

# Wireless-G Router User's Guide

# Table of Contents

## **Chapter 1: Introduction**

Installing Your Router  
System Requirements  
Installation Instructions

## **Chapter 2: Preparing Your Network**

Preparing Your Network  
Configuring Windows for IP Networking  
Collect ISP Information

## **Chapter 3: Configuring the Router's Basic Functions**

Basic Functions  
Setup  
Global Address  
Wireless  
Tools  
Status  
DHCP  
Log  
Statistic

## **Chapter 4: Configuring the Router's Advanced Functions**

Advanced Functions  
Virtual Server  
Filters  
IP/URL Block  
Special Apps  
DMZ Host  
MAC Clone  
Dynamic DNS  
Proxy DNS

# Chapter 1: Introduction

## · Installing Your Router

In this chapter, you'll learn how to connect your router.

## · System Requirements

- One or more PCs (desktop or notebook) with Ethernet interface
- Broadband Internet access
- Ethernet cables
- Wireless interface (if planning to use wireless functions)

## · Installation Instructions

Connecting the Router:

1. Make sure all **systems are** turned off, including the router, PC(s), and the cable or DSL modem (if applicable).
2. Connect the **WAN port** on the router to your cable/**DSL** modem, Ethernet Server, or hub.
3. Connect one or more client PCs to the **LAN port(s)**.
4. Connect the power adapter (5VDC, 2A) to the **power jack** on the router. Then, plug the power cable into an outlet.
5. Turn on your PC(s).

# Chapter 2: Preparing Your Network

## · Preparing Your Network

In this chapter, you'll learn what to do before configuring your router.

Before you can configure your router, you need to set up all the computers on your network for TCP/IP networking. You also need to know certain information from your ISP.

## · Configuring Windows for IP Networking

You need to configure each computer in your network for TCP/IP networking. If you plan to use the DHCP feature (recommended), you should configure each computer to receive an IP address automatically. See the procedure below for instructions.

If you don't plan to use DHCP, you'll need to manually assign an IP address to each computer. Refer to your Windows documentation for instructions on how to do this.

To configure Windows to receive dynamic IP address:

### Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network** icon.
2. On the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. Click the **Properties** button.



3. Click the **IP Address** tab. Select **Obtain an IP address automatically**



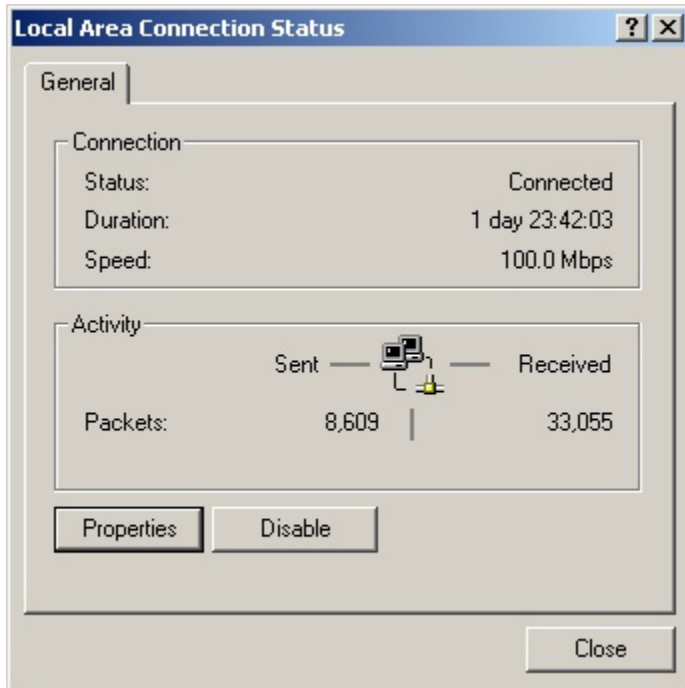
4. Now click the **Gateway** tab, and verify that the *Installed Gateway* field is blank. Click the **OK** button.

5. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CDROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (if "D" is the letter of your CD-ROM drive).

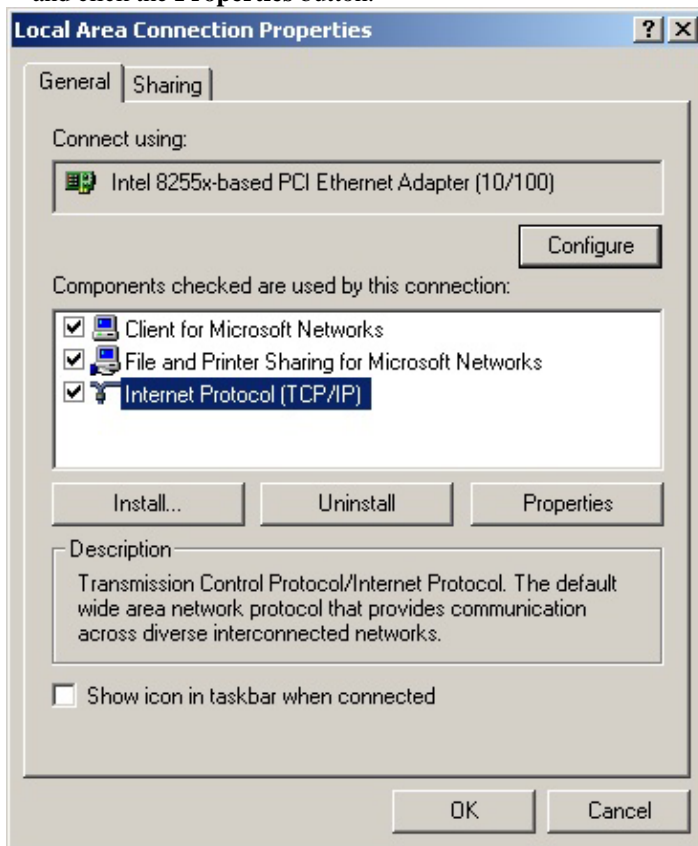
6. Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

## Configuring Windows 2000 PCs

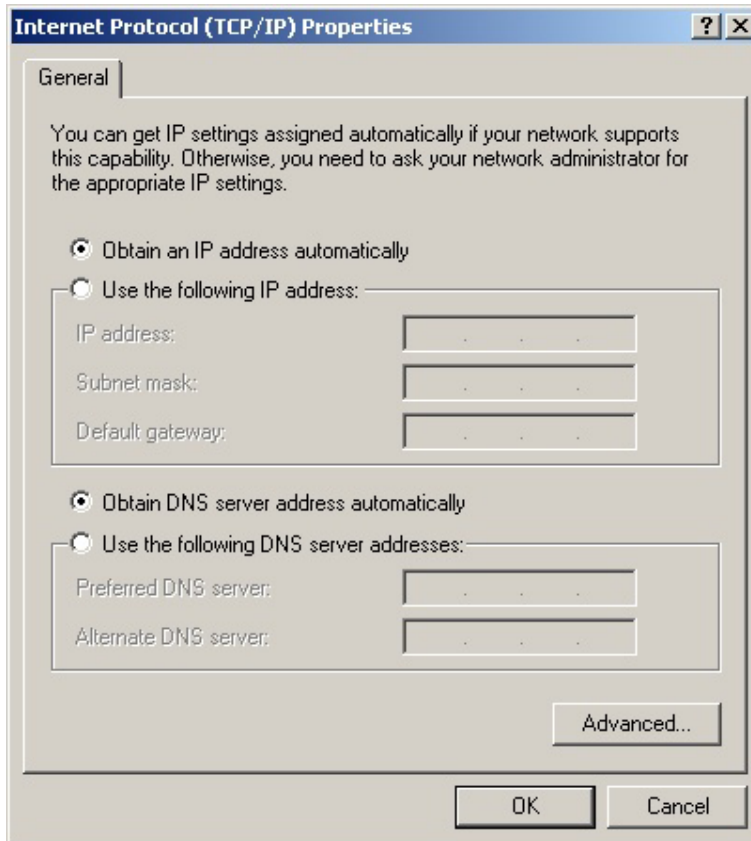
1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network and Dial-up Connections** icon.
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button



