

# ***802.11g Wireless Cable Residential Gateway***

**CBW500/501**

**User's Manual**

For 1 Port and 4 Ports Model

## **Federal Communication Commission Interference Statement**

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 to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the 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 Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

### **IMPORTANT NOTE:**

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

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

# Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>2</b>
<b>2</b>	<b>FEATURES .....</b>	<b>2</b>
<b>3</b>	<b>PACKAGE CONTENTS.....</b>	<b>3</b>
<b>4</b>	<b>HARDWARE CONNECTION .....</b>	<b>3</b>
<b>5</b>	<b>LED INDICATORS .....</b>	<b>2</b>
	Mode .....	2
<b>6</b>	<b>GETTING STARTED .....</b>	<b>3</b>
<b>7</b>	<b>CONFIGURATION MENU.....</b>	<b>4</b>
	7.1 STATUS.....	4
	7.1.1 <i>Software</i> .....	4
	7.1.2 <i>Connection</i> .....	5
	7.1.3 <i>Security</i> .....	6
	7.1.4 <i>Diagnostics</i> .....	7
	7.2 BASIC.....	8
	7.2.1 <i>Setup</i> .....	8
	7.2.2 <i>DHCP</i> .....	9
	7.3 ADVANCED .....	10
	7.3.1 <i>Options</i> .....	10
	7.3.2 <i>IP Filtering</i> .....	12

7.3.3	<i>MAC Filtering</i> .....	13
7.3.4	<i>Port Filtering</i> .....	14
7.3.5	<i>Forwarding</i> .....	15
7.3.6	<i>Port Triggers</i> .....	16
7.3.7	<i>DMZ Host</i> .....	17
7.3.8	<i>RIP Setup</i> .....	18
7.4	<b>FIREWALL</b> .....	19
7.4.1	<i>ToD Filter</i> .....	19
7.4.2	<i>Web Filter</i> .....	20
7.4.3	<i>Local Log</i> .....	21
7.4.4	<i>Remote Log</i> .....	22
7.5	<b>PARENTS CONTROL</b> .....	23
7.5.1	<i>Basic</i> .....	23
7.6	<b>WIRELESS</b> .....	24
7.6.1	<i>Basic</i> .....	24
7.6.2	<i>Security</i> .....	26
7.6.3	<i>Access Control</i> .....	29
7.6.4	<i>Advanced</i> .....	30

## 8

### **TROUBLESHOOTING .....33**

<i>Basic Connection</i> .....	33
<i>Browsing Configuration Utility</i> .....	33
<i>Connecting to the Internet</i> .....	34
<i>Wireless Network Connection</i> .....	34

## 9

### **TECHNICAL SPECIFICATION .....36**

## 1 Introduction

The CBW500 Wireless Cable Residential Gateway is a broadband gateway product combining Ethernet network and wireless together. With IEEE 802.11g standard wireless integration, this device not only allows you to take an advantage of wired-free data transmission, but also allows you to have 4 of 10/100 Mbps Ethernet connections with auto-sensing switch Ethernet ports. This combination of router and switch product eliminates the needs to buy an additional hub or switch to serve your network, so users on either WLAN (wireless LAN) or wired LAN can share files, other networking resource, and even for a single account of Internet access by having this device connect to a Cable modem.

The CBW500 allows up to 253 total (128 wireless) users to share a single Cable connection. A high-speed routing engine and 54Mbps (802.11g standard) wireless throughput easily handle large data transmission, including those from multimedia applications.

802.11g also backward-compatible with 802.11b WLAN equipment, preserving existing network investments.

The CBW500 can work as DHCP server to assigns an IP Address to every PC on the LAN automatically and/or work as DHCP client to get an IP address dynamically assigned by ISP. CBW500 Cable Residential Gateway is easy to setup and maintain. All functions can be configured via web browsers such as Internet Explorer.

## 2 Features

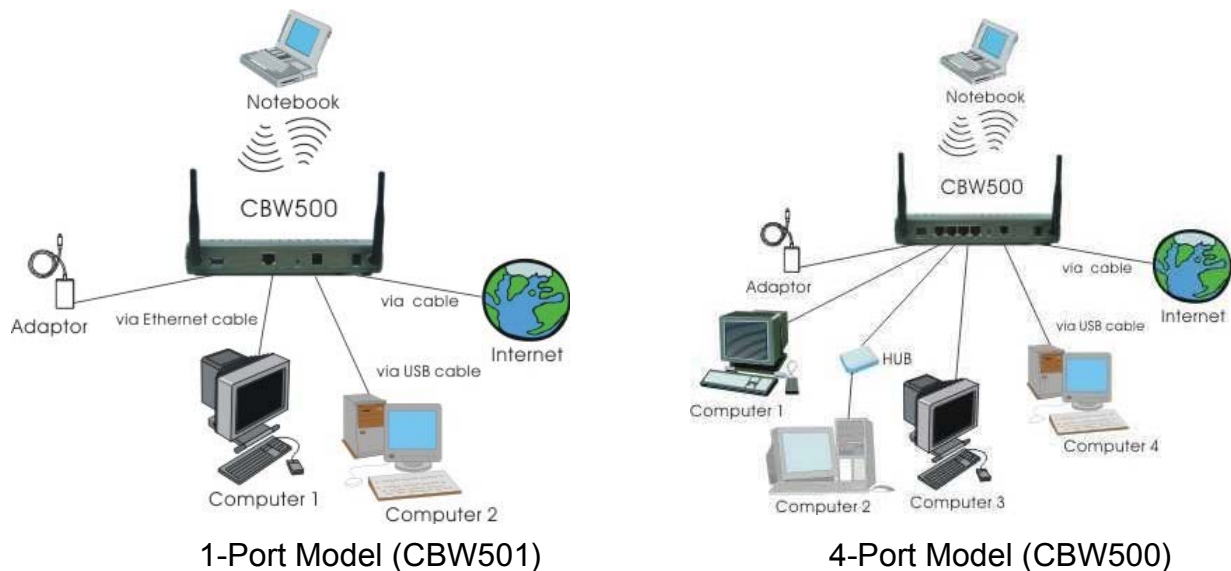
- Enhance upstream performance, up to 30Mbps
- DOCSIS 2.0 and CableHome 1.0 compliant
- High speed wireless connection, up to 54Mbps
- Ethernet (w/A-MDIX) or USB Interface for easy installation
- QoS enhancement
- MSO SNMP remote network management
- Web Browser Management auto detect cable modem status
- Field software upgradeable by MSO
- Support up to 253 network clients
- Provide MIBs DOCSIS1.0/1.1

### 3 Package Contents

- 1 x CBW500 Wireless Cable Residential Gateway with antennas
- 1 x Quick Installation Guide
- 1 x CD-ROM containing USB driver\* and User's Manual
- 1 x 12V DC/1A Power Adapter
- 1 x Ethernet cable
- 1 x USB cable (optional)

\*USB interface depends on your model type, you may not have USB driver contained in the CD-ROM.

### 4 Hardware Connection



**Power:** This port is for the 12V DC power supply connection.

**Cable:** Connect a DOCSIS 2.0/1.1/1.0 equivalent cable feed to the F-connector on the back of the CBW500.

**LAN:** (1-Port Model) This LAN port is used to connect Ethernet device to the LAN via Ethernet cable. You may use a HUB to extend the connections.

**L1-L4:** (4-Port Model) The four LAN ports are used to connect Ethernet devices to the LAN via Ethernet cables.

**Reset:** Click RESET button to restart the system while press in and hold RESET button for about three seconds to reset the CBW500 to the factory default settings.

**Antenna:** These connection ports are reverse polarity.

## 5 LED Indicators

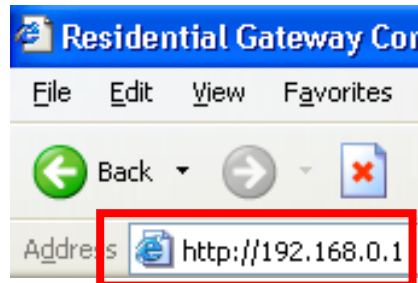


LED		Color	Mode	Status
Power		Green	On	O.K.
Cable		Green	On	Connected
WLAN		Green	On	WLAN interface has data transmitting
USB (optional)		Green	On	Connected
LAN or LAN1~4	Activity	Green/Orange	Blinking	Data transmitting
	10/100Linked	Green/Orange	On	Green as 10Mbps Orange as 100Mbps

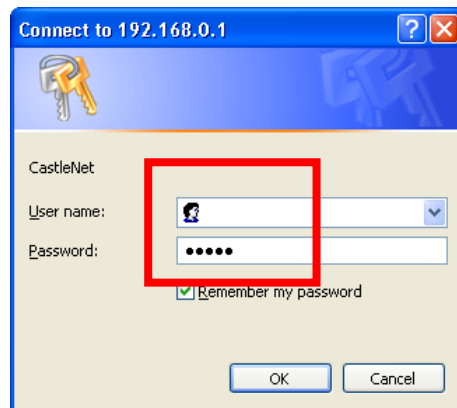
## 6 Getting Started

### Web Configuration

You can access the Configuration Page by opening the web-browser and typing in the IP Address of the CBW500. The default IP Address of the CBW500 is shown as right.



Leave the User name as blank and the password as **cable** and then press **OK** button. It is recommended that you change the default password for security purposes. Please go to Status > Security to change your password.



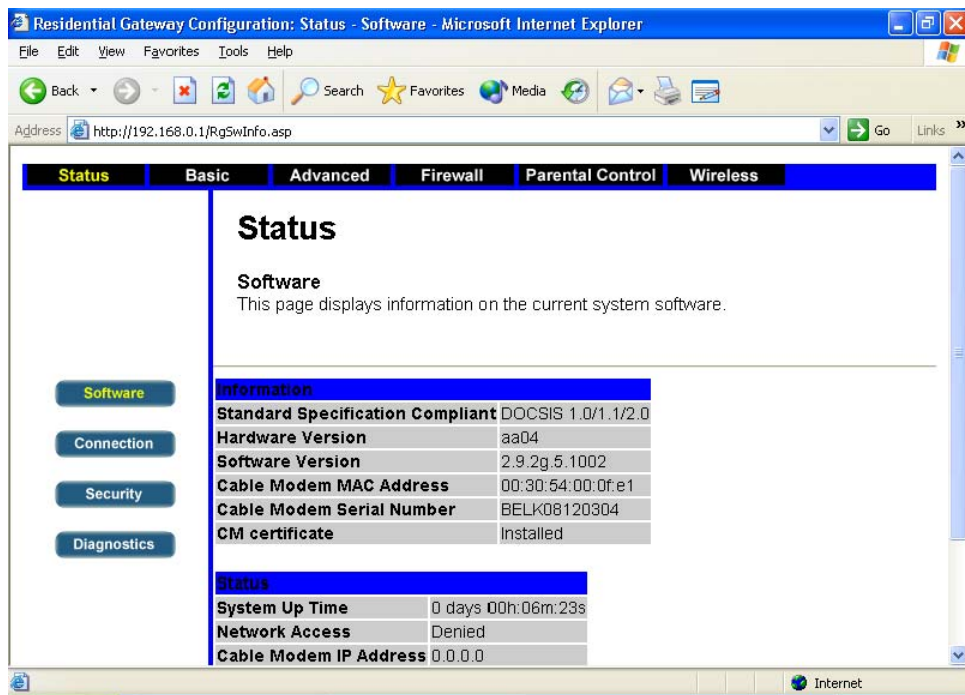


# 7 Configuration Menu

## 7.1 Status

### 7.1.1 Software

This page displays information of current system software.



