



DRG600-WiFi

USER GUIDE

P/N: DFB601CW

Copyright © 2008. All Rights Reserved.

Printed May 15, 2008

All trademarks and trade names are the properties of their respective owners.

Contents

INTRODUCTION.....	10
DRG600 WiFi FEATURES.....	10
<i>Internet Access Features.....</i>	<i>10</i>
<i>Advanced Internet Functions.....</i>	<i>11</i>
<i>Wireless Features.....</i>	<i>11</i>
<i>LAN Features.....</i>	<i>11</i>
<i>Configuration & Management.....</i>	<i>12</i>
<i>Security Features.....</i>	<i>12</i>
PACKAGE CONTENTS.....	13
PHYSICAL DETAILS.....	14
<i>Top mounted LEDs.....</i>	<i>14</i>
<i>Bottom Panel.....</i>	<i>15</i>
INSTALLATION.....	16
REQUIREMENTS.....	16
INSTALLATION PROCEDURE.....	16
SETUP.....	18
OVERVIEW.....	18
CONFIGURATION PROGRAM.....	19
<i>Preparation.....</i>	<i>19</i>
<i>Using UPnP.....</i>	<i>19</i>
<i>Using your Web Browser.....</i>	<i>19</i>
SETUP WIZARD.....	21
STATUS SCREEN.....	24
<i>Navigation & Data Input.....</i>	<i>25</i>
LAN SCREEN.....	26
<i>TCP/IP.....</i>	<i>26</i>
DHCP.....	27

<i>What DHCP Does</i>	27
<i>Using the DRG600-WiFi DHCP Server</i>	27
<i>Using another DHCP Server</i>	27
<i>PC Database</i>	28
PC DATABASE SCREEN.....	29
<i>PC Properties</i>	29
WIRELESS	31
<i>Identification</i>	31
<i>Options</i>	32
<i>Wireless Security</i>	32
<i>Access point</i>	32
WIRELESS SECURITY SCREEN.....	34
WIRELESS SECURITY - WEP.....	35
<i>WEP</i>	35
WIRELESS SECURITY - WPA-PSK/WPA2-PSK/WPA-PSK+WPA2-PSK.....	36
WI-FI PROTECTED SETUP.....	37
<i>What is WPS (Wi-Fi Protected Setup)?</i>	37
<i>WPS</i>	37
<i>Status</i>	37
<i>PBC</i>	37
<i>Wireless Access Point</i>	37
PASSWORD SCREEN.....	39
PC CONFIGURATION	40
OVERVIEW	40
TCP/IP SETTINGS - OVERVIEW	40
<i>Checking TCP/IP Settings - Windows 9x/ME:</i>	41
<i>Using "IP Address" (DHCP)</i>	41
<i>Using "Specify an IP Address"</i>	42
CHECKING TCP/IP SETTINGS - WINDOWS NT4.0	43
<i>Obtain an IP address from a DHCP Server</i>	44

<i>Specify an IP Address</i>	45
CHECKING TCP/IP SETTINGS - WINDOWS 2000:	47
<i>Obtain an IP Address automatically</i>	48
<i>Use the following IP Address</i>	48
CHECKING TCP/IP SETTINGS - WINDOWS XP	49
<i>Using DHCP</i>	50
<i>Using a fixed IP address</i>	50
INTERNET ACCESS	51
<i>For Windows 9x/ME/2000</i>	51
<i>For Windows XP</i>	51
<i>Macintosh Clients</i>	51
<i>Linux Clients</i>	52
Fixed IP Address	52
To act as a DHCP Client (recommended).....	52
<i>Other Unix Systems</i>	52
WIRELESS STATION CONFIGURATION.....	53
STATUS	54
STATUS SCREEN.....	54
<i>Internet</i>	54
<i>Wireless</i>	55
<i>LAN</i>	56
<i>System</i>	56
CONNECTION STATUS - PPPoE	57
<i>Connection</i>	57
<i>Connection Log</i>	58
<i>Buttons</i>	58
<i>Connection Log Messages</i>	58
CONNECTION DETAILS - FIXED/DYNAMIC IP ADDRESS	60
<i>Internet</i>	60
ADVANCED FEATURES	62

OVERVIEW	62
ACCESS CONTROL	63
ACCESS CONTROL SCREEN	63
<i>Group</i>	63
<i>Internet Access</i>	64
<i>Define Schedule</i>	64
<i>View Log</i>	64
<i>Clear Log</i>	64
MEMBERS SCREEN	65
DEFINE SCHEDULE.....	66
SERVICES SCREEN	67
<i>Available Services</i>	67
<i>Add New Service</i>	67
DYNAMIC DNS (DOMAIN NAME SERVER)	68
DYNAMIC DNS SCREEN	69
<i>DDNS Data</i>	69
DMZ.....	70
VIRTUAL SERVERS.....	71
VIRTUAL SERVERS SCREEN.....	72
<i>Servers</i>	72
<i>Properties</i>	73
DEFINING YOUR OWN VIRTUAL SERVERS.....	74
<i>Create a new Server</i>	74
<i>Modify (Edit) a Server</i>	74
<i>Delete a Server</i>	74
<i>Connecting to the Virtual Servers</i>	74
WAN PORT CONFIGURATION SCREEN	75
<i>Identification</i>	75
<i>IP Address</i>	75
<i>DNS</i>	76

<i>Backup DNS</i>	76
MTU.....	76
Login.....	76
ROUTING.....	78
ROUTING SCREEN.....	79
<i>Static Routing Table</i>	79
RIP.....	79
<i>Static Routing</i>	79
<i>Properties</i>	80
<i>Generate Report</i>	80
CONFIGURING OTHER ROUTERS ON YOUR LAN.....	80
<i>Local Router</i>	80
<i>Other Routers on the Local LAN</i>	81
<i>Static Routing - Example</i>	81
DRG600-WiFi Routing Table.....	81
Router A Default Route.....	82
Router B Default Route.....	82
SECURITY.....	83
<i>Firewall</i>	83
<i>URL Filter</i>	83
<i>Options</i>	84
URL FILTER SCREEN.....	85
<i>Filter Strings</i>	85
<i>Add Filter String</i>	85
UPNP.....	86
UPnP.....	86
ADMINISTRATION.....	87
OVERVIEW.....	87
DEFAULT CONFIG SCREEN.....	88
<i>Retrieve Config file</i>	88

<i>Default Config</i>	88
LOGS SCREEN.....	89
<i>Enable Logs</i>	89
<i>E-Mail Reports</i>	90
<i>E-Mail Address</i>	90
<i>Local Time</i>	91
NETWORK DIAGNOSTICS SCREEN.....	92
<i>Ping</i>	92
<i>DNS Lookup</i>	92
LOCAL ADMINISTRATION SCREEN.....	93
<i>Local Administration</i>	93
UPGRADE FIRMWARE SCREEN.....	95
<i>Upgrade Firmware</i>	95
TROUBLESHOOTING	96
OVERVIEW.....	96
<i>General Problems</i>	96
<i>Internet Access</i>	96
<i>Wireless Access</i>	97
ABOUT WIRELESS LANS	98
MODES.....	98
<i>Ad-hoc Mode</i>	98
<i>Infrastructure Mode</i>	98
BSS/ESS.....	98
<i>BSS</i>	98
<i>ESS</i>	98
CHANNELS.....	99
WEP.....	99
WPA-PSK.....	100
WPA2-PSK.....	100
WIRELESS LAN CONFIGURATION.....	101

<i>Mode</i>	101
<i>SSID (ESSID)</i>	101
<i>Security</i>	101
SPECIFICATIONS	102
MULTI-FUNCTION DRG600-WiFi.....	102
<i>Wireless Interface</i>	103
REGULATORY APPROVALS.....	103

Introduction

1

This Chapter provides an overview of the DRG600 WiFi features and capabilities.

Congratulations on the purchase of your new **DRG600 WiFi** wireless router. The DRG600-WiFi is a multi-function device providing the following services:

- Broadband router for all LAN users.
- **2-Port Fast Ethernet Switch** for 10BaseT or 100BaseT connections.
- **Wireless Access Point** for 802.11b and 802.11g Wireless Stations.

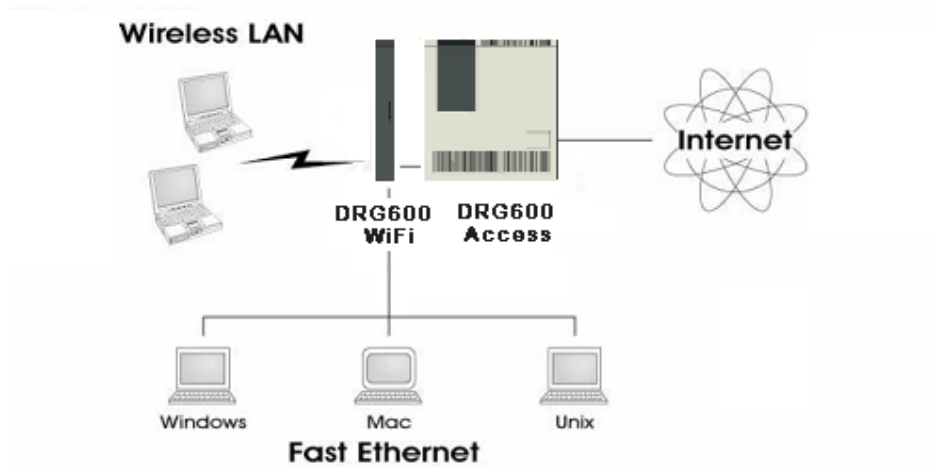


Figure 1. DRG600 in the broadband network

DRG600 WiFi Features

The DRG600-WiFi incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the DRG600-WiFi, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation)
- **Fixed or Dynamic IP Address.** On the Internet connection, the DRG600-WiFi supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.
- **PPPoE support.** Connecting to the Internet using Point to Point Protocol over Ethernet (PPPoE) is also supported.

Advanced Internet Functions

- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **DDNS Support.** DDNS (Dynamic DNS) allows Internet users to connect to Virtual Servers on your LAN using a domain name, even if your IP address is not fixed.
- **DMZ.** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- **URL Filter.** Use the URL Filter to block access to undesirable Web sites by LAN users.
- **Internet Access Log.** See which Internet connections have been made.
- **Access Control.** Using the Access Control feature, you can assign LAN users to different groups, and determine which Internet services are available to each group.
- **VPN Pass through Support.** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPsec are transparently supported - no configuration is required.

Wireless Features

- **Standards Compliant.** The DRG600-WiFi complies with the IEEE802.11 b/g specifications for Wireless LANs.
- **Supports both 802.11b and 802.11g Wireless Stations.** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- **Speeds up to 54Mbps.** All speeds up to the 802.11g maximum of 54Mbps are supported.
- **WEP support.** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- **WPA support.** Support for WPA is included. WPA is more secure than WEP, and should be used if possible.
- **WPA2 support.** Support for WPA2 is also included. WPA2 uses the extremely secure AES encryption method.
- **Wireless MAC Access Control.** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.
- **WPS Support.** WPS (Wi-Fi Protected Setup) can simplify the process of connecting any compatible device to the wireless network by using the push button configuration (PBC) on the Wireless Access Point, or entering a 8-digit PIN code.

LAN Features

- **2-Port Fast ethernet switch.** The DRG600-WiFi incorporates a 2-port 10/100BaseT fast ethernet switch, making it easy to create or extend your LAN.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The DRG600-WiFi can act as a **DHCP Server** for devices on your local

LAN and WLAN.

- **Multi Segment LAN Support.** LANs containing one or more segments are supported, via the DRG600-WiFi's RIP (Routing Information Protocol) support and built-in static routing table.

Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN or WLAN for configuration (if permitted by service provider).
- **Network Diagnostics.** You can use the DRG600-WiFi to perform a *Ping* or *DNS lookup*.
- **UPnP Support.** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the NAT service on DRG600-WiFi. UPnP is by supported by Windows ME, XP, or later.

Security Features

- **Password - protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **Wireless LAN Security.** WEP, WPA and WPA2 data encryption protocols are supported, as well as wireless access control, to prevent unknown wireless stations from accessing your LAN.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the DRG600-WiFi.
- **Stateful Inspection Firewall.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Protection against DoS attacks.** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The DRG600-WiFi incorporates protection against DoS attacks.

Package Contents

The following items are included in your DRG600-WiFi package:

- DRG600-WiFi Unit
- TP LAN cable
- Quick Guide leaflet
- CD-ROM containing this online manual

If any of the above items are damaged or missing, please contact your vendor immediately.

Physical Details

Top mounted LEDs



Figure 2. Top mounted LEDs



This button has two (2) functions:

Reset. When this button is pressed and released, the DRG600-WiFi will reboot (restart).

Clear All Data. This button can also be used to clear ALL data and restore ALL settings to the factory default values. To clear all data and restore the factory default values, press this button for 8 seconds and then release it.



OFF- Power OFF.

GREEN - Power ON. If flashing, the module is still starting up. When the DRG600-WiFi is operating correctly, it is constantly lit.

RED- WAN error. If this LED is lit, then it means that there is an irreparable operating error. Contact your ISP (Internet Service Provider).



ON – WLAN connection is available. If blinking, WLAN connection is ACTIVE.

OFF- WLAN is OFF.

Bottom Panel

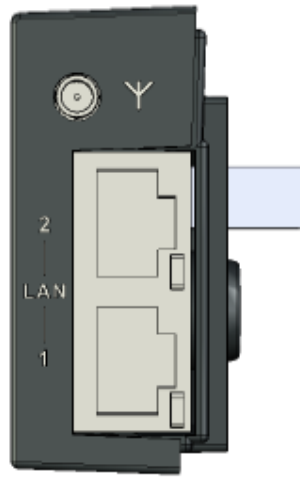


Figure 3. Bottom Panel

Y Antenna External antenna socket

LAN 1-2 Local Area Network (LAN) device ports. Use standard LAN cables (RJ45 connectors) to connect your LAN devices to these ports.

Installation

2

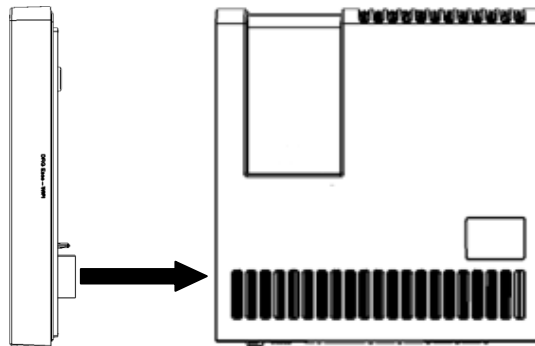
This chapter describes the physical installation of the DRG600 WiFi.

Requirements

- Network cable. Use standard 10/100BaseT network (UTP) cables with RJ45 connector.
- DRG600-Access with a valid Internet subscription must be available.
- All wireless devices must be compliant with the IEEE802.11b or IEEE802.11g specifications.

