

Installation and User's Manual

PENTAGRAM Cerberus Wi-Fi Lite (P 6381-0)



*The latest versions of manual, drivers and applications are available on
www.pentagram.eu*

2007-06-28

NOTE! Any information and technical data are subject to change without prior notification and/or indication in this manual.

© 2007 PENTAGRAM

All rights reserved; copying and reproduction is strictly forbidden.

INDEX

INTRODUCTION	5
FEATURES	5
PACKAGE CONTENTS	5
PRODUCT OVERVIEW	6
IMPORTANT NOTES	6
FRONT PANEL	6
BACK PANEL	7
DEFAULT SETTINGS	7
RESETTING ROUTER	8
CONNECTING CERBERUS TO COMPUTER	8
CONFIGURE TCP/IP	8
CONFIGURE ROUTER VIA WEB BROWSER	13
LOGIN	13
NAVIGATION	14
SETUP WIZARD	15
OPERATION MODE	24
LAN INTERFACE SETUP	25
WAN INTERFACE SETUP	26
WIRELESS	28
FIREWALL	40
VPN SETTINGS	45
ADVANCED	50
MANAGEMENT	53
EVENT LOG	62
TROUBLESHOOTING	63
USING LEDS TO DIAGNOSE PROBLEMS	63
PROBLEMS WITH THE WEB INTERFACE	63
PROBLEMS WITH THE LOGIN USERNAME AND PASSWORD	64
PROBLEMS WITH LAN INTERFACE	64
PROBLEMS WITH THE INTERNET ACCESS	64

Introduction

Thank you for choosing the Cerberus Wi-Fi Lite (P6381-0). With the Wireless-G Router, you can share one Internet connection among multiple computers and extend wireless connectivity to mobile users easily and securely.

With its compact design, the Wireless-G Router is easy to set up and configure with the embedded web-based configuration screens.

Features

- IEEE 802.11g and 802.11b Wireless LAN Access.
- Data and network security with wireless 64-bit and 128-bit WEP data encryption.
- Wi-Fi WPA and WPA2 wireless security.
- Firewall features to protect network with:
IP, MAC, Port and URL filtering.
NAT with Port Forwarding/Redirection and DMZ.
- Wireless access control by MAC addresses.
- WDS to extend wireless coverage.
- VPN IPSec & Pass-through.

Package Contents

1. PENTAGRAM Cerberus Wi-Fi Lite (P6381-0)
2. Power adapter 9 V, 0,8 A
3. Ethernet cable (RJ-45)
4. Telephone cable (RJ-11)
5. CD
6. Quick Installation Guide



Product Overview

Important Notes

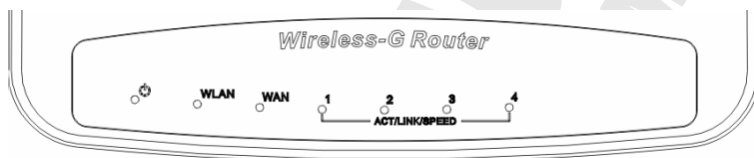


- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.



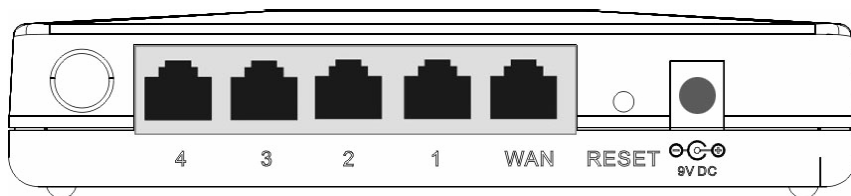
- Avoid using this product and all accessories outdoors.
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Front Panel



LED	Color	Action	Description
PWR	Green	Off	No power is supplied to the device
		Steady light	Connected to an AC power supply
WLAN	Green	Off	Access point is disabled
		Steady light	Access point is enabled
		Blinking light	Transmitting/Receiving data
WAN	Green	Off	The WAN port is not connected
		Steady light	The WAN port is connected
		Blinking light	Transmitting/Receiving data
ACT/LINK/SPEED (1-4)	Yellow	Off	No Ethernet connection
		Steady light	Connected to an Ethernet port
		Blinking light	Transmitting/Receiving data

Back Panel



Label	Used for...
1-4 (RJ-45)	Connecting to computers/devices using the Ethernet cable
WAN (RJ-45)	Connecting to a cable/DSL modem using the Ethernet cable
RESET	Resetting the device.
PWR	Connecting with supplied power adapter (9V 0,8A)

Default Settings

Before changing configuration familiarize yourself with these default settings.

IP Address	192.168.1.254
Subnet Mask	255. 255. 255.0
SSID	Wireless-G Router
DHCP Server	Enabled
DHCP Server IP Address Pool	100 IP addresses from 192.168.1.100
IP Address Lease Time	86400 seconds (24 hours)
User Name	root
Password	1234

It is recommended to change default password as soon as possible.