3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



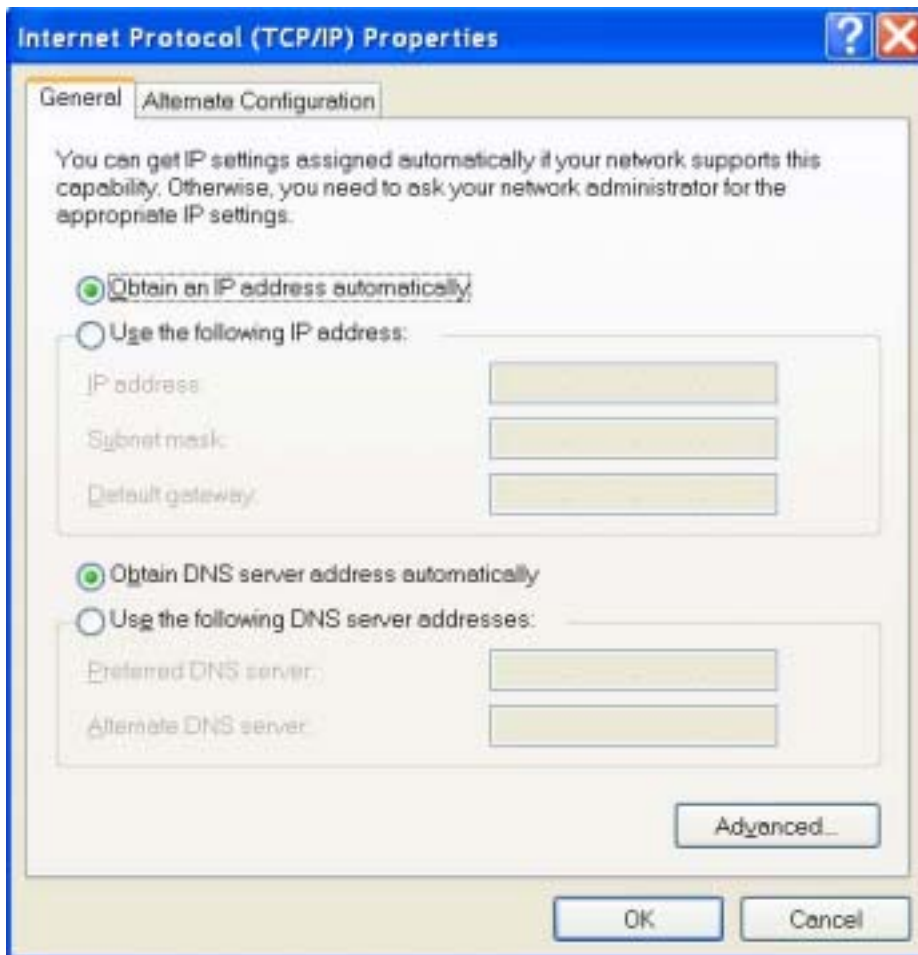
5. Restart your computer.



## Configuring Windows XP PCs

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

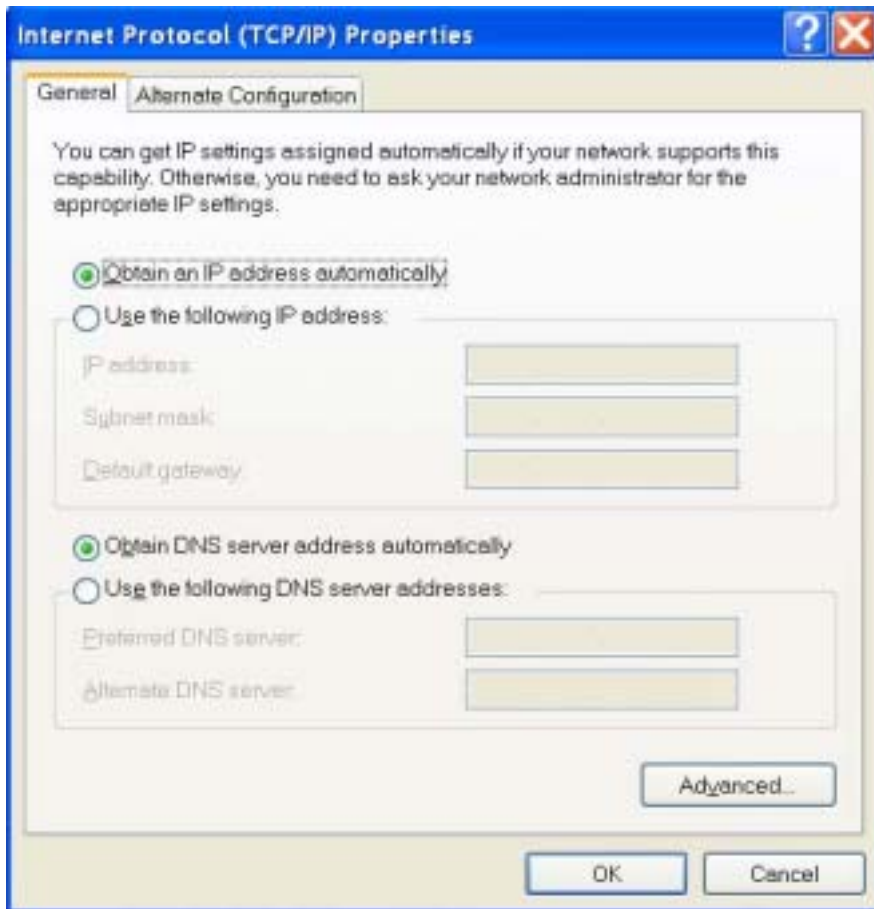
1. Click the Start button and then the Control Panel icon. Click the Network and Internet Connections icon. Then click the Network Connections icon.
2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



## Collecting ISP Information

The following information needs to be gathered from the ISP before you can configure your router:

- Has your ISP assigned you a static IP address, or will they assign one to you dynamically?  
If they have given you a static IP, what is it?
  - Does your ISP use PPPoE? If so, what is your PPPoE username and password?
- Call your ISP if you're not sure of the answers to these questions.

## Chapter 3: Configuring the Router's Basic Functions

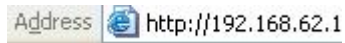
### Basic Functions

Basic administrative functions include Setup, Global Address, Wireless, Tools, Status, DHCP, Log, and Statistics.

The Wireless-G Router comes with a web-based tool that you can use to set up and customize the router settings. You can access this tool from any computer on your network.

#### To open the web-based Admin Tool:

1. Open a browser on your PC.
2. Type `http://192.168.62.1` in the **Address** field:



A logon dialog box will appear:



3. Type **admin** in the User Name field. Then, type a Password and click OK. The default password is **1234**.  
The Wireless-G Router Admin Tool will appear

## Setup

The Setup screen shows the basic configuration parameters for your router, such as Host Name, LAN IP Address, and PPPoE Login. Although most users will be able to accept the default settings, every Internet Service Provider (ISP) is different. Check with your ISP if you're not sure which settings they require.