Installation Procedure

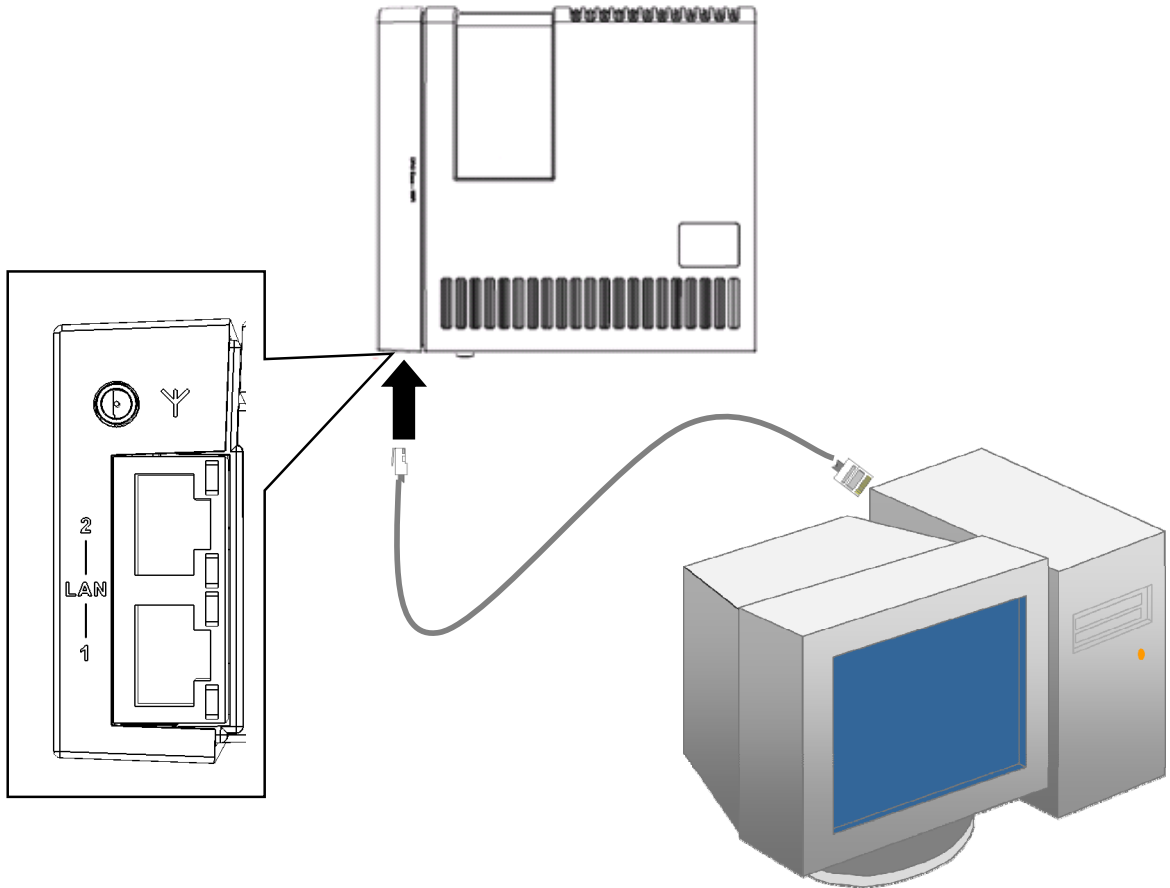
1. Locate the docking socket for the DRG600-WiFi on the DRG600-Access internet access module installed in your home.



2. Connect LAN Cable

Use the supplied standard LAN cable to connect a PC to one of the LAN ports on the bottom of the DRG600-WiFi.

If required, connect any port to a normal port on another Hub, using a standard LAN cable. Any LAN port on the DRG600-WiFi will automatically function as an "Uplink" port when required.



3. Check the LEDs

- The *Power* LED should be **GREEN**. (If it is **RED**, then the Internet connection is not available, you can still run the configuration software as this is stored on the device itself).
- The *WLAN* LED should be **GREEN**
- For each LAN (PC) connection, the LAN *Link/Act* LED should be ON (provided the PC is also ON.)

For more information, refer to *Top-mounted LEDs* in Chapter 1.

This Chapter provides details on how to setup your network with the DRG600-WiFi.

Overview

This chapter describes the setup procedure for:

- Internet Access
- Wireless setup
- LAN configuration
- Assigning a Password to protect the configuration data.

PCs on your local LAN may also require configuration. For details, see *PC Configuration* on page 40.

Other configuration may also be required, depending on which features and functions of the DRG600-WiFi you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	PC Configuration on page 40
Check DRG600-WiFi operation and Status.	Operation and Status on page Error! Bookmark not defined.
Use any of the following Advanced features: <ul style="list-style-type: none"> • Access Control • Dynamic DNS • DMZ • Routing (RIP and Static Routing) • Security • UPnP • Virtual Servers (Port Forwarding) • WAN Port 	Advanced Features on page 62
Use any of the following Administration Configuration settings or features:	Administration on page 87

- | | |
|--|--|
| <ul style="list-style-type: none">• Default Config• Logs• Network Diagnostics (Ping, DNS Lookup)• Local Administration• Upgrade Firmware | |
|--|--|

Configuration Program

The DRG600-WiFi contains an HTTP server. This enables you to connect to the server and configure the device using your web browser. **Your browser must support Javascript.**

The configuration program has been tested on the following browsers:

- Safari version 1.2 or later
- Firefox version 2.0 or later
- Internet Explorer version 6.0 or later

Preparation

Before attempting to configure the DRG600-WiFi, please ensure that:

Your PC can establish a physical connection to the DRG600-WiFi. The PC and the DRG600-WiFi must be directly connected (using the LAN ports on the DRG600-WiFi) or on the same LAN segment.

The DRG600-WiFi must be installed and powered ON.

Using UPnP

If your Windows system supports UPnP, an icon for the DRG600-WiFi will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut to the newly-discovered device.

Unless you intend to change the IP Address of the DRG600-WiFi, you can accept the desktop shortcut.

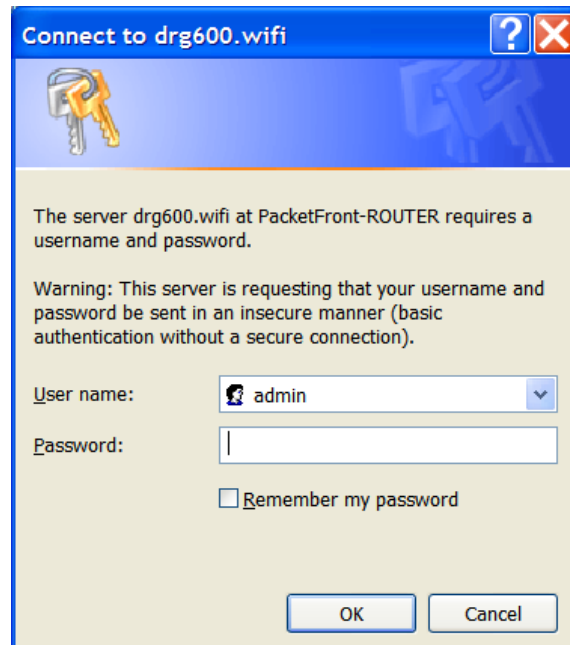
Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places* (previously called *Network Neighborhood*).

Double-click the icon for the DRG600-WiFi (either on the Desktop, or in *My Network Places*) to start the configuration. Refer to the following section *Setup Wizard* for details of the initial configuration process.

Using your Web Browser

To establish a connection from your PC to the DRG600-WiFi:

1. After installing the DRG600-WiFi and any LAN devices, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. Go to <http://drg600.wifi> or use the DRG600-WiFi IP Address: <http://192.168.0.1>
The Login screen will appear.



4. To connect to the DRG600-WiFi, logon with the user name **admin**. There is no password by default. Click **OK**.

If you cannot connect to the DRG600-WiFi setup webpage

If the DRG600-WiFi does not respond, check the following:

- The DRG600-WiFi is properly attached, WLAN/LAN and Power LEDs are ON.
- You can test the connection by using the "Ping" command. To do this:
 1. Open the MS-DOS window or command prompt window.
 2. Enter the command: `ping 192.168.0.1`

If no response is received, either the connection is not working, or your PC IP address is not compatible with the DRG600-WiFi IP Address. (See next item.)

3. If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the DRG600-WiFi default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *PC Configuration* on page 40 for details on checking your PC TCP/IP settings.
- Ensure that your PC and the DRG600-WiFi are on the same network segment. (If you don't have a router, this must be the case.)
 - Ensure you are using the wired LAN interface.

Setup Wizard

It is recommended to use the Setup Wizard link on the main menu. This Wizard guides you through configuration of the DRG600-WiFi for Internet access and wireless settings.



Figure 4. Setup Wizard start screen

1. Click Next to proceed to the **Internet Access** screen.
(If DRG600-WiFi has successfully established WAN connection using DHCP, this step will be skipped and you will go directly to the **Wireless Settings** screen described in step 3)



Figure 5. Setup Wizard for Internet Access


2. You need to know the type of Internet connection service used by your ISP. The common connection types are explained in the table below.

Type	Details	ISP Data required
------	---------	-------------------

DHCP	Your IP Address is allocated automatically, when you connect to your ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	Assigned IP address and netmask, IP addresses of the default gateway and DNS server(s). Some ISP's may also require you to use a particular Host-name, Domain name, or MAC (physical) address.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.

3. If your connection is already setup, then you will go directly to the wireless configuration:

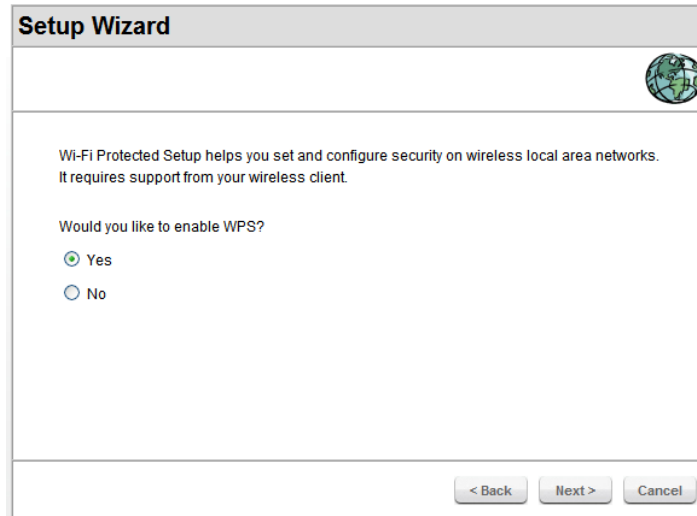
Setup Wizard



You had set up your Router, would you like to use Wizard to configure **Wireless** part now?

Yes
 No

4. If you want to deactivate WPS for any reason, then you will get a chance to do so:



Setup Wizard

Wi-Fi Protected Setup helps you set and configure security on wireless local area networks. It requires support from your wireless client.

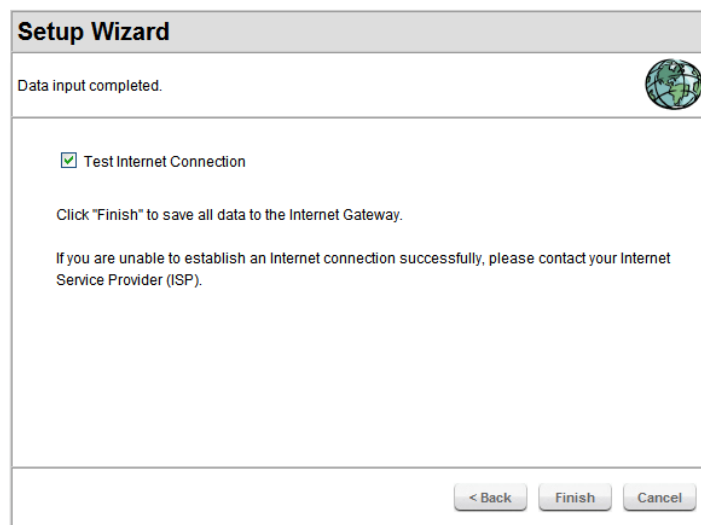
Would you like to enable WPS?

Yes

No

< Back Next > Cancel

5. Finally, you can test that your Internet connection is working properly (the test takes about 25 seconds):



Setup Wizard

Data input completed.

Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

If you are unable to establish an Internet connection successfully, please contact your Internet Service Provider (ISP).

< Back Finish Cancel

If the connection test fails:

- Check your data, the Access LEDs, and all connections.
- Check that you have entered all data correctly.
- Your ISP may have recorded the MAC (physical) address of your PC. Go to **Advanced**, and on the **WAN Port** screen, use the *Copy from PC* button to copy the MAC address from your PC to the DRG600-WiFi.

Status Screen

After finishing the Setup Wizard, you will see the *DRG600-WiFi* home page. Hereafter, you will see this screen whenever you connect. An example of the home page is shown below.

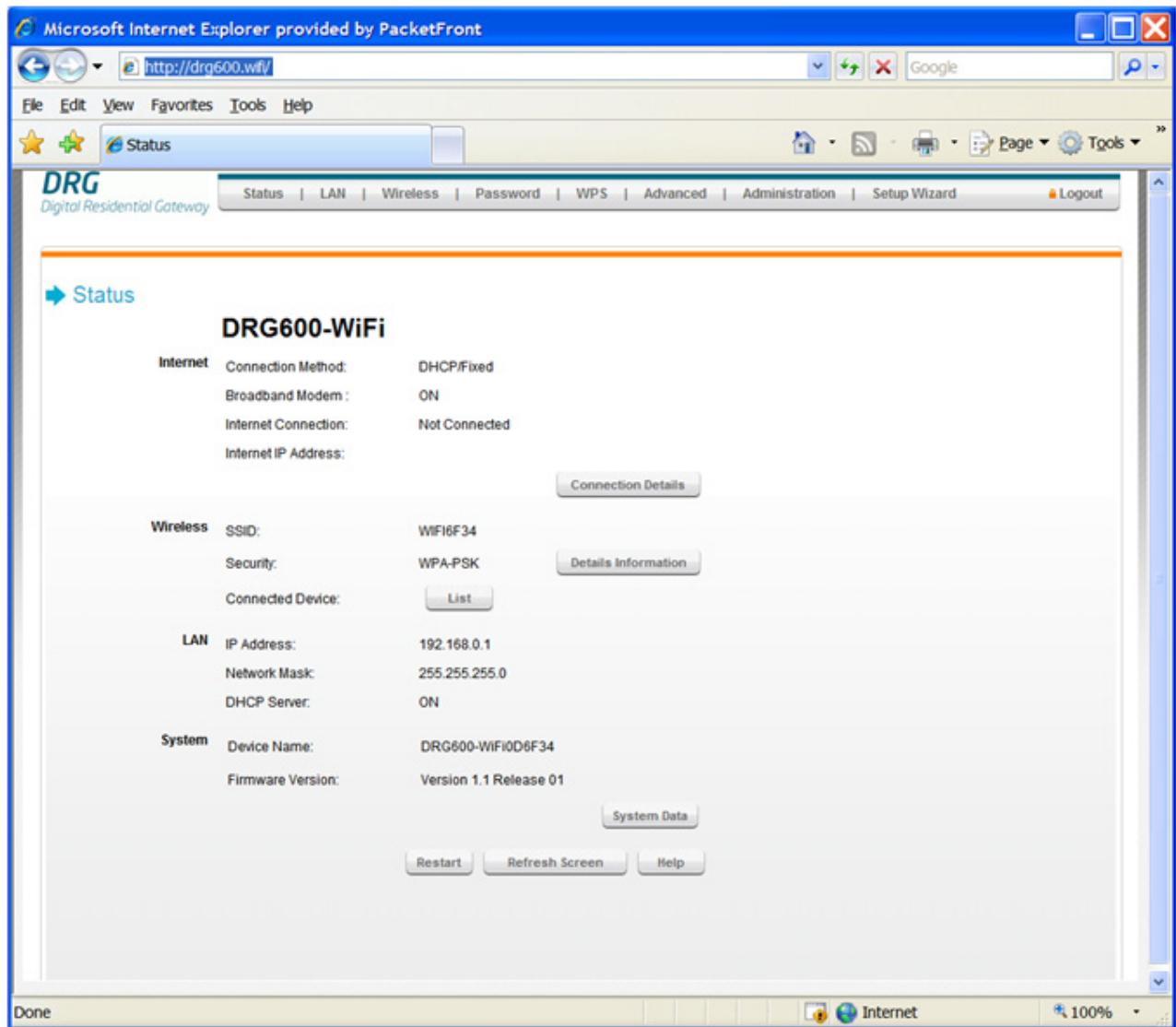


Figure 6. DRG600-WiFi home page

Navigation & Data Input

Use the menu bar at the top of the screen for navigation.

Changing to another screen without clicking **Save** does NOT save any changes you may have made. You must use **Save** before changing screens, or your changes will be discarded.



On each screen, clicking the **Help** button will display help for that screen.

LAN Screen

Use the *LAN* link on the main menu to reach the LAN screen. An example screen is shown below.

Figure 7. LAN Screen

TCP/IP

IP Address	IP address for the DRG600-WiFi, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Network Mask for the LAN segment to which the DRG600-WiFi is attached. i.e. the same value as the PCs on that LAN segment.
DHCP Server	<p>If Enabled, the DRG600-WiFi will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled.</p> <p>If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the DRG600-WiFi as the default Gateway. See the following section for further details.</p> <p>The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.</p> <p>See the following section for further details on using DHCP.</p>
Save	This button saves any changes you have made. Note that if you change the DRG600-

	WiFi's IP address, your connection will be lost. You will have to reconnect using the new IP address (or the URL http://drg600.wifi).
Cancel	The Cancel button will discard any data you have entered and reload the file from the DRG600-WiFi.

DHCP

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

The client request is made when the client device starts up (boots).

The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.

The DRG600-WiFi can act as a **DHCP server**.

Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".

You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the DRG600-WiFi DHCP Server

This is the default setting. The DHCP Server settings are on the **LAN** screen. On this screen, you can:

Enable or Disable the DRG600-WiFi's *DHCP Server* function.

