

# Configuration Utility

## Domain Filter

Domain Filter let you prevent users under this device from accessing specific URLs.

### **Domain Filter Enable**

Check if you want to enable Domain Filter.

### **Log DNS Query**

Check if you want to log the action when someone accesses the specific URLs.

### **Privilege IP Addresses Range**

Setting a group of hosts and privilege these hosts to access network without restriction.

### **Domain Suffix**

A suffix of URL to be restricted. For example, “.com”, “xxx.com”.

### **Action**

When someone is accessing the URL met the domain-suffix, what kind of action you want.

Check **drop** to block the access. Check **log** to log these access.

### **Enable**

Select “Enable” to enable each rule.

Welcome to  
**WIRELESS-G**  
LOGSAR Broadband Networking Setup Wizard

Home Logout System LAN Wireless Internet Security NAT Advance Summary

Security - Domain Filters

**WIRELESS-G**  
Domain Filters  
Let you prevent users under this device from accessing specific URLs.

Domain Filter  Enable  Disable  
Log DNS Query  Enable  Disable  
Privilege IP Addresses Range From  To

ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
3	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
4	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
5	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
6	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
7	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
8	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
9	<input type="text"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
10	* (all others)	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input type="checkbox"/>

Screen | Index | Help

## URL Blocking

URL Blocking will block Lan computers to connect to pre-defined Websites.

### **URL Blocking Enable**

*Check* if you want to enable URL Blocking.

### **URL**

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

### **Enable**

Select "Enable" to enable each rule.

Welcome to  
**WIRELESS-G**  
VOEGEAR Broadband Networking Setup Wizard

Home Logout System LAN Wireless Internet Security NAT Advance Summary

Security - URL Blocking

**WIRELESS-G**

**URL Blocking**  
URL Blocking will block LAN computers to connect to pre-defined websites.

URL Blocking  Enable  Disable

ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

Save Undo Help

## Configuration Utility

### DMZ

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

**Note:** This feature should be used only when needed.

The screenshot displays the IOGEAR Wireless-G Broadband Networking Setup Wizard. The main window is titled "Security - DMZ" and features the "WIRELESS-G" logo. A sidebar on the left lists navigation options: Packet Filter, Domain Filters, URL Blocking, DMZ (selected), and Miscellaneous. The main content area includes the following text: "DMZ" followed by "Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed." Below this, there are two rows of configuration options: "DMZ" with radio buttons for "Enable" (selected) and "Disable", and "IP Address of DMZ Host" with a text input field containing "192.168.123". At the bottom right of the form are "Save", "Undo", and "Help" buttons. The IOGEAR logo is visible in the bottom right corner of the window.

## Miscellaneous

### **WAN ICMP Blocking**

When this feature is enabled, any host on the WAN cannot ping this product.

### **SPI Mode**

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

### **DoS Attack Detection**

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

The screenshot displays the IDGEAR Wireless-G configuration utility interface. At the top, it says "Welcome to WIRELESS-G" and "IDGEAR Broadband Networking Setup Wizard". A navigation menu includes "Home", "Logout", "System", "LAN", "Wireless", "Internet", "Security", "NAT", "Advance", and "Summary". On the left, a sidebar lists configuration categories: "Packet Filter", "Domain Filters", "URL Blocking", "DMZ", and "Miscellaneous" (which is highlighted in pink). The main content area is titled "Security - Miscellaneous" and features the "WIRELESS-G" logo. Below the logo, the text reads: "Miscellaneous You can setup 'WAN ICMP Blocking', 'SPI (Stateful Packet Inspection)' and 'DoS Attack Detection' to avoid hacker's attack." There are three rows of settings, each with "Enable" and "Disable" radio buttons: "WAN ICMP Blocking" (Enable selected), "SPI mode" (Enable selected), and "DoS Attack Detection" (Enable selected). At the bottom right of the settings area are "Save", "Undo", and "Help" buttons. The footer contains "©2001 IDGEAR, Inc. All rights reserved. IDGEAR is the registered service" and the IDGEAR logo.

