SSID & Channel

Here is where you may modify the SSID and Channel of your Wireless-G Broadband Router.

- **SSID (Service Set ID, or Network Name):**
  Enter the name you wish to give your Wireless-G Broadband Router (ex. "JOHN" or "IOGEAR"). Every Wireless Clients (PC card, USB and PCI adaptors) in your network must be configured to accept with the same SSID.

- **Channel**
  It can be left as Default, unless you plan on using multiple access points. When multiple Wireless Networks presenting, please ensure they are not using the same channel, preferably at least 5 channels apart to each other.

- **Accept Broadcast SSID**
  By broadcasting SSID, all wireless devices at surrounding area can see your wireless router and easy to associate with it. However, it is a good security practice not to broadcast SSID, just configure SSID info to those client devices you want them to access you network.

Authentication & Encryption

It allows you to configure the setting of network authentication and data encryption.

- **Network Authentication:**
  You can specify the authentication type.
  - "Both" allows wireless client devices access your router no matter with shared key or not.
  - "Share Key" only allows devices with same WEP (Wired Equivalent Privacy) key to access your wireless router.
  - "802.1X" and "WPA" require you to type in Radius server IP and server key. Please check with your Network Administrator for related information.
  - "WPA-PSK" needs a pre-shared key to be set on your wireless router and all wireless client devices.

• **Encryption:**
- WEP Configuration

Click the drop-down menu to select WEP to enable the WEP function and select 64 bits or 128 bits. The 128 bits gives a higher level of security. The selection must be the same between all connected network devices. For 64-bit WEP key, it should be five ASCII characters (a-z and 0-9, for example: gear56) or ten hexadecimal digits in length (a through f, and 0 through 9, for example: 2af30bc9d5); for 128 bit WEP key, the length will be 13 characters for ASCII or 26 digits for Hexadecimal. WEP keys 1-4 enable you to create an encryption scheme for wireless LAN transmissions.

WPA and WPA-PSK configuration

Wi-Fi Protected Access (WPA) is a sub-set of the forthcoming IEEE 802.11i security standard. WPA addresses those known weakness of WEP and provides stronger security to wireless network.

IOGEAR Wireless-G Broadband Router supports three authentication modes:

- 802.11x (need RADIUS server to authenticate the clients, using WEP keying)
- WPA (same 802.1x, but with TKIP keying support); WPA-PSK (Pre-Shared Key, no RADIUS server needed)

- WPA-PSK

There are two ways to configure WPA Pre-Shared Key: - WPA

1. **PassPhrase Mode**: Input a phrase into the field. The Wireless-G Broadband Router will automatically generate a Pre-Shared Key based on the phrase you enter. The phrase can be within 8 to 63 characters (we recommend at least 12 characters to achieve a sufficient level of security).

2. **Hex mode**: Input 64 hexadecimal digits. Please write down the key you enter. You will need to enter same key to your wireless client side.

WPA Group Rekey Interval
This router could change the group key periodically. Enter the period you want into the WPA Group Rekey Interval field.

Encryption Type
The current version only supports TKIP encryption. AES encryption will be available soon.

RADIUS Server IP
Please enter the IP address of RADIUS server

RADIUS Server Port
This field specifies the port on which RADIUS server is listening.

RADIUS Server Key
This field carries the shared secret for RADIUS authentication. Some information need to be encrypted in a RADIUS packet, this key is used to encrypt and decrypt this information (such as password).

Reconfirm RADIUS Server Key
Make sure RADIUS Server Key is correct.

WPA Group Rekey Interval
It is the same as WPA-PSK configuration

Encryption Type
It is the same WPA-PSK configuration

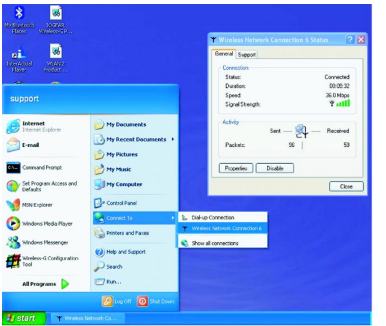
Note:
To complete the WPA operation, you also need to enable the WPA client at the wireless client site (the computer running wireless client's devices, such as the GWP511 Cardbus card GWP512 Cardbus Card or GWU513 USB adaptor).

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). IOGEAR's GWP512 Wireless-G Network PC Card has it built-in.

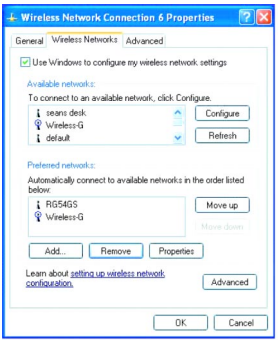
The WPA client for Windows XP can be found in the Microsoft Knowledge Base Article 815485 (http://support.microsoft.com/default.aspx?scid=kb;en-us;815485) or downloaded directly from Microsoft http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

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.