Set the range of IP Addresses allocated to PCs by the DHCP Server function.



Note!

You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the DRG600-WiFi's, the following procedure is required.

1. Disable the DHCP Server feature in the DRG600-WiFi. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the DRG600-WiFi's IP Address as the *Default Gateway*.
3. Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME.

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC). For most users, it eliminates the need to enter IP addresses, and also prevents errors.

However, if you need to configure the Wireless Router BEFORE installation, you must use this functionality.

Known PCs	This lists all current entries (PCs or network devices).															
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC "hostname".															
IP Address	If adding a new PC to the list, enter the IP Address of the PC here. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.															
Add	Use this button to add the PC to the list. The data for the selected PC will then be shown while it is selected. (Click "Refresh" to reload the current data.)															
Advanced Administration	Use this button to see more details. You will be taken to the PC Database screen where you can edit more properties. See "PC Database screen" on page 29.															
Delete	Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none"> • The PC has been removed from your LAN. • The entry is incorrect. 															
Refresh	Updates the fields in this screen. Any new clients discovered will be displayed in the Known PCs field															
Generate Report	This opens the report window and displays details for all PCs in the PC Database: <div data-bbox="430 1215 1242 1491" data-label="Image"> <table border="1"> <thead> <tr> <th colspan="5">PC Database</th> </tr> <tr> <th>Name</th> <th>IP Address</th> <th>Physical Address (Hardware Address)</th> <th>Type</th> <th>DHCP Client</th> </tr> </thead> <tbody> <tr> <td>unknown</td> <td>192.168.0.3</td> <td>00-15-c5-08-fe-e0</td> <td>LAN</td> <td>DHCP</td> </tr> </tbody> </table> </div>	PC Database					Name	IP Address	Physical Address (Hardware Address)	Type	DHCP Client	unknown	192.168.0.3	00-15-c5-08-fe-e0	LAN	DHCP
PC Database																
Name	IP Address	Physical Address (Hardware Address)	Type	DHCP Client												
unknown	192.168.0.3	00-15-c5-08-fe-e0	LAN	DHCP												

PC Database screen

This screen is displayed if the "Advanced Administration" button in the **LAN** screen is clicked. It provides more configuration options than the standard *PC Database* fields in the **LAN** screen.

➔ PC Database (Admin)

Any PC may be added, edited or deleted. If adding a PC which is not connected and On, you must provide the MAC (hardware) address

Known PCs

unknown 192.168.0.3 (LAN) 0015c508fee0(DHCP)

Edit Delete

PC Properties

Name:

IP Address: Automatic (DHCP Client)
 DHCP Client - reserved IP address: . . .
 Fixed IP address (set on PC): . . .

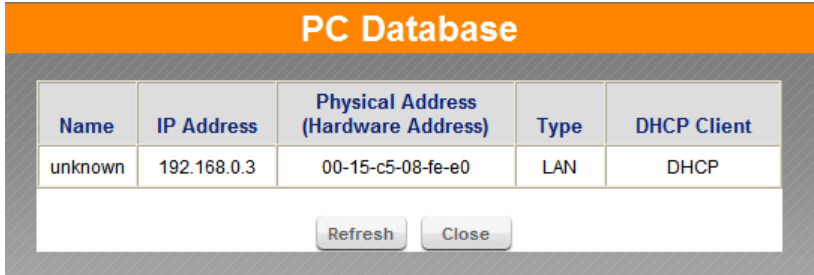
MAC Address: Automatic discovered (PC must be available on LAN)
 MAC address is

Add as New Entry Update Selected PC Clear Form

Refresh Generate Report Back Help

PC Properties

Name	Enter the name for the PC here. It is best if this matches the PC "hostname".
IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> • <i>Automatic</i> - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The Wireless Router will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • <i>DHCP Client - Reserved IP Address</i> - Select this if the PC is set to be a DHCP client, and you wish to guarantee that the Wireless Router will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the Wireless Router's IP address. • <i>Fixed IP Address</i> - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)
MAC Address	<p>Select the appropriate option</p> <ul style="list-style-type: none"> • <i>Automatic discovery</i> - Select this to have the Wireless Router contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On.

	<ul style="list-style-type: none"> • <i>MAC address is</i> - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The Wireless Router uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank. 															
Add as New Entry	This button add a new PC to the list, using the data in the "PC Properties" box.															
Update Selected PC	This button updates the selected PC with the data in the fields.															
Clear Form	This button clears the "Properties" box to data for a new PC.															
Refresh	This button updates the data on the screen.															
Generate Report	<p>This opens a report window and displays details for all PCs in the PC Database.</p>  <table border="1"> <thead> <tr> <th colspan="5">PC Database</th> </tr> <tr> <th>Name</th> <th>IP Address</th> <th>Physical Address (Hardware Address)</th> <th>Type</th> <th>DHCP Client</th> </tr> </thead> <tbody> <tr> <td>unknown</td> <td>192.168.0.3</td> <td>00-15-c5-08-fe-e0</td> <td>LAN</td> <td>DHCP</td> </tr> </tbody> </table> <p>Refresh Close</p>	PC Database					Name	IP Address	Physical Address (Hardware Address)	Type	DHCP Client	unknown	192.168.0.3	00-15-c5-08-fe-e0	LAN	DHCP
PC Database																
Name	IP Address	Physical Address (Hardware Address)	Type	DHCP Client												
unknown	192.168.0.3	00-15-c5-08-fe-e0	LAN	DHCP												
Back	Click this button to go back to the "LAN" screen.															

Wireless

The DRG600-WiFi settings must match the other Wireless stations.



By default, the DRG600-WiFi will automatically accept both 802.11b and 802.11g connections, and no configuration is required for this feature.

To change the DRG600-WiFi's default settings for the Wireless Access Point feature, use the *Wireless* link on the main menu to reach the **Wireless** screen. An example screen is shown below.

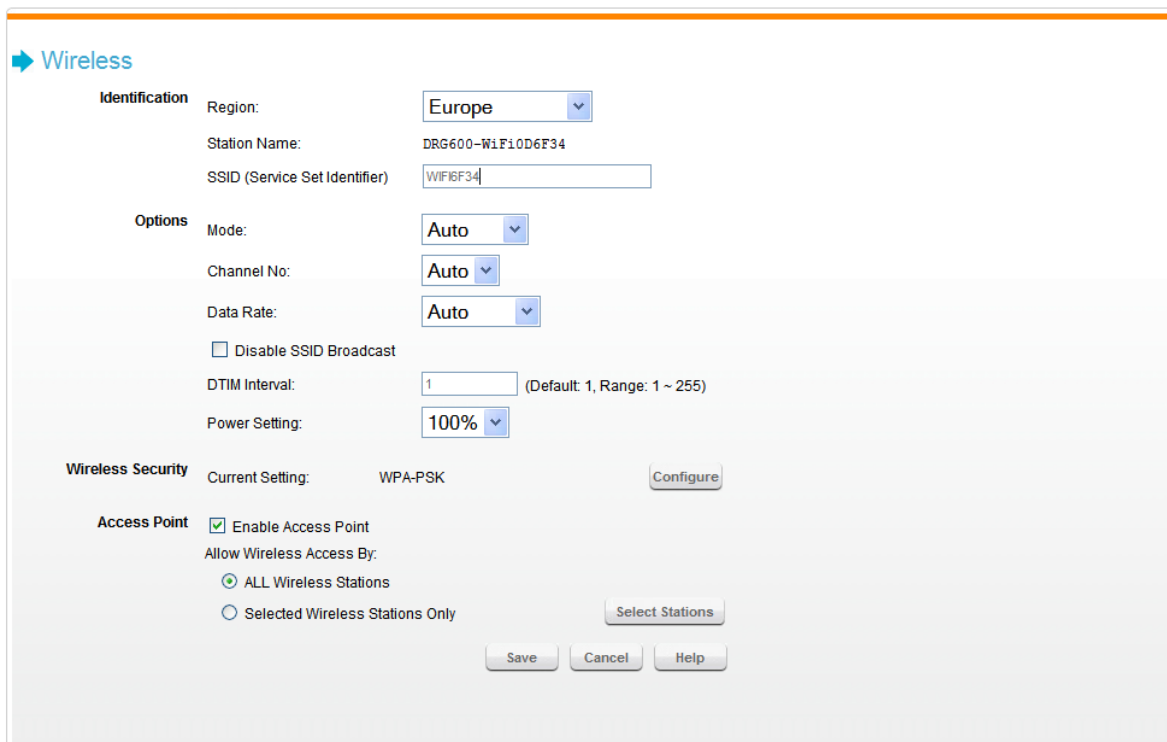


Figure 8. Wireless Screen

Identification

Region	Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency for more information on which channels you are allowed to use, and select a region which allows those channels. (The channel list changes according to the selected region.)
Station Name	The device name is displayed (cannot be changed).
SSID	On your PC, some Wireless status screens may display this name as the Access Point in use. If using an ESS (Extended Service Set, with multiple access points) this ID is called an

ESSID (Extended Service Set Identifier).

To communicate, all Wireless stations should use the same SSID/ESSID.

Options

Mode	<p>Auto - This is the default, and should normally be used. Both 802.11b and 802.11g wireless stations can use the wireless network..</p> <p>802.11g - Only 802.11g Wireless stations can use the Wireless Router.</p> <p>802.11b - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the DRG600-WiFi if they are fully backward-compatible with the 802.11b standard.</p>
Channel No.	<p>This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. The default is Auto.</p>
Broadcast SSID	<p>If Enabled, the SSID will broadcast its name to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point..</p>
DTIM Interval	<p>(Advanced feature) Increasing DTIM interval allows wireless clients to conserve power more effectively but may increase delays in reception of multicast traffic.</p>
Power setting	<p>Adjusts the power strength of the wireless signal. Reduce the power strength may reduce the wireless coverage.</p>

Wireless Security

Current Setting	<p>The current wireless security encryption method is displayed. Default value is WPA-PSK. Click the “Configure” button to access the Wireless security sub-screen, and modify the security settings as required. See “Wireless Security Screen” on page 34 for more details.</p>
------------------------	--

Access point

Enable Access	<p>When this setting is selected, traffic is allowed to pass according to the following:</p>
----------------------	--

Point	<ul style="list-style-type: none">• All Wireless stations – when checked, Internet access is allowed for all connected wireless clients. Otherwise, all traffic is blocked.• Selected Wireless stations only – Only selected wireless stations use the access point to access the Internet. To select the required wireless stations, click the "Select Stations" button.
Save	This button saves the data displayed on the screen.
Cancel	This button will discard any data you have entered since the last “Save” operation.

Wireless Security Screen

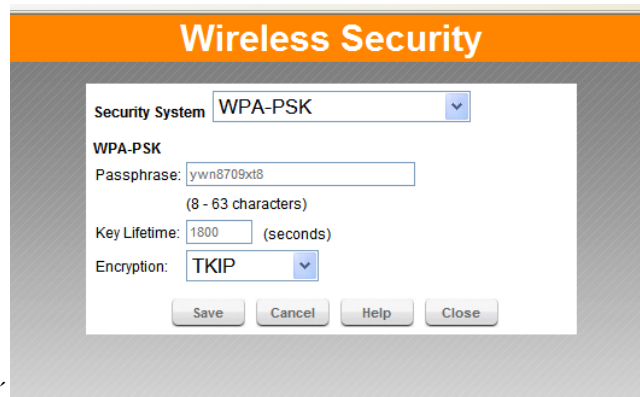


Figure 9. Wireless Security Screen

This screen is accessed by clicking the *Configure* button on the **Wireless** screen. There are five options for Wireless security:

- **None** - no data encryption is used.
- **WEP** - data is encrypted using the WEP standard.
- **WPA -PSK** - data is encrypted using the WPA standard. This is a later standard than WEP, and provides much better security than WEP.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security.
- **WPA-PSK + WPA2-PSK** - This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK OR WPA2-PSK.

Wireless Security - WEP



Figure 10. Figure 8: WEP Screen

WEP

Authentication	<p>Normally this can be left at the default value of "Auto". If that fails, select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.</p>
Key Size	<p>Select the WEP Encryption level:</p> <ul style="list-style-type: none"> • 64-bit (sometimes called 40-bit) encryption • 128-bit encryption
Passphrase	<p>Enter a word or group of printable characters in the Passphrase box and click the "Generate " button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key fields will be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key field will be given a key value.</p>
Key 1-4	<p>Use the radio buttons to select the default key.</p> <p>Enter the key value you wish to use. Other stations must have the same key values.</p> <p>Keys must be entered in Hex. Hex characters are the digits (0 ~ 9) and the letters A ~ F.</p>

Wireless Security - WPA-PSK/WPA2-PSK/WPA-PSK+WPA2-PSK

If WPA-PSK, WPA2-PSK, or WPA-PSK+WPA2-PSK is selected, the screen will look like the following example:

Figure 11. WPA/WPA2-PSK screen

Passphrase (PSK)	Enter the Network key value. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Key Lifetime	This determines how often the encryption key is changed. Enter the desired value.
Encryption	Select the desired option. Wireless Stations must use the same method.

Wi-Fi Protected Setup

What is WPS (Wi-Fi Protected Setup)?

WPS (Wi-Fi Protected Setup) was introduced and developed by the Wi-Fi Alliance (<http://www.wi-fi.org/>) to help standardize and simplify ways of setting up and configuring security on a wireless network. WPS simplifies the wireless network security configuration so that it can be done by simply typing a short PIN (numeric code) or by pushing a button (Push-Button Configuration).

Click *Wi-Fi Protected Setup* on the Wireless screen to view a screen like the following.

Figure 12. Wi-Fi Protected Setup Screen

WPS

Select “enable” or “disable”.

Status

Displays the WPS status. Press “Clear” to reset.

PBC

Click *WPS* to configure WPS certified devices with Push Button Configuration (PBC).

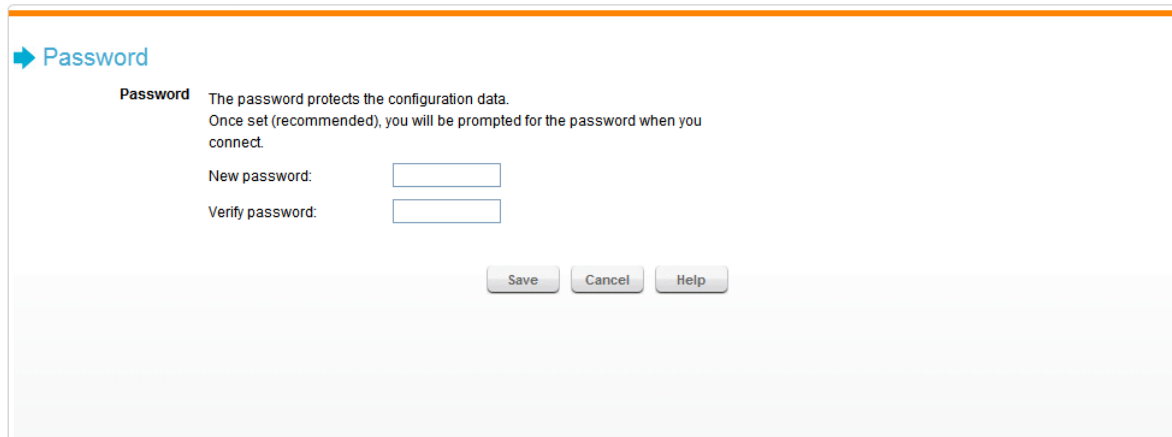
Wireless Access Point

Enrollee’s PIN	Enter the PIN code and click <i>Add Client to AP</i> to add the client device.
Device PIN	Displays the current device PIN

Generate PIN	Click the <i>Generate PIN</i> button to have the new pin code displayed in the field. <i>Set Default PIN</i> reloads the factory settings for WPS.
--------------	--

Password Screen

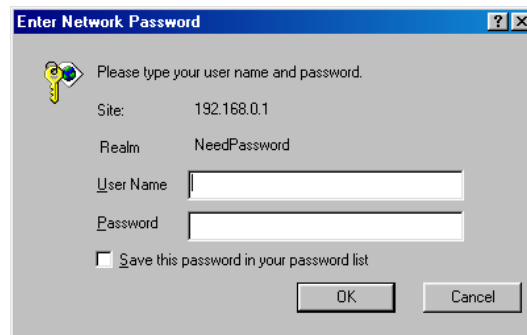
To prevent unauthorized persons changing the DRG600-WiFi settings, the password screen allows you to assign a password to the DRG600-WiFi configuration.