Residential Gateway Configuration: Status - Software - Microsoft Internet Explorer

Address: http://192.168.0.1/RgSwInfo.asp

**Status** | Basic | Advanced | Firewall | Parental Control | Wireless

### Status

**Software**  
This page displays information on the current system software.

---

**Information**

<b>Standard Specification Compliant</b>	DOCSIS 1.0/1.1/2.0
<b>Hardware Version</b>	aa04
<b>Software Version</b>	2.9.2g.5.1002
<b>Cable Modem MAC Address</b>	00:30:54:00:0f:e1
<b>Cable Modem Serial Number</b>	BELK08120304
<b>CM certificate</b>	Installed

---

**Status**

<b>System Up Time</b>	0 days 00h:06m:23s
<b>Network Access</b>	Denied
<b>Cable Modem IP Address</b>	0.0.0.0

## 7.1.2 Connection

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

The screenshot shows the 'Residential Gateway Configuration: Status - Connection' page in Microsoft Internet Explorer. The browser address bar shows 'http://192.168.0.1/RgConnect.asp'. The page has a navigation menu with tabs for Status, Basic, Advanced, Firewall, Parental Control, and Wireless. The 'Status' tab is selected, and the 'Connection' sub-tab is active. The main content area displays the following information:

**Status**

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

**Startup Procedure**

Procedure	Status	Comment
Acquire Downstream Channel	In Progress	
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Configuration File		
Security	Disabled	Disabled

**Downstream Channel**

Lock Status	Not Locked	Modulation	unknown
Channel ID	0	Symbol rate	Unknown
Downstream Frequency		Downstream Power	-46.2 dBmV
SNR	22.0 dB		

**Upstream Channel**

Lock Status	Not Locked	Modulation	QPSK
Channel ID	0	Symbol rate	0 Ksym/sec
Upstream Frequency		Upstream Power	8.3 dBmV

**CM IP Address**

Duration	Expires
D: -- H: -- M: -- S: --	--:--:--:--:--:--

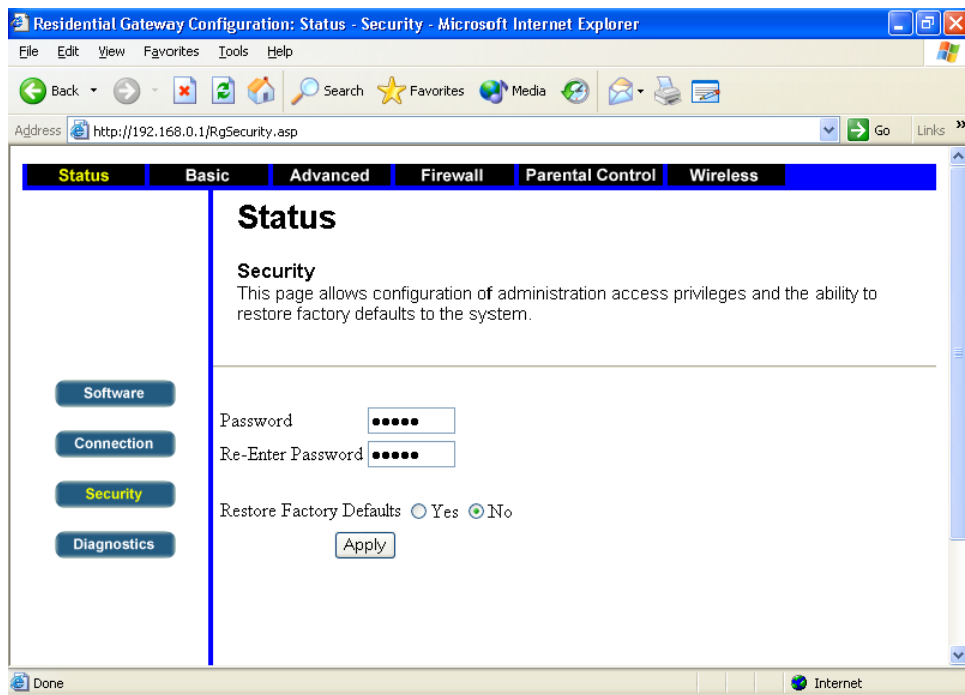
Current System Time: --:--:--:--:--:--

### 7.1.3 Security

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

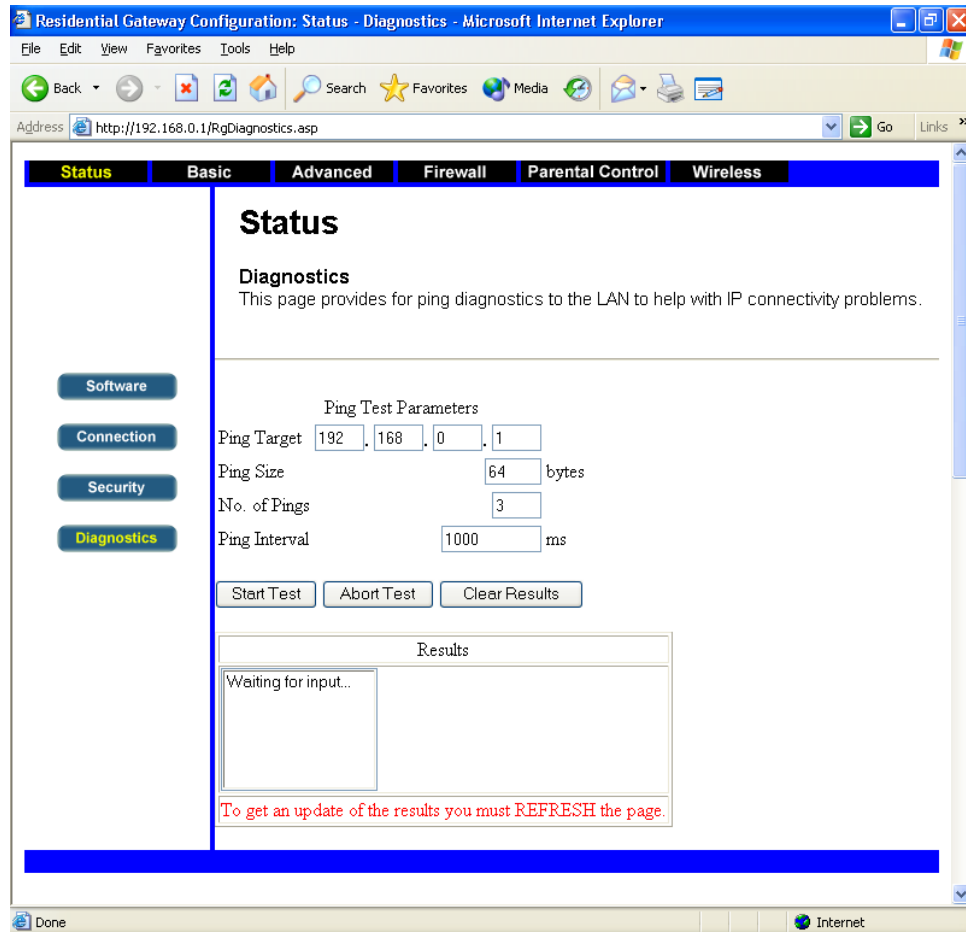
Administrator can change the logging password in this page. It is recommended that you change the password once you have accessed the CBW500 for the first time. The password can be up to 64 characters.

This page also provides an easy way to restore the factory defaults settings if you want to clean all the existing settings or reset your settings.



## 7.1.4 Diagnostics

This page provides ping diagnostics function to help user solve IP connectivity problems.



PING is a utility, which is used to determine whether a device is active at the specified IP address. PING is normally used to test the physical connection between two devices, to ensure that everything is working correctly. Enter the settings of Ping target and then press **Start Test** to start the diagnostic. The results will display in Results table and you need to refresh this web page to update the diagnostic results.

## 7.2 Basic

### 7.2.1 Setup

This page allows configuration of the basic features of the broadband gateway related to your ISP's connection.

There are three options of obtaining a WAN IP address.

1. Obtain WAN IP Address by DHCP
2. Static WAN IP Address (for most leased line users)
3. Obtain WAN IP Address by PPPoE (for most dial-up users)

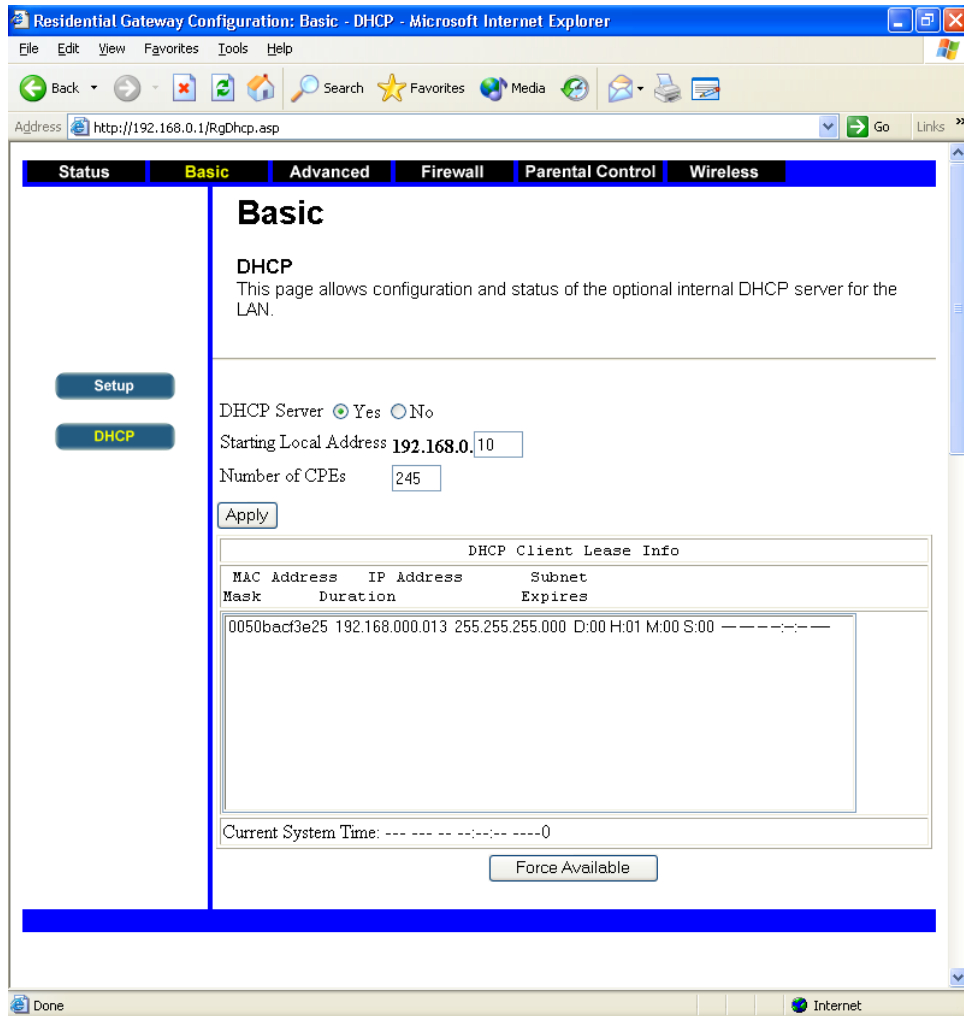
Select the item according to your situation and enter the information required by your ISP. Press **Apply** to confirm the settings.