If you ever forget the password to log in, you may need to reset router to restore the factory default settings. This procedure is described on the next page.

Resetting router

- Turn router on and wait about 2 minutes for router initialization.
- Hold the **RESET** button until the LEDs all turn Off, turn On and then turn Off. The router performs configuration factory reset and the router reboots. You can then access the router from the web GUI.

Connecting Cerberus to Computer.

Cerberus can be connected to computer via Ethernet or WLAN:

Connecting via Ethernet Port (Ethernet Card)

If there is an available LAN card present on your PC, you just simply connect router and PC through the Ethernet cable. Once you establish Internet connection, you could browse the Web through the Ethernet cable.

Connecting via WLAN Interface (Wireless Card)

To connect PC to Cerberus via WLAN, Wireless Adapter must be properly installed and configured and both router and PC must be in the same subnet.

Configure TCP/IP

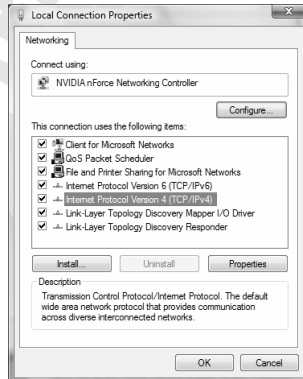
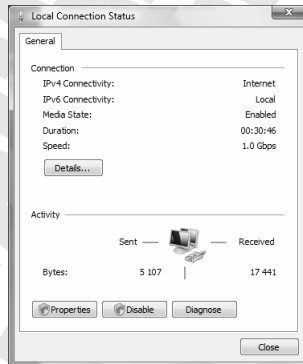
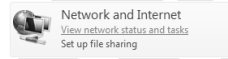
This part will help you to configure your computer to communicate with router properly. Computer must be either equipped with network adapter connected directly to router or wireless network adapter (compatible with Wi-Fi 802.11b/g standard). Wireless network adapter must have the same session ID (ESSID) and establish connection with the network created by router. You can also connect to router via network hub/switch. Default IP address of the router is 192.168.1.254 and subnet mask is 255.255.255.0. Fastest and easiest method to configure your computer is to obtain an IP address automatically from router's DHCP server.

Make sure that TCP/IP protocol and network adapter are installed on your computer.

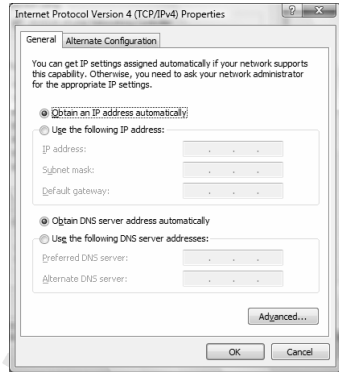
Windows Vista

Note: Network configuration require administrator privileges. When *User Account Control* window pops up, either click Continue (Administrator user) or select Administrator user and enter valid password (Standard user).

1. Click **Start** → **Control Panel**.
2. Click **View network status and tasks**.
3. Click **View status** for appropriate connection.
4. On **General** tab, Click the **Properties** button.
5. On **General** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

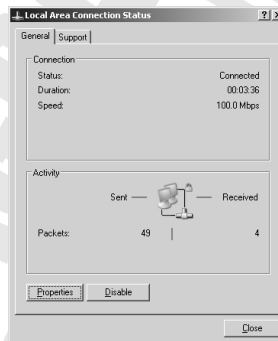
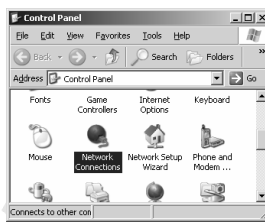


6. On **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save settings and close **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

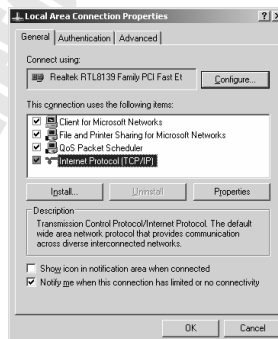


Windows 2000/XP

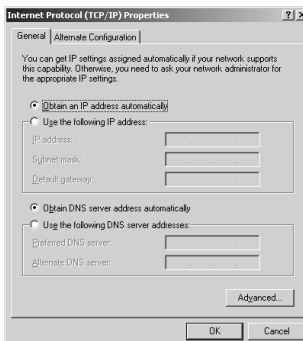
1. Click **Start** → **Settings** → **Control Panel**.
Double-click the **Network Connections** icon (2000/XP Classic view) or click **Network and Internet Connections** icon and then **Network Connections** icon (XP Default view).
2. Double-click the **Local Area Connection** icon.
3. On **General** tab, Click the **Properties** button.



