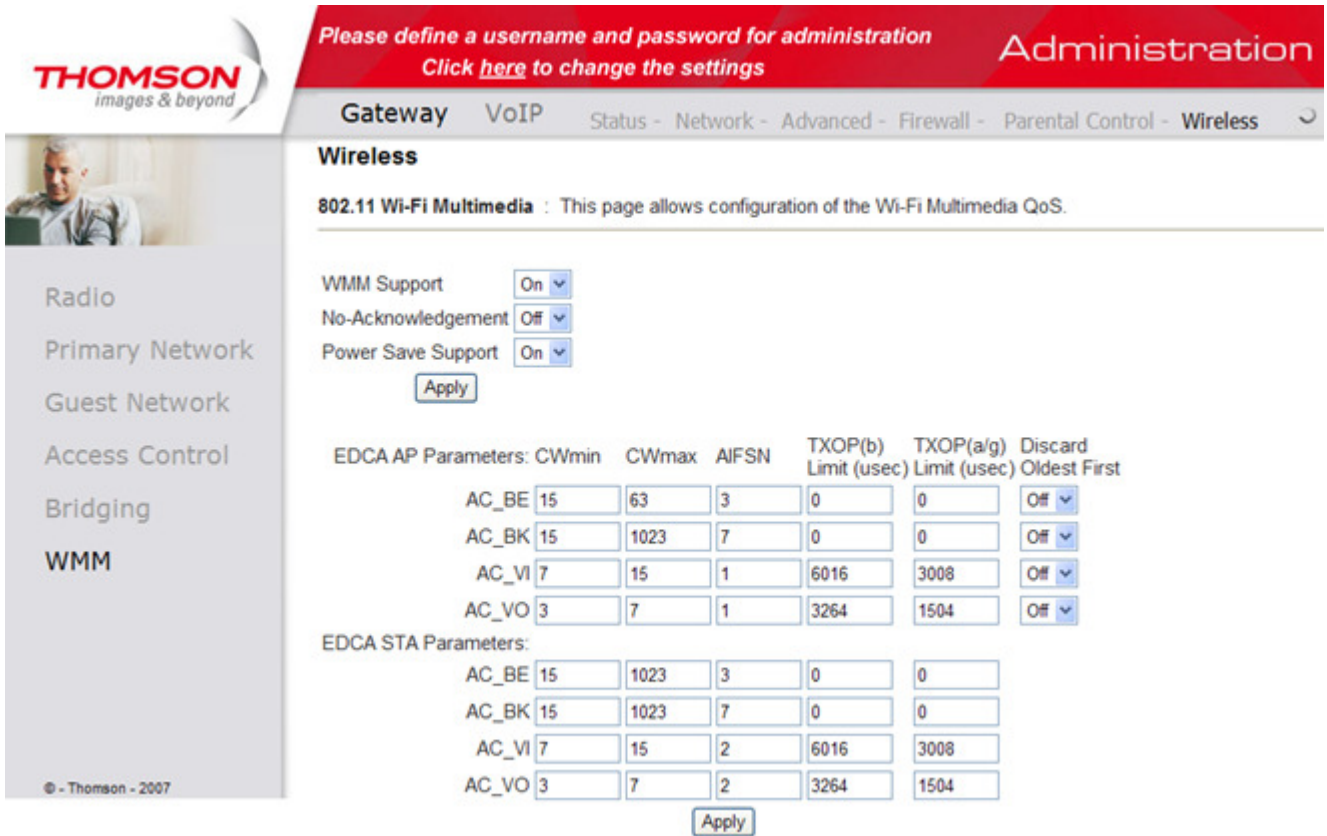


Fig. 48 Gateway\Wireless\WMM

Chapter 2: WEB Configuration

VoIP – Basic Web Page Group

1. Basic LAN

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

THOMSON
images & beyond

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

Administration

Gateway VoIP Basic

Basic Status

Basic LAN

RF Parameters

RF Parameters - Downstream

Channel	Frequency	Power	Signal to Noise Ratio	Modulation
1	0.0 MHz	0.0 dBmV	0.0 dB	None
2	0.0 MHz	0.0 dBmV	0.0 dB	None
3	0.0 MHz	0.0 dBmV	0.0 dB	None
4	0.0 MHz	0.0 dBmV	0.0 dB	None
5	0.0 MHz	0.0 dBmV	0.0 dB	None
6	0.0 MHz	0.0 dBmV	0.0 dB	None
7	0.0 MHz	0.0 dBmV	0.0 dB	None
8	0.0 MHz	0.0 dBmV	0.0 dB	None