The screenshot shows a web browser window titled "Residential Gateway Configuration: Basic - Setup - Microsoft Internet Explorer". The address bar shows "http://192.168.0.1/RgSetup.asp". The page has a navigation menu with tabs: Status, Basic (selected), Advanced, Firewall, Parental Control, and Wireless. The main content area is titled "Basic" and "Setup". It contains a "Network Configuration" section with fields for LAN IP Address (192.168.0.1), MAC Address (00:30:54:05:00:05), and WAN IP Address (1.1.1.1). Below this are three radio button options for obtaining a WAN IP address: "Obtain WAN IP Address by DHCP", "Static WAN IP Address", and "Obtain WAN IP Address by PPPoE". The DHCP option is selected. Under DHCP, there are fields for "Duration" and "Expires", both set to "PPPoE IP address", and a "Renew NAT Lease" button. The Static IP option has fields for Host Name, Domain Name, Static IP Address (1.1.1.1), Static IP Mask (255.255.255.0), Default Gateway (1.1.1.254), Primary DNS (0.0.0.0), and Secondary DNS (0.0.0.0). The PPPoE option has fields for User Name (CTI) and Password (masked), and an "Apply" button. On the left side of the page, there are two buttons: "Setup" and "DHCP".

## 7.2.2 DHCP

This page allows configuration of DHCP server for LAN.

You need to enable (default) DHCP server feature and indicate the Starting Local Address for the DHCP server to start with when issuing IP addresses and the number of CPEs (clients).



**Starting Local Address** Because the CBW500's default IP address is 192.168.0.1, the Starting Local address must be 192.168.0.2 or greater, but smaller than 192.168.0.253. The default Starting Local Address is 192.168.0.10.

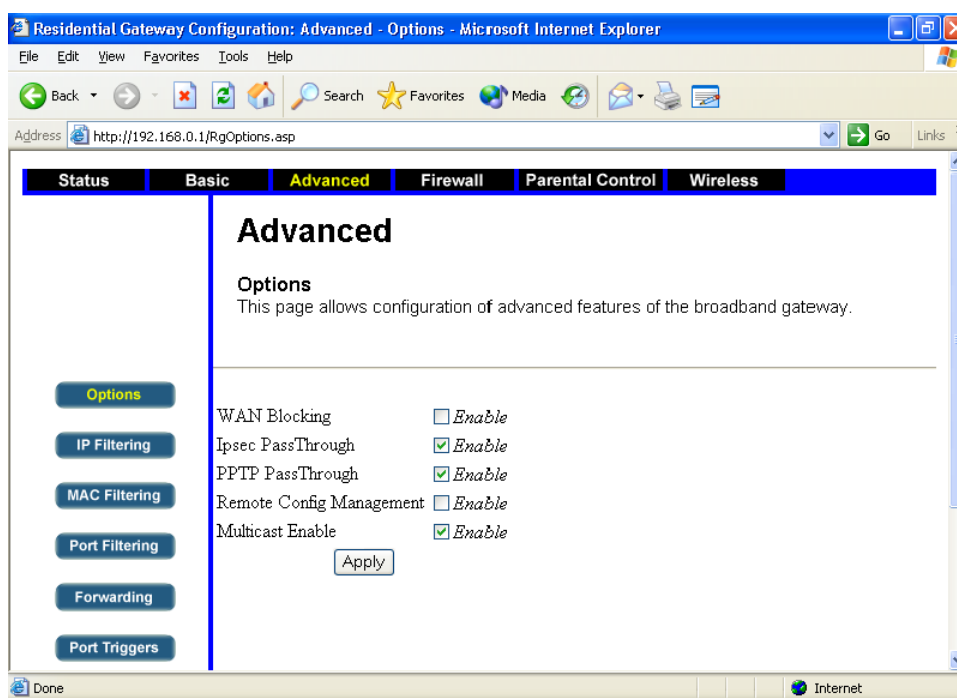
**Number of CPEs** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number can not be greater than 253 and the default is 245.

The DHCP Client Lease Info table displays the PCs that are given IP addresses by the CBW500. For each PC, the list shows the MAC Address, IP Address, Subnet Mask, Duration and Expires.

## 7.3 Advanced

### 7.3.1 Options

This page allows configuration of advanced features of the CBW500.



**WAN Blocking** By enabling the Block WAN feature, you can prevent your network from being pinged or detected by other Internet users. This feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network.

**IPsec PassThrough** IPsec (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPsec tunnels to pass through the CBW500, IPsec PassThrough is enabled by default.

**PPTP PassThrough** PPTP (Point to Point Tunneling Protocol) is the method used to enable VPN\* sessions to a Windows NT4.0, 2000 server. To allow tunnels to pass through the CBW500. The default setting is enable.

\*VPN (Virtual Private Networking) is a security measure that basically creates a secure connection between two remote locations.

**Remote Config Management** This feature allows you to manage your Gateway from a remote location, via the Internet. To enable this feature, tick Enable, and use the specified port (default is 8080) on your PC to remotely manage the CBW500. You must also change the CBW500's default password if you haven't already. A unique password will increase security.

To remotely manage the Router, enter `http://xxx.xxx.xxx.xxx:8080` (the x's represent the CBW500's Internet IP address, and 8080 represents the specified port) in your web browser's Address field. You will be asked for the CBW500's password. After successfully entering the password, you will be able to access the Gateway's web-based utility.

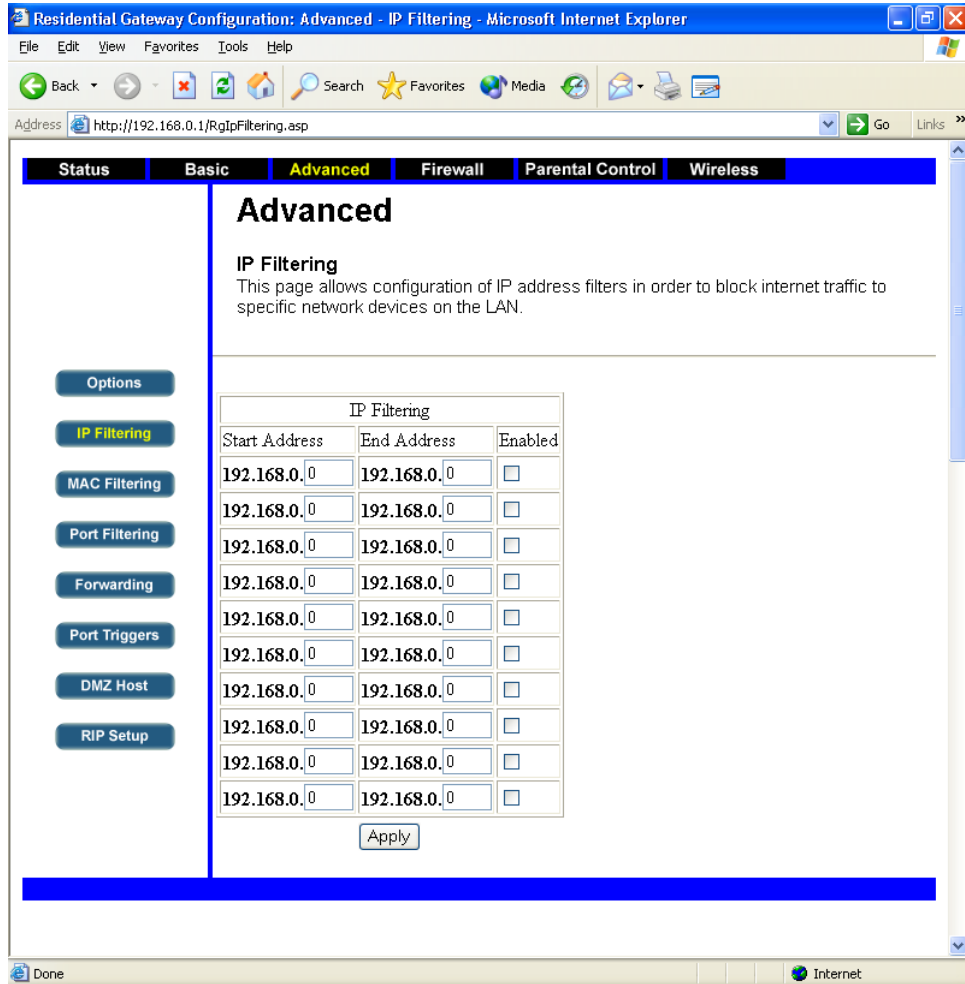
**Multicast Enable** IP Multicasting occurs when a single data transmission is sent to multiple recipients at the same time. With Multicast feature enable, the CBW500 allows IP multicast packets to be forwarded to the appropriate computers.



### 7.3.2 IP Filtering

This page allows configuration of IP address filters in order to block Internet traffic to specific network on the LAN.