# Configuration Utility

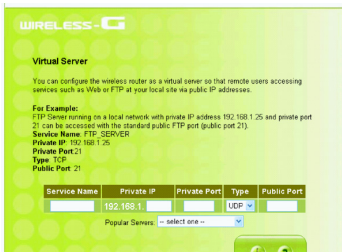
## NAT Page

The screenshot shows the 'NAT' 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' and 'IOGEAR Broadband Networking Set-up Wizard'. Below this is a navigation bar with links: Home, Logout, System, LAN, Wireless, Internet, FireWall, NAT (highlighted), and Summary. On the left side, there are two menu items: 'Virtual Server' and 'Special Applications', both with a green circular icon. The main content area is titled 'NAT' and features the 'WIRELESS-G' logo. Below the logo, the heading 'NAT Settings' is followed by a paragraph: 'Network Address Translation allows multiple users at your local site to access the internet over a single user account. It can also prevent hacker attacks by mapping local addresses to public addresses for key services such as Web or FTP.' At the bottom of the page, there is a footer with the IOGEAR logo and the text '©2003 IOGEAR, Inc. All other trademarks belong to their respective owners.'

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.



**Virtual Server** enables WWW, FTP and other services on your LAN to be accessible to Internet users. Refer [Internet Services](#) for well known ports.

### Example

ID	Service Ports	Server IP
1	21	192.168.123.1
2	80	192.168.123.1
3	1723	192.168.123.2
4	2000-2999	192.168.123.3

### Comment

The above example provides 4 type of services: FTP Server (port 21), Web Server (port 80), PPTP VPN Server (port 1723, PPTP) and a user defined server (ports 2000-2999).

## Configuration Utility

### 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 8:30~17:30, and there is a FTP server which IP is 192.168.123.15 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 access this FTP server only at 08:30~17:30 everyday. If the time exceeds this range, the WAN users can't access the LAN FTP server.

## Special Applications

Home Logout System LAN Wireless Internet Security NAT Advance Summary

Virtual Server  
Special Applications

**NAT - Special Applications**

**WIRELESS - G**

**Special Applications**

This configuration allows some applications to connect, and work with the NAT router.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Popular applications   ID

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony and so on. Due to the firewall function, these applications can not work with pure NAT

router. *Special Applications* makes some of these applications to work with NAT router. The settings are:

Trigger	The outbound port number issued by the application.
Incoming ports	When the trigger packet is detected, the inbound packets to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings. Select your application and click *Copy to* to add the predefined setting to your list. If the mechanism of *Special Applications* fails to make an application to work, try DMZ host instead.

**NOTE:** *At any time, only one PC can use each Special Application.*



# Configuration Utility

## Log Setting

The screenshot shows the 'Log setting' page in the IOGEAR configuration utility. The page title is 'Advance - Log setting'. It features a navigation menu on the left with options: Log setting (selected), SNMP, Routing, Schedule Rule, UPnP Setting, and Miscellaneous. The main content area includes the 'WIRELESS-G' logo and the heading 'Log setting'. Below this, it states 'Send system log to a dedicated host or email to specific receipts.' There are several input fields and checkboxes: 'IP Address for Syslog' (192.168.123) with an 'Enable' checkbox; 'IP Address of Outgoing Mail Server' (Send Mail Now) with an 'Enable' checkbox; '+ SMTP Server IP/Port' (empty); '+ E-mail addresses' (empty); '+ E-mail Subject' (empty); '+ User name' (empty); and '+ Password' (empty). At the bottom, there are buttons for 'View Log', 'Save', 'Undo', and 'Help'. The IOGEAR logo is visible at the bottom right of the page.

This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

### IP Address for Syslog

Host IP of destination where syslogs will be sent to. **Check Enable** to enable this function.

### E-mail Alert Enable

Check if you want to enable Email alert(send syslog via email).

### SMTP Server IP and Port

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example,"192.168.1.100:26".

### **Send E-mail alert to**

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

### **E-mail Subject**

The subject of email alert. This setting is optional.

### **Username and Password**

To fill some SMTP server's authentication requirement, you may need to input Username and Password that offered by your ISP.

## Configuration Utility

### SNMP

#### Enable SNMP

You must check either Local or Remote or both to enable SNMP function. If *Local* is checked, this device will response request from LAN. If *Remote* is checked, this device will response request from WAN.

#### Get Community

Setting the community of GetRequest your device will response.

#### Set Community

Setting the community of SetRequest your device will accept.