The screenshot shows a web-based configuration interface titled "Password". It includes a heading "Password" with a blue arrow icon. Below the heading, there is explanatory text: "The password protects the configuration data. Once set (recommended), you will be prompted for the password when you connect." There are two input fields: "New password:" and "Verify password:". At the bottom of the form, there are three buttons: "Save", "Cancel", and "Help".

Figure 13. Password Screen

Once you have assigned a password to the DRG600-WiFi (on the *Password* screen above), you will be prompted for the password the next time you connect to the setup program, as shown below.



The screenshot shows a Windows-style dialog box titled "Enter Network Password". It contains a key icon and the text "Please type your user name and password." Below this, there are fields for "Site:" (192.168.0.1) and "Realm:" (NeedPassword). There are also input fields for "User Name" and "Password". At the bottom, there is a checkbox labeled "Save this password in your password list" which is currently unchecked. There are "OK" and "Cancel" buttons at the bottom right.

Figure 14. Password Dialog

To start the setup program, do the following:

1. Enter default user name, **admin**.
2. Enter the password for the DRG600-WiFi, as set in the *Password* screen above.

PC Configuration

4

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration
- Windows Clients

This section describes how to configure Windows clients for Internet access via the DRG600-WiFi.

The first step is to check the PC's TCP/IP settings.

The DRG600-WiFi uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using the default DRG600-WiFi settings, and the default Windows TCP/IP settings, no changes need to be made.

By default, the DRG600-WiFi will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.

For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required.

The *Gateway* must be set to the IP address of the DRG600-WiFi

The *DNS* should be set to the IP address of the DRG600-WiFi and/or the address provided by your ISP.



If your LAN has a Router, the LAN Administrator must reconfigure the Router itself. Refer to the *Advanced Setup* chapter for details.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

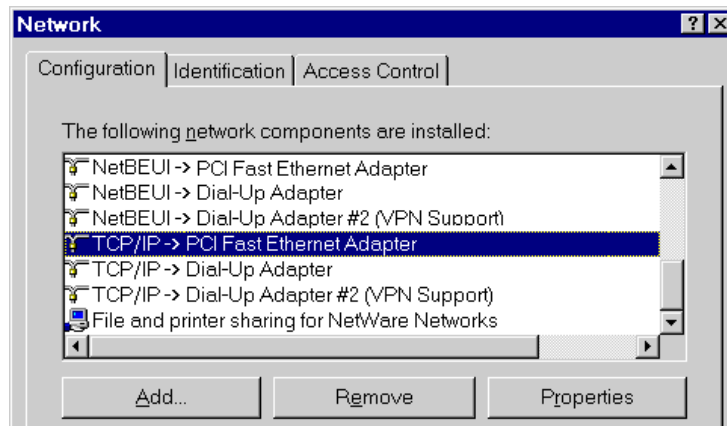


Figure 15. Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

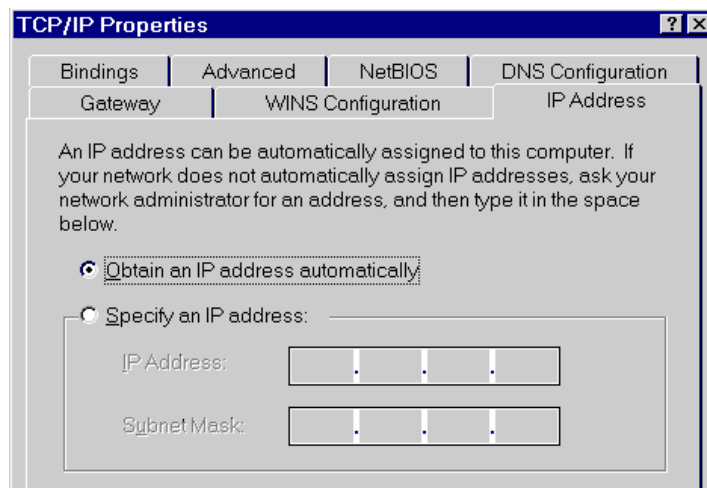


Figure 16. IP Address (Win 95)

Ensure your TCP/IP settings are correct, as described in the following sections:

Using “IP Address” (DHCP)

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the DRG600-WiFi will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the DRG600-WiFi.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

1. On the *Gateway* tab, enter the DRG600-WiFi's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the DRG600-WiFi.

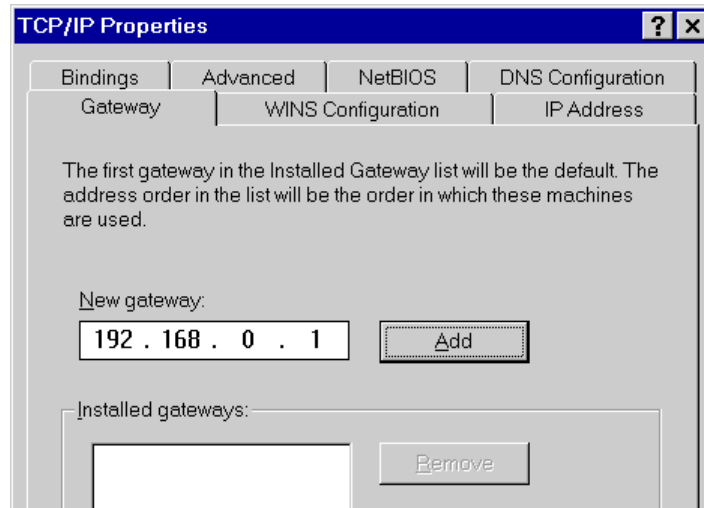


Figure 17. Gateway Tab (Win 95/98)

2. On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the the IP address of DRG600-WiFi or the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

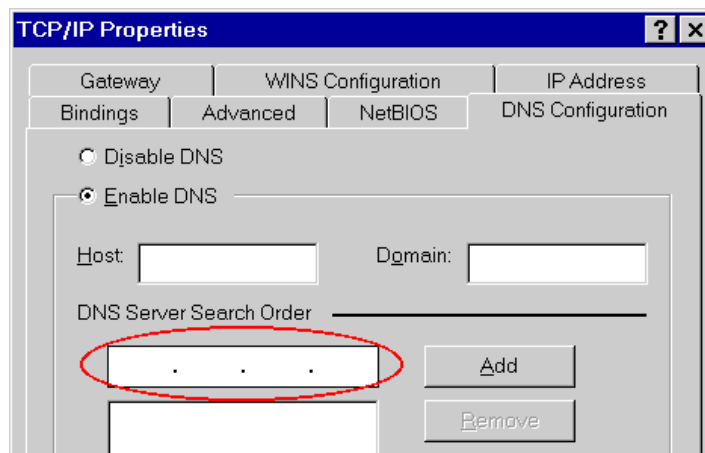


Figure 18. DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below:

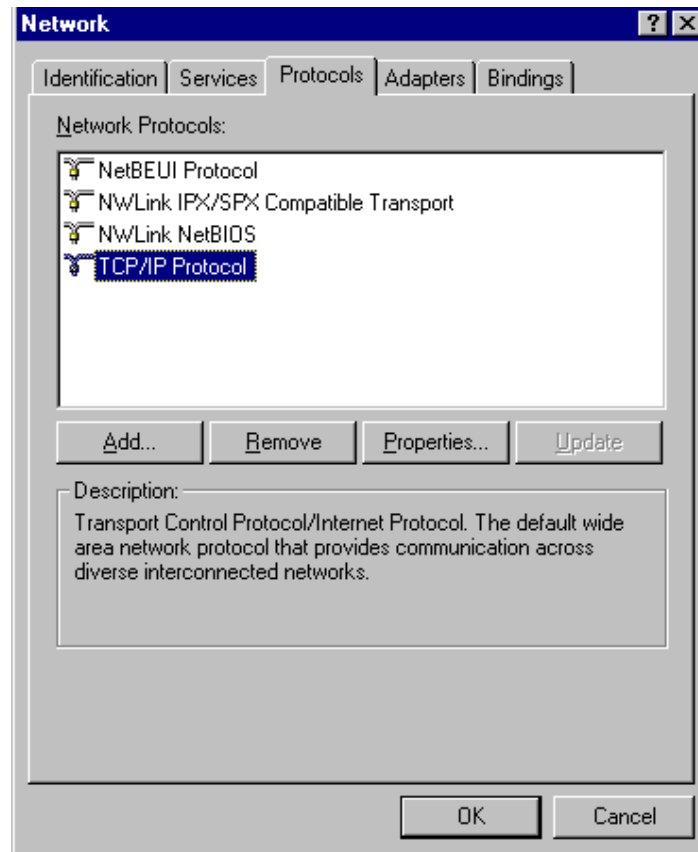


Figure 19. Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.

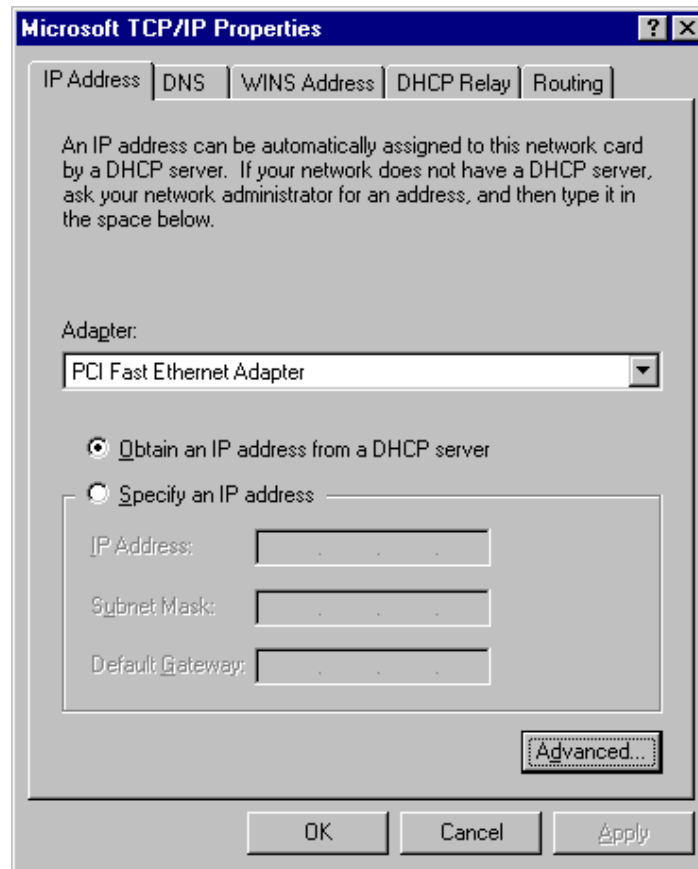


Figure 20. Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - Obtain an IP address from a DHCP Server or Specify an IP Address, as explained below.

Obtain an IP address from a DHCP Server

This is the default Windows setting. **Using this is recommended.** By default, the DRG600-WiFi will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the DRG600-WiFi.

Specify an IP Address

If your PC is already configured, check with your network administrator before making the following changes.

The *Default Gateway* must be set to the IP address of the DRG600-WiFi. To set this:

1. Click the *Advanced* button on the screen above.
2. On the following screen, click the *Add* button in the *Gateways* panel, and enter the DRG600-WiFi's IP address, as shown in Figure 19 below.
3. If necessary, use the *Up* button to make the DRG600-WiFi the first entry in the *Gateways* list.

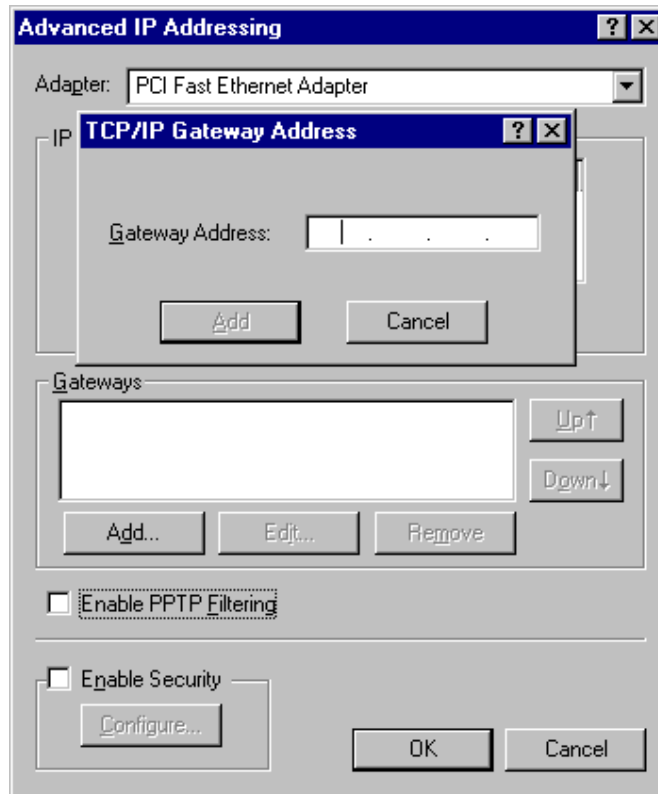


Figure 21. Windows NT4.0 - Add Gateway

The DNS should be set to the address provided by your ISP, as follows:

1. Click the *DNS* tab.
2. On the DNS screen, shown below, click the *Add* button (under *DNS Service Search Order*), and enter the IP address of DRG600-WiFi or the DNS provided by your ISP.

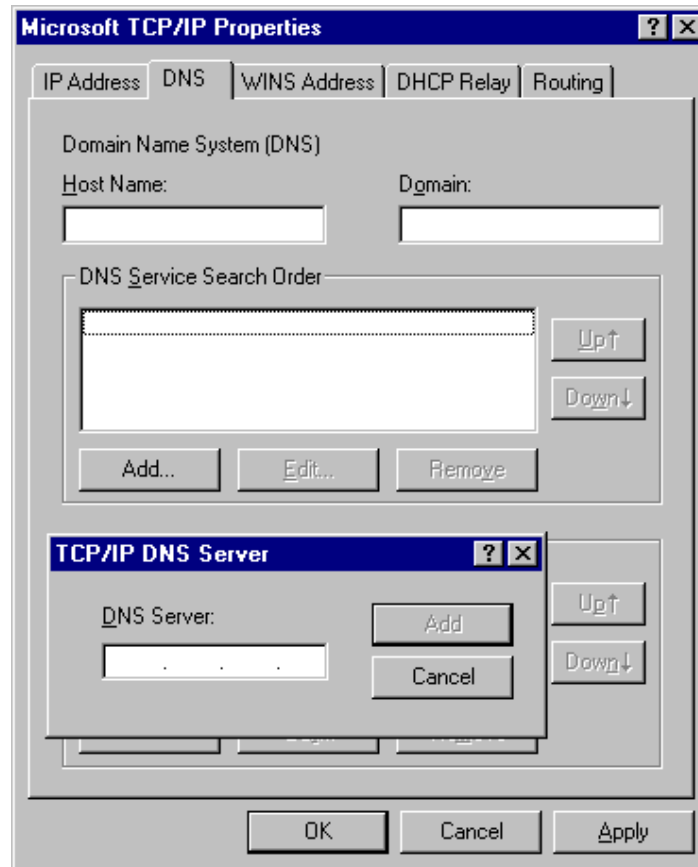


Figure 22. Windows NT4.0 – DNS

Checking TCP/IP Settings - Windows 2000:

1. Select Control Panel - Network and Dial-up Connection.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

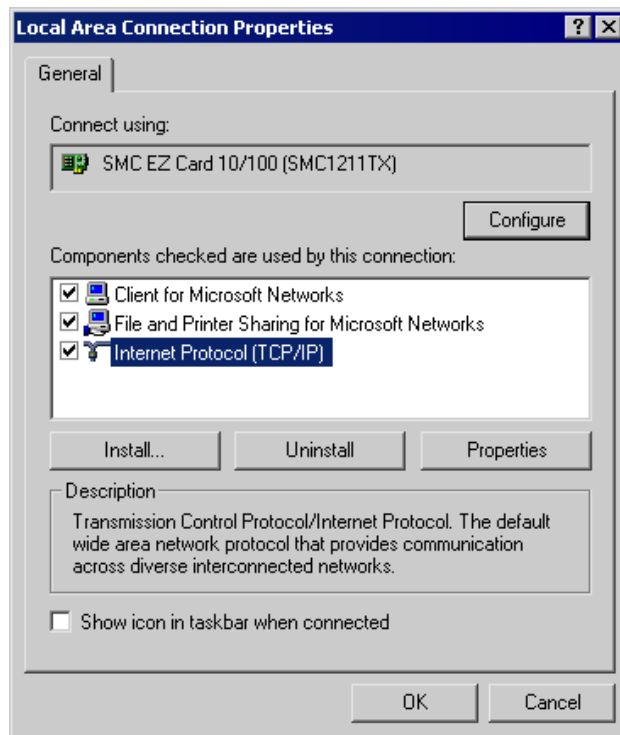


Figure 23. Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.