RF Parameters - Upstream

Channel	Frequency	Power	Upstream Data Rate	Modulation
1	0.0 MHz	5.0 dBmV	0 Ksym/sec	QPSK
2	0.0 MHz	0.0 dBmV	0 Ksym/sec	QPSK
3	0.0 MHz	0.0 dBmV	0 Ksym/sec	QPSK
4	0.0 MHz	0.0 dBmV	0 Ksym/sec	QPSK

Status

System uptime	0 days 06h:47m:16s
Computers detected	0
CM Status	Not synchronized
WAN Isolation	OFF
Time and Date	-----:--:--

Interface Parameters

Interface Name : LAN

Provisioned	Enabled	State	Up
Speed	0 Mbps	MAC address	00-10-95-de-ad-02

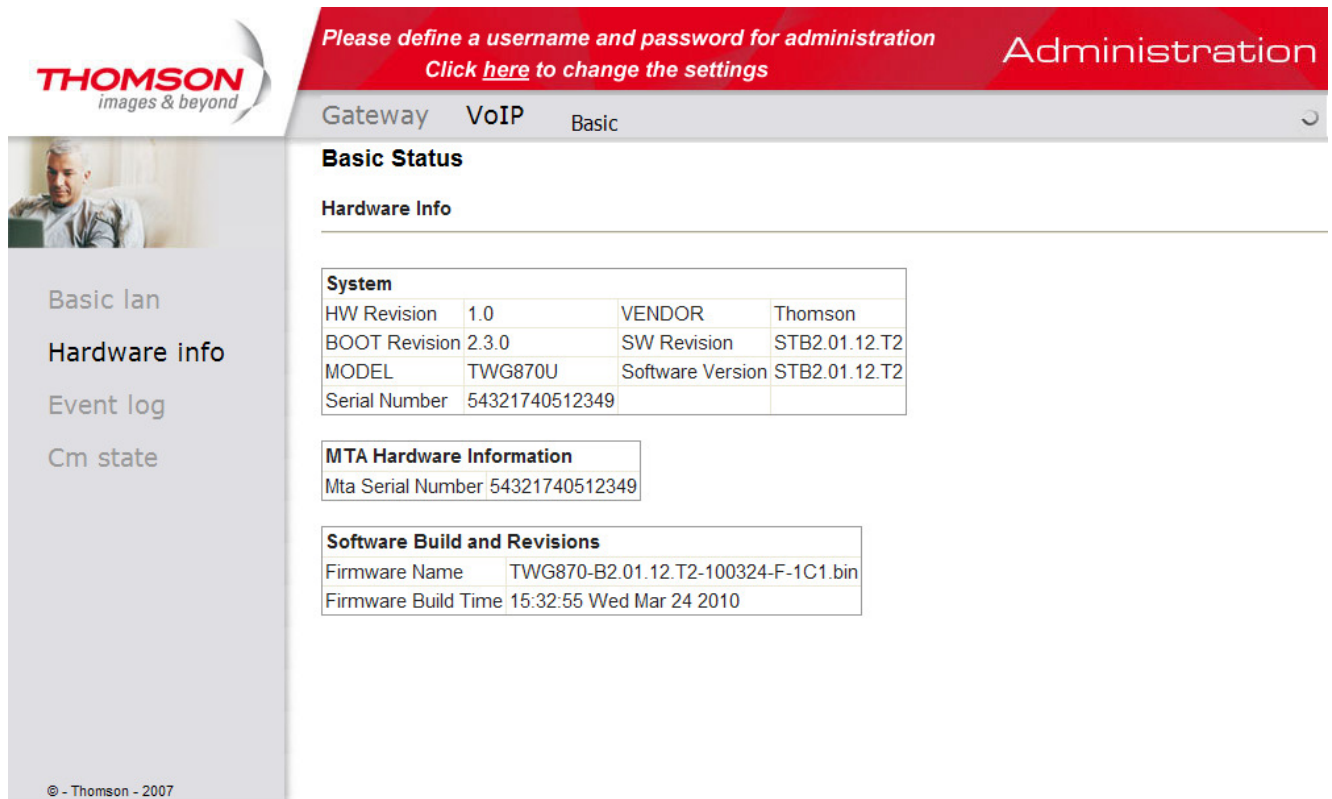
© - Thomson - 2007

Fig. 49 VoIP\Basic\Basic LAN

Chapter 2: WEB Configuration

2. Hardware Info

The hardware Info is displayed on this page.



The screenshot shows the Thomson VoIP Basic configuration page. 