The Setup screen is shown in the figure below.

**SOHO Router**

Setup Global Address Wireless Tools Status DHCP Log Statistics Advanced Help

**Host Name:**  (Required by some ISPs)

**Domain Name:**  (Required by some ISPs)

**Firmware Version:** 20-07-00, Dec 10 2003 21:36:43

**Time:** Thu Jan 1 16:36:06 1970

**Set Time Zone:** (GMT-08:00)Pacific Time(US&Canada)Tijuana

**Daylight Savings:**  Enable  Disable

**Daylight Period:** JAN 01 - JAN 01

**LAN IP Address:**

LAN IP Address: 192 . 168 . 62 . 1

Subnet Mask: 255 . 255 . 255 . 0

**WAN IP Address:**  Obtain an IP Address Automatically

Specify an IP Address

WAN IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

ISP Gateway Address: 0 . 0 . 0 . 0

DNS: 1) 0 . 0 . 0 . 0

2) 0 . 0 . 0 . 0

3) 0 . 0 . 0 . 0

**PPPoE Login:**  Enable  Disable

User Name:

Password:

Connect on Demand  Connect Manually

Use the Setup screen to configure your SOHO Router. Although most users will be able to accept the default settings, every Internet Service Provider (ISP) is different. Check with your ISP if you're not sure which settings they require.

### To configure Setup parameters:

1. Type the **Host Name** (optional). This value is sometimes called System Name or Account Name. Check with your ISP if you're not sure whether to provide this information.
2. Type the **Domain Name** of your ISP, such as xyz.isp.com (optional). Check with your ISP if you're not sure whether to provide this information.
3. Review the **Firmware Version**. This value tells you the version number and date of the firmware you are currently using.

4. Select your **Time Zone**.
- 5 .Enable or disable **Daylight Savings**.
6. Review the **LAN IP Address** information and change it if necessary. These fields show the **Device IP Address** and **Subnet Mask** as seen by others on your Local Area Network (LAN). Most users will not need to change these values.

If your ISP uses PPPoE, choose Enable and go on to Step 8; otherwise, choose Disable and skip to Step 7.

7. For **WAN IP Address** (also called the **Public IP**), choose either **Obtain an IP Address Automatically** (most users) or **Specify an IP Address** (if your ISP assigns static IPs). If you choose the second option, type in the Wide Area Network (**WAN**) **IP Address, Subnet Mask, ISP Gateway Address**, and **DNS** information. Your ISP should provide these values.
8. Select your Point-to-Point Protocol over Ethernet (**PPPoE**) settings. PPPoE allows your ISP to authenticate your connection by requiring you to submit a username and password.
9. Type in the PPPoE User Name and Password provided by your ISP.
10. Click Apply when you finish choosing your settings, or click Cancel to undo your changes.

## Global Address

Use the Global Address screen to set up Network Address Translation (NAT), a process that provides internal to external IP address mapping. If your router is configured to retrieve an IP address dynamically, you will not need to use this function.

The Global Address screen is shown in the figure below.



## Wireless

Use the Wireless screen to configure your router for wireless access. Most users will only need to look at the Basic settings, which include Wireless Enable/Disable, ESSID, Channel, and WEP options. Some users may choose to configure the Advanced wireless settings, such as Beacon Interval, Authentication Type, and Enhanced Security options. The Wireless screen is shown in the figure below

The screenshot shows the 'Radio Setting' tab of the wireless configuration interface. It includes sections for basic settings (Wireless Enable/Disable, FirmWare Version, Mode, ESSID, Channel) and advanced settings (Beacon Interval, RTS Threshold, Fragmentation Threshold, DTIM Interval, Preamble Type, Distribution System). There are also fields for Peer AP MAC addresses and buttons for Apply, Cancel, and Help. A sidebar on the right provides default values for radio settings.

Beacon Interval	100
RTS Threshold	2432
Fragmentation Threshold	2346
DTIM Interval	1
Preamble Type	Long Preamble
Distribution System	Disable

### Radio Setting:

#### To configure the Basic wireless options:

1. First, choose to **Enable** or **Disable** wireless access. None of the router's wireless functions will work unless you choose Enable.
2. Review the **Firmware Version**. This value tells you the version number of the wireless firmware you are currently using.
3. Select Wireless Mode: If you have Wireless-G and Wireless-B devices in your network, then keep the default setting, **MIXED**. If you have only Wireless-G devices, select **G\_ONLY**. If you have only Wireless-B devices, select **B\_ONLY**.
4. Type in the Extended Service Set Identifier (**ESSID**)



5. Select the **Channel** number

## Advanced Wireless Options

Most users will not need to configure the advanced wireless options.

### To configure the Advanced wireless options:

1. Type a **Beacon Interval**. This value represents the time interval between beacons broadcast by the Access Point (AP).

Note that the default values for the advanced wireless settings are shown in a table on the right-hand side of the screen:

Default Values for Radio Settings	
Beacon Interval	100
RTS Threshold	2432
Fragmentation Threshold	2346
DTIM Interval	1
Preamble Type	Long Preamble
Distribution System	Disable

2. Type a value for **RTS Threshold**. This value represents the minimum size of data frames above which Request-To-Send (RTS) protocol is used. RTS helps prevent data collision from hidden nodes.

3. Type a value for **Fragmentation Threshold**. For efficiency in high-traffic situations, large files are split into fragments. This parameter specifies the default packet size.

4. Type a value for **DTIM Interval**. This parameter specifies the number of beacon intervals between successive Delivery Traffic Indication Maps (DTIMs).

5. Choose a Preamble Type, either Short (72 bits) or Long (144 bits).

6. Click Apply to put your changes in effect, or click Cancel to undo your changes.

## Distribution System

This is WDS Function. WDS can extended your Wireless scope.

<b>Distribution System:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Peer AP MAC Address 1:</b>	<input type="text"/>
<b>Peer AP MAC Address 2:</b>	<input type="text"/>
<b>Peer AP MAC Address 3:</b>	<input type="text"/>
<b>Peer AP MAC Address 4:</b>	<input type="text"/>
<b>Peer AP MAC Address 5:</b>	<input type="text"/>
<b>Peer AP MAC Address 6:</b>	<input type="text"/>
<b>Peer AP MAC Address 7:</b>	<input type="text"/>
<b>Peer AP MAC Address 8:</b>	<input type="text"/>

1. Select **Enable**
2. Fill the MAC Address of another Access Point which has WDS function. For example another Access Point's MAC Address is 00:08:A1:02:25:A2. In the **Peer AP MAC Address 1**, you must fill **00:08:A1:02:25:A2**

## Security Setting:

The screenshot shows a web-based configuration interface for a router. At the top, there is a navigation bar with tabs: Setup, Global Address, Wireless, Tools, Status, DHCP, Log, Statistics, Advanced, and Help. The 'Wireless' tab is selected. Below the navigation bar, there are three sub-tabs: Radio Setting, Security Setting (which is active), and Status. The main content area is divided into several sections:

- Authentication Type:** Three radio buttons are present: Open System, Shared Key, and Both. The 'Both' option is selected.
- Encryption:** Two radio buttons are present: Enable and Disable. The 'Disable' option is selected. Below this is a button labeled 'Set WEP Keys'.
- Wireless Access Control:** Two radio buttons are present: On and Off. The 'Off' option is selected. Below this is a button labeled 'Set Access List'.
- Enhanced Security:** A checkbox labeled 'Hide SSID in Beacon frame' is present and is currently unchecked.