4. Click on the *Properties* button. You should then see a screen like the following:

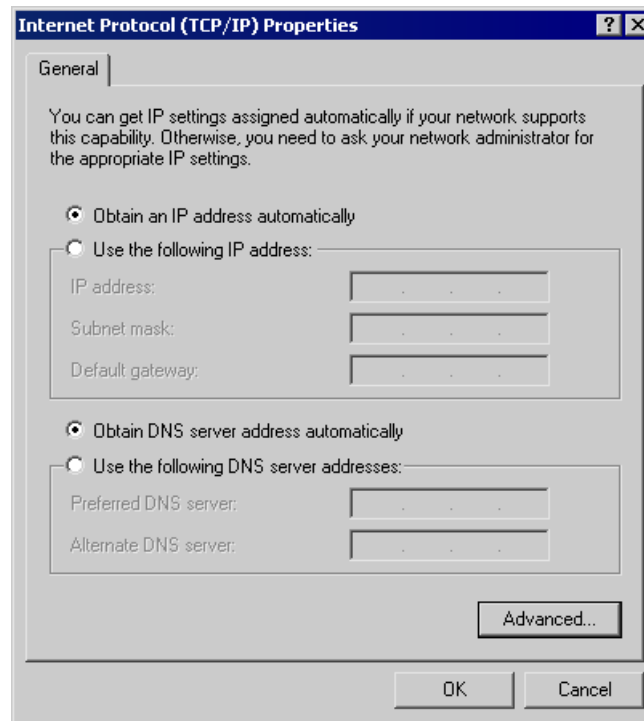


Figure 24. TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct, as described below.

Obtain an IP Address automatically

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this setting is recommended.** By default, the DRG600-WiFi will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the DRG600-WiFi.

Use the following IP Address

If your PC is already configured with a fixed IP address, select the radio button *Use the following IP address:*.

Check with your network administrator before making the following changes.

1. Enter the DRG600-WiFi's IP address in the *Default gateway* field and click *OK*.
2. If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the the IP address of DRG600-WiFi or the DNS address provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

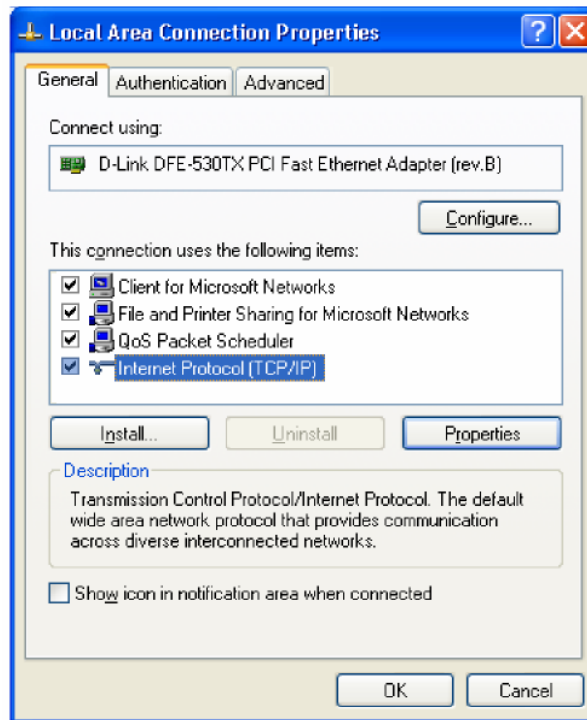


Figure 25. Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.

- Click on the *Properties* button. You should then see a screen like the following:

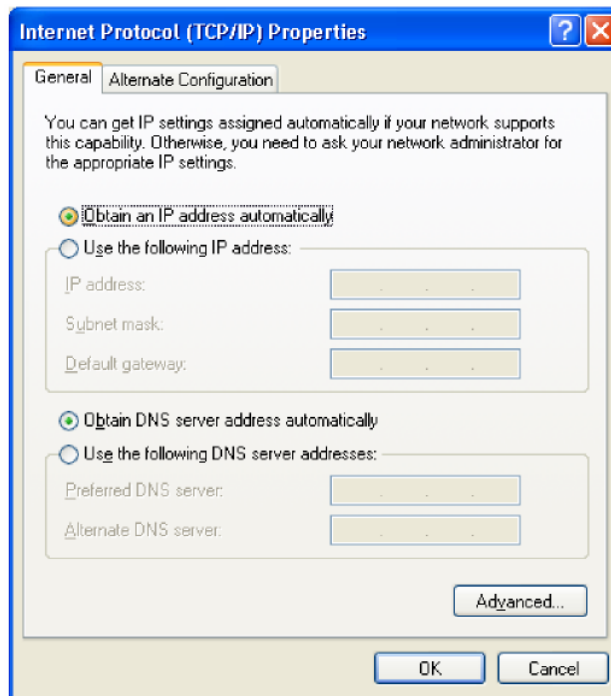


Figure 26. TCP/IP Properties (Windows XP)

- Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the DRG600-WiFi will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the DRG600-WiFi.

Using a fixed IP address

If your PC is already configured with a fixed IP address, select the radio button *Use the following IP address:*

Check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the DRG600-WiFi's IP address and click *OK*.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Internet Access

To configure your PCs to use the DRG600-WiFi for Internet access:

- Ensure that the DRG600-Access module is functioning.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 9x/ME/2000

1. Select Start Menu - Settings - Control Panel - Internet Options.
2. Select the Connection tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?".
7. Click *Finish* to close the Internet Connection Wizard. Setup is now completed.

For Windows XP

1. Select Start Menu - Control Panel - Network and Internet Connections.
2. Select Set up or change your Internet Connection.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard. Setup is now completed.

Macintosh Clients

From your Macintosh, you can access the Internet via the DRG600-WiFi. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If you are using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the DRG600-WiFi's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the DRG600-WiFi, it is only necessary to set the DRG600-WiFi as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

1. Set your "Default Gateway" to the IP Address of the DRG600-WiFi.
2. Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select Control Panel - Network
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.

To apply your changes

- Use the "Deactivate" and "Activate" buttons, if available.
- OR, restart your system.

Other Unix Systems

To access the Internet via the DRG600-WiFi:

- Ensure the "Gateway" field for your network card is set to the IP Address of the DRG600-WiFi.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration

This section applies to all Wireless stations wishing to use the DRG600-WiFi's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the DRG600-WiFi, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to Infrastructure.
SSID (ESSID)	This must match the value used on the DRG600-WiFi. The default value is printed on a label on the DRG600-WiFi. Note! The SSID is case sensitive.
Wireless	By default, Wireless security on the DRG600-WiFi is enabled with WPA-PSK and the passphrase is printed on a label on the DRG600-WiFi.
Security	If Wireless security is disabled on the DRG600-WiFi, all stations must have wireless security disabled. If Wireless security is enabled on the DRG600-WiFi, each station must use the same settings as the DRG600-WiFi.

This Chapter describes the status screens of the DRG600-WiFi

Status Screen

Select **Status** on the main menu to view this screen.

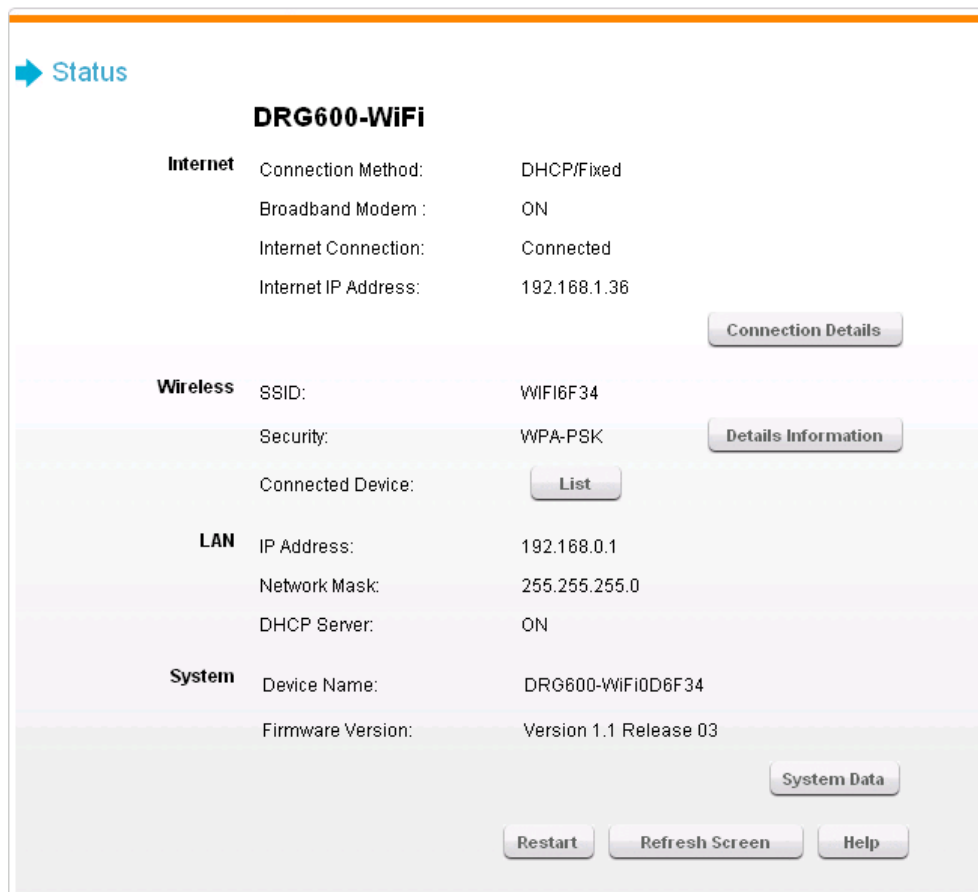


Figure 27. Status Screen

Internet

Connection Method	This indicates the current connection method, as set in the <i>Setup Wizard</i> or <i>WAN Port</i> screen.
-------------------	--

Broadband Modem	This shows the status of the connection from the DRG600-WiFi to the Broadband Modem.
Internet Connection	This shows the current connection status. If there is an error, you can click the "Connection Details" button to find out more information.
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If there is no current connection, this will be blank or 0000.
"Connection Details" Button	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "Connection Log" may also be available.

Wireless

SSID	The name of the wireless network.
Security	This indicates the Wireless security system currently used. Click the "Details Information" to see more details.
Connected Device	This lists the connected devices. Click "List" to generate a current list of all connected devices.
Details Information	Click this button to open a window that displays current wireless information..

LAN

IP Address	The IP Address of the DRG600-WiFi.
Network Mask	The Network Mask (Subnet Mask) for the IP Address.
DHCP Server	This shows the status of the DHCP Server function - either "Enabled" or "Disabled".

For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the *PC Database* option on the *LAN* menu.

System

Device Name	This displays the current name of the DRG600-WiFi.
Firmware version	The current version of the firmware installed in the DRG600-WiFi. Click the "System Data" button to display all system information in a sub-window
Restart	Clicking this button will restart (reboot) the DRG600-WiFi. All existing connections through the DRG600-WiFi will be lost.
Refresh Screen	Update the data displayed on screen

Connection Status - PPPoE

If using PPPoE (PPP over Ethernet), a screen like the following example will be displayed when the "Connection Details" button is clicked.

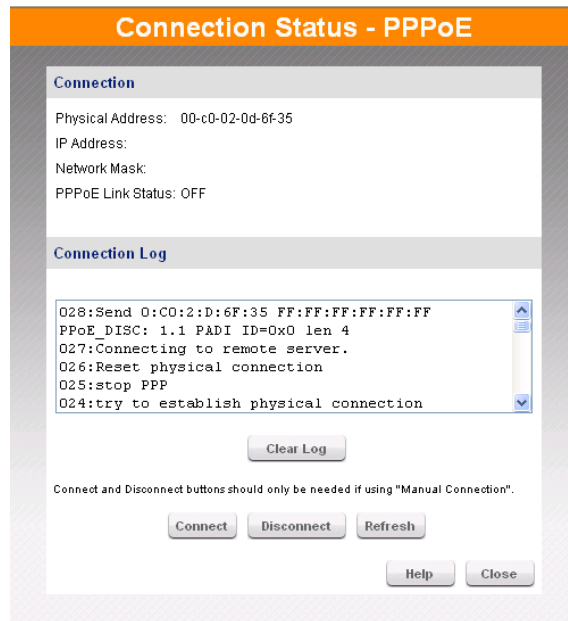


Figure 28. PPPoE Status Screen

Connection

Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.

PPPoE Link Status	<p>This indicates whether or not the connection is currently established.</p> <p>If the connection does not exist, the "Connect" button can be used to establish a connection.</p> <p>If the connection currently exists, the "Disconnect" button can be used to break the connection.</p>
-------------------	--

Connection Log

Connection Log	<p>The Connection Log shows status messages relating to the existing connection.</p> <p>The most common messages are listed in the table below.</p> <p>The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.</p>
----------------	--

Buttons

Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Log Messages

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect automatically, as required" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.

Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated..
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

Connection Details - Fixed/Dynamic IP Address

If your access method is "Direct" (no login), a screen like the following example will be displayed when the "Connection Details" button is clicked.

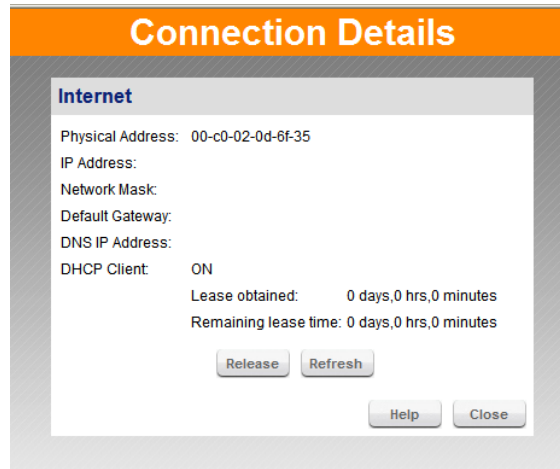


Figure 29. Connection Details Screen

Internet

Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	<p>This will show "Enabled" or "Disabled".</p> <p>If "Enabled", the Internet IP Address from your ISP is allocated automatically upon connection. (Dynamic IP Address). In this case the "Lease obtained" and "Remaining lease time" fields provide additional information. Note that the lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.</p> <p>If "Disabled", the Internet IP Address from your ISP is Fixed or Static. In this case, the "Release/Renew" button is not operational.</p>

The *Renew* button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic

IP address). Otherwise, it has no effect.

If the DRG600-WiFi is currently using an IP Address allocated by the ISP's DHCP Server., clicking the *Release* button will release the IP Address and break the connection.

If the button says "Release", this indicates that the ISP's DHCP Server has not allocated an IP Address for the DRG600-WiFi. Clicking the "Renew" button will re-establish the connection and obtain an IP Address from the ISP's DHCP Server.

Refresh updates the data shown on screen.

Advanced Features

6

This Chapter explains when and how to use the DRG600-WiFi "Advanced" Features.

Overview

The following advanced features are provided under the **Advanced** menu

- Access Control
- Dynamic DNS
- DMZ
- Virtual Servers
- WAN Port
- Routing
- Security
 - URL Filter
- UPnP

Access Control

This feature is accessed by the *Access Control* link on the **Advanced** menu.

The Access Control feature allows administrators to restrict the level of Internet Access available to PCs on your LAN. With the default settings, everyone has unrestricted Internet access.

To use this feature:

1. Set the desired restrictions on the "Everyone" group. All PCs are in the "Everyone" group unless explicitly moved to another group.
2. Set the desired restrictions on the other groups ("Group 1", "Group 2", "Group 3" and "Group 4") as needed.
3. Assign PC to the groups as required.

Restrictions are imposed by blocking "Services", or types of connections. All common Services are pre-defined. If required, you can also define your own Services.

Access Control Screen

To view this screen, select the *Access Control* tab of the **Advanced** menu.