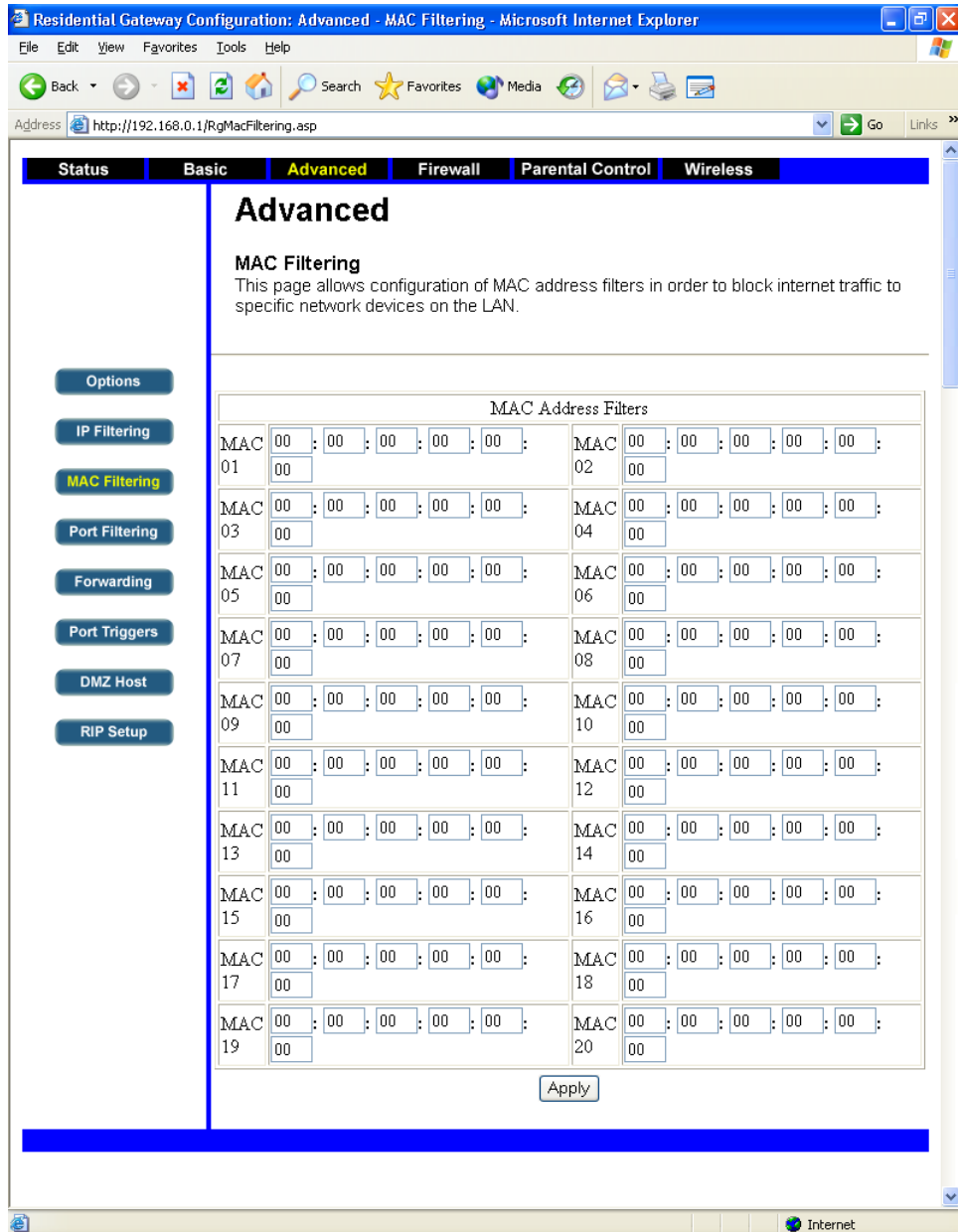
Tick Enable check box and enter the IP address or IP address range you want to block and then click **Apply** button.



### 7.3.3 MAC Filtering

This page allows configuration of MAC address filters in order to block Internet traffic to specific network on the LAN.

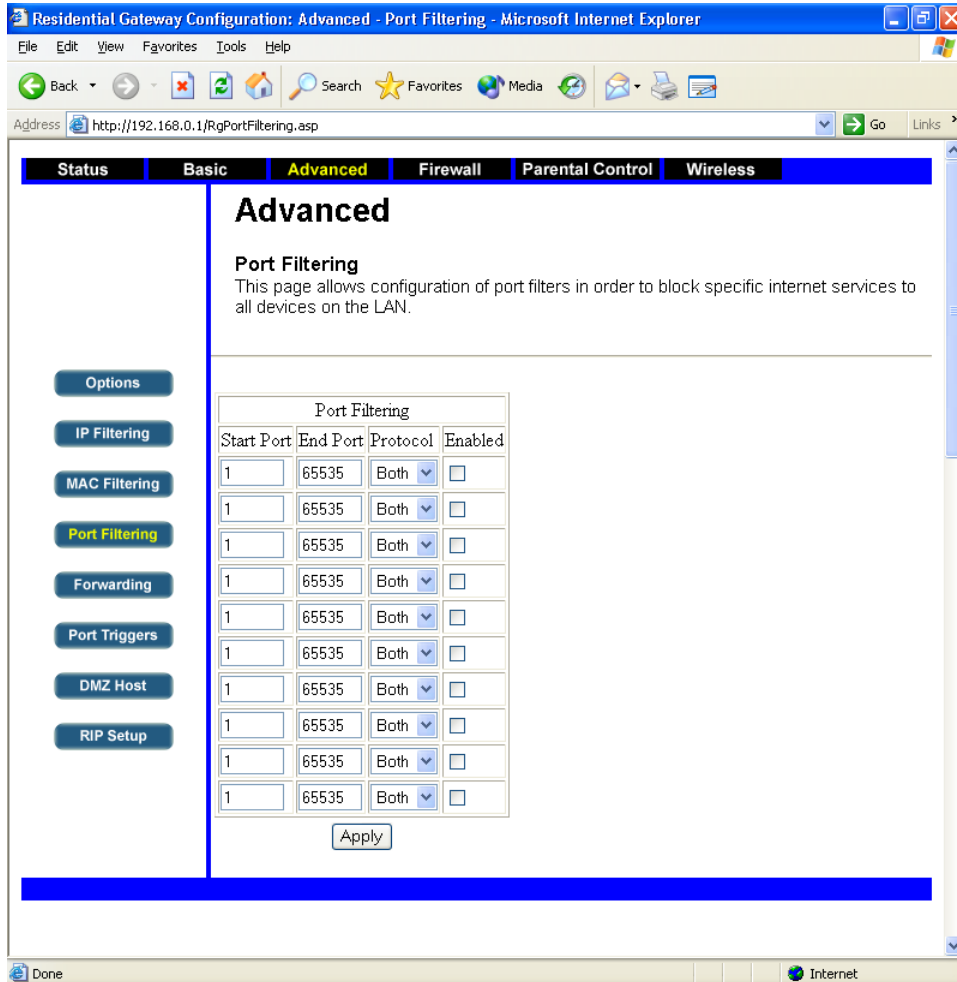
Enter the MAC address you want to block and then click **Apply** button.



### 7.3.4 Port Filtering

This page allows configuration of port address filters in order to block Internet traffic to specific network on the LAN.

Tick Enable check box and enter the port or port range you want to block. Select Protocol type and then click **Apply** button.



### 7.3.5 Forwarding

This allows for incoming requests on specific port numbers to reach web, FTP server and mail servers, etc. so they can be accessed from the public Internet.

The table on the right is commonly used port numbers.

Tick Enable check box and enter the Local IP address, port or port range you want to block. Select Protocol type and then click **Apply** button.

**Advanced**

**Forwarding**

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

Options

IP Filtering

MAC Filtering

Port Filtering

**Forwarding**

Port Triggers

DMZ Host

RIP Setup

Local IP Addr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Application Port

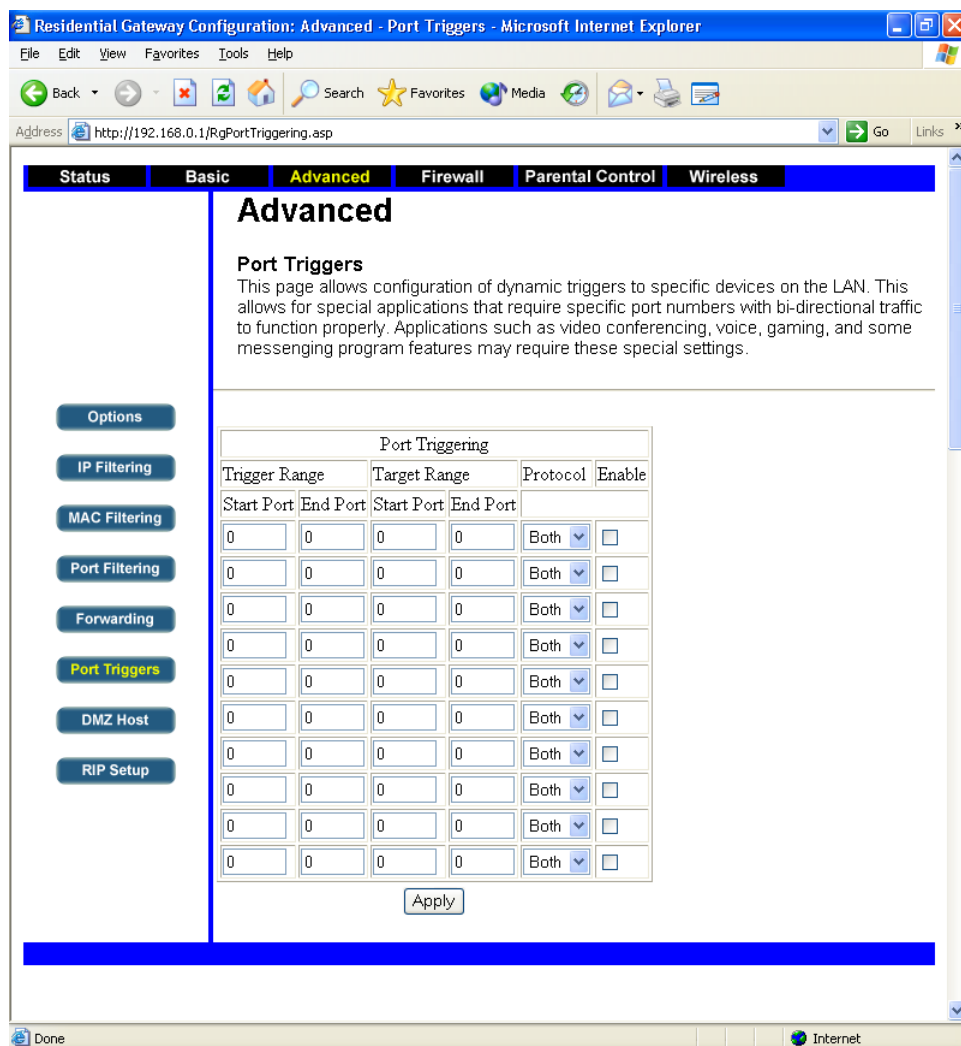
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NNTP	119
Telnet	23
IRC	194
SNMP	161
Finger	79
Gopher	70
Whois	43
rlogin	107
LDAP	389
UUCP	540

Apply

### 7.3.6 Port Triggers

This page allows configuration of dynamic triggers to specific devices on the LAN. It allows special applications that require specific port number with bi0directional traffic of function properly. Applications such as video conferencing, video, gaming, and some messaging program features may require these special settings.

Tick Enable check box and enter the trigger range, target range. Select Protocol type and then click **Apply** button.