At the bottom of the configuration area, there are three buttons: Apply, Cancel, and Help. On the right side of the screen, there is a help text box that reads: 'Use the Wireless Security Setting screen to configure your Gateway for wireless security access.'

**Authentication Type:** The default is set to **Both**, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. If you want to use only Shared Key authentication, then select Shared Key.

## To set WEP keys:

1. To enable Wireless encryption function (recommended), select the **Enable** button and click “**Set WEP Keys**” button. The Set WEP Keys window is shown in the figure below.

To create new WEP keys, enter a passphrase and click **Generate**. Or, you can manually enter the key elements into the table below.

**Encryption Level:**  64 Bit  128 Bit

**WEP Key Type:**  Automatic  Manually

Alphanumeric: 5 characters

Hexadecimal: 10 digits(0-9, A-F)

**Passphrase:**

Key 1:

Key 2:

Key 3:

Key 4:

**Default TX Key:** 1

2. In the Set WEP Keys window, select the **Encryption Level** (64 Bit or 128 Bit).

**Note: Although 128 Bit encryption uses a more secure encryption algorithm, it can slow down your network’s data transmission rates.**

3. Specify WEP keys by entering a **Passphrase** and clicking **Generate**, or by manually typing up to four keys. Use the **Clear Keys** button to delete any unwanted key information.
4. Select the **Default TX Key** from the drop-down list. This value will determine the default encryption key to be used.
5. Click **Apply** to put your changes in effect, or click **Cancel** to undo your changes.
6. Close the window when you are finished.

## Wireless Access Control

Use the Wireless Control List window to allow access to the Internet based on users' Media Access Control (MAC) address.

### To set wireless access controls:

1. Click **On**.
2. Click the **Set Access List** button on the Filters screen to launch the Wireless Control List window:

**Wireless Control List**

<b>mac 1</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 2</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 3</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 4</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 5</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 6</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 7</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 8</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 9</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 10</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 11</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 12</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 13</b>	<input type="text" value="XXXXXXXXXX"/>
<b>mac 14</b>	<input type="text" value="XXXXXXXXXX"/>

3. Type the MAC address(es) that you want to allow into the table. You can allow access to up to 80 addresses.
4. Click **Refresh** to automatically update the values in the table.
5. To save your changes, click **Submit** at the bottom of the Wireless Control list; then close the window.

**Enhanced Security:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting. If you do not want to broadcast the Router's ESSID, then select **Hide SSID in Beacon frame**.

## Status:

This table lists detailed statistics about the access point's radio, including Status, Max.MB/s, IP Address, MAC Address, Radio SSID, Receive data, and Transmit data. Click Refresh to automatically update the values in the table

## To display the Wireless association table

1. Click Display Association Table to launch the Wireless Association Table:

### Wireless Association Table

Refresh

Index	Time	Mac Address	Status	Add/Delete from Access List
1	2004.01.11 07:16:06	00:02:8a:c1:59:f2	Associated	<u>Add</u> / <u>Delete</u>
2	2004.01.11 08:48:39	00:90:4b:25:ee:ff	Associated	<u>Add</u> / <u>Delete</u>

2. Click Refresh to automatically update the values in the table.
3. Click Add to add a new device to the wireless access control list. The address is added to the Wireless Control List table.
4. Click Delete to remove a device from the wireless access control list. The address is deleted from the Wireless Control List table.
5. Click Refresh to automatically update the values in the table

## Tool

We strongly recommend that you change the password once you've accessed the router for the first time. The Tools screen is shown in the figure below.

### To change the administrative password:

1. Type in the Old Password. The factory default password is **1234**.
2. Enter a New Password. The password you choose must be less than 64 characters.
3. Confirm your password in the Confirm Password field.
4. Click Apply to put your changes in effect, or click Cancel to undo your changes.

### To restore the factory default settings:

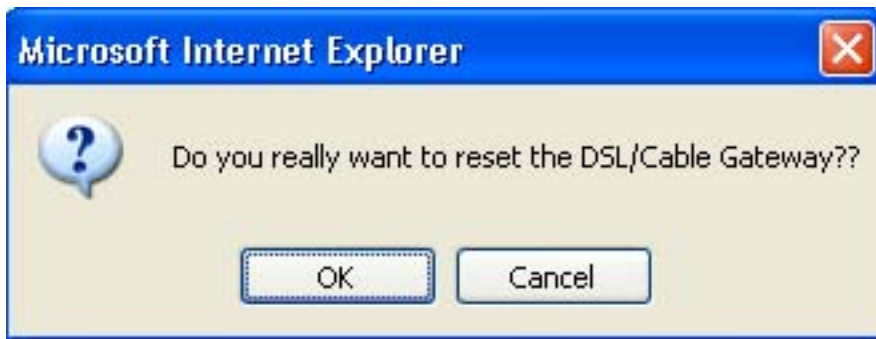
1. Click Restore to Default. A warning dialog box appears:



2. Click OK. All your router's settings will be restored to their factory default values.

## To reset the Router:

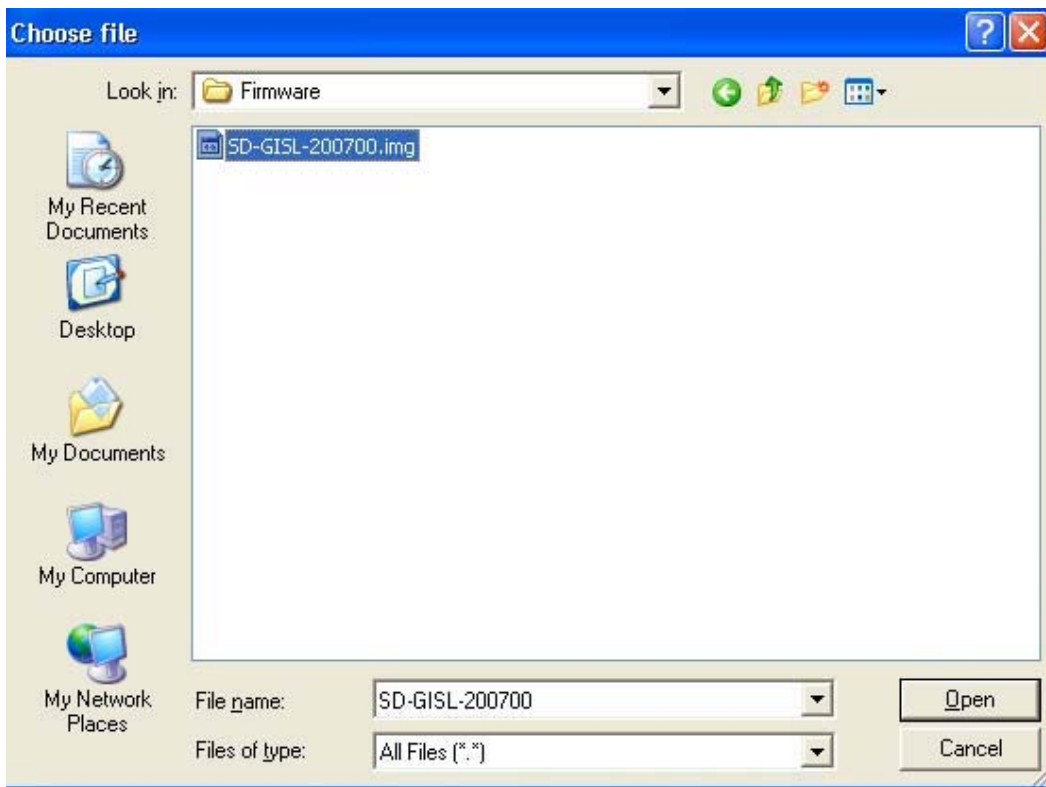
1. Click Reset. A warning dialog box appears:



2. Click OK. Your router will Reset immediate.

## To upgrade the router's firmware:

1. Download a firmware image file from the router website and save it to your hard drive. Make sure to write down the file location.
2. Type the filename and path location directly into the **Upgrade Firmware** field, or click **Browse...** to launch the **Choose file** dialog box:



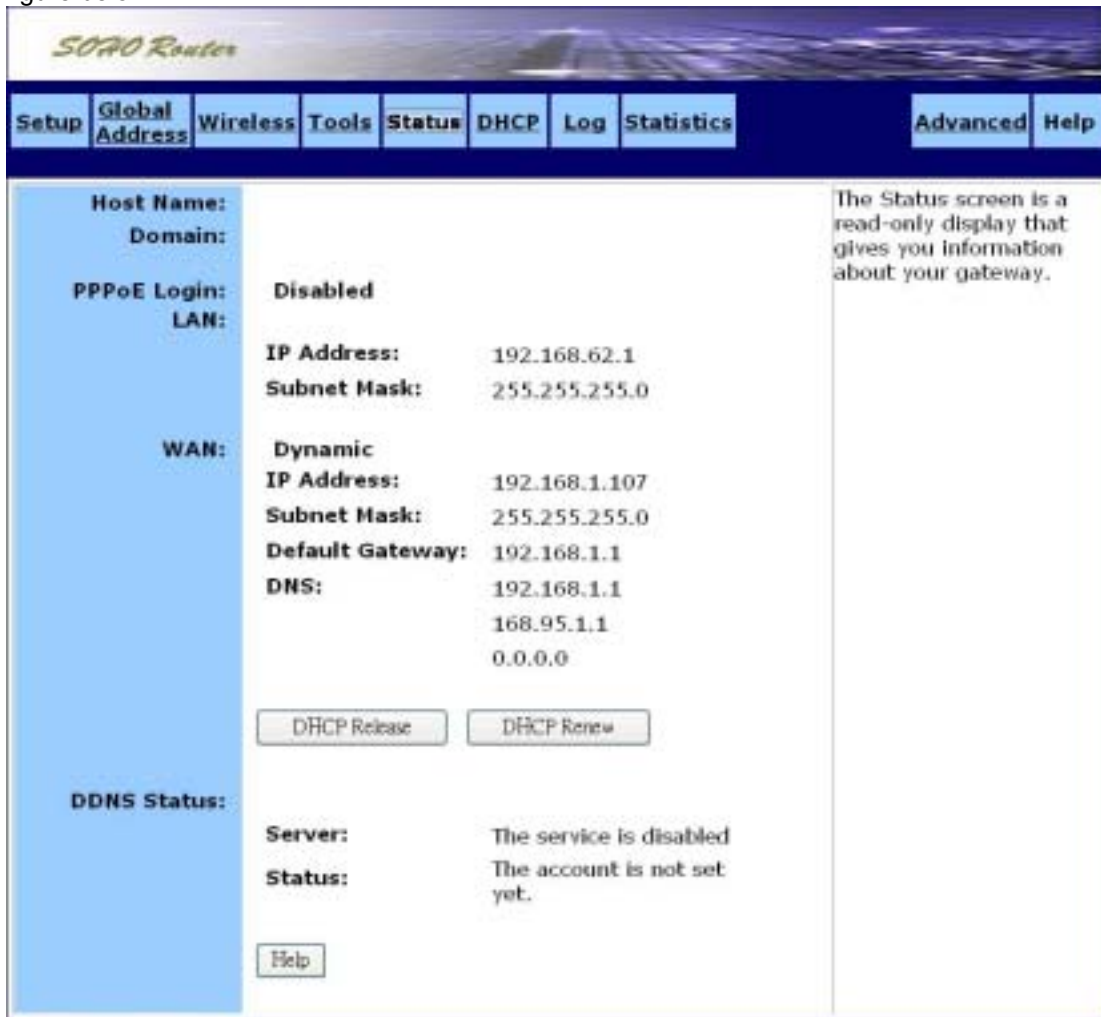
Locate the firmware you downloaded and click Open.

3. Click Upgrade Now. The firmware of the device will be upgraded.



## Status

The Status screen is a read-only display that gives you information about your router. The data displayed may change depending on your current configuration. The Status screen is shown in the figure below.



**Host Name:**  
**Domain:**

**PPPoE Login:** Disabled  
**LAN:**  
**IP Address:** 192.168.62.1  
**Subnet Mask:** 255.255.255.0

**WAN:** Dynamic  
**IP Address:** 192.168.1.107  
**Subnet Mask:** 255.255.255.0  
**Default Gateway:** 192.168.1.1  
**DNS:** 192.168.1.1  
168.95.1.1  
0.0.0.0

**DDNS Status:**  
**Server:** The service is disabled  
**Status:** The account is not set yet.

The Status screen is a read-only display that gives you information about your gateway.

The displayed data may include:

Host Name

Domain

PPPoE Login (Enabled or Disabled)

LAN settings (IP Address and Subnet Mask)

WAN settings (IP Address, Subnet Mask, Default Gateway, and DNS information)

DDNS (Dynamic DNS) status (Server and Status)

To change any of these settings, go to the Setup screen.

### DHCP Release and DHCP Renew

If you chose the Dynamic IP and PPPoE Disable options in the Setup screen, you'll see the DHCP Release and DHCP Renew buttons below the status information. Use these buttons to release or renew the WAN IP address.

To release the WAN IP address:  
Click DHCP Release.

To renew the WAN IP address:  
Click DHCP Renew.

## · DHCP

Use the DHCP screen to set up your router as a Dynamic Host Configuration Protocol (DHCP) server. DHCP servers automatically assign IP addresses to all the clients on your network. The DHCP screen is shown in the figure below.

The screenshot shows the DHCP configuration interface for a SOHO Router. The navigation bar at the top includes tabs for Setup, Global Address, Wireless, Tools, Status, DHCP, Log, Statistics, Advanced, and Help. The DHCP configuration area is divided into a left sidebar and a main content area. The sidebar has a blue background. The main content area contains the following settings:

- DHCP Server:**  Enable  Disable
- IP Pool Starting Address:** 192.168.62.50
- IP Pool Ending Address:** 192.168.62.100
- Lease Time:** 24 Hours.

Below the settings is a button labeled "Display DHCP Table". At the bottom of the configuration area are three buttons: "Apply", "Cancel", and "Help". On the right side of the screen, there is a help text box that reads: "Use the DHCP screen to set up your NAT/Firewall Gateway as a Dynamic Host Configuration Protocol (DHCP) server. DHCP servers automatically assign IP addresses to all the clients on your network."

### To set up your router as a DHCP server:

1. Make sure there is not already a DHCP server running on your network.
2. Make sure that each computer on your network is configured to receive an IP address automatically.
3. On the DHCP screen, click Enable.
4. Type the IP Pool Starting Address. The address you specify will be the first IP address that can be assigned to a computer on the network. Type the IP Pool Ending Address. The address you specify will be the last IP address that can be assigned.
5. Click Apply to put your changes in effect, or click Cancel to undo your changes.

### Display DHCP Table

Click Display DHCP Table to launch the DHCP Active IP window. In this screen, the DHCP Active IP Table lists information about the computers that have been assigned IP addresses by the DHCP server. For each active client, the table shows:

- Index number
- Client Hostname
- IP Address
- Mac Address

In addition, the DHCP Server IP Address is listed above the table.