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 page title is "Administration". Below the banner, there are tabs for "Gateway", "VoIP", and "Basic". The "Basic" tab is selected. The main content area is titled "Basic Status" and "Hardware Info". It contains three tables: "System", "MTA Hardware Information", and "Software Build and Revisions".

System			
HW Revision	1.0	VENDOR	Thomson
BOOT Revision	2.3.0	SW Revision	STB2.01.12.T2
MODEL	TWG870U	Software Version	STB2.01.12.T2
Serial Number	54321740512349		

MTA Hardware Information	
Mta Serial Number	54321740512349

Software Build and Revisions	
Firmware Name	TWG870-B2.01.12.T2-100324-F-1C1.bin
Firmware Build Time	15:32:55 Wed Mar 24 2010

Fig. 50 VoIP\Basic\Hardware Info

Chapter 2: WEB Configuration

3. Event Log

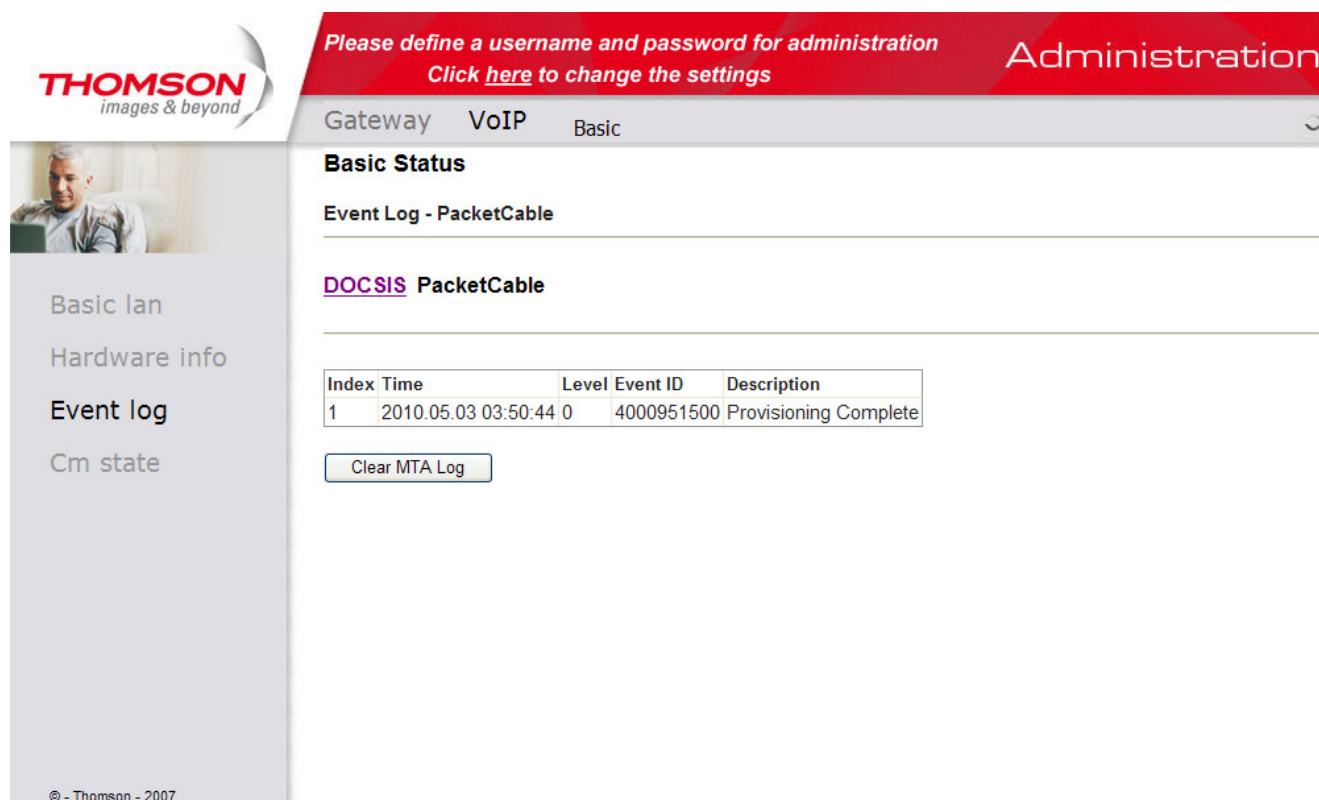
The event logs are displayed on this web page. You can check them whenever you need.