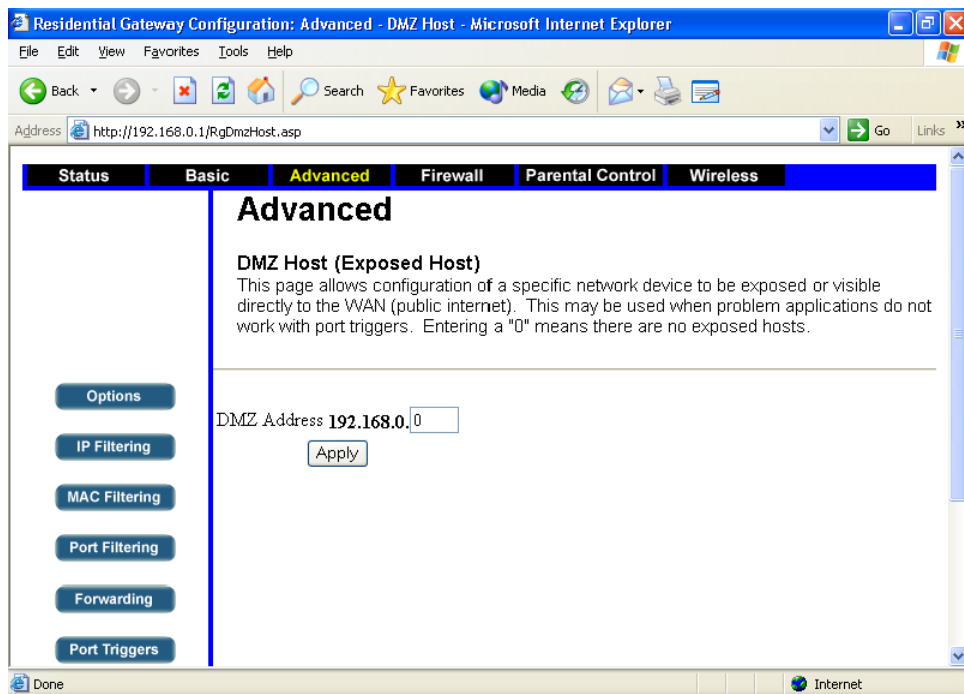


### 7.3.7 DMZ Host

This page allows configuration of a specific network device to be exposed or visible directly to the WAN (public Internet). This may be used when problem applications do not work with port triggers.

This may be necessary if the firewall is causing problems with an application such as a game or video conferencing application. However, since DMZ feature places the specify computer on your network outside of the firewall, use this feature on a temporary basis. The computer in the DMZ is NOT protected from hacker attacks.

Enter the last digits of its IP address in the IP field and then click **Apply**. Enter a "0" (default) means there are no exposed hosts.

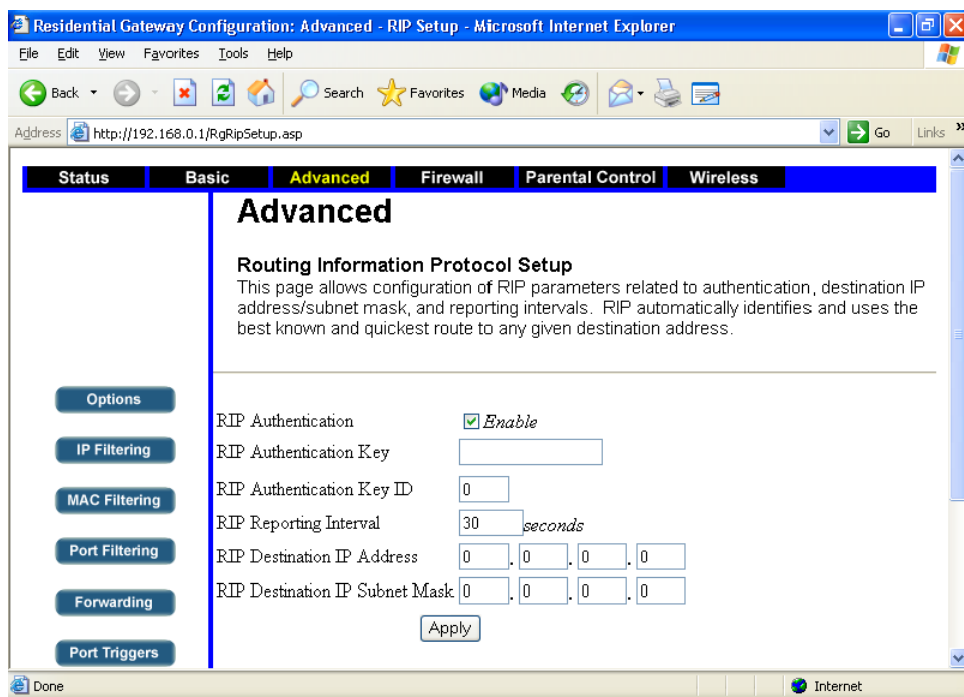


### 7.3.8 RIP Setup

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

You need to enable (default) RIP (Routing Information Protocol) feature and configure its related settings and then click **Apply**.

RIP determines a route based on the smallest hop count between source and destination. It is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.



## 7.4 Firewall

### 7.4.1 ToD Filter

This page allows configuration of web access filters to block all Internet traffic to and from specific network devices based on time of day settings.

Follow the instructions below to create the Time of Day (ToD) filters:

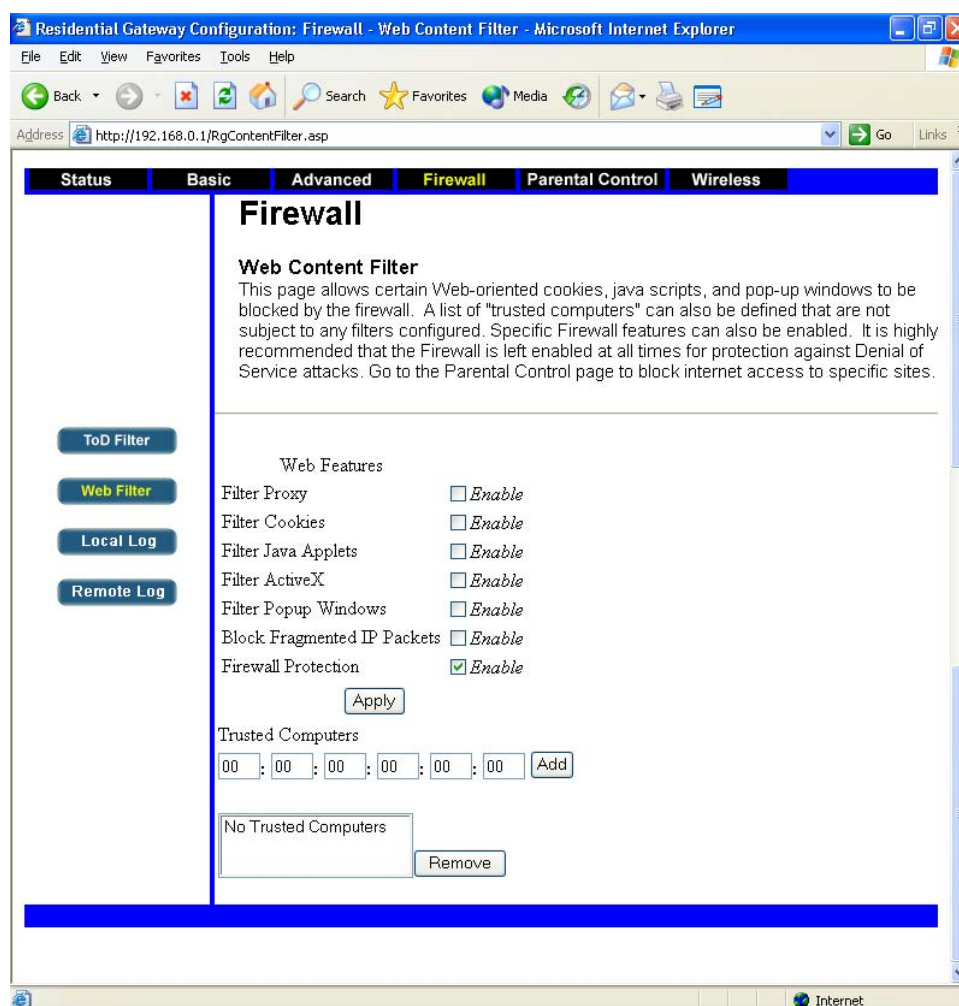
1. Indicate the MAC address in the field and then click **Add**.
2. Select the filter items from drop-down list and then tick the **Enabled** check box.
3. Set the days and/or time when access will be filtered and then click **Apply**.

The screenshot shows a web browser window titled "Residential Gateway Configuration: Firewall - ToD Filter - Microsoft Internet Explorer". The address bar shows "http://192.168.0.1/RgTodFilter.asp". The page has a navigation menu with tabs: Status, Basic, Advanced, Firewall (selected), Parental Control, and Wireless. The main content area is titled "Firewall" and contains a section for "Time of Day Access Filter". Below this section, there are several configuration options: a "ToD Filter" button, a "Web Filter" button, a "Local Log" button, and a "Remote Log" button. The "ToD Filter" section includes a form with six input fields for MAC address (00 : 00 : 00 : 00 : 00 : 00) and an "Add" button. Below this is a dropdown menu showing "No filters entered.", an "Enabled" checkbox, and a "Remove" button. The "Days to Block" section has checkboxes for "Everyday", "Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", and "Saturday". The "Time to Block" section has an "All day" checkbox and "Start" and "End" time pickers. The "Start" time is set to 12 (hour) 00 (min) AM, and the "End" time is set to 12 (hour) 00 (min) AM. An "Apply" button is located at the bottom of the configuration area.



## 7.4.2 Web Filter

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



**Filter Proxy** Use of WAN proxy servers may compromise the CBW500's security. Denying Filter Proxy will disable access to any WAN proxy servers.

**Filter Cookies** A cookie is data stored on your PC and used by Internet sites when you interact with them.

**Filter Java Applets** Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language.

**Filter ActiveX** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language.

**Filter Popup Windows** Deny to open popup windows trigger form Internet.

**Block Fragmented IP Packages** Block the IP packages that been cut into smaller units when transmitting over a network medium.