4. On **General** tab, select **Internet Protocol (TCP/IP)** and click **Properties**.

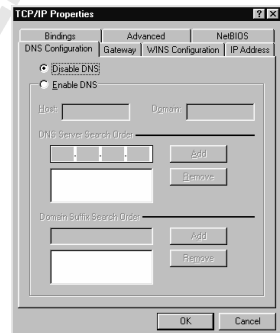
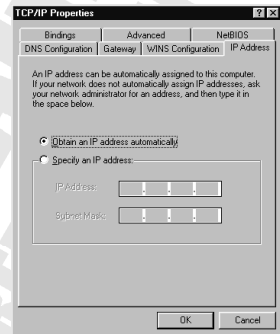
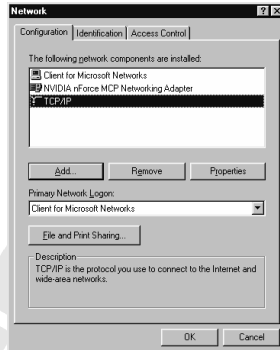


5. On **General** tab, select **Obtain an IP address automatically** and **DNS server address automatically**.
6. Click **OK** to save settings and close **Internet Protocol (TCP/IP) Properties** window.



Windows 95/98/Me

1. Click **Start** → **Settings** → **Control Panel**. Double-click the **Network** icon.
2. On **Configuration** tab, select **TCP/IP** for appropriate network adapter and click **Properties**.
3. On **IP Address** tab, select **Obtain an IP address automatically**.
4. On **DNS Configuration** tab, select **Disable DNS**.
5. Click **OK** to save settings and close **TCP/IP Properties** window.



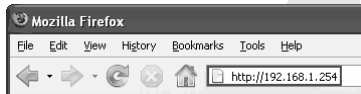
To make sure that network adapter properly obtained an IP address from router's DHCP server, click **Start** > **Run** and type **cmd** (Win 2000/XP) or **command** (Win 95/98/ME). In command line type **ipconfig /all** and check that value of the **IP Address** is **192.168.1.x**

Configure router via web browser

Cerberus Wi-Fi Lite (P6381-0) router can be configured via web browser, which is usually integrated with operating system. Router offers clear and simple interface.

Login

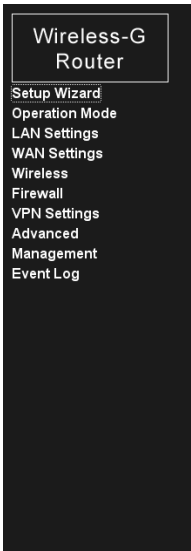
1. Launch the Web browser
2. In address bar enter the default IP address: `http://192.168.1.254`



3. Enter username and password – default **root / 1234**



Navigation



Setup Wizard

The setup wizard will guide you to configure Wireless-G Router for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you through the following steps. Begin by clicking on **Next**.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Setup Wireless LAN

Next>>

Buttons

Next>> – Click **Next>>** to proceed in a series of screens.

<<Back – Click **<<Back** to return to the previous screen. You will lost all unsaved settings in the current screen.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Setup Wizard

You can use the **Setup Wizard** to configure NTP (Network Time Protocol), LAN, WAN and wireless port settings. The main **Setup Wizard** screen displays every time you access the Wireless-G Router. Or, click **Setup Wizard** in the navigation panel. **Click Next>>** to continue.

Setup Wizard

The setup wizard will guide you to configure Wireless-G Router for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you through the following steps. Begin by clicking on **Next**.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Setup Wireless LAN

Next>>

Setup Wizard: Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
- Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Gateway – In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Wireless ISP – In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Next>> – Click **Next>>** to continue to the next screen.

Setup Wizard: Time Zone Settings

Configure NTP (Network Time Protocol) in the first **Setup Wizard** screen. NTP allows the Wireless-G Router to automatically update system date and time from a time server.

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Enable NTP client update

Time Zone Select : (GMT+08:00)Taipei

NTP server : 192.5.41.41 - North America

Cancel <<Back Next>>

Enable NTP client update – Select this option to set the Wireless-G Router as an NTP client to automatically update the system date and time from a time server on the network. Then set the fields below. Clear this check box to disable this feature. In this case, logs will not show the correct system time.

Time Zone Select – Select the time zone of the geographical location in which the Wireless-G Router is installed.

NTP Server – Select a pre-defined time server.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Next>> – Click **Next>>** to continue to the next screen.

Setup Wizard: LAN Interface Setup

Configure the IP address and subnet mask of the LAN interface on the Wireless-G Router in the second Setup Wizard screen.

3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Wireless-G Router. Here you may change the setting for IP address and subnet mask.

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Domain Name:	<input type="text"/>

IP Address – This field displays the router's current LAN IP address, which is used to access WebGUI. To change the setting, specify a new IP address for the LAN interface. Enter the IP address in dotted decimal notation. For example, 192.168.1.254.