The screenshot shows the Thomson VoIP Basic administration 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, there are tabs for "Gateway", "VoIP", and "Basic". The "Basic Status" section is active, showing "Event Log - DOCSIS". A link for "DOCSIS PacketCable" is visible. A table lists event logs with columns for Date/Time, Event ID, Event Level, and Description. A "Clear Log" button is at the bottom.

Date/Time	Event ID	Event Level	Description
03/30/2010 08.50	82000500	03	Started Unicast Maintenance Ranging - No Response received - T3 time-out;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
03/29/2010 16.59	68000300	05	DHCP WARNING - Non-critical field invalid in response ;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
03/29/2010 16.58	66010100	04	Missing BP Configuration Setting TLV Type: 17.9;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
03/29/2010 16.58	66010100	04	Missing BP Configuration Setting TLV Type: 17.8;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
01/01/1970 00.00	68000300	05	DHCP WARNING - Non-critical field invalid in response ;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	82000200	03	No Ranging Response received - T3 time-out;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:30:b8:c9:eb:00;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	82000200	03	No Ranging Response received - T3 time-out;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020300	05	MDD message timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:30:b8:c9:eb:00;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020200	05	Lost MDD Timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:30:b8:c9:eb:00;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020200	05	Lost MDD Timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020300	05	MDD message timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;

Fig. 51-1 VoIP\Basic\Event log\DOCSIS

Chapter 2: WEB Configuration



The screenshot displays the Thomson VoIP Basic 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 displayed in white on the right side of the banner. Below the banner, there are navigation tabs for "Gateway", "VoIP", and "Basic". The "Basic" tab is selected. The main content area is titled "Basic Status" and includes a section for "Event Log - PacketCable". Below this, there is a section for "DOCSIS PacketCable" which contains a table with the following data:

Index	Time	Level	Event ID	Description
1	2010.05.03 03:50:44	0	4000951500	Provisioning Complete