**Firewall Protection** Firewall feature will protect your network from a wide array of common hacker attacks.

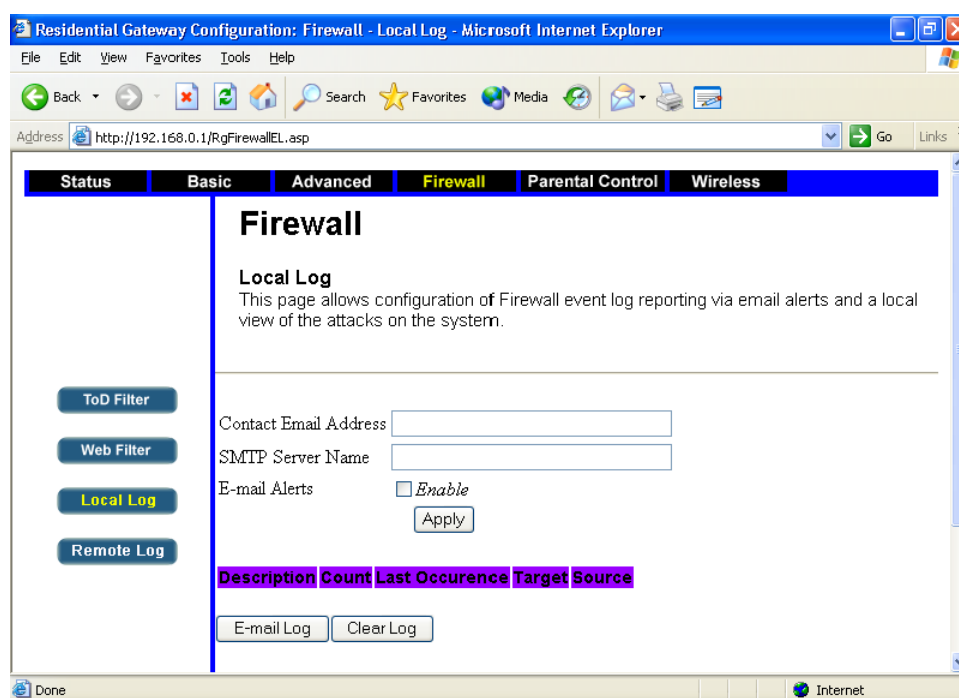
### 7.4.3 Local Log

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

Follow the instructions below to create the Time of Day (ToD) filters:

1. Enter the contact Email Address and SMTP Server Name.
2. Tick the **Enabled** check box and then click **Apply**.

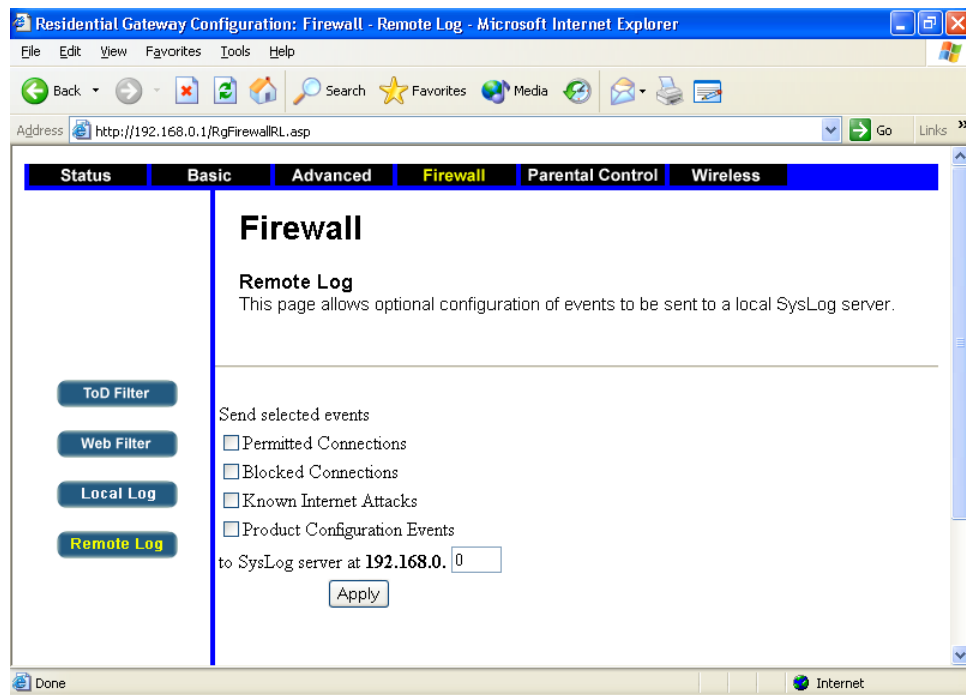
The event logs will be listed in the table in this page.



## 7.4.4 Remote Log

This page allows optional configuration of events to be sent to a local system log server.

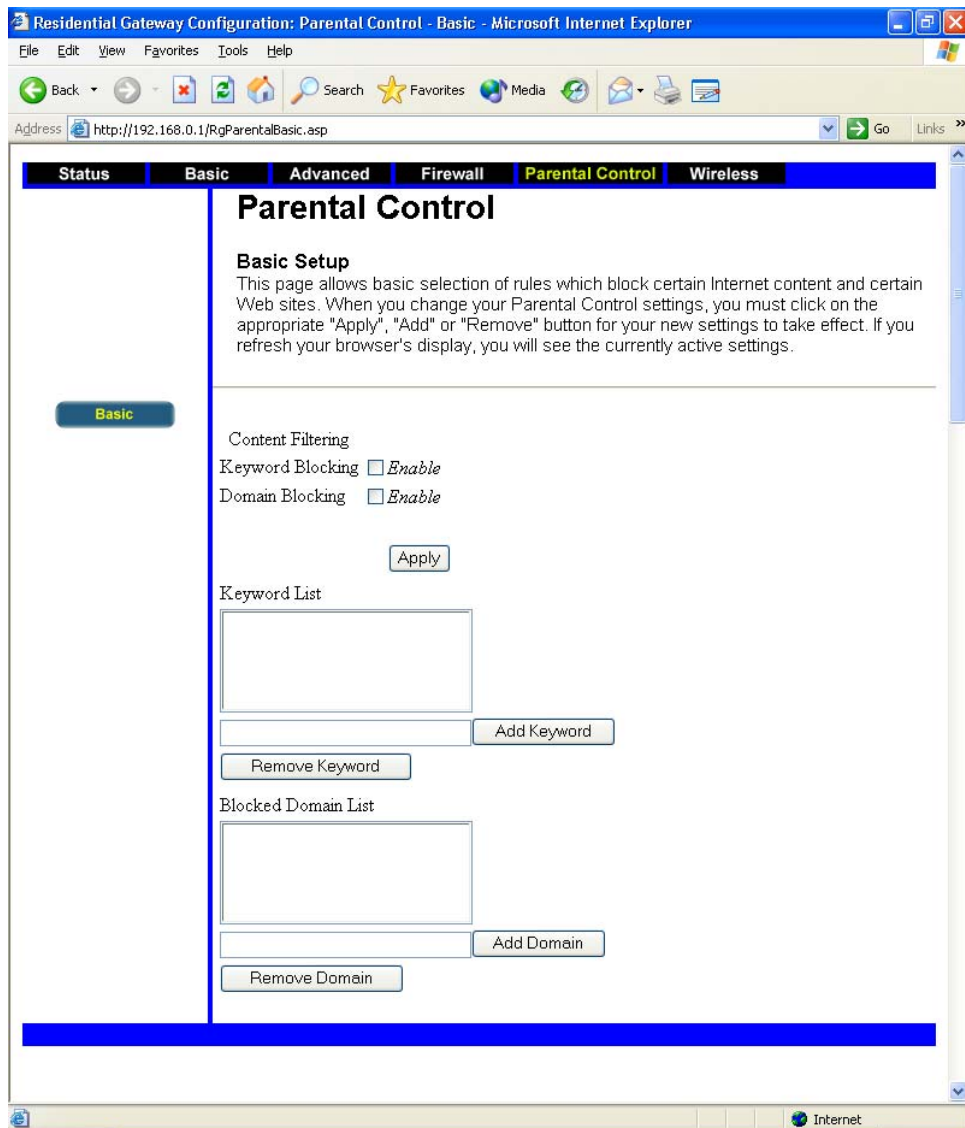
Tick the events you want to be sent to the system log server and indicate the system log server's IP address and then click **Apply** to active remote log feature.



## 7.5 Parents Control

### 7.5.1 Basic

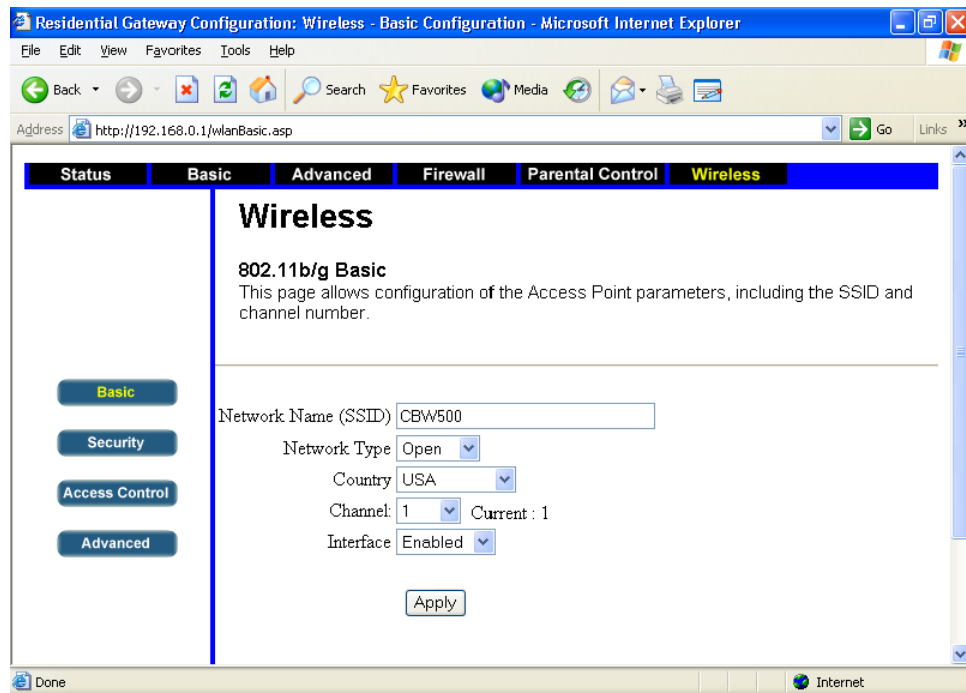
This page allows basic selection of rules which block certain Internet content and Web sites. When you change your Parental Control settings, you must click on the appropriate “Apply”, “Add” or “Remove” button for your new settings to take effect. Refresh your browser to see the currently active settings.



## 7.6 Wireless

### 7.6.1 Basic

This page allows configuration of the AP (Access Point) parameters, including the SSID and channel number.



**Network Name (SSID)** SSID (Service Set Identifier) is a unique identifier for your wireless network. You must have the same SSID entered into the CBW500 and each of its wireless clients. The default SSID is **CBW500**.

**Network Type** Select **Open** to indicate the network as an open network system and select **Closed** to indicate the network as a closed network system.

**Country/Channel** Select your region and proper channel. Channel is a similar concept to any radio device. The CBW500 allows you to choose different radio channels in the wireless spectrum.

<b>Regional</b>	<b>Channel</b>
North American	1-11
Japan	1-14
European (ETSI)	1-13
Spain	10-11
France	10-13

Enter the correct channel in field to correspond with your network settings. All devices in your network must set to the same channel in order to function properly.

## 7.6.2 Security

This page allows configuration of the WEP keys and/or passphrase. CBW500 is equipped with WPA (Wireless Protected Access), the latest security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). You must first determine which standard you want to use and then configure the related settings.

**Note:** To use WPA security, all your clients must be upgraded to drivers and software that support it. A free security patch download is available from Microsoft. This patch works only with the Windows XP. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers.