Subnet Mask – This field displays the current subnet mask. To change, enter a new subnet mask in dotted decimal notation. For example, 255.255.255.0.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Next>> – Click **Next>>** to continue to the next screen.

Setup Wizard: WAN Interface Setup

Configure Internet access settings in the third **Setup Wizard** screen. This screen varies depending on the connection type you select. Configure the fields in this screen with the information provided by your ISP.

- **WAN Interface Setup: DHCP Client**

If your ISP does not give you any IP address and/or user name and password information, select **DHCP Client** in the **WAN Access Type** field.

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Wireless-G Router. Here you may change the method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:

Host Name:

- **WAN Access Setup: Static IP**

If your ISP provide you with a static WAN IP address without user name or password information, select Static IP in the WAN Access Setup field. Set the network information with the information provided by your ISP.

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Wireless-G Router. Here you may change the method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:	<input type="text" value="Static IP"/>
IP Address:	<input type="text" value="192.168.10.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.10.254"/>
DNS :	<input type="text"/>

IP Address – Enter the WAN IP address (in dotted decimal notation) as provided by your ISP. For example. 10.10.10.1.

Subnet Mask – Enter the subnet mask (in dotted decimal notation) for the WAN IP address. For example. 255.255.255.0.

Default Gateway – Enter the IP address of the default gateway device.

DNS – A DNS (Domain Name System) server keeps mappings of IP addresses and domain names. Thus you don't have to enter an IP address to access a web site/device. Enter the IP address of a DNS server in dotted decimal notation. For example, 192.168.1.10.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Next>> – Click **Next>>** to continue to the next screen.

• **WAN Interface Setup: PPPoE**

If your ISP provides you with a user name and password, then most likely you are using a PPPoE connection. Select **PPPoE** in the **WAN Access Type** field.

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Wireless-G Router. Here you may change the method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: 

User Name:

Password:

User Name – Enter the account user name as provided by the ISP. The user name is case-sensitive.

Password – Enter the password associated with the user name above. The password is case-sensitive.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Next>> – Click **Next>>** to continue to the next screen.

- **WAN Interface Setup: PPTP**

PPTP is mostly available in European countries. If your ISP provides you a fixed WAN IP address, user name and password, then you are probably using PPTP connection type. Select **PPTP** in the **WAN Access Type** field.

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Wireless-G Router. Here you may change the method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:	<input type="text" value="PPTP"/>
IP Address:	<input type="text" value="172.1.1.2"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Server IP Address:	<input type="text" value="172.1.1.1"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>

IP Address – Enter the WAN IP address (in dotted decimal notation) as provided by your ISP. For example. 10.10.10.1.

Subnet Mask – Enter the subnet mask (in dotted decimal notation) for the WAN IP address. For example. 255.255.255.0.

Server IP Address – Enter the IP address of the access server on the ISP network.

User Name – Enter the account user name as provided by the ISP. The user name is case-sensitive.

Password – Enter the password associated with the user name above. The password is case-sensitive.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Next>> – Click **Next>>** to continue to the next screen.

• Setup Wizard: Wireless Basic Settings

Configure basic wireless LAN and wireless security settings in the fourth **Setup Wizard** screen.

5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Wireless-G Router.

Disable Wireless LAN Interface

Band:

Mode:

Network Type:

SSID:

Channel Number:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode

SSID of Extended Interface:

Band – If your wireless network contains only IEEE 802.11b devices, select **802.1 B**. If your wireless network contains only IEEE 802.11g devices, select **802.1 G**. If your wireless network contains both IEEE 802.11b and IEEE 802.11g devices, select **802.1 B/G**.

Mode – In addition to setting the Wireless-G Router as an **AP** (access point) bridging the wireless and wired networks, you can also set the Wireless-G Router to other operating modes.

- The **Client** mode allows you to use the Wireless-G Router as a wireless adapter for a computer. This allows the computer to connect to a wireless network.
- To wirelessly bridge two wired networks, use the **WDS** mode.
- Select **AP + WDS** mode to set the Wireless-G Router to wireless bridge two networks and work as an access point at the same time.

Network Type – This field is applicable when you select **Client** in the **Mode** field. Select **Infrastructure** to allow a computer to connect to a wireless network via an access point. Select **Ad-hoc** to allow a computer to connect to another wireless-enabled computer.

SSID – An SSID uniquely identifies a wireless network. All devices in a wireless network must use the same SSID to communicate with each other. Enter the name of a wireless network to which the computer connects.

Channel Number – A channel is the operating frequency in which a wireless device transmits data. The number of channels you can select varies depending on your country's regulation. Select a channel number the Wireless-G Router is to use for wireless communication. To reduce interference, select a channel number that is further away from what the nearest wireless device/network uses. For example, if the nearest wireless device/network is using channel 6, set the Wireless-G Router to use channel 11.