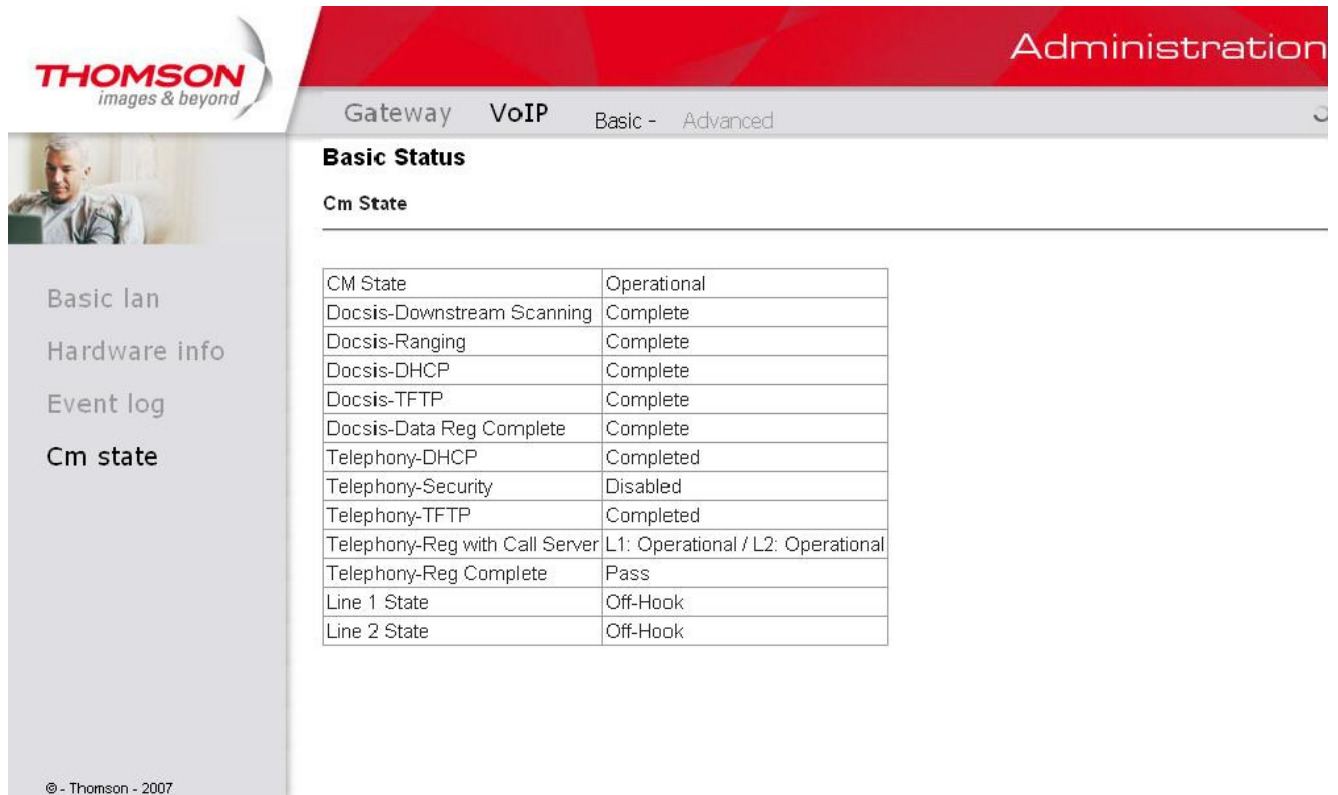
Below the table is a button labeled "Clear MTA Log". On the left side of the interface, there is a sidebar with a Thomson logo and the tagline "images & beyond". The sidebar contains a list of menu items: "Basic lan", "Hardware info", "Event log", and "Cm state". At the bottom left of the sidebar, there is a copyright notice: "© - Thomson - 2007".

Fig. 51-2 VoIP\Basic\Event log\PacketCable

Chapter 2: WEB Configuration

4. CM State

This page shows the current state of the cable modem.



The screenshot shows the Thomson Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Basic -', and 'Advanced'. The left sidebar contains menu items: 'Basic lan', 'Hardware info', 'Event log', and 'Cm state'. The main content area is titled 'Basic Status' and 'Cm State'. A table displays the following data:

CM State	Operational
Docsis-Downstream Scanning	Complete
Docsis-Ranging	Complete
Docsis-DHCP	Complete
Docsis-TFTP	Complete
Docsis-Data Reg Complete	Complete
Telephony-DHCP	Completed
Telephony-Security	Disabled
Telephony-TFTP	Completed
Telephony-Reg with Call Server	L1: Operational / L2: Operational
Telephony-Reg Complete	Pass
Line 1 State	Off-Hook
Line 2 State	Off-Hook

© - Thomson - 2007

Fig. 52 VoIP\Basic\Cm state

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 and USB hubs, 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