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

Radio Setting

Here you can configure Wireless radio settings. Please note that these settings are for advanced users or network administrators. If you are unfamiliar with how to configure these parameters, we recommend that you keep them at their default value.

- **Mode:** The Wireless-G Broadband Router can be set at three wireless modes: Auto, 802.11g only and 802.11b only. If both 802.11g and 802.11b clients presenting at your network, please select "Auto" mode (This is default mode). "802.11g only" mode only supports 802.11g clients, and gives better performance to whole network. However, all 802.11b clients will not be able to use your network at this mode setting. In some situation, 802.11b clients with old drivers cannot work with Auto mode; "802.11b only" mode can accommodate this problem, but decrease the performance of 802.11g devices.

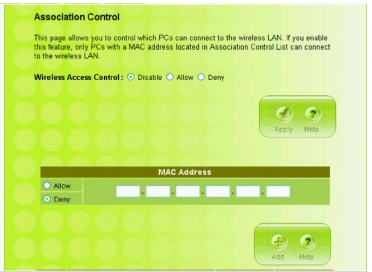
- **Beacon Period**: Beacons are packets sent by the router to synchronize a wireless network. The value of beacon interval is depending on the environment where the router is operating. Specify a Beacon interval value between 1 and 1000(units: ms). The default value is set to 100 milliseconds, i.e., ten beacons per second.

- **RTS Threshold**: The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. Each station can have a different RTS threshold. If you encounter inconsistent data flow, only minor modifications are recommended. The default value for RTS Threshold is set to **2347**.

- **Fragment Threshold**: This value should remain at its default setting of **2346**. If you experience a high packet error rate, you may modify slightly your "Fragmentation" value within the value range of 800 to 2346. Setting the Fragmentation value too low may result in poor performance.

- **DTIM Period**: Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value for DTIM interval is set to **1**.

Association Control



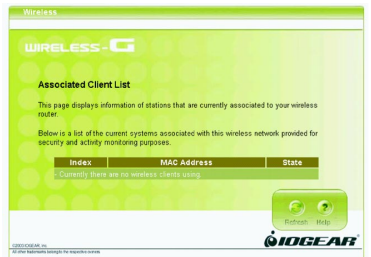
This page allows you to control which computers can connect to the Wireless-G Broadband Router.

If you enable this feature, only computers with a MAC address listed located in Association Control List can connect to the wireless LAN.

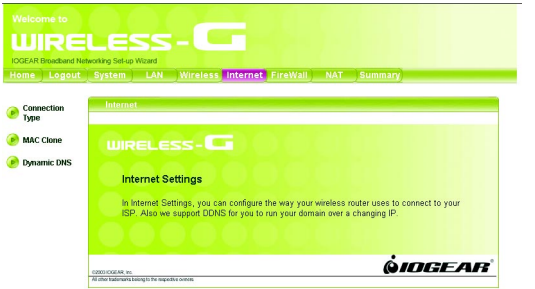
To add an association, enter the MAC address in the address field, specify **Allow** or **Deny** attribute and click **Add** button.
To delete an association, click **Delete** button from the Association Client List.

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

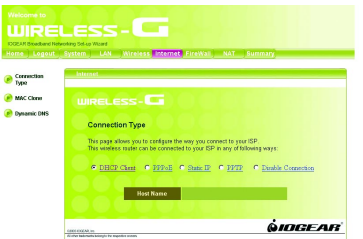


In Internet Settings, you can configure the way your Wireless-G Broadband Router uses to connect to your ISP.

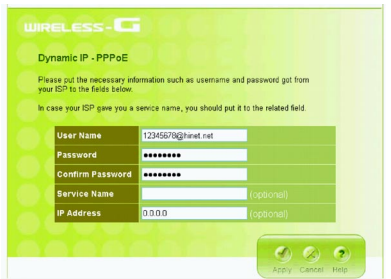
Connection Type

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 and PPTP

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

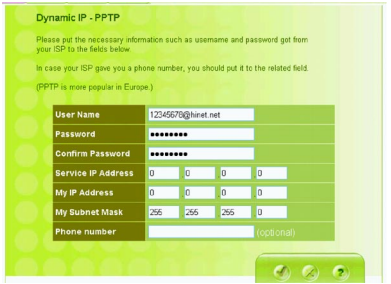


- Dynamic IP - PPPoE: Complete User name, password, confirm password fields.



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

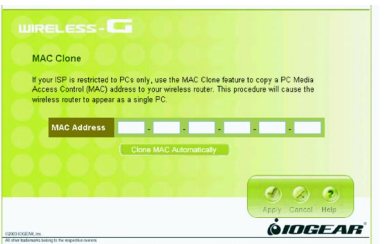
- Dynamic IP - PPTP: Complete fields on this screen. Those information can get from your ISP.