Cancel – Click **Cancel** to start configuring the Setup Wizard again.

<<Back – Click **<<Back** to discard the changes and go back to the previous screen.

Finished – Click **Finished** to save the settings. The Wireless-G Router will reboot to make the changes take effect.

Note: If you have changed the LAN IP address, you must use the new IP address to access the WebGUI again.

- **Testing Your Connection**

You have completed the wizard screens. To test your Internet connection, open a web browser on any connected computer and enter any web site address (such as <http://www.pentagram.eu>).

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and WISP function.

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL or Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
- Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Apply Change

Reset

Gateway – In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Wireless ISP – In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

LAN Interface Setup

The LAN (Local Area Network) is the network connected to a LAN port on the Wireless-G Router. To configure LAN interface settings, click **LAN Settings** in the navigation panel.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Wireless-G Router. Here you may change the setting for IP address, subnet mask, etc..

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
802.1d Spanning Tree:	<input type="button" value="Disabled"/>
Clone MAC Address:	<input type="text" value="000000000000"/>

IP Address – This field displays the router's current LAN IP address, which is used to access WebGUI. To change the setting, specify a new IP address for the LAN interface. Enter the IP address in dotted decimal notation. For example, 192.168.1.254.

Note: *When you change the LAN IP address, this also changes the DHCP client pool settings in the DHCP Settings screen. If DHCP server is enabled, restart your computer or network adapter to obtain an IP address from the Wireless-G Router again. To access the WebGUI again, enter the new LAN IP address.*

Subnet Mask – This field displays the current subnet mask. To change, enter a new subnet mask in dotted decimal notation. For example, 255.255.255.0.

Default Gateway – Enter the IP address of the default gateway device.

802.1d Spanning Tree – IEEE 802.1d spanning tree protocol detects and eliminates network loops. A network loop may create duplicate broadcast packets that reduce network performance. Select **Enabled** to activate this feature.

Clone MAC Address – You can set the Wireless-G Router to use the same MAC address on all outgoing packets through the LAN interface. Thus the LAN network appears as a single device to the external network. This increases the security level. Enter a computer's MAC address in six pairs of hexadecimal notation. For example, 00a0f45a0010.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

WAN Interface Setup

Configure advanced WAN interface settings in the WAN Interface Setup screen. This screen varies depending on the connection type you select.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Wireless-G Router. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:

Host Name:

MTU Size: (1400-1492 bytes)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable UPnP
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

The following list describes the new fields in this screen. For other field descriptions, refer to **Setup Wizard: WAN Interface Setup** section of this manual.

MTU Size – MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1452, to have the router select the best MTU for your Internet connection.

Attain DNS Automatically – A DNS (Domain Name System) server keeps mappings of IP addresses and domain names. Thus you don't have to enter an IP address to access a web site/device. If your ISP dynamically assigns DNS information, select this option to obtain DNS server IP address automatically.

Set DNS Manually – Select this option if you have DNS server IP address(es) provided by your ISP.

DNS 1 .. 3 – Enter the IP address of a DNS server in dotted decimal notation. For example, 192.168.1.10.

Clone MAC Address – Some ISPs performs authentication based on a MAC address to allow only one computer to use the Internet connection. To allow more than one computer to share an Internet connection, enter a computer's MAC address to copy to the WAN interface.

Enable UPnP – UPnP (Universal Plug and Play) is a communication standard that allows simple peer-to-peer network connectivity between UPnP-enabled devices. With UPnP, a device can automatically join a network, obtain an IP address, convey its presence and manage other UPnP-enabled devices without additional configuration. Select this option to activate this feature. This allows you to view the Wireless-G Router information and remotely manage the Wireless-G Router through a UPnP-ready operating system (such as Windows XP).

Enable IPsec Pass through on VPN Connection – IPsec (Internet Protocol Security) is a standard protocol that allows a device to establish secure connections at the IP layer. Select this option to allow IPsec tunnels to pass through the Wireless-G Router.

Enable PPTP Pass through on VPN Connection – PPTP (Point-to-Point Tunneling Protocol) allows you to establish VPN sessions to a Windows computer (such as Windows XP). Select this option to allow PPTP tunnel to pass through the Wireless-G Router.

Enable L2TP Pass through on VPN Connection – L2TP (Layer 2 Tunneling Protocol) allows you to establish a secure connection on the MAC layer. Select this option to allow L2TP tunnel to pass through the Wireless-G Router.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

New fields on the DHCP Client connection screen:

Host Name – Some ISP require a host name to get a DHCP address

New fields on the PPPoE connection screen:

Service Name – A PPPoE service name is either an ISP name or a class of service that is configured on the PPPoE server.