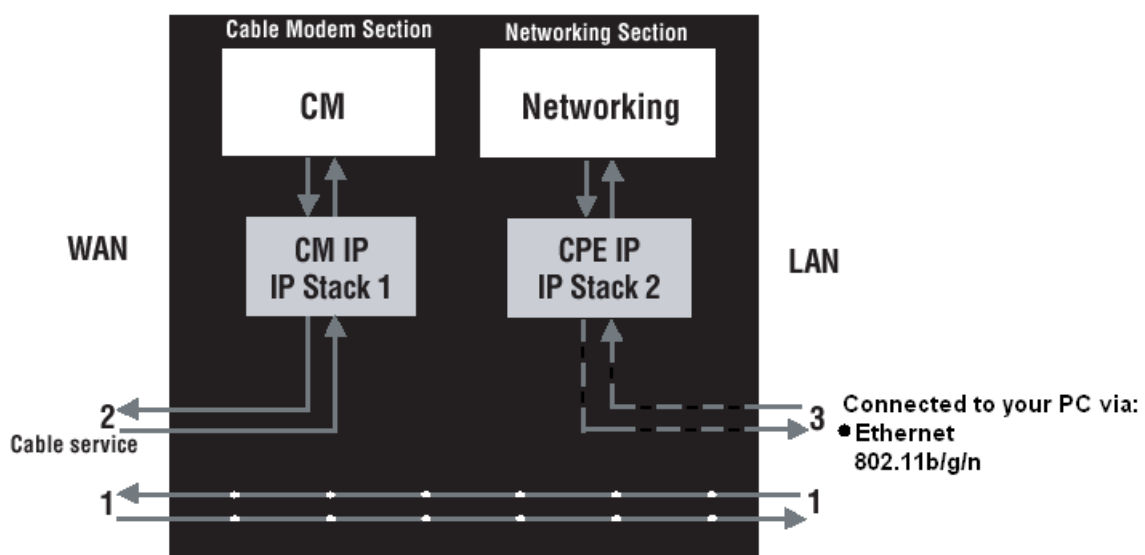


Fig.53 Communication between your PCs and the network side

Example: The Wireless Cable Gateway offers a number of built-in web pages which you

Chapter 3: Networking

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 results, 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 DOCSIS Standard cable modem technology. 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 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, USB, and 802.11b/g wireless network interfaces on the LAN side and the DOCSIS network interface on the WAN side.

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

Chapter 3: Networking

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. All units ship from the factory set for the RG mode, but a configuration file which the cable company sends the cable modem section during its initialization can change it.