The screenshot displays the 'Wireless' configuration page in a Microsoft Internet Explorer browser window. The browser's address bar shows the URL 'http://192.168.0.1/wlanSecurity.asp'. The page has a blue header with navigation tabs: 'Status', 'Basic', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Wireless' tab is selected. The main content area is titled 'Wireless' and includes a sub-section '802.11b/g Privacy' with the text: 'This page allows configuration of the WEP keys and/or passphrase.' On the left side, there is a vertical menu with buttons for 'Basic', 'Security', 'Access Control', and 'Advanced'. The 'Security' button is highlighted. The main configuration area contains the following fields and controls:

- Network Authentication: 802.1x (dropdown menu)
- WPA Pre-Shared Key: [text input field]
- WPA Group Rekey Interval: 0 (text input field)
- RADIUS Server: 0.0.0.0 (text input field)
- RADIUS Port: 1812 (text input field)
- RADIUS Key: [text input field]
- Data Encryption (WEP): Off (dropdown menu)
- Shared Key Authentication: Optional (dropdown menu)
- PassPhrase: [text input field] with a 'Generate WEP Keys' button to its right
- Network Key 1: [text input field]
- Network Key 2: [text input field]
- Network Key 3: [text input field]
- Network Key 4: [text input field]
- Current Network Key: 1 (dropdown menu)
- An 'Apply' button is located at the bottom center of the configuration area.

The browser's status bar at the bottom shows 'Done' on the left and 'Internet' on the right.

There are two types of WPA security: WPA Pre Shared Key (without server) and WPA (with server).

WPA Pre Shared Key uses a so-called pre-shared key as the security key. A pre-shared key is a password. Each client uses the same key to access the network. Typically, this mode will be used in a home environment.

WPA (with server) is a configuration when there is a radius server distributes the keys to the clients automatically. This is typically used in a business environment.

### **Network Authentication**

**802.1x** 802.1x authentication protocol allows users to authenticate into a wireless network by means of a RADIUS Server. In standard Wi-Fi, 802.1x authentication is optional but a requirement for WPA.

**WPA Pre-Shared Key** This can be from 8 to 40 characters and can be a combination of letters, numbers, and other characters. This same key must be used on all of the clients that you set up.

**WPA Group Rekey Interval** Rekey interval is how often the keys are distributed (in packets).

**RADIUS Server/Port/Key** Use a RADIUS (Remote Authentication Dial-In User Service) server to distribute keys to the clients. You also need to configure RADIUS port and Key. All the clients must set to match these settings.

**Data Encryption (WEP)** WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm. Wireless device without a valid WEP key may be excluded from network traffic. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

**Shared Key Authentication** Select **Optional** or **Required** for the sender and the receiver use a WEP key for authentication.



**PassPhrase** Passphrase is used much like a password. It simplifies the WEP encryption process by automatically generating the WEP keys for the CBW500. A passphrase is an easy way to generate hexadecimal keys. Enter any word, up to 30 characters, and then click **Generate WEP Keys** button, or manually typing up to four keys. If your wireless cards support passphrase, you can enter the same passphrase on all the wireless cards. Or you may also manually enter the key elements into the setting table.

In 64-bit WEP, the passphrase will generate 4 different keys. However, in 128-bit WEP, this method only generates 1 key which is replicated for all 4 keys. The passphrase can be up to 30 characters long and may contain any alphanumeric characters.

**Network Key 1-4** WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"- "9" and "A"- "F".

If you encounter any difficulty when you enable WEP ensure that you check each key on your wireless computer is exactly the same as each key on the CBW500. In other words, Key 1 on the wireless computer must have the same Hexadecimal number as Network Key 1 on the CBW500, Key 2 on the wireless computer must match Network Key 2 on the CBW500 and so on.

**Current Network Key** Show the Network key in use.

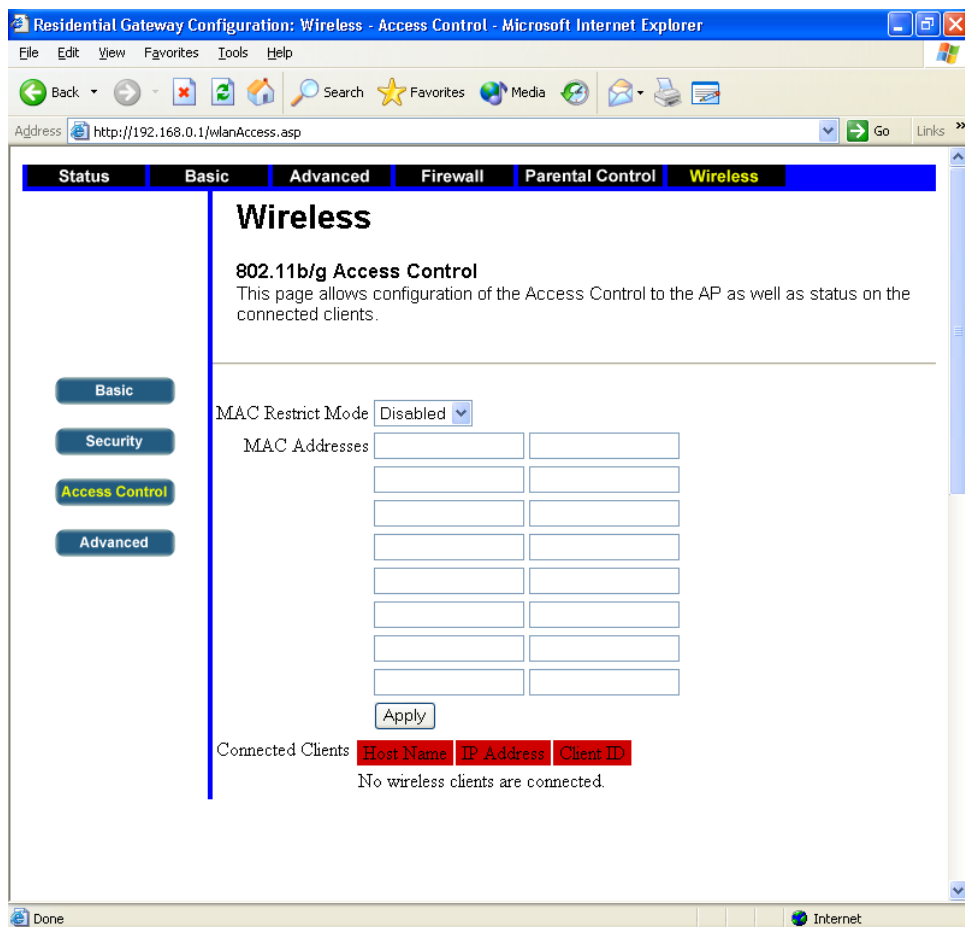
### 7.6.3 Access Control

This page allows configuration of the Access Control to the AP as well as status on the connected clients.

Access Control allows you to control which wireless-equipped PCs may communicate with the CBW500 according to their MAC addresses.

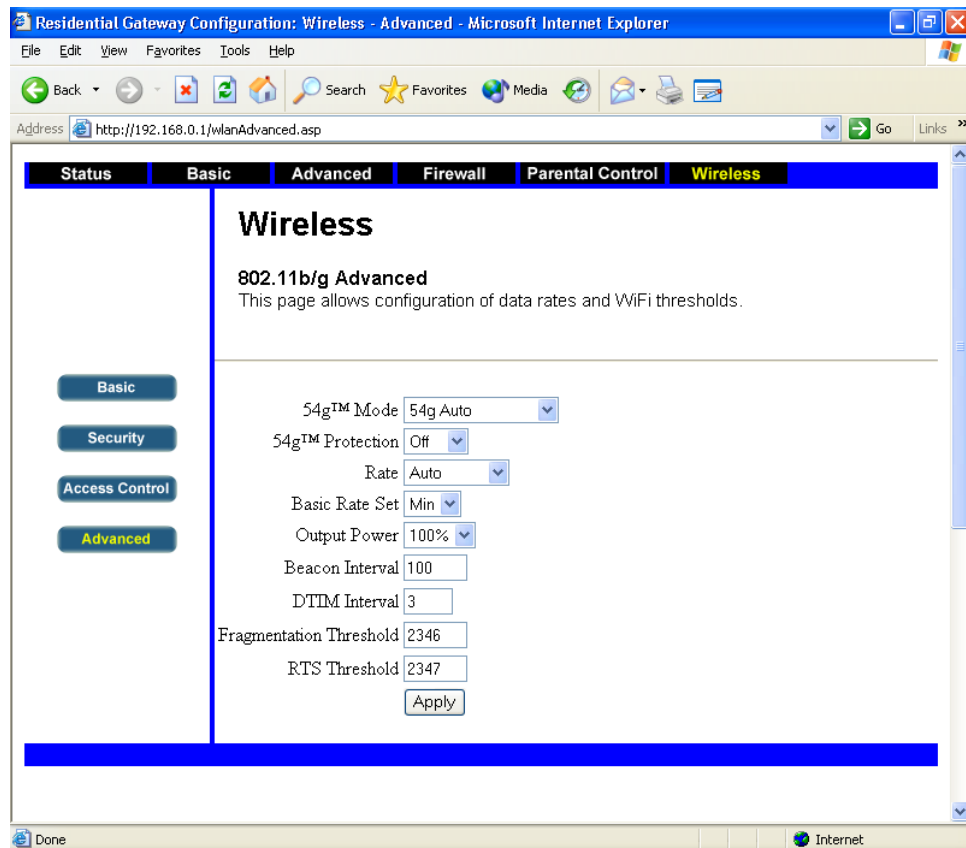
The number is up to a maximum of 80 MAC addresses.

Select the MAC Restrict Mode (**Allow** or **Deny**) and indicate the MAC address in the field and then click **Apply**.



## 7.6.4 Advanced

This page allows configuration of data rates and Wi-Fi thresholds.



### 54g™ Mode

**54g Auto** In this mode, the CBW500 is compatible with 802.11b and 54g wireless clients simultaneously. This is the factory default mode and ensures successful operation with all Wi-Fi-compatible devices. If you have a mix of 802.11b and 54g clients in your network, we recommend you set the CBW500 to 54g-Auto mode. This setting should only be changed if you have a specific reason to do so.

**54g Only** 54g-Only mode works with 54g clients only. This mode is recommended only if you want to prevent 802.11b clients from accessing your network.

**54g LRS** It is recommended that DO NOT use this mode unless you have a very specific reason to do so. 54g LRS (Limited Rate Support) mode exists only to solve unique problems that may occur with some 802.11b client adapters and is NOT necessary for interoperability of 54g and 802.11b standards.

Note: In some cases, older 802.11b clients may not be compatible with 54g wireless. These adapters tend to be of inferior design and may use older drivers or technology. 54g-LRS allows these clients to be compatible with the newer 54g technology. Switching to this mode may solve problems that sometimes occur with these clients. If you suspect that you are using a client adapter that falls into this category of adapters, first check with the adapter vendor to see if there is a driver update. If there is no driver update available, switching to 54g-LRS mode may fix your problem. Please note that switching to 54g-LRS mode may decrease 54g performance slightly.