Connection Type – There are three connection types – continuous, connect on demand and manual.

- **Continuous** – the connection to the ISP is always connected.
- **Connect On Demand** – the connection to the ISP is initialized only when an application is active to connect the Internet.
- **Manual** – the connection to the ISP is set manually. You can click the **Connect** or **Disconnect** button any time.

Idle Time – Active only when **Connect On Demand** is selected. This is the time it takes for the router to disconnect from the ISP if no access request is received.

New fields on the PPTP connection screen:

Request MPPE Encryption – MPPE is Microsoft Point-To-Point Encryption, and is described in RFC3078. You will need to enable it if your PPTP Server requires it.



Wireless

Wireless: Wireless Basic Settings

Click **Wireless > Wireless Basic Settings**. Configure basic wireless settings in this screen.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Wireless-G Router. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band:

Mode:

Network Type:

SSID:

Regulation Domain:

Channel Number:

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode

SSID of Extended Interface:

Disable Wireless LAN Interface – Select this option to deactivate wireless capability on the Wireless-G Router. No wireless connection is allowed.

Band – If your wireless network contains only IEEE 802.11b devices, select **802.1 B**. If your wireless network contains only IEEE 802.11g devices, select **802.1 G**. If your wireless network contains both IEEE 802.11b and IEEE 802.11g devices, select **802.1 B/G**.

Mode – In addition to setting the Wireless-G Router as an AP (access point) bridging the wireless and wired networks, you can also set the Wireless-G Router to other operating modes.

- The **Client** mode allows you to use the Wireless-G Router as a wireless adapter for a computer. This allows the computer to connect to a wireless network.
- To wirelessly bridge two wired networks, use the **WDS** mode.
- Select **AP + WDS** mode to set the Wireless-G Router to wireless bridge two networks and work as an access point at the same time.

Note: If you set the Wireless-G Router in WDS modes, make sure you activate the spanning tree protocol to avoid network loops.

Network Type – This field is applicable when you select **Client** in the **Mode** field. Select **Infrastructure** to allow a computer to connect to a wireless network via an access point. Select **Ad-hoc** to allow a computer to connect to another wireless-enabled computer.

Site Survey – This button is applicable when you select **Client** in the **Mode** field and **Infrastructure** in the **Network Type** field. Click **Site Survey** to open a screen displaying a list of available wireless networks/devices within transmission range. You can set the Wireless-G Router to connect to a wireless network/device.

SSID – An SSID uniquely identifies a wireless network. All devices in a wireless network must use the same SSID to communicate with each other. Enter the name of a wireless network to which the computer connects.

Regulation Domain – Select the name of your regulation domain.

Channel Number – A channel is the operating frequency in which a wireless device transmits data. The number of channels you can select varies depending on the regulation domain you select. Select a channel number the Wireless-G Router is to use for wireless communication.

To reduce interference, select a channel number that is further away from what the nearest wireless device/network uses. For example, if the nearest wireless device/network is using channel 6, set the Wireless-G Router to use channel 11.

Associated Clients – Click **Show Active Clients** to display a screen showing the list of wireless clients that are currently connected to the Wireless-G Router.

Enable MAC Cloning (Single Ethernet Client) – You can set the Wireless-G Router to use the same MAC address on all outgoing packets through the WLAN interface. Thus the wireless network appears as a single Ethernet device to the external network. This increases the security level. Enter a computer's MAC address in six pairs of hexadecimal notation. For example, 00a0f45a0010.

Enable Universal Repeater Mode – When you enable this universal repeater function, the Wireless-G Router will extend the wireless distance to connect another wireless router or AP.

SSID of Extended Interface – Input the Parent SSID, when you select the **Universal Repeater Mode**.

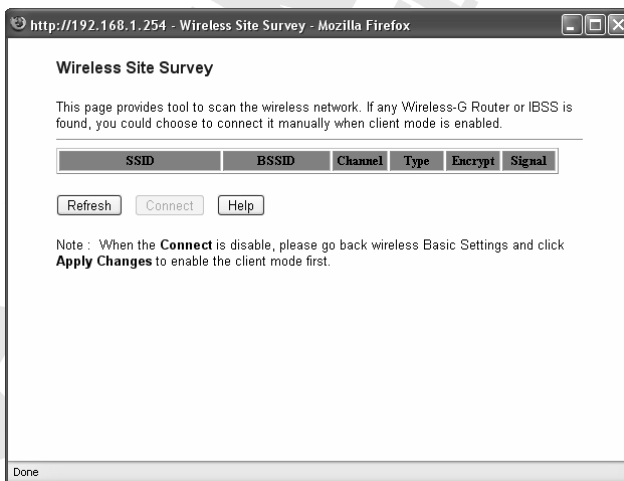
Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click Reset to undo the changes.

Help – Click Help to display on-line help information in a pop-up screen.