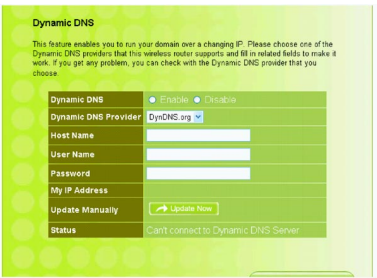
MAC Clone

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 Automatically**.



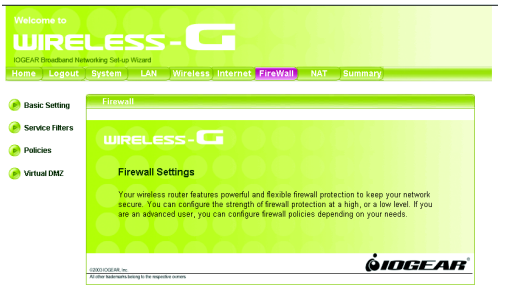
Dynamic DNS



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 **Update Now** button to update the information. Click the radio button of **Disable** to disable this function.

Firewall Page



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

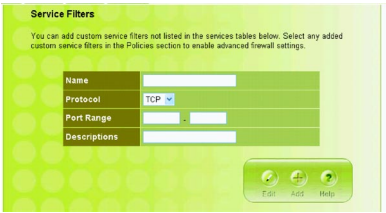
You can configure the strength of firewall protection at a high or low level. If you are an advanced user, you can configure firewall policies depending on your needs.

Basic Setting

Configure the basic settings to enable the firewall to protect your network from hacker attacks. Choose High, Low or Disable button will enable its corresponding settings.

Please be careful on these configurations. Any incorrect settings might cause the firewall to block all traffic or make your network vulnerable to outside hacker attacks.

Service Filter



You can add custom service filters not listed in the services tables. Select any added custom service filters in the Policies section to enable advanced firewall settings.

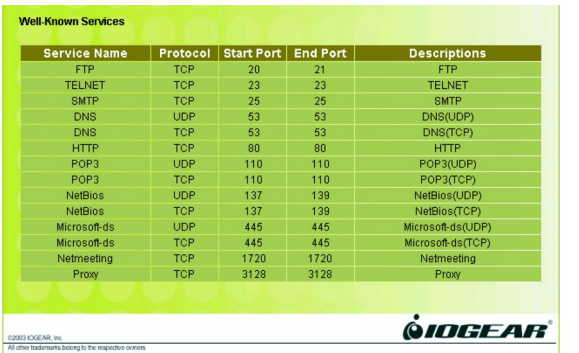
Name field: Enter the name you wish to give to any application.

Protocol: Click the drop-down menu to select TCP or UDP protocol.

Port range: Check the application's documentation and enter the port range.

Descriptions: Describe the application.

Some of the popular applications and protocol/port numbers settings are defined below:

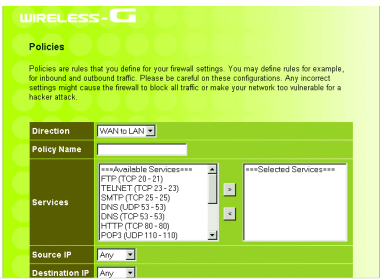


Well-Known Services

Service Name	Protocol	Start Port	End Port	Descriptions
FTP	TCP	20	21	FTP
TELNET	TCP	23	23	TELNET
SMTP	TCP	25	25	SMTP
DNS	UDP	53	53	DNS(UDP)
DNS	TCP	53	53	DNS(TCP)
HTTP	TCP	80	80	HTTP
POP3	UDP	110	110	POP3(UDP)
POP3	TCP	110	110	POP3(TCP)
NetBios	UDP	137	139	NetBios(UDP)
NetBios	TCP	137	139	NetBios(TCP)
Microsoft-ds	UDP	445	445	Microsoft-ds(UDP)
Microsoft-ds	TCP	445	445	Microsoft-ds(TCP)
Netmeeting	TCP	1720	1720	Netmeeting
Proxy	TCP	3128	3128	Proxy

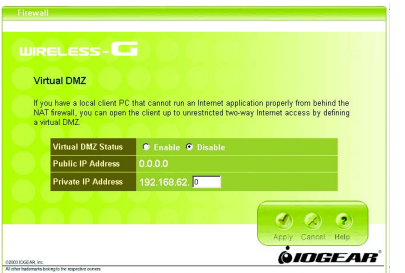
Policies

Policies are rules that you define for your firewall settings. You may define rules, for example, for inbound and outbound traffic.