The screenshot displays the configuration utility interface for a Wireless-G device. At the top, it says "Welcome to WIRELESS-G" and "IDEGEAR Broadband Networking Set-up Wizard". A navigation bar includes "Home", "Logout", "System", "LAN", "Wireless", "Internet", "Security", "NAT", "Advance", and "Summary". A sidebar on the left lists menu items: "Log setting", "SNMP", "Routing", "Schedule Rule", "UPnP Setting", and "Miscellaneous". The main content area is titled "Advance - SNMP" and "WIRELESS-G SNMP". It provides a description: "Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events." Below this, there are input fields for "Enable SNMP" (with radio buttons for "Local" and "Remote"), "Get Community" (set to "public"), "Set Community" (set to "private"), and "WAN Access IP Address" (set to "0.0.0.0"). "Save", "Undo", and "Help" buttons are at the bottom right. The footer contains "©2003 IDEGEAR, Inc." and "All other trademarks belong to its respective owners."

## Routing

Routing Table settings are used to setup the functions of static routing.

### Static Routing

For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

The screenshot displays the 'WIRELESS-G' Configuration Utility interface. At the top, it says 'Welcome to WIRELESS-G' and 'OGEAR Broadband Networking Setup Wizard'. A navigation bar includes 'Home', 'Logout', 'System', 'LAN', 'Wireless', 'Internet', 'Security', 'NAT', 'Advance', and 'Summary'. The main content area is titled 'Advance - Routing' and contains the 'WIRELESS-G Routing' section. Below the title, there is a paragraph: 'If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.' Below this text is a table with 8 rows and 6 columns: ID, Destination, Subnet Mask, Gateway, Hop, and Enable. Each row has input fields for the first five columns and a checkbox for the 'Enable' column. At the bottom right of the table area are 'Save', 'Undo', and 'Help' buttons.

Log setting  
SNMP  
Routing  
Schedule Rule  
UPnP Setting  
Miscellaneous

Advance - Routing

WIRELESS-G

Routing

If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>

Save Undo Help

# Configuration Utility

## Schedule Rule

Select if you want to Enable the Scheduler.

### **Edit**

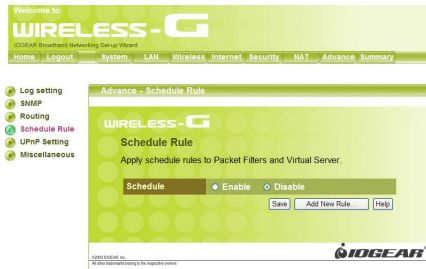
To edit the schedule rule.

### **Delete**

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

### **Add New Rule**

Click “Add New Rule” to enter “Schedule Rule Setting” page to increase a new schedule rule.



## UNP Setting

UPnP is short for Universal Plug and Play which is designed to simplify device and network service installation and management. If you enable this function, the router will work with UPnP devices/softwares.

The screenshot displays the configuration utility interface for the IDGEAR WIRELESS-G router. At the top, it says "Welcome to WIRELESS-G" and "IDGEAR Broadband Networking Setup Wizard". Below this is a navigation menu with options: Home, Logout, System, LAN, Wireless, Internet, Security, NAT, Advance, and Summary. The "Advance" option is selected, leading to the "UPnP Setting" page. On the left side, there is a sidebar menu with icons and labels: Log setting, SNMP, Routing, Schedule Rule, UPnP Setting (which is highlighted), and Miscellaneous. The main content area of the "UPnP Setting" page features the "WIRELESS-G" logo, the title "UPnP Setting", and the description "Allows you to enable UPnP function." Below this, there is a section labeled "UPnP setting" with two radio buttons: "Enable" (which is selected) and "Disable". At the bottom right of this section are three buttons: "Save", "Undo", and "Help". The footer of the page includes the IDGEAR logo and the text "©2005 IDGEAR, Inc. All other trademarks belong to the respective owners."

## Configuration Utility

### Miscellaneous

#### Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. *This setting will be lost after rebooting.*

#### MAC Address for Wake-on-LAN

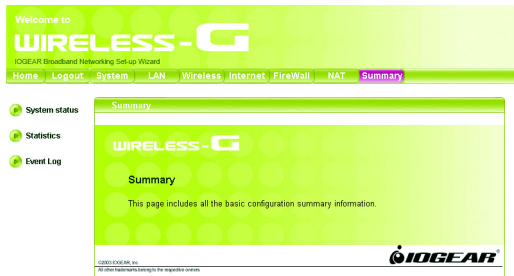
Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

#### Ping Test

Allow you to configure an IP address or a Domain Name, and ping the device. You can ping a specific IP to test whether it is alive.