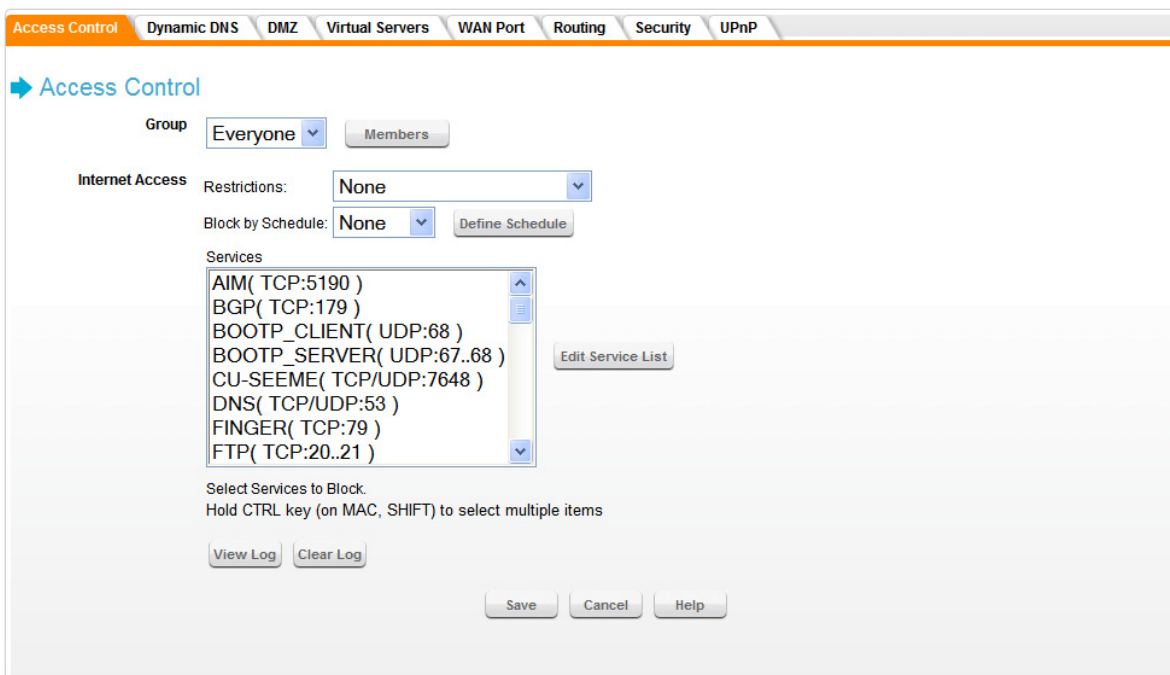


Figure 30. Access Control Screen

Group

Select the desired user group. Groups are named "Everyone", "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be renamed. Click the *Members* button to see the details for the selected group.

Internet Access

Select the desired options for the current group:

Restrictions	<p>None - Nothing is blocked. Use this to create the least restrictive group.</p> <p>Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group.</p> <p>Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.</p>
Block by Schedule	<p>If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)</p>
Services	<p>This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)</p>
Edit Service List Button	<p>If you wish to define additional Services, or manage the Service list, click this button to open the "Services" screen.</p>

Define Schedule

Click this to open the Schedule sub-window where you can define the schedule for access control to be applied.

View Log

Click this to open a sub-window where you can view the "Access Control" log. This log shows attempted Internet accesses which have been blocked by the Access Control feature.

Clear Log

Click this to clear and restart the "Access Control" log, making new entries easier to read.

Members Screen

This screen is selected by clicking the Members button in the **Access Control** screen.

Groups are pre-named "Everyone", "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be renamed.

All PCs are in the "Everyone" group, unless moved to another group.

A PC can be a member of 1 group only.

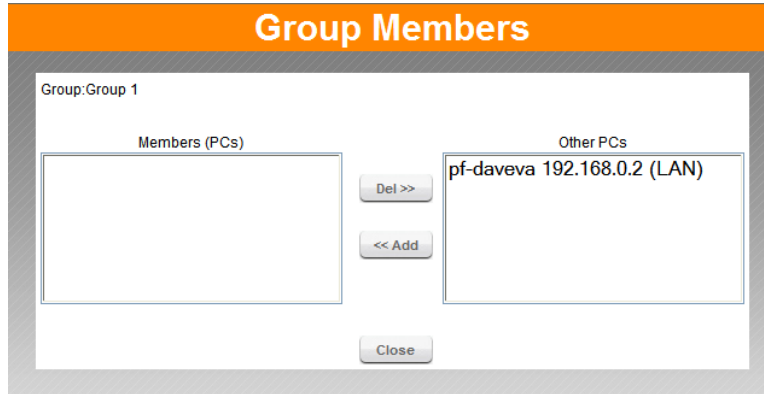


Figure 31. Group Members Screen

Group	Select the desired Group. The screen will update to display the PCs for the selected Group.
Members	This lists all PCs, which are currently members of the selected group.
Other PCs	This lists all other PCs – those, which are not currently members of the selected group.
Del >>	Use this button to remove members from the current Group. Select the members you wish to delete from this group, and click this button. (Members can not be deleted from the "Everyone" group.)
<< Add	Use this button to add members to the current Group. In the "Other PCs" list, select the members you wish to add to this group, and click this button. The PCs will be moved from their existing group to the current group.

PCs not assigned to any group will be in the "Everyone" group. PCs deleted from any other Group will be added to the "Everyone" group.

Define Schedule

The schedule can be used for the **Access Control** and **URL Filter** features.

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Tuesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Wednesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Thursday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Friday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Saturday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Sunday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 32. Default Schedule Screen

Two (2) separate sessions or periods can be defined.

Times must be entered using a 24 hr clock.

If the time for a particular day is blank, no action will be performed.

Services Screen

This screen is displayed when the *Edit Service List* button on the **Access Control** screen is clicked.

Figure 33. Access Control, Services Screen

Available Services

This lists all the available services.

Use the *Delete* button to delete the selected Service from the list.

Add New Service

Name	Enter a descriptive name to identify this service.
Type	Select the correct type for this Service.
Start Port	If the "Type" (above) is TCP, UDP, or TCP/UDP, enter the port number for this Service. If a port range is required, enter the beginning of the range here, and the end of the range in the "Finish Port" field.
Finish Port	If the "Type" (above) is TCP, UDP, or TCP/UDP, this field can be used to enter the end of range of port numbers. This can be left blank if not required.
ICMP Type	If the "Type" (above) is ICMP, enter the ICMP type here. Otherwise, this field should be left blank.

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The Service works as follows:

1. You must register for the service at one of the listed DDNS Service Providers.
2. After registration, follow the service provider's procedure to request a Domain Name and have it allocated to you.
3. Enter your DDNS data on the DRG600-WiFi's DDNS screen.
4. The DRG600-WiFi will then automatically ensure that your current IP Address is recorded at the DDNS server.
5. If the DDNS Service provides software to perform this "IP address update"; you should disable the "Update" function, or not use the software at all.
6. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain Name.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

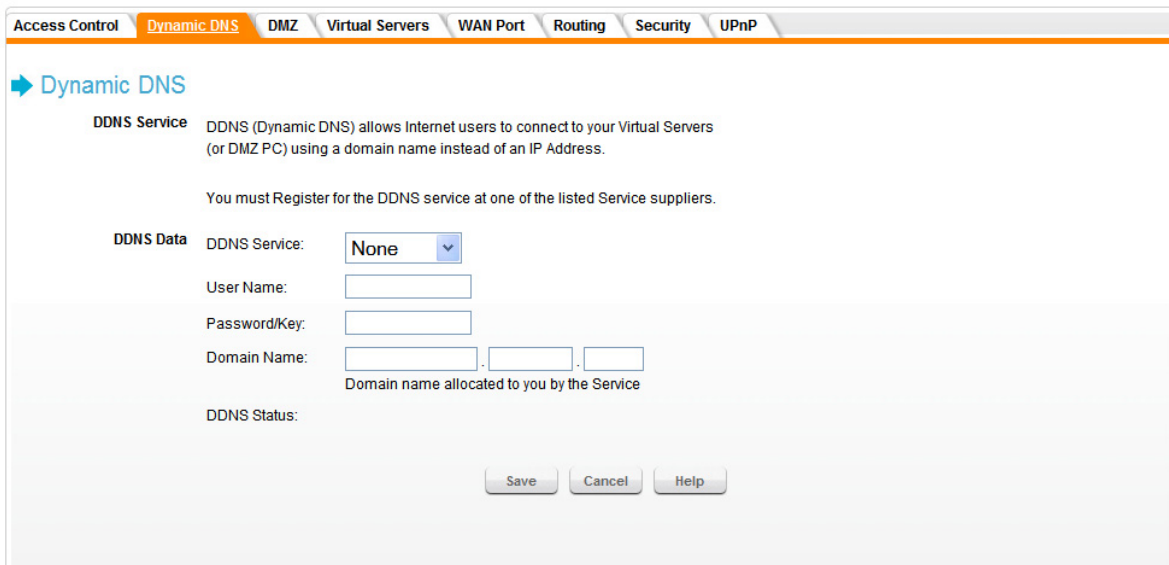


Figure 34. Dynamic DNS Screen

DDNS Data

DDNS Service	Select the desired DDNS Service. To disable DDNS, select "None".
User Name	Enter your Username for the DDNS Service.
Password/Key	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one domain name, enter the name you wish to use. This device supports one name only.
DDNS Status	This message is returned by the DDNS Server. Normally, this message should be something like "Update successful" (current IP address was updated on the DDNS server). If the message is "No host", this indicates the host name entered was not allocated to you. If you see this, or some other error message, you need to contact the DDNS Service and correct the problem.

DMZ

This screen allows you to configure the LAN PCs as a “DMZ”. The DMZ PC will receive the same IP address as the WAN.

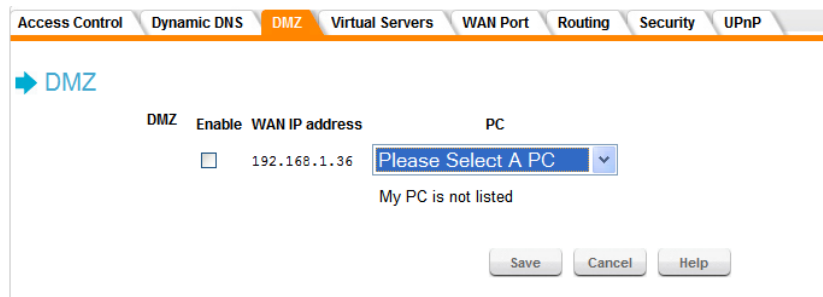


Figure 35. DDNS Screen Data - Dynamic DNS Screen

A DMZ allows a single computer on your LAN to expose ALL of its ports to the Internet. When doing this, the exposed computer is no longer ‘behind’ the firewall.

The "DMZ" PC will receive all "Unknown" connections and data. This feature is normally used with applications which do not usually work when behind a Firewall.

Note that the DMZ PC is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

Enable WAN IP address	DMZ uses the default WAN IP address so no input is required. If known, the current WAN IP address is displayed. If you are using a dynamic IP address and there is no Internet connection, the WAN IP address is unknown.
PC	For each DMZ, you must select a PC from the list. If the DMZ PC uses a fixed IP address and is not in the list, you can add it using the “PC Database” option in the <i>LAN</i> screen.

Virtual Servers

This feature, sometimes called *Port Forwarding*, allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

Your Server does not have a valid external IP Address.

Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

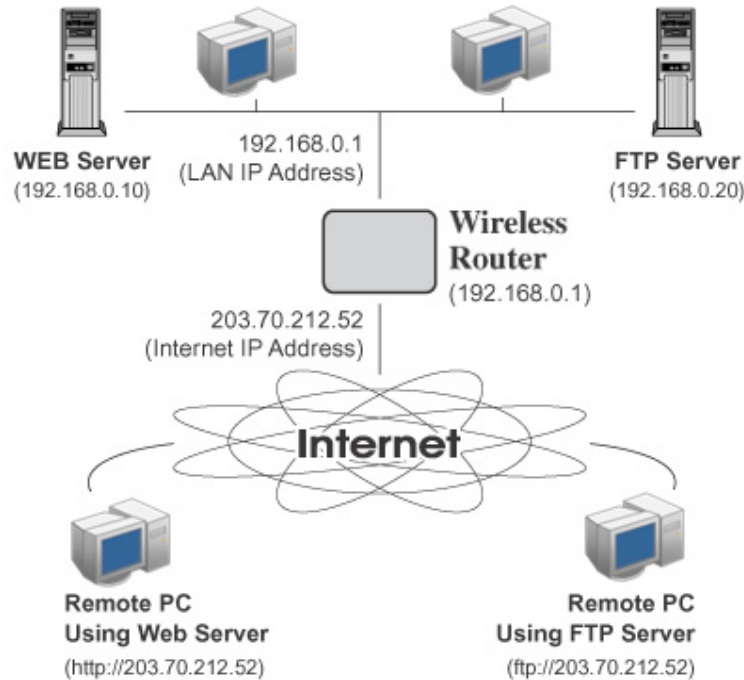


Figure 36. Virtual Servers

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

The *Virtual Servers* screen is reached by the *Virtual Servers* tab on the **Advanced** screen. An example screen is shown below.

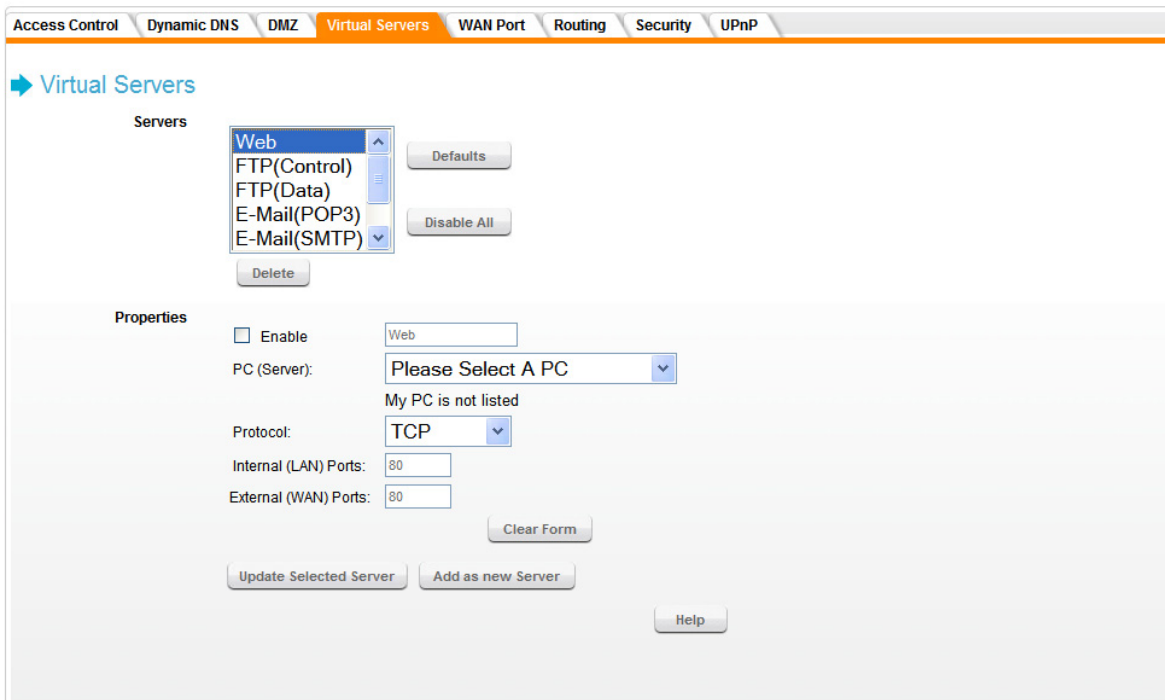


Figure 37. Virtual Servers Screen

Servers

This lists a number of pre-defined Servers, plus any Servers you have defined. Details of the selected Server are shown in the "Properties" fields.

Defaults	This will delete any Servers you have defined, and set the predefined Servers to use their default port numbers.
Disable All	This will cause the "Enable" setting of all Virtual Servers to be set OFF.
Delete	This remove the selected server from the list. Note that the pre-defined Servers cannot be deleted. Only Servers you have defined yourself can be deleted

Properties

Enable	Use this to Enable or Disable support for this Server, as required.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.
Protocol	Select the protocol (TCP or UDP) used by the Server.
Internal (LAN) Ports	Enter the range of port numbers which the Server software is configured to use.
External (WAN) Ports	Traffic from the Internet using this range of port numbers will be sent to the Server. This is normally the same as the Internal Port Numbers. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use a different port range to the clients.
Clear Form	Clear all data from the "Properties" area, ready for input of a new Virtual Server entry.
Update Selected Server	Update the current Virtual Server entry, using the data shown in the "Properties" area on screen.
Add as new Server	Add a new entry to the Virtual Server list, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.