You can click Refresh to see the latest data. Close the window when you are finished looking at the table. The DHCP Active IP window is shown in the figure below.

DHCP Active IP Table - Microsoft Internet Explorer

### DHCP Active IP Table

**DHCP Server IP Address: 192.168.62.1**

Index	Client Host Name	IP Address	MAC Address
1	sony-e7x46145qg	192.168.62.52	00:02:8a:c1:59:f2
2	test-va39bb6ima	192.168.62.51	00:90:4b:25:ee:ff

## Log

Use the Log screen to set up and view log files that record the access activity of LAN and WAN clients. The Log screen is shown in the figure below.



### To set up logging on your router:

1. Click Enable for Access Log on the Log screen.
2. Click Apply to put your changes in effect, or click Cancel to undo your changes.

### Session Event Log

Click Session Event Log to launch the Session Event Log window. In this screen, the Session Event Log Table lists session event entries. The table shows the Index number, Transport Type, Source IP, Source Port, Destination IP, Destination Port, and Terminate Reason for each event.

You can click Refresh to see the latest data. Make sure to close the window when you are finished looking at the log.

The Session Event Log is shown in the figure below.

Session Event Log Table

Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2004.01.10 07:37:15	ICMP	192.168.1.1	0:3	192.168.1.107	255-255	NORMAL
2	2004.01.10 07:37:15	ICMP	192.168.1.1	0:3	192.168.1.107	255-255	NORMAL

### Block Event Log

Click Block Event Log to launch the Block Event Log window. In this screen, the Block Event Log Table lists blocking event entries. The table shows the Index number, Transport Type, Source IP,

Source Port, Destination IP, Destination Port, and Terminate Reason for each event.

You can click Refresh to see the latest data. Make sure to close the window when you are finished looking at the log.

The Block Event Log is shown in the figure below.

**Block Event Log Table**

Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2004.01.10 07:24:46	UDP	192.168.1.2	137	192.168.1.255	137	Disallowed Destination IP
2	2004.01.10 07:24:47	UDP	192.168.1.2	137	192.168.1.255	137	Disallowed Destination IP

### Intrusion Event Log

Click Intrusion Event Log to launch the Intrusion Event Log window. In this screen, the Intrusion Event Log Table lists intrusion event entries. The table shows the Index number, Record Time, and Intrusion Type for each intrusion event.

You can click Refresh to see the latest data. Make sure to close the window when you are finished looking at the log.

The Intrusion Event Log is shown in the figure below.

**Intrusion Event Log Table**

Index	Record Time	Intrusion Type
1	None	None

### Wireless Event Log

Click Wireless Event Log to launch the Wireless Event Log window. In this screen, the Wireless Event Log table lists wireless event entries. The table shows the Index number, Time, Severity, and Description for each event.

You can click Refresh to see the latest data. Make sure to close the window when you are finished looking at the log.

The Wireless Event Log is shown in the figure below.

**Wireless Event Log Table**

Index	Time	Severity	Description
1	2004.01.10 06:13:17	Info	WLAN zone information is not set
2	2004.01.10 06:13:17	Info	WLAN Access Point started

## Statistics

Use the Statistics screen to view statistics for the LAN, WAN, and AP Radio ports.

### LAN Statistics

This table lists detailed statistics on the LAN port.

LAN Statistics			
<a href="#">Refresh</a>			
<b>Status:</b> up <b>Max.Mb/s:</b> 100.0 <b>IP Addr:</b> 192.168.62.1 <b>MAC Addr:</b> 00:0a:15:00:00:00			
Receive		Transmit	
total bytes	0	total bytes	3046678
unicast pkts	12804	unicast pkts	0
multicast pkts	0	multicast pkts	8558
discards	0	discards	0
errors	0	errors	0
unknown protocols	847	packets queued	0

### WAN Statistics

This table lists detailed statistics on the WAN port.

WAN Statistics			
<a href="#">Refresh</a>			
<b>Status:</b> up <b>Max.Mb/s:</b> 100.0 <b>IP Addr:</b> 192.168.1.107 <b>MAC Addr:</b> 00:0a:15:00:00:01			
Receive		Transmit	
total bytes	306258732	total bytes	30084019
unicast pkts	278409	unicast pkts	192888
multicast pkts	820	multicast pkts	54
discards	0	discards	0
errors	0	errors	0
unknown protocols	8460	packets queued	0

### AP Radio

This table lists detailed statistics on the access point's radio.

## AP Radio

[Refresh](#)

**Status:** up **Max.Mb/s:** 54 MBps **IP Addr:** 192.168.62.1 **MAC Addr:**  
00:0a:15:00:00:02  
**Radio SSID:** WLAN

Receive		Transmit	
successful unicast frames	8904	successful unicast frames	9280
successful multicast frames	7	successful multicast frames	0
dropped frames	0	dropped frames	0
failed frames	0	failed frames	121



## Chapter 4: Configure the Router's Advanced Function

### Advanced Functions

Advanced administrative functions include Virtual Servers, Filters, IP/URL Block, Special Apps, DMZ Host, and MAC Clone, Proxy DNS.

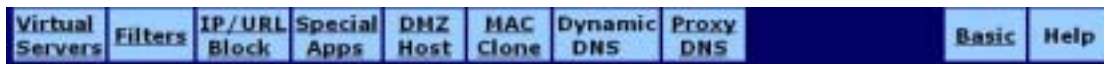
The web-based Admin Tool allows you to set up advanced services and perform special functions, such as filtering or cloning your MAC address. Most users will not need to use these features.

#### To toggle between Basic and Advanced Functions:

1. From the Basic functions screen set, click Advanced on the far right side of the menu bar to access the Advanced screens:



2. Once you are in the Advanced screen set, click **Basic** on the far right side of the menu bar to return to the Basic screens:



## Virtual Server

Use the Virtual Servers screen to provide remote services, such as FTP or Telnet, from computers in your network. The Virtual Servers screen is shown in the figure below.

Service	Public IP Address	Public Port	Private Port	Protocol	Private IP Address
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0

To set up a computer on your network as a Virtual Server:

1. Enter the name you wish to give each application in Service field..
2. Select a Public IP Address from the drop-down list.
3. Specify a Service Port. For help on which port to choose, refer to the Well-known Ports table on the right-hand side of the screen:

Well-known Ports	
7	Echo
21	FTP
23	TELNET
25	SMTP
53	DNS
79	finger
80	HTTP
110	POP3
113	auth
119	NNTP
161	SNMP
162	SNMP
1723	Trap
	PPTP

4. Select a **Protocol** (TCP, UDP, or **Both**) from the drop-down list.

5. Specify the **Private IP Address**. You only need to type the last part of the address; the first part is set automatically.

6. Click **Apply** to put your changes in effect, or click **Cancel** to undo your changes.

**To delete Virtual Servers:**

For any Virtual Server you want to delete, select 0.0.0.0 for Public IP Address and click Apply.

## Filters

Use the Filters screen to create and apply filters that can selectively allow traffic to pass in and out of your network. Your router comes with several filters predefined for you. The Filters screen is shown in the figure below.