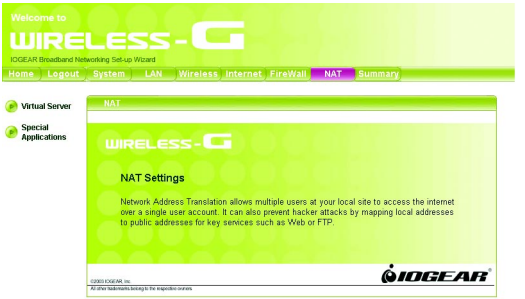


Virtual DMZ

If you have a local client computer that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ.



NAT Page



Network Address Translation allows multiple computers on your network to access the Internet over a single user account. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as Web or FTP.

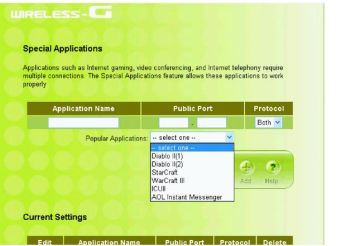
Virtual Server

You can configure the Wireless-G Broadband Router as a virtual server so that remote users can access services such as Web or FTP at your local site via public IP addresses.

For example: a FTP server (public port 21) will be translated into a local site (private 192.168.1.25) through private port 1502.

Virtual Server

Special Applications such as Internet gaming, video conferencing, and Internet telephony software usually require multiple connections. The Special Applications feature allows these applications to work properly.



Summary Page

This page includes all the basic configuration of the Broadband Router.

System Status

You can view the status of your Wireless-G Broadband Router from this window. The system status of the router is divided into four sections: General information, Internet Settings, LAN Settings and Wireless Settings. Click **Refresh** button to update all information.

Statistic

List the data transmission status of the router. Click **Refresh** button to update statistics.

Event Log

You can view any/all system events sent through your network from this window. Click **Refresh** button to update the list.

Standards	IEEE 802.11b, IEEE 802.11g Wireless LAN IEEE 802.3 10BASE-T, IEEE 802.3u 100 BASE-TX, IEEE 802.3x flow control
Ports	LAN: Four 10/100Mbps RJ-45 switch ports WAN: One 10/100Mbps RJ-45 port for DSL/Cable modem
Wireless Frequency band	2.400 - 2.497 GHz
Modulation Technique	DSSS (DBPSK, DQPSK, CCK), OFDM
Data rate	54 Mbps, 48, 36, 24,18,12, 11, 9, 6, 5.5, 2, 1 Mbps (auto-fallback)
Wireless Operating Channels	1-11 US/Canada, 1-13 Europe (ETSI), 10-13 France, 10-11 Spain
Wireless Operating range	Indoor environment: 20-100 meters Outdoor environment: > 200 meters
RF Output Power	21 dBm (Typical)
Receiver Sensitivity	-68dBm@54Mbps (ERP-OFDM); -82dBm@11Mbps (ERP-DSSS/CCK)
Antenna	One Dipole type external antenna and one patch type internal antenna
Antenna gain	Peak Gain = 7dBi

Specification

Platforms Supported	PC or MAC
Protocols Supported	TCP/IP, NAT, UDP, PPPoE, PPTP, DHCP (client and server) ,HTTP, TFTP, CSMA/CD for wire, CSMA/CA for wireless, -NAT/PAT
WAN type Supported	Static IP address, dynamic IP address (DHCP), PPPoE client, and PPTP
Max. Users Supported	253
Management	Embedded Web server for browser management Wireless Access Control Firmware upgrade via HTTP Upload/download configuration file via HTTP Restore to factory default setting
Security	NAT nature firewall, stateful packet inspection (SPI) IP Packet filtering (IP address/Port number) MAC address filtering 64-bit/128-bit WEP encryption, AES

Technical Support

If you need technical support, please check out our IOGEAR Tech Info Library (T.I.L.) at **www.iogear.com/support** for the latest tips, tricks, and troubleshooting. The IOGEAR T.I.L. was designed to provide you with the latest technical information about our products. Most of the answers to your questions can be found here, so please try it out before contacting technical support.

Technical support is available Monday through Friday from 8:00 am to 5:00 pm PST and can be reached at (949) 453-8782 or by email **support@iogear.com**.

Radio & TV Interference Statement

WARNING!!! This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

IN NO EVENT SHALL THE DIRECT VENDOR'S LIABILITY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, DISK OR ITS DOCUMENTATION EXCEED THE PRICE PAID FOR THE PRODUCT.

The direct vendor makes no warranty or representation, expressed, implied, or statutory with respect to the contents or use of this documentation, and especially disclaims its quality, performance, merchantability, or fitness for any particular purpose.

The direct vendor also reserves the right to revise or update the device or documentation without obligation to notify any individual or entity of such revisions, or updates. For further inquires please contact your direct vendor.

Regulatory Compliance FCC Warning

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.
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 or more 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.

Changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.
1) To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2) This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contact info.

23 Hubble • Irvine, CA 92618 • (P) 949.453.8782 • (F) 949.453.8785 • www.iogear.com