- **Wireless Basic Settings: Site Survey**

When you set the Wireless-G Router to work in wireless client mode, you can view a list of available wireless networks/devices in the **Site Survey** screen. Use this screen to establish a wireless connection to a device/network.



SSID – This field displays the name of a wireless network/device.

BSSID – This field displays for Infrastructure mode. This field displays the name of a wireless network.

Channel – This field displays the wireless channel number the wireless network/device uses.

Type – This field displays the wireless operating type (Infrastructure or Ad-hoc).

Encrypt – This field displays whether security is activated on the wireless network/device.

Note: *If communication to a wireless network is encrypted, you must first configure the same wireless security settings and then connect to that wireless network.*

Signal – This field displays the signal strength to the wireless network/device.

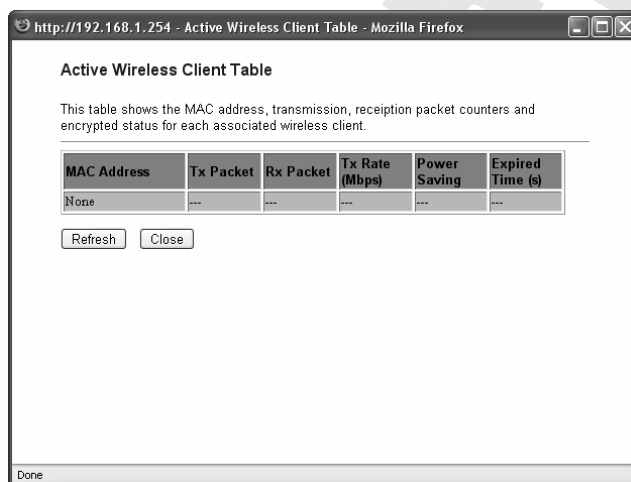
Refresh – Click **Refresh** to update this screen.

Connect – Click **Connect** to establish a connection to the select wireless network.

Help – Click **Help** to display on-line help information in a pop-up screen.

- **Wireless Basic Settings: Show Active Clients**

When you set the Wireless-G Router to work in access point (AP) mode, you can view a list of connected wireless clients in the **Active Wireless Client Table** screen.



MAC Address – This field displays the MAC address of a connected wireless client.

Tx Packet – This field displays the number of packets transmitted to this wireless device.

Rx Packet – This field displays the number of packets received from this wireless device.

Tx Rate (Mbps) – This field displays the transmission rate to this wireless device.

Power Saving – The power saving feature allows a computer to stop transmitting through the wireless adapter during sleep mode. This allows the computer (especially a notebook) to save energy. This field displays whether this feature is activated on the wireless client.

Expired Time (s) – By default, the Wireless-G Router disconnects a wireless client after 300 seconds of inactivity (no beacon or data transmission). This field displays the time that remains before the Wireless-G Router disconnects the wireless connection to the wireless client. The Wireless-G Router resets this timer back to 300 when a beacon or data packet is received.

Refresh – Click **Refresh** to update this screen.

Close – Click **Close** to close this screen.

Wireless: Wireless Advanced Settings

Click **Wireless > Advanced Wireless Settings** to display the configuration screen. The default wireless settings in this screen work in most wireless network environment.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Wireless-G Router.

Authentication Type: Open System Shared Key Auto
Fragment Threshold: (256-2346)
RTS Threshold: (0-2347)
Beacon Interval: (20-1024 ms)
Data Rate:
Wireless network coverage
Preamble Type: Long Preamble Short Preamble
Broadcast SSID: Enabled Disabled
IAPP: Enabled Disabled
802.11g Protection: Enabled Disabled
Turbo Mode: Auto Always Off

Authentication Type – IEEE 802.11b defines a basic authentication security using WEP (Wireless Equivalent Protocol) keys.

- Select **Open System** if you don't want to use a WEP key for authentication.
- Select **Share Key** to set the Wireless-G Router and the peer wireless devices to authenticate each other with a WEP key.
- Select **Auto** to allow both open or shared authentication.

Note: The peer wireless device must also set to use the same authentication type.

Fragmentation Threshold – Specify the maximum packet size allowed before the Wireless-G Router fragments data. If there are many error packets on the network, slightly increase the threshold. Setting the threshold too low decreases network performance. Always make a small change to the default settings.

RTS Threshold – The Wireless-G Router will send a Request To Send (RTS) packet to a sending host. When an acknowledgement is received, the Wireless-G Router sends a Clear To Send (CTS) packets to that host to allow data transmission. RTS/CTS eliminates the “hidden node” problem where two hosts are within range of each other but does not know each other's presence. If the number of packets is lower than the RTS threshold, this feature is not activated. If you are experiencing inconsistent data flow on the network, slightly reduce this number.