Virtual Servers | **Filters** | IP/URL Block | Special Apps | DMZ Host | MAC Clone | Dynamic DNS | Proxy DNS | Basic | Help

Filtering Page: Page 1 (1-12)

ID	Filtering Layer	Proto Num	Direction	Private Port Range	Protocol
1	Port Filtering	0	Outbound	80 - 80	TCP
2	Port Filtering	0	Outbound	53 - 53	UDP
3	Port Filtering	0	Outbound	25 - 25	TCP
4	Port Filtering	0	Outbound	110 - 110	TCP
5	Port Filtering	0	Outbound	1720 - 1720	TCP
6	Port Filtering	0	Outbound	1509 - 1509	TCP
7	Port Filtering	0	Outbound	443 - 443	TCP
8	Raw IP	1	Both	0 - 0	TCP
9	Port Filtering	0	Outbound	21 - 21	TCP
10	Port Filtering	0	Inbound	0 - 0	TCP
11	Port Filtering	0	Inbound	0 - 0	TCP
12	Port Filtering	0	Inbound	0 - 0	TCP

Use this screen to create and apply filters that can selectively allow traffic to pass in and out of your network. If no filters are enabled, all traffic will be blocked. The Gateway comes with nine filters predefined for you.

NAT:  Enable  Disable  
 Firewall:  Enable  Disable  
 Remote Management:  Enable  Disable  
 IPSec Pass Through:  Enable  Disable  
 PPTP Pass Through:  Enable  Disable  
 Intrusion Detection:  Enable  Disable

### To set up a filter:

1. Select the Filtering Page from the drop-down list (1~12, 13~24, or 25~36).
2. Select the Filtering Layer from the drop-down list, either Raw IP or Port Filtering.
3. If you chose Raw IP, enter the **Port Num** (the IP Protocol Number, between 0 and 255). If you chose Port Filtering, skip to Step 4.
4. Select the Direction from the drop-down list, either **Inbound**, Outbound, or Both.
5. If you chose Port Filtering in Step 2, type the Private Port Range (the range of ports that you want to allow) and select the Protocol from the drop-down list (TCP, UDP, or Both).
6. If you are finished setting up your filters, click Apply to put your changes in effect, or click Cancel to undo your changes.

### Additional Filtering Options

You can enable additional filtering options, such as Remote Management, IPSec Pass Through, and Intrusion Detection.

#### To configure additional filtering options:

1. Choose whether to Enable or Disable each filtering option. The options are summarized in the table below.

<b>NAT</b>	Enabling this feature allows you to set up Network Address Translation (NAT).
<b>Firewall</b>	Enabling this feature allows you to protect your network with a firewall.
<b>Remote Management</b>	Enabling this feature lets you access your router's web-based admin tool through your WAN connection.
<b>IPSec Pass Through</b>	Enabling this feature lets you use IP Security Pass Through.
<b>PPTP Pass Through</b>	Enabling this feature lets you use Point-to-Point Tunneling Protocol (PPTP), used to enable VPN sessions
<b>Intrusion Detection</b>	Enabling this feature allows you to detect and record intrusion attempts into your network.

2. Click Apply to put your changes in effect, or click Cancel to undo your changes.

### Deleting Filters

You can delete existing filters from the filter list.

#### To delete a Raw IP filter:

1. Type zero in the Proto Num field.
2. Click Apply.

#### To delete a Port Filtering filter:

1. Type zero in both Private Port Range fields.
2. Click Apply.

## IP/URL Block

### IP Block

Use the IP Block screen to create and apply filters to selectively block traffic from specific IP addresses from passing in and out of your network.

You can block a single IP address or a range of IP addresses. If the IP address in the left IP field (the From field) is the same as the IP address in the right IP field (the To field), a single IP address is blocked. The IP Block screen is shown in the figure below.

	IP Block Starting Address	IP Block Ending Address
1	0 . 0 . 0 . 0	0 . 0 . 0 . 0
2	0 . 0 . 0 . 0	0 . 0 . 0 . 0
3	0 . 0 . 0 . 0	0 . 0 . 0 . 0
4	0 . 0 . 0 . 0	0 . 0 . 0 . 0
5	0 . 0 . 0 . 0	0 . 0 . 0 . 0
6	0 . 0 . 0 . 0	0 . 0 . 0 . 0

Apply Cancel Clear All Help

Use this screen to create and apply filters that can selectively block traffic to pass in and out of your network according to the IP addresses.

#### To block a range of IP addresses:

1. Select "IP Block" Page.
2. Type the first IP address of the range in the To field.
3. Type the last IP address of the range in the From field.
4. Click Apply to put your changes in effect, or click Cancel to undo your changes.

#### To remove a block against IP addresses:

For any IP block that you want to delete, type 0.0.0.0 for both IP ranges and click Apply.

### URL Block

URL Block can also be filtered by URL Address, the address entered to access Internet sites. The URL Block screen is shown in the figure below.

Virtual Servers	Filters	IP/URL Block	Special Apps	DMZ Host	MAC Clone	Dynamic DNS	Proxy DNS	Basic	Help
		<input type="radio"/> IP Block <input checked="" type="radio"/> URL Block							
		URL Block Domain Name							
1		<input type="text"/>							
2		<input type="text"/>							
3		<input type="text"/>							
4		<input type="text"/>							
5		<input type="text"/>							
6		<input type="text"/>							
7		<input type="text"/>							
8		<input type="text"/>							
9		<input type="text"/>							
10		<input type="text"/>							

Use this screen to create and apply filters that can selectively block traffic to pass in and out of your network according to the URL domain name.

**To block a URL Address:**

1. Select "URL Block" Page.
2. Type the URL Domain in "URL Block Domain Name" to field.
3. Click Apply to put your changes in effect, or click Cancel to undo your changes.

**To remove a block URL Domain:**

For any URL block that you want to delete, mark and delete the URL Domain and click Apply.

## Special Apps

Use the Special Applications screen to allow certain ports to communicate with computers outside your network. This feature may be necessary for multi-session applications like online gaming and video conferencing. The Special Apps screen is shown in the figure below.



### To configure Special Apps using the Popular Applications feature:

1. Select the application you wish to enable from the Popular Applications drop-down list:

**Popular Applications:** -- select one --  ID: --

2. Choose a specific line in the table by selecting its number from the ID drop-down list.
3. Click Copy to. The configuration settings for the selected application will appear in the table.
4. Click Apply to put your changes in effect, or click Cancel to undo your changes.

### Manual Configuration

Although you can manually configure special applications, only expert users should do so. We recommend that you always use the Popular Applications feature unless you know exactly which settings to choose.

### To manually configure Special Apps:

1. Choose a line item to configure.
2. Select the communication Protocol used by the application from the drop-down list (TCP, UDP, or Both).
3. Specify a Trigger Port Range. This parameter identifies the range of ports that, when used for outgoing traffic, will trigger the gateway to accept certain incoming requests.
4. Type a Maximum Activity Interval. This parameter specifies the maximum number of



milliseconds after the port trigger action during which incoming requests will be accepted.

5. Choose Enable or Disable from the drop-down list for Session Chaining. This parameter specifies whether or not dynamic sessions can be chained, allowing multi-level session triggering.
6. If you chose Enable in Step 5, you may now choose Enable or Disable for Chaining on UDP. If you chose Disable in Step 5, skip to Step 7.
7. Choose Enable or Disable from the drop-down list for Address Replacement. This parameter specifies whether or not binary address replacement should be performed.
8. If you chose Enable in Step 7, you may now choose the Address Translation Type (TCP or UDP). If you chose Disable in Step 7, skip to Step 9.
9. Choose Enable or Disable from the drop-down list for Multi Hosts. Enabling this parameter allows a new session to be initiated from/to different remote hosts.
10. Click Apply to put your changes in effect, or click Cancel to undo your changes.

