

## Configuration Utility

**802.1X** : Accept normal clients and work simultaneously with RADIUS Server. The encryption key is got from RADIUS Server dynamically.

- **Encryption Key Length**

You can select either 64 bits or 128 bits.

- **RADIUS Server IP**

The 802.1X server's IP address.

- **RADIUS port**

The 802.1X server's service port.

- **RADIUS Shared Key**

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



**WPA-PSK** : Accept WPA clients only and Pre-share key (encryption key) must be entered manually. You can input either 8 to 63 ASCII characters or 64 Hexadecimal digits as Pre-share key.

- **Pre-share Key Mode**

Either ASCII or HEX can be selected.

- **Pre-share Key**

Please input either 8 to 63 ASCII characters or 64 Hexadecimal digits as Pre-share key.



## Configuration Utility

**WPA** : Accept WPA clients only and work simultaneously with RADIUS Server. The encryption key is got from RADIUS Server dynamically.

- **RADIUS Server IP**

The 802.1X server's IP address.

- **RADIUS port**

The 802.1X server's service port.

- **RADIUS Shared Key**

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



**Note:** If you enable 802.1X or WPA feature, you must also have a RADIUS Server ready.

### Description:

- **WEP Encryption:** The WEP encrypts frames transmitted through wireless module using pre-entered WEP key. You can configure 4 key sets, and select one of them to apply.
- **WPA Encryption:** Wi-Fi protected Access is designed to improve Data protection and implement access control for Wireless LAN system. It encrypts frames transmitted through wireless module using Pre-share key (PSK) or the key got dynamically from RADIUS Server.
- **802.1X:** When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service. The most common method of implementing 802.1X is by having a RADIUS Server on your LAN containing an authentication database, so the router can work simultaneously with the server and get the user's authentication profile for comparison.

### Note:

To complete the WPA operation, you also need to enable the WPA client at the wireless client site (the computer running wireless client's devices, such as the GWP514 Cardbus card GWP514 Cardbus Card or GWU523 USB adaptor).

Microsoft provides a free WPA upgrade for Windows XP Service Pack 1 (SP1) and later or Windows Server 2003. For any OS other than Win XP, there is client software available from third-party suppliers such as Funk Software's Odyssey ([www.funk.com](http://www.funk.com)).

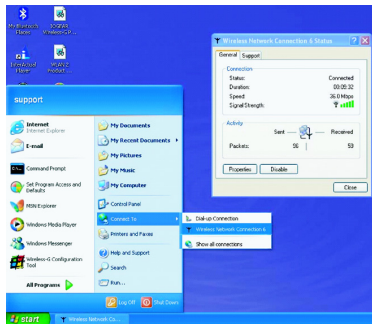
The WPA client for Windows XP can be found in the Microsoft Knowledge Base Article 815485 (<http://support.microsoft.com/default.aspx?scid=kb;en-us;815485>) or downloaded directly from Microsoft

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

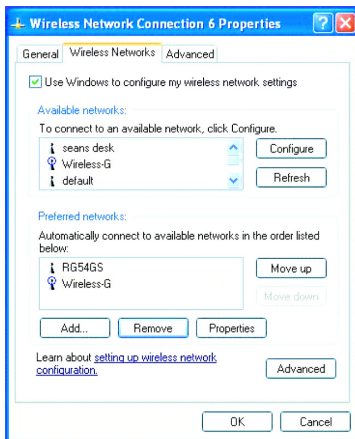
## Configuration Utility

After installed, the Windows WPA Client will update the wireless network configuration dialog boxes to support new WPA options.

1. Click **Connect To>Wireless Network Connection** to bring up the dialogue window of **Wireless Network Connection Status**. Click the **Properties** box to bring up next dialogue window.
2. In the **Wireless Network Connection Properties** window, under **Wireless Networks** tab, please check the box of **“Use Windows to configure my wireless network settings”** to turn on the Wireless Zero Configuration service. Select the wireless access point you want to associate to, then click **Configure** box at the right side to bring up next dialogue window.