Cable Modem (CM) Mode

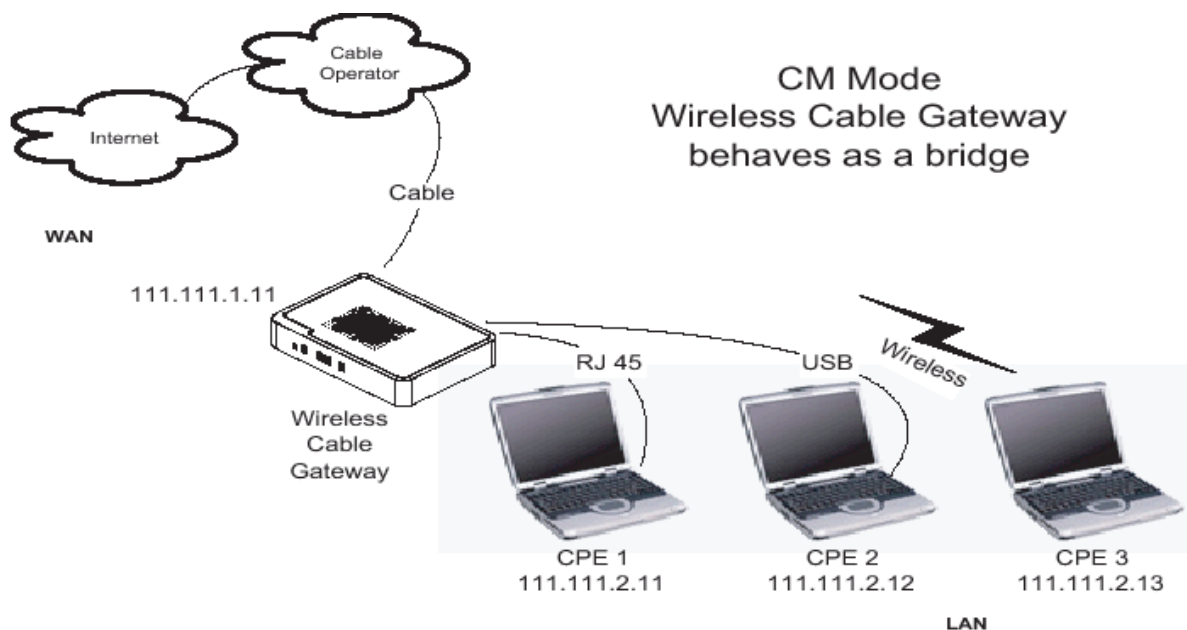


Fig. 54 Cable Modem Mode

Chapter 3: Networking

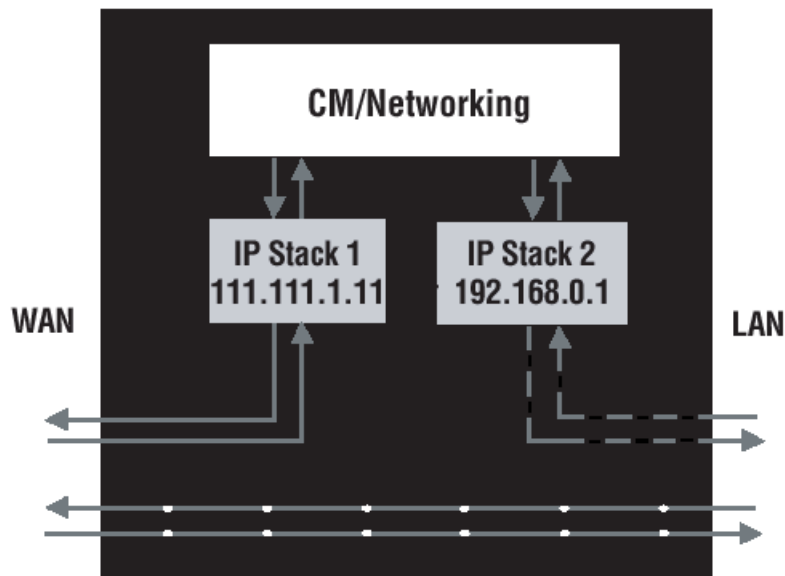


Fig. 55 Two IP stacks are activated in cable modem mode

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

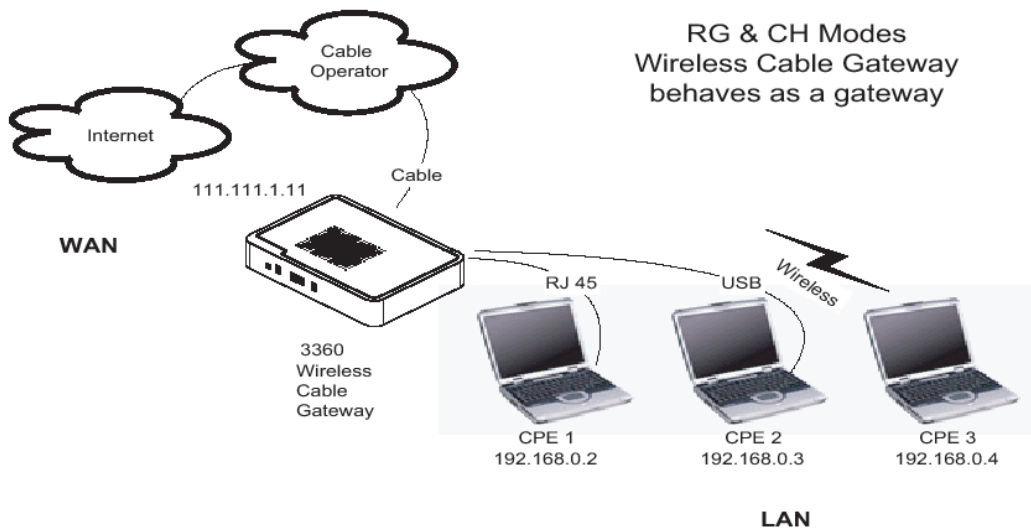


Fig. 56 Residential Gateway Mode

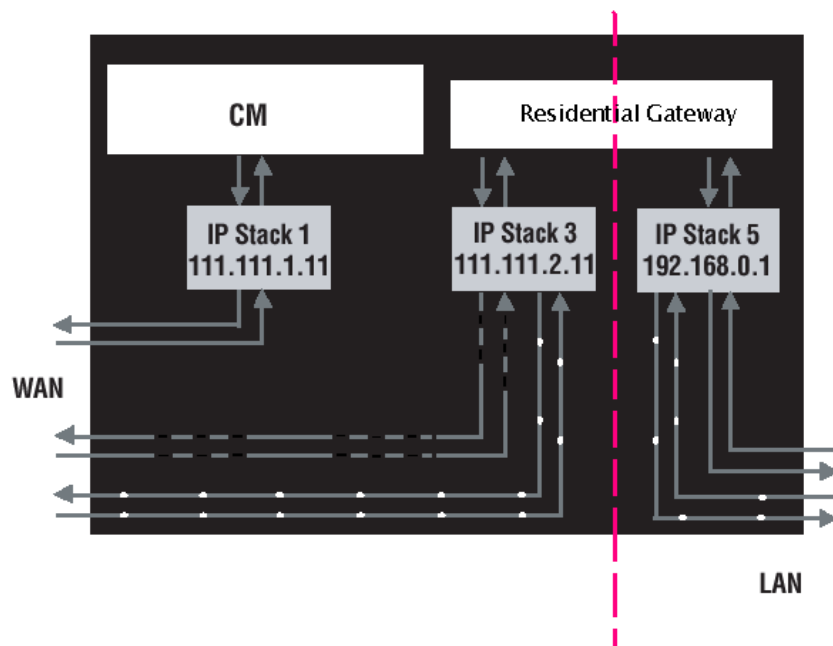


Fig. 57 Three IP stacks are activated in Residential mode

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.
- 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

Chapter 3: Networking

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.

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. It should be set to "1".

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

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

Q. It seems that the wireless network is not working

A. Check the WiFi LED on the front panel. If it is no lighted, press on the WPS button (on the side of the modem) during 3 seconds and then check again the WiFi LED. If it is lighted, then the WiFi is enabled.

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

A. Absolutely!

Q. What do you mean by "Broadband?"

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

Q. What is DOCSIS and what does it mean?

A. "Data over Cable Service Interface Specifications" is the industry standard that most cable companies are adopting as they upgrade their systems. Should you ever decide to move, the Wireless Voice Gateway

Chapter 4: Additional Information

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

Q. What is PacketCable and what does it mean?

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

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

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

* Monthly subscription fee 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 or USB port may not be working. Check each product's documentation for more information.