**To delete a special application:**

1. Enter 0 - 0 for Trigger Port Range.
2. Click Apply.

## DMZ Host

Use the DMZ Host screen to expose one or more computers on your network to the Internet. This feature is often used for online games that require unrestricted two-way communication. The total number of DMZ hosts you can have is limited by the total number of Global Addresses that you have configured in the Global Address screen. For example, if you have defined five Global Addresses (including the Default Public IP), you are limited to five DMZ hosts. The DMZ Host screen is shown in the figure below.

Public IP Address	Private IP Address
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0

### To set up a computer on your network as a DMZ Host:

1. Select a Public IP Address from the drop-down list.
2. Specify the Private IP Address. You only need to type the last part of the address; the first part is set automatically.
3. Click Apply to put your changes in effect, or click Cancel to undo your changes.

### To delete DMZ Hosts:

For any DMZ Host you want to delete, select 0.0.0.0 for Public IP Address and click Apply.

## MAC Clone

If your ISP restricts service to PCs only, use the MAC Clone feature to copy a PC Media Access Control (MAC) address to your router. This procedure will cause the router to appear as a single PC, while allowing online access to multiple computers on your network. The MAC Clone screen is shown in the figure below.



The screenshot shows a web interface for configuring the MAC Clone feature. At the top, there is a navigation bar with tabs for Virtual Servers, Filters, IP/URL Block, Special Apps, DMZ Host, MAC Clone (selected), Dynamic DNS, and Easy DNS. On the right side of the navigation bar are tabs for Basic and Help. The main content area has a light blue background. On the left, there are three labels: 'WAN Port Mac Address:' followed by an empty text input field; 'Current WAN Port Mac Address:' with the value '00:0e:15:00:00:01'; and 'Factory Default Mac Address:' with the value '00:0e:15:00:00:01'. Below these labels are three buttons: 'Mac Clone', 'Restore', and 'Help'. On the right side of the main content area, there is a text box containing the following text: 'If your ISP restricts service to PCs only, use the Mac Clone feature to copy a PC Media Access Control (MAC) address to your NAT/Firewall Gateway. This procedure will cause the gateway to appear as a single PC, while allowing online access to multiple computers on your network.'

### To clone the MAC address:

1. Type a PC MAC Address in the WAN Port Mac Address field. You may need to use the Ethernet MAC Address of the Network Interface Card (NIC) from the PC that is registered with your ISP.
2. Click Mac Clone to put your changes in effect, or click Restore to undo your changes.

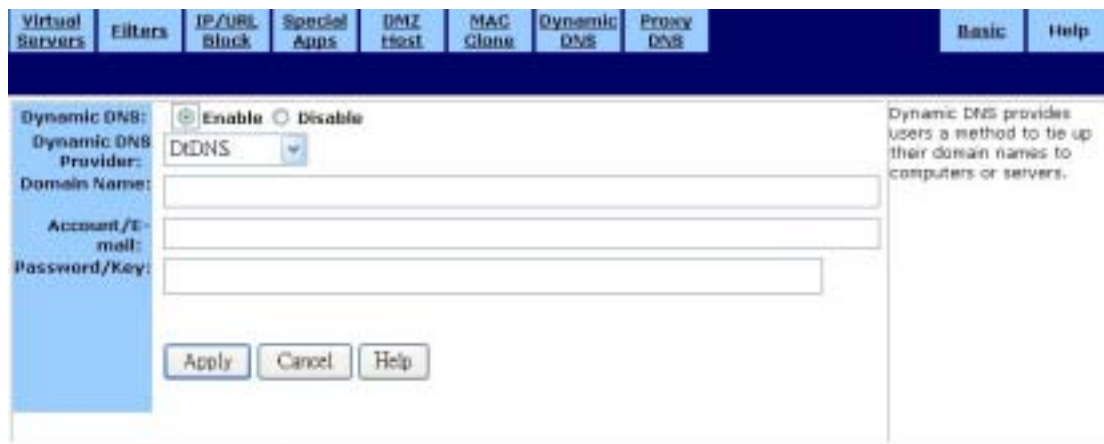
## Dynamic DNS

Use the Dynamic DNS screen to map your domain names to DNS servers connected via DSL, PPPoE, or another service that does not provide users with static IP addresses.

When you register the Wireless-G Router with the dynamic DNS service and connect to the Internet using a dynamic IP address, the dynamic DNS service works with the DNS server to forward the correct IP address to the requestor. These providers allow you to associate a static hostname with a dynamic IP address. This allows you to connect to the Internet with a dynamic IP address and use applications that require a static IP address.

The Wireless-G Router supports the following dynamic DNS providers: DynDNS.org, no-IP.com, and DtDNS. For more information about these providers, see [www.DynDNS.org](http://www.DynDNS.org), [www.no-IP.com](http://www.no-IP.com), and [www.DtDNS.com](http://www.DtDNS.com).

The Dynamic DNS screen is shown in the figure below.



The screenshot shows a web interface for configuring Dynamic DNS. At the top, there is a navigation bar with tabs: Virtual Servers, Filters, IP/URL Block, Special Apps, DMZ Host, MAC Clone, Dynamic DNS (selected), Proxy DNS, Basic, and Help. The main content area is titled 'Dynamic DNS:' and contains the following elements:

- Enable  Disable
- Dynamic DNS Provider: DtDNS (selected from a dropdown menu)
- Domain Name: [Text input field]
- Account/E-mail: [Text input field]
- Password/Key: [Text input field]
- Buttons: Apply, Cancel, Help

On the right side of the form, there is a help text box that reads: 'Dynamic DNS provides users a method to tie up their domain names to computers or servers.'

### To configure a dynamic dns server:

1. On the Dynamic DNS screen, click Enable.
2. Select a Dynamic DNS Provider from the list (DynDNS.org, no-IP.com, or DtDNS).
3. Type your Domain Name.
4. Type your Account or E-mail address.
5. Type the Password or Key for your account or E-mail address.

6. Click Apply to put your changes in effect, or click Cancel to undo your changes.

## Proxy DNS

Use the Proxy DNS screen to map a domain name to its server's IP address. This feature acts as a DNS server for the internal and DMZ networks, allowing you to connect to local machines without using an external DNS server. This simplifies network configuration and management. The Proxy DNS screen is shown in the figure below.

The screenshot shows the Proxy DNS configuration interface. At the top, there is a navigation bar with tabs for Virtual Servers, Filters, IP/URL Block, Special Apps, DMZ Host, MAC Clone, Dynamic DNS, and Proxy DNS. The Proxy DNS tab is selected. Below the navigation bar, the Proxy DNS section is visible. It includes a 'Proxy DNS:' label with radio buttons for 'Enable' (selected) and 'Disable'. There are three rows of input fields for 'Domain Name' and 'Virtual IP Address'. The 'Virtual IP Address' field is a dotted IP address format with three octets and a trailing zero. A help text box on the right states: 'Proxy DNS acts as a DNS Server for the Internal and DMZ networks.'

### To configure a Proxy DNS server:

1. On the DHCP screen, click Enable.
2. Type a name for the local machine in the Domain Name field.
3. Type the IP address of the local machine in the Virtual IP Address field.
4. Click **Apply** to put your changes in effect, or click **Cancel** to undo your changes.

### To delete a Proxy DNS server:

1. Delete the domain name of the proxy DNS server that you want to remove.
2. Type 0.0.0.0 for **Virtual IP Address**.
3. Click **Apply** to put your changes in effect, or click **Cancel** to undo your changes.

### **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.

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

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

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

Cnet declared that CWR-854 is limited in CH1~11 from 2400 to 2483.5 MHz by specified firmware controlled in USA.