For each entry, the PC must be running the appropriate Server software.

Defining your own Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can define and manage your own Servers:

Create a new Server:

1. Click "Clear Form".
2. Enter the required data, as described above.
3. Click "Add".
4. The new Server will now appear in the list.

Modify (Edit) a Server:

1. Select the desired Server from the list
2. Make any desired changes (for example, change the Enable/Disable setting).
3. Click "Update" to save changes to the selected Server.

Delete a Server:

1. Select the entry from the list.
2. Click "Delete".



Note!

You can only delete Servers you have defined. Pre-defined Server cannot be deleted.

From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP) e.g.

`http://203.70.212.52`

`ftp://203.70.212.52`

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature, described on page 68, to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.

WAN Port Configuration screen

Select the *WAN Port* tab.

Figure 38. WAN Port Screen

Identification

Normally, there is no need to change the default name, but if your ISP requests that you use a particular *Hostname*, enter it here.

If your ISP provided a *Domain Name*, enter it here. Otherwise, this may be left blank.

The *WAN Port MAC address* is a low-level identifier, as seen from the WAN port. Normally there is no need to change this, but some ISPs require a particular value, often that of the PC initially used for Internet access.

You can use the *Copy from PC* button to copy your PC's address into this field, the *Default* button to insert the default value, or enter a value directly.

IP Address

The *Dynamic IP Address* is the default setting, and the most common. Leave this selected if your ISP allocates an IP Address to the DRG600-WiFi upon connection.

The *Static IP Address* is to be selected if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered.

- IP Address: The IP Address allocated by the ISP.
- Network Mask: This is also supplied by your ISP. It must be compatible with the IP Address above.
- Gateway IP Address: The address of the router or gateway, as supplied by your ISP. This information is also supplied by your ISP. It must be compatible with the IP Address above.

DNS

If the radio button *Automatically obtain from server* is selected, the DNS (Domain Name Server) address will be obtained automatically from your ISP server.

To use a fixed IP address, select *Use this DNS* and enter the IP address of the DNS (Domain Name Server) you wish to use.

Backup DNS

If the DNS is unavailable, the "Backup DNS" servers configured here will be used.

MTU

MTU (Maximum Transmission Unit) value should only be changed if advised to do so by Technical Support.

Enter a value between 500 and 1492.

This device will still auto-negotiate with the remote server, to set the MTU size. The smaller of the 2 values (auto-negotiated, or entered here) will be used.

For direct connections (FixIP/DHCP), the MTU used is always 1500.

Login

Login Method	<p>If your ISP does not use a login method (username, password) for Internet access, leave this at the default value FixIP/DHCP. Otherwise, check the documentation from your ISP, select the login method used, and enter the required data.</p> <p>PPPoE - this is the most common login method, widely used with DSL modems. Normally, your ISP will have provided some software to connect and login. This software is no longer required, and should not be used.</p>
Login User Name	The User Name (or account name) provided by your ISP.
Login Password	Enter the password for the login name above.
Connection Behavior	<p>Select the desired option:</p> <ul style="list-style-type: none"> • Keep alive (maintain connection) The connection will never be disconnected by this device. If disconnected by your ISP, the connection will be re-established immediately. (However, this does not ensure that your Internet IP address will remain unchanged.) • Automatic Connect/Disconnect An Internet connection is automatically made when required, and disconnected when idle for the time period specified by the "Auto-disconnect Idle Time-out". • Manual Connect/Disconnect You must manually establish and terminate the connection.

Auto-disconnect Idle Time-out	<p>This field has no effect unless using the Automatic Connect/Disconnect setting.</p> <p>If using this setting, enter the desired idle time-out period (in minutes). After the connection to your ISP has been idle for this time period, the connection will be terminated.</p>
----------------------------------	--

Routing

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the DRG600-WiFi is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router on your LAN, and the DRG600-WiFi is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If you are using Windows 2000 Data center Server as a software Router, you must enable RIP on the Wireless Router, and ensure the following Windows 2000 settings are correct:
 - Open Routing and Remote Access
 - In the console tree, select Routing and Remote Access , [server name], IP Routing, RIP
 - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
 - On the "General" tab, set Outgoing packet protocol to "RIP version 2 broadcast", and Incoming packet protocol to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the *Routing* tab of the **Advanced** menu.

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, as explained above, although it is possible to use both methods simultaneously.

Static Routing Table

If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.

The other Routers must also be configured. See *Configuring Other Routers on your LAN* later in this chapter for further details and an example.

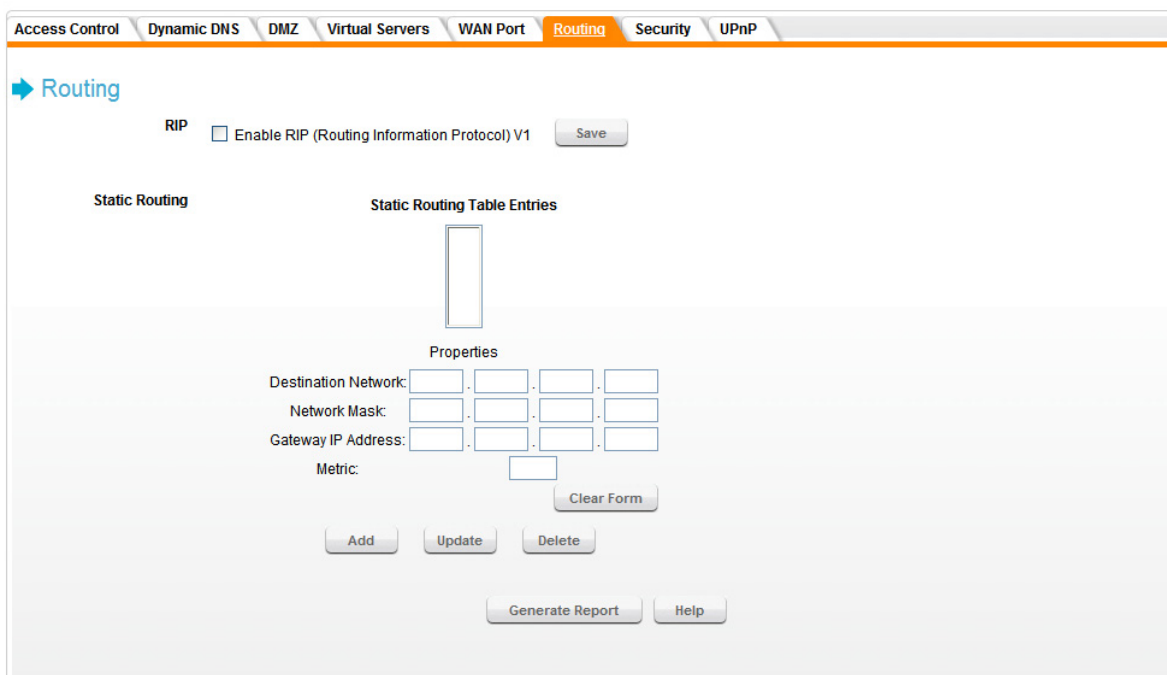


Figure 39. Routing Screen

RIP

Enable RIP v1	Check this to enable the RIP (Routing Information Protocol) feature of the DRG600-WiFi. The DRG600-WiFi supports RIP 1 only. Click the “Save” button to save this RIP setting. This has no effect on the Static Routing Table.
---------------	--

Static Routing

This list shows all entries in the Routing Table. Details for the selected item in the list will be displayed in the *Properties* fields.

Properties

Change any the properties as required, then click *Update* to save the changes to the selected entry. Click *Add* to enter a new routing table entry. Click *Delete* to remove a selected entry. Click *Clear Form* to clear all data from the "Properties" area, ready for input of a new entry for the Static Routing table.

Destination Network - The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0.

Network Mask - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0

Gateway IP Address - The IP Address of the Gateway or Router which the DRG600-WiFi must use to communicate with the destination above. (**NOT** the router attached to the remote segment.)

Metric - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 2.

Generate Report

This button generates a list of all the entries in the routing table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the DRG600-WiFi, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the DRG600-WiFi as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the DRG600-WiFi. This router requires that the *Default Route* is the DRG600-WiFi itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the DRG600-WiFi.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the DRG600-WiFi's *Local Router* as the *Default Route*. The entries will be the same as the DRG600-WiFi's local router, with the exception of the *Gateway IP Address*.

For a router with a direct connection to the DRG600-WiFi's local Router, the *Gateway IP Address* is the address of the DRG600-WiFi's local router.

For routers which must forward packets to another router before reaching the DRG600-WiFi's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example

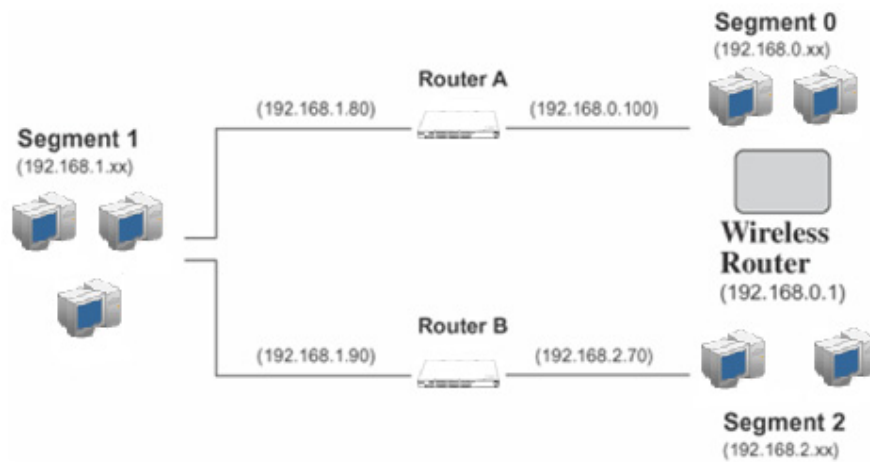


Figure 40. Routing Example

DRG600-WiFi Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the DRG600-WiFi requires 2 entries as follows.

Entry 1 (Segment 1)

Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (DRG600-WiFi's local Router)
Metric	2

Entry 2 (Segment 2)

Destination IP Address	192.168.2.0
------------------------	-------------

Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

Router A Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (DRG600-WiFi IP Address)

Router B Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (DRG600-WiFi's local router)

Security

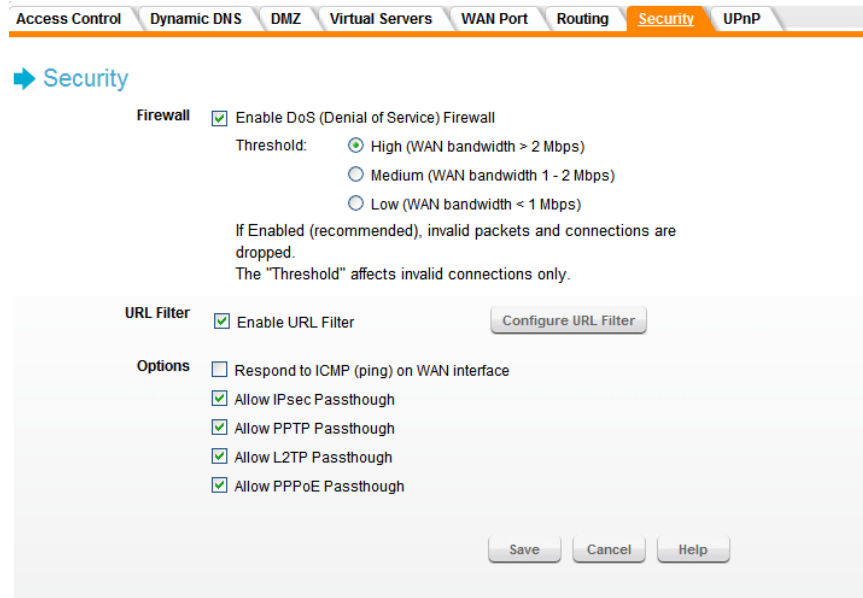


Figure 41. Security Screen

Firewall

If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled..

Note:

Enable DoS Firewall

A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable.

This device uses "Stateful Inspection" technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.

Threshold

This setting affects the number of "half-open" connections allowed.

A "half-open" connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server response.

Threshold is the optimum number of "half-open" connections allowed and it depends on many factors. The most important factor is the available bandwidth of your Internet connection.

Select the setting to match the bandwidth of your Internet connection.

URL Filter

You can filter out webpages by specifying which URLs to block. Click *URL Filter* to access the **URL Filter** screen. See "URL Filter Screen" on page 85 for more details.

Options

Respond to IGMP (ping) on WAN interface	<p>The ICMP protocol is used by the "ping" and "traceroute" programs, and by network monitoring and diagnostic programs.</p> <p>If checked, the DRG600-WiFi will respond to ICMP packets received from the Internet.</p> <p>If not checked, ICMP packets from the Internet will be ignored.</p> <p>Disabling this option provides a slight increase in security.</p>
Allow IPSec Pass through	<p>The IPSec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs.</p> <p>If checked, IPSec connections are allowed.</p> <p>If not checked, IPSec connections are blocked.</p> <p>Note: IPSec sessions must NOT use AH (Authentication Header).</p> <p>Packets using AH cannot be routed correctly.</p>
Allow PPTP Pass through	<p>The PPTP protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs.</p> <p>If checked, PPTP connections are allowed.</p> <p>If not checked, PPTP connections are blocked.</p>
Allow L2TP Pass through	<p>The L2TP protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs.</p> <p>If checked, L2TP connections are allowed.</p> <p>If not checked, L2TP connections are blocked.</p>
Allow PPPoE Pass through	<p>If checked, it allows LAN PCs to establish PPPoE connection through DRG600-WiFi to your ISP. LAN PC will have a valid IP Address.</p>

URL Filter Screen

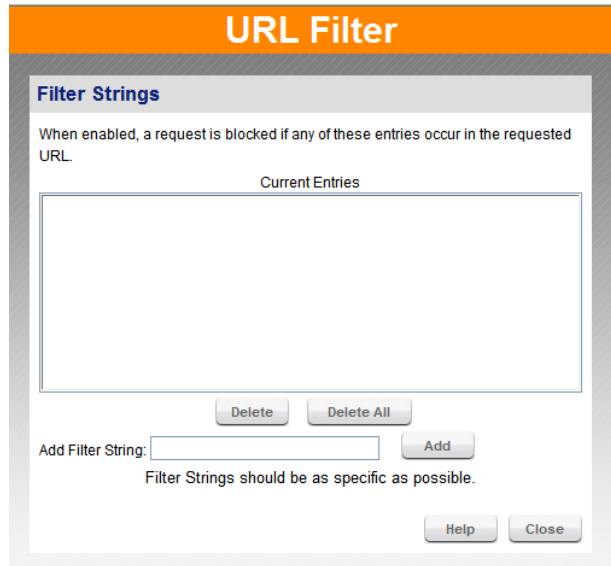


Figure 42. URL Filter Screen

Filter Strings

Current Entries	This field lists any existing entries. If you have not entered any values, this list will be empty.
Delete	Use this to delete the selected entry or entries, as required. Multiple entries can be selected by holding down the CTRL key while selecting. (On the Macintosh, hold the SHIFT key while selecting.)
Delete All	Use this button to delete all entries, if required.

Add Filter String

To add an entry to the list, enter it here, and click the "Add" button. An entry may be a Domain name (e.g. www.trash.com) or simply a string (e.g. ads/)

Any URL which contains ANY entry ANYWHERE in the URL will be blocked.

Click the "Add" button to add the entry in the *Filter String* list above.

UPnP

UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is supported by Windows ME, XP, or later.