- The Network Properties of your operating system may not be installed correctly or the settings may be incorrect. Check with your ISP or cable company.

All of the lights are flashing in sequence.

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

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

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

The modem won't register a cable connection.

- If the modem is in Initialization Mode, the INTERNET light will be flashing. Call your Cable Company if it has not completed this 5-step process within 30 minutes, and note which step it is getting stuck on.
- 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 DOCSIS compliant and PacketCable compliant by calling your cable provider.

Chapter 4: Additional Information

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.net/GlobalEnglish/Deliver/Cable/cable-modems-routers-gateways/Pages/default.aspx>

Chapter 4: Additional Information

Service Information

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

Chapter 4: Additional Information

Glossary

10/100/1000 Mbps – Unshielded, twisted pair cable with an RJ-45 connector, used with Ethernet LAN (Local Area Network). “10/100/1000” indicates speed (10/100/1000 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 adapters – A plug-in circuit board installed in an expansion slot of a personal computer. The Ethernet card (sometimes called a Network Interface Card , network adapter or NIC) takes parallel data from the computer, converts it to serial data, puts it into a packet format, and sends it over the 10/100/1000 Mbps LAN cable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

THOMSON

101 West 103rd Street,

Indianapolis, IN 46290, USA

For more information

THOMSON

101 West 103rd Street,

Indianapolis, IN 46290, USA <http://www.technicolor.com>

© 2006 Thomson Inc. - Trademark(s) Registered - Marca(s) Registrada(s)

Photos and features subject to change without notice.

Illustration of product finish may vary from actual color.

RCA
by **THOMSON**