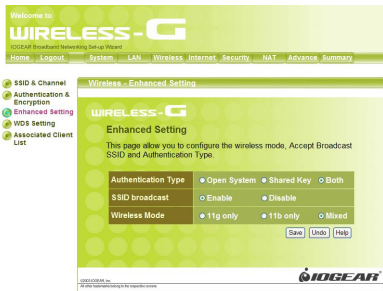
## Configuration Utility



3. Set up your WPA configuration by selecting the **Network Authentication** mode and **Data encryption**, and input same **Network key** as you input at the Wireless-G Broadband Gateway. Then, you are served by a more secured wireless network

# Configuration Utility

## Enhanced Setting



### Authentication Type

If Shared Key is selected, the Access Point will not be seen on the wireless network except to the wireless clients which share the same WEP key as the Access Point. If Open System is chosen, the Access Point will be visible to all clients on the

network, but only the wireless clients with the same WEP key can communicate on the wireless network.

### SSID broadcast

If the option is enabled, the SSID of the AP could be seen in the site survey of wireless client's utility. If the option is disabled, the SSID of the AP will not be seen in the wireless client's utility.

### Wireless Mode

11g only: The AP could let the 11g wireless clients to connect only.

11b only: The AP could let the 11b and 11g wireless clients to connect, but the 11g wireless clients will connect the AP in 11b mode.

Mixed: The AP could let both 11b and 11g wireless clients to connect

### WDS Setting



The Wireless Distribution System (WDS) provides wireless point-to-point bridging, and point-to-multipoint bridging for deployment over large area. With the WDS feature, the WLAN coverage range can be easily extended.

#### Wireless Bridging

The wireless bridging feature can be enabled by setting the mode to Enable. The default setting is Disable, only access point function is available. Once the Wireless Bridging is enabled, both wireless bridging and wireless access point functions are simultaneously available.

#### Remote AP MAC

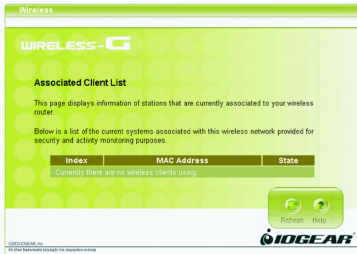
Please enter the MAC Address of WDS-enabled AP. Only authorized AP can access this router through WDS feature to extend the WLAN coverage range. Up to 3 AP's MAC are allowed.



# Configuration Utility

## Associated Client List

It displays information of stations that are currently associated to your wireless router. You can check who are linking to your network, for security and activity monitoring purposes. Click **Refresh** button to update the list.



### Internet Page

In Internet Settings, you can configure the way your Wireless-G Broadband Router uses to connect to your ISP.

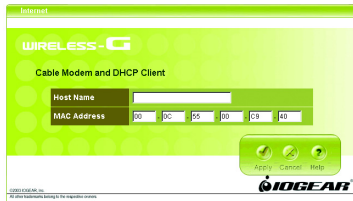
The screenshot shows the 'Internet' configuration page of the IOGEAR Broadband Networking Set-up Wizard. The page has a green and white color scheme. At the top, it says 'Welcome to WIRELESS-G IOGEAR Broadband Networking Set-up Wizard'. Below this is a navigation bar with buttons for Home, Logout, System, LAN, Wireless, Internet (selected), Security, NAT, Advance, and Summary. On the left side, there is a list of menu items: Connection Type, MAC Clone, Virtual Computers, and Dynamic DNS, each with a green arrow icon. The main content area is titled 'Internet' and contains the 'WIRELESS-G Internet Settings' section. The text in this section reads: 'In Internet Settings, you can configure the way your wireless router uses to connect to your ISP. Also we support DDNS for you to run your domain over a changing IP.' At the bottom of the page, there is a copyright notice: '©2003 IOGEAR, Inc. All other trademarks belong to the respective owners.' and the IOGEAR logo.

# Configuration Utility

## Connection Type

It allows you to configure the way you connect to your ISP. This Wireless Broadband Router can be connected to your ISP in any of the following ways: DHCP Client, PPPoE, Static IP, L2TP and Dynamic IP.