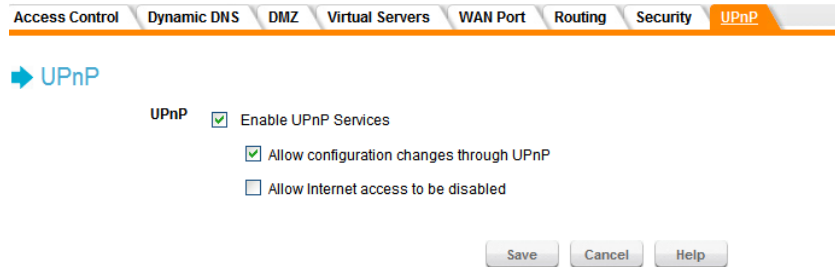


Figure 43. UPnP screen

UPnP

Enable UPnP Services	<ul style="list-style-type: none"> • If Enabled, this device will be visible via UPnP • If Disabled, this device will not be visible via UPnP .
Allow configuration changes through UPnP	<ul style="list-style-type: none"> • If checked, then UPnP users can change the configuration. • If Disabled, UPnP users can only view the configuration. But currently, this restriction only applies to users running Windows XP, who access the <i>Properties</i> via UPnP. (e.g. Right - click the DRG600-WiFi in <i>My Network Places</i>, and select <i>Properties</i>)
Allow Internet access to be disabled	<ul style="list-style-type: none"> • If checked, then UPnP users can disable Internet access via this device. • If Disabled, UPnP users can NOT disable Internet access via this device. But currently, this restriction only applies to users running Windows XP, who access the <i>Properties</i> via UPnP. (e.g. Right - click the DRG600-WiFi in <i>My Network Places</i>, and select <i>Properties</i>)

This Chapter explains the settings available via the "Administration" section of the menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

- **Default Config.** Reset the DRG600-WiFi to its factory default settings.
- **Logs.** View or clear all logs, set E-Mailing of log files.
- **Network Diagnostics.** Ping, DNS Lookup.
- **Local Administration.** Allow settings to be changed from local LAN.
- **Upgrade Firmware.** Upgrade the Firmware (software) installed in DRG600-WiFi.

Default Config screen

This screen allows you to set the DRG600-WiFi back to its factory default configuration. Any existing settings will be deleted.

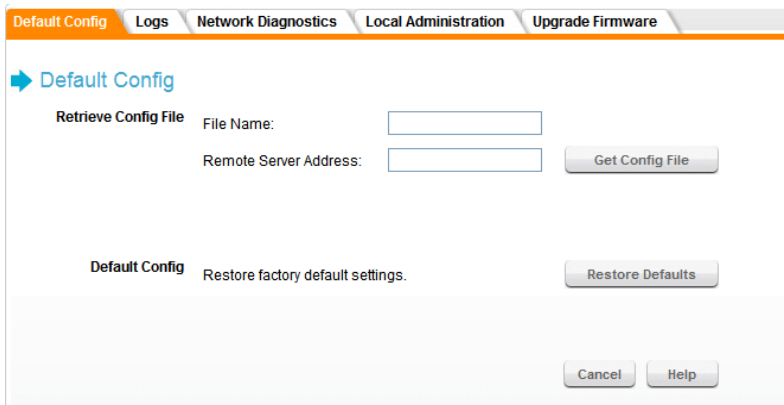


Figure 44. Default Config screen

Retrieve Config file

File name	Enter the file name of configuration that you want from Remote Server.
Remote Server Address	Enter the IP Address of Remote Server which stores the configuration file.
Get Config File	Click this button, DRG600-WiFi will get the configuration file from a remote server and use it after rebooting.

Default Config

Clicking the *Restore Defaults* button will reset the DRG600-WiFi to its factory default settings.

WARNING! This will delete ALL of the existing settings.

Logs screen

The Logs record various types of activity on the DRG600-WiFi. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Since only a limited amount of log data can be stored in the DRG600-WiFi, log data can also be e-mailed to your PC.

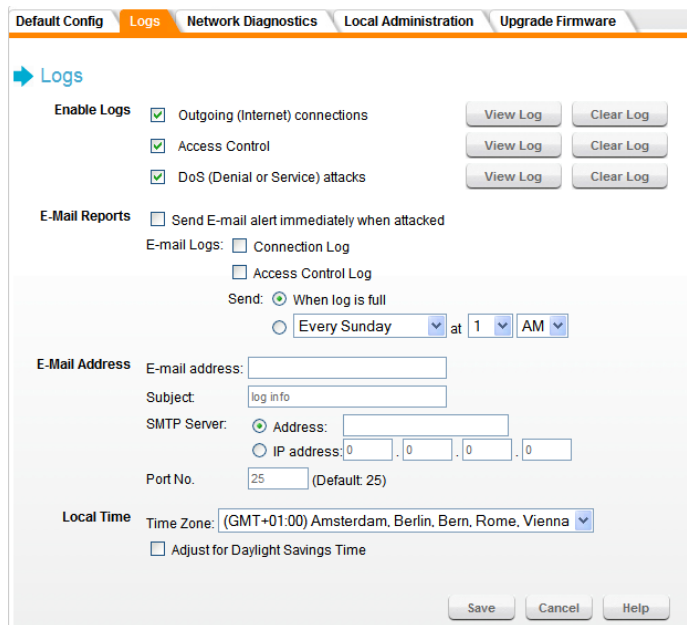


Figure 45. Logs Screen

Enable Logs

Outgoing	If selected, outgoing Internet connections are logged. Normally, the (Internet) "Destination" will be shown as an IP address. But if the "URL Filter" is enabled, the "Destination" will be shown as a URL.
Access Control	If enabled, the log will include attempted outgoing connections which have been blocked by the "Access Control" feature.
DoS Attacks	If enabled, this log will show details of DoS (Denial of Service) attacks which have been blocked by the built-in Firewall.
View Log button	Use this to view each log, as required.

Clear Log button	Use this to restart the required log. This makes it easier to read the latest entries.
------------------	--

E-Mail Reports

Send E-mail alert immediately when attacked	If enabled, an E-mail will be sent immediately if a DoS (Denial of Service) attack is detected. Note that if this is enabled, the E-mail address information must be provided.
E-mail logs	<p>Enable the logs you wish to send:</p> <p>Connection log - If selected, Outgoing Connection log will be sent.</p> <p>Access Control log - If selected, Access Control log will be sent.</p> <p>If no checkboxes are enabled, no logs will be sent.</p>

E-Mail Address

E-mail Address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Subject	Text to be added to subject field in email message.
SMTP Server	Enter the address (domain name) or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing Email.
Port No.	Enter the port number used to connect to the SMTP Server. The default value is 25.

Local Time

Timezone	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.
Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.

Network Diagnostics screen

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

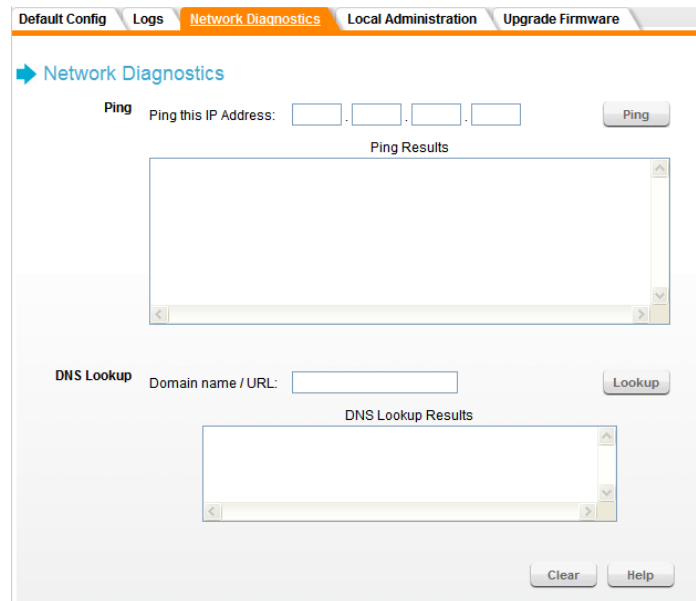


Figure 46. Network Diagnostics Screen

Ping

Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.

After entering the IP address, click the "Ping" button to start the ping procedure. The results will be displayed in the *Ping Results* field.

DNS Lookup

Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.

After entering the Domain name/URL, click *Lookup* to start the "DNS Lookup" procedure. The results will be displayed in the *DNS Lookup Results* pane.

Local Administration screen

This feature allows you to manage the DRG600-WiFi via the LAN port.

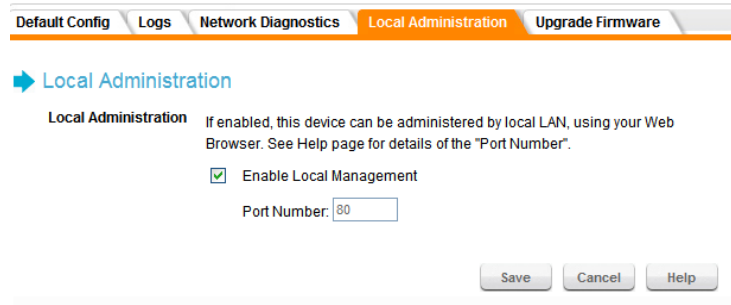


Figure 47. Local Administration Screen

Local Administration

<p>Enable Local Management</p>	<p>Check to allow administration/management via local LAN. (To connect, see “Port Number” below).</p> <p>If <i>Disabled</i>, this device will ignore Administration connection attempts from local LAN.</p>
<p>Port Number</p>	<p>Enter a port number between 1024 and 65535. The default value is 80. .</p> <p>The port number must be specified in your Browser when you have changed it. To specify the port number :</p> <ol style="list-style-type: none"> 1. Start your Browser. 2. In the "Address" or "Location" field, enter the IP address of this device, followed by the port number, as follows: <code>http://ip_address:port_number</code> <p>where:</p> <p><code>ip_address</code> is the IP address of this device.</p> <p><code>port_number</code> is the port number assigned on this screen.</p> <p>You should then be prompted for the password for this device. (You must assign a password!)</p>

**Note!**

If Local Administration is disabled, you will not be able to manage this device via local LAN by using web browser. Unless you reset device to factory default by reset button.

Upgrade Firmware screen

The firmware (software) in the DRG600-WiFi can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade Firmware* on the **Administration** menu. You will see a screen like the following.

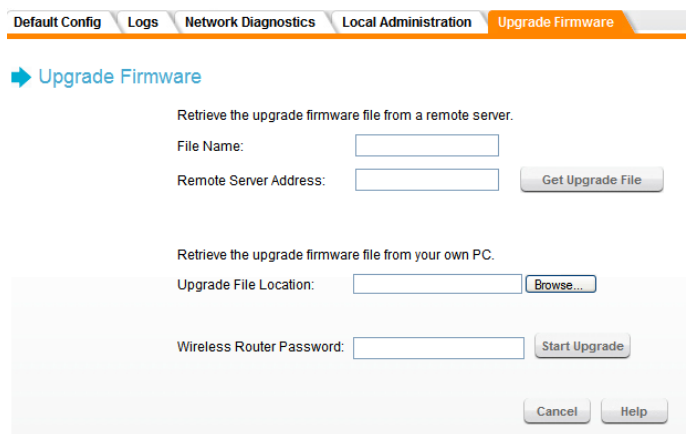


Figure 48. Upgrade firmware screen

Upgrade Firmware

File Name	Enter the file name of firmware that you want from Remote Server.
Remote Server Address	Enter the IP Address of Remote Server which stores the firmware file.
Get Upgrade File	Click this button, DRG600-WiFi will get firmware file from remote server and use it to operate by reboot.

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. If you have set a configuration password, enter it. If not, leave the field blank.
4. Click the *Start Upgrade* button to commence the firmware upgrade.

The DRG600-WiFi is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to, or through, the DRG600-WiFi will be lost.

Troubleshooting

8

This chapter covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the DRG600-WiFi and some possible solutions to them. If you follow the suggested steps and the DRG600-WiFi still does not function properly, contact your dealer for further advice.

General Problems

Problem: *Can't connect to the DRG600-WiFi to configure it.*

Solution: Check the following:

- The DRG600-WiFi is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the DRG600-WiFi are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the DRG600-WiFi's default IP Address of 192.168.0.1. Also, the Network Mask should be set to 255.255.255.0 to match the DRG600-WiFi.

In Windows, you can check these settings by using **Control Panel, Network** to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: *When I enter a URL or IP address I get a time out error.*

Solution 1: A number of things could be causing this. Try the following troubleshooting steps:

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the DRG600-WiFi. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the DRG600-WiFi is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: *Some applications do not run properly when using the DRG600-WiFi.*

Solution 2: The DRG600-WiFi processes the data passing through it, so it is not transparent.

Use the DMZ function. This should work with almost every application.

This should work with almost every application, but it is a security risk, since the firewall is disabled.

Only one (1) PC can use this feature.

Wireless Access

Problem 1: My PC can't locate the Wireless Access Point.

Solution 1: Check the following:

- Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the DRG600-WiFi must have the same setting for wireless security. The default setting for the DRG600-WiFi is WPA-PSK, so your wireless station should also have WPA-PSK enabled, and the key must match.
- If the DRG600-WiFi's *Wireless* screen is set to *Allow Wireless Access by Wireless Stations only*, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the DRG600-WiFi.
- Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: Wireless connection speed is very slow.

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- DRG600-WiFi location:
Try adjusting the location and orientation of the DRG600-WiFi.
- Wireless Channel:
If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference:
Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding:
Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the DRG600-WiFi.

About Wireless LANs

9

This chapter provides some background information about using Wireless LANs (WLANs).

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.



Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access

Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.

In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match
WEP Authentication	Open System or Shared Key.

WPA-PSK

WPA-PSK is another standard for encrypting data before it is transmitted. This is a later standard than WEP (Wired Equivalent Privacy), and provides greater security for your data. Data is encrypted using a 256Bit key which is automatically generated and changed often.

If all your Wireless stations support WPA-PSK, you should use this instead of WEP.

If WPA-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

WPA2-PSK

This is a later version of WPA (WPA-PSK). The major change is the use of AES (Advanced Encryption System) for protecting data. AES is very secure, considered to be unbreakable. The PSK (Pre-shared Key) must be entered on each Wireless station.

If WPA2-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA2 PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is
Encryption	The same encryption method must be used. The most common encryption method is AES.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode

On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)

Most Wireless stations will set the correct mode automatically.

SSID (ESSID)

Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.

Security

The Wireless Stations and the Access Point must use the same settings for Wireless security. (Off, WEP, WPA-PSK, WPA2-PSK, WPA-PSK+WPA2-PSK).

WEP If WEP is used, the Key size (64Bit, 128Bit), Key value, and Authentication settings must be the same on the Wireless Stations and the Access Point.

WPA-PSK: If WPA is used, all Wireless Stations must be set to use WPA-PSK, and have the same Pre-shared Key and encryption system.

WPA2-PSK: If WPA2 is used, all Wireless Stations must be set to use WPA2-PSK, and have the same Pre-shared Key and encryption system.

WPA-PSK +WPA2-PSK: If WPA-PSK +WPA2-PSK is used, all Wireless Stations must be set to use WPA-PSK +WPA2-PSK, and have the same Pre-shared Key and encryption system.

For **Ad-hoc networks** (no Access Point), all Wireless stations must use the same security settings.

Specifications

10

Multi-Function DRG600-WiFi

Model	DRG600-WiFi
Dimensions	34mm(W)×166mm(H)×53mm(D)
Operating Temperature/ Humidity	0°C to 40°C (32°F to 104°F) 5% to 95% Non-Condensing
Storage Temperature/ Humidity	-10°C to 70°C (14°F to 158°F) 5% to 95% Non-Condensing
Network Protocol:	TCP/IP
Network Interface:	FastEthernet: LAN: two 10/100Base TX RJ-45 ports one connector for WAN
LEDs	Power, WLAN, LAN (1, 2)
Power Adapter	12V±10% (10.8V to 13.2V), DC 0.5A, Magnetics center-tap power taken from the Access module

Wireless Interface

Standards	IEEE 802.11b/g compliance
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 11 Channels, depending on regulatory authorities
Modulation	DSSS BPSK/QPSK/CCK, OFDM/CCK
Data Rate	Up to 54 Mbps
Coverage Area	Indoors: 15m @54Mbps, 120m @6Mbps or lower Outdoors: 40m @54Mbps, 300m @6Mbps or lower
Encryption	WEP, WPA, WPA-PSK, and WPA2-PSK authentication
Output Power	IEEE 802.11b: 18.62 dBm, IEEE 802.11g: 19.76 dBm (typical)
Receiver Sensitivity	-70dBm Min.

Regulatory Approvals

Health and safety	CE Marking
Safety	ETL Mark
Safety	CB certified
Safety	IEC/EN/UL 60950
Safety	IEC/EN/UL 60825
Emission	FCC Part 15 Subpart B
Emission	EN 55022 (CISPR 22)
RoHS	Directive 2002/95/EC
WEEE	Directive 2002/96/EC
Immunity	EN 55024 (IEC61000-4-2,3,4,5,6,8,11)

Harmonics	EN 61000-3-2
Flicker	EN 61000-3-3
Radio	EN 5360, EN50385, EN300328, EN 301489-1, EN301489-17, FCC Part 15 subpart C

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.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

REMARK

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.