The screenshot shows the 'Advance - Miscellaneous' configuration page. At the top, there is a navigation menu with 'Home', 'Logout', 'System', 'LAN', 'Wireless', 'Internet', 'Security', 'NAT', 'Advance', and 'Summary'. The 'Advance' menu item is selected. On the left side, there is a sidebar with a tree view containing 'Log setting', 'SNMP', 'Routing', 'Schedule Rule', 'UPnP Setting', and 'Miscellaneous', with 'Miscellaneous' being the active selection. The main content area is titled 'Miscellaneous' and contains the following text: 'Allow you to setup "MAC Address for Wake-on-LAN", "Ping Test" and "Non-standard FTP port" function.' Below this text is a bulleted list of three items: 'MAC Address for Wake-on-LAN' (described as letting you power up another network device remotely), 'Ping Test' (described as allowing you to configure an IP and ping the device), and 'Non-standard FTP port' (described as configuring an item for accessing an FTP server with a non-21 port number). At the bottom of the page, there are three input fields: 'Non-standard FTP port' with a value of '0', 'MAC Address for Wake-on-LAN' with an empty field and a 'Wake up' button, and 'Ping Test' with an empty field and a 'Ping' button. At the very bottom right, there are 'Save', 'Undo', and 'Help' buttons.

## Summary Page



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



# Configuration Utility


## 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.

System Status	
<b>General information</b>	
System Time	2003/12/25 21:19:17
Firmware Version	0.1rc2_beta1
Hardware Version	MWL2104
Firewall	Enabled
<b>Internet Settings</b>	
Connection Status	Dynamic IP - PPPoE
Connection Type	PPPoE
WAN IP Address	Internet connection unsuccessful
Subnet Mask	None
Default Gateway	None
Primary DNS	None
WAN MAC Address	00:0C:55:00:88:1A
Clone MAC Address	00:00:00:00:00:00

## Statistic

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

Statistics			
<b>LAN statistics</b>			
	Transmit		Receive
Total Bytes	6237491	Total Bytes	1211502
Non-unicast packets	0	Non-unicast packets	0
Uni-cast packets	16389	Uni-cast packets	13051
Discards	0	Discards	0
Errors	0	Errors	0
		Unknown Protocols	0
			
<b>WAN statistics</b>			
	Transmit		Receive
Total Bytes	7356	Total Bytes	0
Non-unicast	0	Non-unicast	0

## Event Log

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

Event Log					
Index	Date	Time	Task Name	ID	Event messages
50	2003/12/29	21:20:02	System	109	Respawning pppd
49	2003/12/29	21:20:02	Network	226	PPPOE error: Timeout waiting for PADO packets
48	2003/12/29	21:19:23	System	109	Respawning pppd
47	2003/12/29	21:19:23	Network	226	PPPOE error: Timeout waiting for PADO packets
46	2003/12/29	21:18:43	System	109	Respawning pppd
45	2003/12/29	21:18:43	Network	226	PPPOE error: Timeout waiting for PADO packets
44	2003/12/29	21:18:04	System	109	Respawning pppd
43	2003/12/29	21:18:04	Network	226	PPPOE error: Timeout waiting for PADO packets
42	2003/12/29	21:17:23	System	109	Respawning pppd
41	2003/12/29	21:17:23	Network	226	PPPOE error: Timeout waiting for PADO packets
40	2003/12/29	21:16:44	System	109	Respawning pppd
39	2003/12/29	21:16:44	Network	226	PPPOE error: Timeout waiting for PADO packets
38	2003/12/29	21:16:05	System	109	Respawning pppd
37	2003/12/29	21:16:05	Network	226	PPPOE error: Timeout waiting for PADO packets
36	2003/12/29	21:15:25	System	109	Respawning pppd
35	2003/12/29	21:15:25	Network	226	PPPOE error: Timeout waiting for PADO packets
34	2003/12/29	21:14:46	System	109	Respawning pppd
33	2003/12/29	21:14:45	Network	226	PPPOE error: Timeout waiting for PADO packets
32	2003/12/29	21:12:51	System	109	Respawning pppd
31	2003/12/29	21:12:51	Network	226	PPPOE error: Timeout waiting for PADO packets
30	2003/12/29	21:12:11	System	109	Respawning pppd
29	2003/12/29	21:12:11	Network	226	PPPOE error: Timeout waiting for PADO packets

## Specification

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 detachable antenna

## 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](http://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 866-946-4327 or by email **[support@iogear.com](mailto: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.

## Limited Warranty

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](http://www.iogear.com)