- DHCP Client: Enter the Host Name if your ISP provides it; otherwise, just leave it blank.



- Dynamic IP - PPPoE: Complete User name, password, confirm password fields.

**WIRELESS - G**

### Dynamic IP - PPPoE

Please put the necessary information such as username and password got from your ISP to the fields below.

In case your ISP gave you a service name, you should put it to the related field.

User Name	<input type="text" value="12345678@hinet.net"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>
Service Name	<input type="text" value=""/> (optional)
IP Address	<input type="text" value="0.0.0.0"/> (optional)

Apply Cancel Help

- Static IP: Complete the IP address, subnet mask, ISP gateway and primary DNS fields.

Internet

### WIRELESS - G

### Static IP - xDSL

Has your Internet Service Provider given you an IP address and Gateway address? If so, enter them below.

IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
ISP Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Primary DNS	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
Secondary DNS	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/> (optional)

Apply Cancel Help

## Configuration Utility


- Dynamic IP - PPTP: Complete fields on this screen. Those information can get from your ISP.

**Dynamic IP - PPTP**

Please put the necessary information such as username and password got from your ISP to the fields below.

In case your ISP gave you a phone number, you should put it to the related field.  
(PPTP is more popular in Europe.)

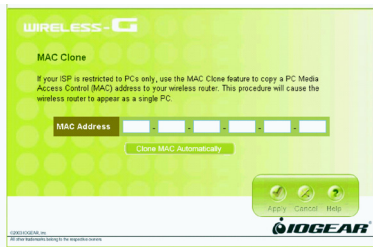
User Name	<input type="text" value="12345678@hinet.net"/>			
Password	<input type="password" value="*****"/>			
Confirm Password	<input type="password" value="*****"/>			
Service IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
My IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
My Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Phone number	<input type="text"/>			(optional)



### MAC Clone

If your ISP restricts connections to pre-registered computers only, use the MAC Clone feature to copy your computer's Media Access Control (MAC) address to your wireless broadband router. This procedure will cause the Wireless-G Broadband Router to appear as a single computer.

To do MAC Clone: click **Clone MAC**.



# Configuration Utility

## Virtual Computers

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- **Global IP:** Enter the global IP address assigned by your ISP.
- **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
- **Enable :** Check this item to enable the Virtual Computer feature

The screenshot shows the configuration utility interface for a Wireless-G router. The main heading is "WIRELESS-G" and the sub-heading is "Virtual Computers". Below the heading, there is a message: "You can click this button to setup mappings of multiple global IP addresses and local IP addresses." Below this message is a table with 5 rows and 4 columns: ID, Global IP, Local IP, and Enable. Each row has a text input field for the Global IP, a text input field for the Local IP, and a checkbox for the Enable column. The Local IP field is pre-filled with "192.168.123.". At the bottom of the table are "Save", "Undo", and "Help" buttons. The IOGEAR logo is visible in the bottom right corner.

ID	Global IP	Local IP	Enable
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>

## Dynamic DNS

This feature enables you to run your domain (ex. www.mywebsite.com) over a changing IP. Before you can use this feature, you need to sign up for DDNS service from one of the Dynamic DNS providers that this Wireless-G Broadband Router supports and fill in related fields to make it work. You may follow the following steps to enable this function.

- Sign up for DDNS service and write down the host name, user name and password.
- Click the radio button of **Enable** to enable the dynamic DNS function.
- Complete the host name, user name and password fields.
- Click **Save** button to update the information. Click the radio button of **Disable** to disable this function.

The screenshot shows a web-based configuration utility for Dynamic DNS. The title is "Dynamic DNS". Below the title is a descriptive paragraph: "This feature enables you to run your domain over a changing IP. Please choose one of the Dynamic DNS providers that this wireless router supports and fill in related fields to make it work. If you get any problem, you can check with the Dynamic DNS provider that you choose." The form contains several fields: "Dynamic DNS" with radio buttons for "Enable" (selected) and "Disable"; "Dynamic DNS Provider" with a dropdown menu showing "DynDNS.org"; "Host Name" with a text input field; "User Name" with a text input field; "Password" with a text input field; "My IP Address" with a text input field; "Update Manually" with a button labeled "Update Now" and a refresh icon; and "Status" with the text "Can't connect to Dynamic DNS Server".

Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Provider	DynDNS.org
Host Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
My IP Address	<input type="text"/>
Update Manually	<input type="button" value="Update Now"/>
Status	Can't connect to Dynamic DNS Server



# Configuration Utility

## Security

Your IOGEAR Wireless-G Broadband Router features powerful and flexible firewall protection to keep your computer and/or network secure.

If you are an advanced user, you can configure firewall policies depending on your needs.

The screenshot displays the configuration utility interface for an IOGEAR Wireless-G Broadband Router. At the top, it says "Welcome to WIRELESS-G" and "IOGEAR Broadband Networking Set-up Wizard". Below this is a navigation menu with options: Home, Logout, System, LAN, Wireless, Internet, Security, NAT, Advance, and Summary. The "Security" option is selected. On the left side, there is a sidebar menu with five items: Packet Filter, Domain Filters, URL Blocking, DMZ, and Miscellaneous, each with a green circular icon. The main content area is titled "Security" and contains the "WIRELESS-G Security Settings" section. The text in this section reads: "Your wireless router features powerful and flexible firewall protection to keep your network secure. You can configure the strength of firewall protection at a high, or a low level. If you are an advanced user, you can configure firewall policies depending on your needs." At the bottom right of the main content area is the IOGEAR logo. At the bottom left, there is a small copyright notice: "©2003 IOGEAR, Inc. All other trademarks belong to the respective owners."

## Packet Filter

Packet Filter enables you to control what packets are allowed to pass the router.

Outbound filter applies on all outbound packets.

However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only.

You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

Home Logout System LAN Wireless Internet Security NAT Advance Summary

Packet Filter  
Domain Filters  
URL Blocking  
DMZ  
Miscellaneous

Security - Packet Filter

WIRELESS-G

Packet Filter

Allows you to control access to a network by analyzing the outgoing and incoming packets and letting them pass or halting them based on the IP address of the source and destination.

Outbound Filter  Enable  Disable

Policies  Allow all to pass except those match the following rules.  Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1			<input checked="" type="checkbox"/>	0
2			<input checked="" type="checkbox"/>	0
3			<input checked="" type="checkbox"/>	0
4			<input checked="" type="checkbox"/>	0
5			<input checked="" type="checkbox"/>	0
6			<input checked="" type="checkbox"/>	0
7			<input checked="" type="checkbox"/>	0
8			<input checked="" type="checkbox"/>	0

Schedule rule: (00)Always Copy to ID -

Save Undo Inbound Filter... Help

## Configuration Utility

You can specify 8 rules for each directions: inbound or outbound.

For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix “T” or “U” to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses.

Each rule can be enabled or disabled individually.

### **Use Rule#**

Choose the schedule when you want to make this service take effect, and select the ID you want to use with the schedule rule. Then click “Copy to” button to copy it into the “Use rule #” box to use the schedule. When choosing rule 0 for always, it is the same as not using schedule.

**Schedule example**

Assume that there is a rule setting in Rule 1 which is Everyday 17:30~24:00, and there is a FTP server which IP is 192.168.123.5 and listening port 21. The Virtual Server's setting is as below:

Virtual Server				
ID	Service Ports	Server IP	Enable	Use Rule#
1	<input type="text" value="21"/>	192.168.123. <input type="text" value="15"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>

**Description:**

It means the WAN users can't access this FTP server only at 17:30~24:00 everyday. If the time exceeds this range, the WAN users can access the LAN FTP server.

Packet Filter				
<b>Inbond Filter</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<b>Policies</b>	<input checked="" type="radio"/> Allow all to pass except those match the following rules <input type="radio"/> Deny all the pass except those match the following rues			
ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text" value="21"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>