**802.11b Only** Use 802.11b Mode only. The maximum data transfer rate of 802.11b standard is 11Mbps.

**54g™ Protection** Protected mode ensures proper operation of 802.11g clients and access points when there is heavy 802.11b traffic in your operating environment. When protected mode is Auto, 802.11g scans for other wireless network traffic before it transmits data. Therefore, using this mode in environments with heavy 802.11b traffic or interference achieves best performance results. If you are in an environment with very little, or no other wireless network traffic, your best performance will be achieved with Protected mode Off.

**Rate** The basic transfer rates should be set depending on the speed of your wireless network. You have to select 1-2Mbps if you have older 802.11 compliant equipment on your network, such as wireless adapter that support only 1 or 2 Mbps. Otherwise, you do not have to limit the basic transfer rates of faster adapters. CBW500 adaptively selects the highest possible rate for transmission. The system will step down in case of obstacles or interference.

**Beacon Interval** The default beacon interval is 100 milliseconds. A beacon is a short frame that is sent from the AP (Access Point) to stations in order to organize and synchronize wireless communication on the WLAN (Wireless LAN). A beacon includes the wireless LAN service area, the AP address, the broadcast destination addresses, a time stamp and DTIM (Delivery Traffic Indication Message). Enter a value between 1 and 65,535 (milliseconds). This value indicates the frequency interval of the beacon.

**DTIM Interval** DTIM (Delivery Traffic Indication Maps) Interval's range is 1 to 65535 milliseconds and the default setting is set to 1. DTIM informs clients of the next window for listening to broadcast and multicast messages. When CBW500 has buffered broadcast or multicast messages for associated clients, it sends the DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

**Fragmentation Threshold** The range is 256 to 2346 bytes. This value should remain at its default setting of 2346. Fragmentation mechanism is used for improving the efficiency when there is heavy traffic within the wireless network. If you transmit large files in a wireless network, you can enable this function and specify the packet size. The mechanism will split the packet according to the packet size you set. But setting Fragmentation threshold too low may cause poor network performance.

**RTS Threshold** RTS (Request to Send) Threshold is transmitters contending for the medium may not be aware of each. If the packet size is smaller than the setting RTS Threshold size, the RTS/CTS (Clear to Send) mechanism will not be enabled. The CBW500 sends RTS frames to a particular receiving station and negotiates the sending of a data frame. After receiving a RTS, the station responds with a CTS frame to acknowledge their right of transmission. This value should remain at its default setting of 2,347, although the range is 256 to 2,432 bytes. Setting this parameter to a small value will cause packets to be sent more often and will consume more available bandwidth and reduce throughput. However, a higher value will send more packets less often. Keep this default setting is recommended.

## 8 Troubleshooting

### Basic Connection

- Check that the CBW500 is connected to your computers and the Cable modem as well as all the equipment is powered on. Check that the LAN and WAN port link status LEDs are lighted, and that any corresponding LEDs and the network adapter are also lighted.
- Ensure that the computer have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable.

### Browsing Configuration Utility

- Confirm that the physical connection between your computer and the CBW500 is OK.
- Ensure that you have configured your computer correctly (refer to chapter 6). Reboot your computer while it is connected to the CBW500 to ensure your computer receives an IP address.
- Ensure that you include the full URL including the prefix `http://` (eg. <http://192.168.0.1>)
- If you cannot browse the CBW500, use `winiipcfg` (for Windows95/98/ME) or `inconfig` (for Windows 2000/XP) utility to verify that your computer has received the correct address information from the CBW500. Check the computer has an IP address of the form `192.168.0.XXX` (where XXX is in the range 2-254), the subnet mask is `255.255.255.0`, and the default Gateway is `192.168.0.1` (the address of the CBW500). If these are not correct, use the Release and Renew functions to obtain a new IP address from the CBW500.
- Ensure that your computers are not configured to use a proxy server. If you do, disable this proxy server temporary. It can be found under Internet Explorer>Tools>Internet Options>Connections tab>LAN Settings.

### **Connecting to the Internet**

- Confirm that the physical connection between the Cable modem and CBW500 is OK, and the link status LEDs on both CBW500 and Modem are lighted.
- Confirm that the connection between the Cable modem and its interface is OK.
- Ensure that you have entered the correct information into the CBW500 configuration screen as required by your ISP.

### **Forgotten Password**

- You need to reset the CBW500 to its factory default settings if you do not know or have forgotten the logging password. And all your configuration changes will be lost if you reset the CBW500. You may need to reinstall the USB driver before you can perform a connection to Internet if you connect the CBW500 to PC via USB interface. Please refer to chapter 4 for reset description.

### **Wireless Network Connection**

- Ensure that you have a 802.11b/g wireless adapter for each wireless computer, and is correctly installed and configured.
- Verify that your wireless computers are configured to work in Infrastructure mode and not AdHoc mode. The CBW500 is designed to operate in Infrastructure mode. AdHoc mode is not supported by the CBW500.
- Check the status of the WLAN LED, it should be lit if wireless connection is performed.
- Ensure that the wireless clients are using the same SSID as the CBW500. The SSID is case-sensitive.
- Ensure that you are using the same level of security on all of your wireless computers (Off, 64 or 128 bit) and all devices are using the same keys and the same order of keys.
- Ensure that you have the wireless computers enabled in the list of allowed MAC addresses if you are using Wireless Access control feature.

- If you are having problem connecting or are operating at a low speed try to change the antenna positions of the CBW500. For more effective coverage you can try to re-orientate your antenna. Place one antenna vertically and the other horizontally to improve the coverage. In addition, moving the wireless computer closer to the CBW500 to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem, consider relocating the wireless computer or the CBW500 or try a different channel on the CBW500.
- 2.4 GHz ISM band is used for 802.11b/g and you may have other devices at your location that operate in the frequency band. You should take care to ensure that there are no devices such as microwave ovens close to the wireless computer or the CBW500. It could affect receiver sensitivity and reduce the performance of your wireless network.
- Most wireless computer adapters will scan the nearby channels. If a wireless computer does not connect to the channel of the CBW500 then try to initiate a search manually or manually set the channel on your wireless computer to correspond to the CBW500's channel.
- The 802.11g standard will automatically choose the best speed depending on the quality of the connection. The speed falls back to a lower speed if the signal quality weakens. Generally, the closer you are to the CBW500 the better speed you will obtain. If your are not achieving the speed you had anticipated then try to adjust the antennas or move the wireless computer closer to the CBW500. In an idea network, the CBW500 should be located on the center of the network with wireless computers distributed around it.



## 9 Technical Specification

Hardware Specifications	
<b>Cable</b>	F-type Connector
<b>LAN</b>	1 or 4 Ethernet 10/100 Mbps auto-MDI/MDIX, RJ-45 ports
<b>WLAN</b>	802.11g module as AP in MiniPCI Interface
<b>LED (1-Port Model)</b>	Power / Cable / WLAN / USB / LAN1-4
<b>LED (4-Port Model)</b>	Power / Cable / WLAN / USB / LAN

WLAN 802.11g	
<b>Host Interface</b>	MiniPCI TYPE III B
<b>Frequency Band</b>	2.400 ~ 2.4835 GHz (subject to local regulations)
<b>Spreading</b>	DSSS (Direct Sequence Spread Spectrum)
<b>Security</b>	WPA support and Internal engine for 64-bit / 128-bit WEP Encryption
<b>Operating Range</b>	Open Space: 100 - 400m Indoor: 30m - 100m
<b>Supported Bit Rate</b>	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54Mbps
<b>Modulation</b>	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK and CCK
<b>Antenna</b>	Internal dipole antenna
<b>Receiver Sensitivity</b>	1E-5@-83dBm
<b>Power</b>	TX power consumption <280mA
<b>Consumption</b>	RX power consumption <220mA
<b>Transmit Power</b>	15dBm±2dBm
<b>Operation Power</b>	DC 3.3V
<b>Roaming</b>	Full mobility and seamless roaming from cell to cell and across Access Point
<b>OS Compatibility</b>	Windows 98/2000/ME/XP
<b>Operating Channels</b>	USA and Canada 1-11 channels European (ETSI) 1-13 channels Japan 1- 14 channels Spain 10-11 channels France- 10-13 channels
<b>Operating Environment</b>	Temperature : 0~50°C for working ; -10~65°C for storing Humidity : 5%~95% ( non-condensing )

## Software Specifications

<b>Routing</b>	<ul style="list-style-type: none"><li>● DNS relay / DHCP server / RIP I&amp;II</li></ul>
<b>Internet Sharing</b>	<ul style="list-style-type: none"><li>● NAT / NAPT / DHCP server / DNS relay</li></ul>
<b>Application protocol</b>	<ul style="list-style-type: none"><li>● SNMP v1/v2/v3, TELNET, TFTP, DHCP Server / Client (up to 253 CPEs)</li></ul>
<b>Network protocols</b>	<ul style="list-style-type: none"><li>● PPPoE, ARP, TCP/IP, DNS proxy, RIP I&amp;II, NAT, NAPT</li><li>● Ping tool via ICMP</li><li>● Speed test tool via UDP</li></ul>
<b>Firewall</b>	<ul style="list-style-type: none"><li>● Stateful Packet Inspection (SPI)</li><li>● Application Level Gateway modules (ALGs)</li><li>● Denial of Services (DoS) and defense against common hacker attacks</li></ul>
<b>Baseline Privacy</b>	<ul style="list-style-type: none"><li>● 40-bit/56-bit DES with RSA key management</li></ul>
<b>DHCP Client</b>	<ul style="list-style-type: none"><li>● DHCP server: LAN DHCP service with and without WAN connection</li><li>● DHCP client: Automatically gets IP and DNS server address from DHCP server at ISP</li></ul>
<b>DNS Server</b>	<ul style="list-style-type: none"><li>● Resolve local host name &amp; return referral upon non-resolution</li></ul>
<b>ToD (RF868)</b>	<ul style="list-style-type: none"><li>● ToD support for local and MSO time synchronization</li></ul>
<b>TFTP Client</b>	<ul style="list-style-type: none"><li>● TFTP support for cable modem configuration file download</li></ul>
<b>Network Protocol</b>	<ul style="list-style-type: none"><li>● Address translation of NAT, NAPT, C-NAT, C-NAPT</li><li>● CableHome QoS Portal</li><li>● Ping tool via ICMP</li><li>● Speed test tool via UDP</li><li>● IP, TCP, ARP RIP</li></ul>
<b>Management</b>	<ul style="list-style-type: none"><li>● Web-based Management Interface utility and Telnet Management utility</li><li>● Controlled MIB access via SNMP v1/v2/v3</li><li>● DOCSIS NmAccess (v1/v2) Coexistence (v1/v2/v3) operation</li><li>● Even configuration and generation</li><li>● PS and FW config file download</li><li>● WAN management IP address and data IP address acquisition</li><li>● Storage and MIB access to DHCP information</li><li>● DHCP and SNMP driven provisioning mode</li></ul>