Beacon Interval – A beacon packet is broadcast by the Wireless-G Router to synchronize the wireless network. The beacon interval allows a wireless client in power saving mode to know when to “wake up” and detect if there's packet waiting to be received. Specify the time period between beacon broadcasts.

Data Rate – Select a transmission rate the Wireless-G Router uses to send data. Select **Auto** to allow the Wireless-G Router to use the maximum transmission rate possible.

Note: If you specify a transmission rate here, make sure the peer wireless devices must also use the same rate for wireless communication.

Wireless network coverage – Select an option to set the wireless coverage range.

Preamble Type – A preamble is used to synchronize transmission timing.

- Select **Long Preamble** if there is interference in your wireless network or you are not sure about the preamble settings on other wireless devices. All IEEE 802.11b devices support long preamble.
- Select **Short Preamble** if all wireless devices support this mode. Short preamble reduces transmission overhead.

Broadcast SSID – You can set the Wireless-G Router not to broadcast its SSID to increase wireless security. This prevents unknown wireless clients from knowing the presence of the Wireless-G Router. Select **Enabled** to hide the SSID. Otherwise, select **Disabled**.

IAPP – IAPP (Inter Access Point Protocol) allows the Wireless-G Router to communicate with neighboring access points for wireless roaming. Select **Enabled** to activate this feature; otherwise, select **Disabled**.

802.11g Protection – Unless you encounter severe connection problem to the Wireless-G Router, do not enable this feature. When you select **Enabled** to activate this feature, the Wireless-G Router will try to get all IEEE 802.11b packets. However, activating this feature reduces performance.

Turbo Mode

- **Auto** – The Wireless-G Router will automatically detect the turbo mode client and adjust its wireless connection speed.
- **Always** – The Wireless-G Router always turn on the turbo mode.
- **Off** – The Wireless-G Router does not turn on the turbo mode.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.



Wireless: Security

Configure security for the wireless interface in the **Wireless Security Setup** screen. The Wireless-G Router supports four wireless security options: **WEP**, **WPA**, **WPA2**, **WPA2 Mixed**. These options offer different security levels for wireless communication.

Note: It is recommended that you use the highest security option to protect your wireless communication.

Click **Wireless > Security** to display the configuration screen. The applicable fields vary depending on the security option you select in the **Encryption** field.

Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption:	<input type="text" value="None"/>	<input type="button" value="Set WEP Key"/>
<input type="checkbox"/> Use 802.1x Authentication	<input checked="" type="radio"/> WEP 64bits	<input type="radio"/> WEP 128bits
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS)	<input checked="" type="radio"/> Personal (Pre-Shared Key)
WPA Cipher Suite:	<input checked="" type="checkbox"/> TKIP	<input type="checkbox"/> AES
WPA2 Cipher Suite:	<input type="checkbox"/> TKIP	<input checked="" type="checkbox"/> AES
Pre-Shared Key Format:	<input type="text" value="ASCII"/>	
Pre-Shared Key:	<input type="text"/>	
<input type="checkbox"/> Enable Pre-Authentication	Port <input type="text" value="1812"/>	IP address <input type="text"/>
Authentication RADIUS Server:	Password <input type="text"/>	

Note: When encryption WEP is selected, you must set WEP key value.

- **Wireless: Security: WEP**

WEP (Wired Equivalent Privacy) uses a key to encrypt and decrypt traffic transmitted wirelessly. WEP keeps wireless communication private.

Note: Both the Wireless-G Router and the connected wireless device(s) must use the same WEP key for communication.

WEP does not provide user authentication. You can enable IEEE 802.1x on the Wireless-G Router to authenticate a user before wireless access is allowed. In the WebGUI, click **Wireless > Security** and select **WEP** in the **Encryption** field.

Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption:
 WEP

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format: ASCII

Pre-Shared Key:

Enable

Pre-Authentication

Authentication RADIUS Server: Port IP address

Password

Note: When encryption WEP is selected, you must set WEP key value.

Encryption – Select **WEP** to basic data encryption.

Set WEP Key – Click **Set WEP Key** to set the WEP keys.

Use 802.1x Authentication – Select this option to enable user authentication. Users must enter the same password (specified in the **Password** field) to access the wireless network. Select the length of the encryption key to protect the password transmitted. Choices are **WEP 64bits** and **WEP 128bits**.

Authentication RADIUS Server – Specify the RADIUS server information in the fields provided.

Port – Enter the authentication port number.

IP Address – Enter the IP address of the RADIUS server in dotted decimal notation. For example, 192.168.1.10.

Password – Specify the password that all users must enter before access to the wireless network is allowed.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Wireless: Security: WEP: Set WEP Key

Click **Set WEP Key** to display the configuration screen as shown.

Wireless WEP Key Setup

This page allows you to setup the WEP key value. You choose either 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

Apply Changes Close Reset

Done

Key Length – Select the encryption key length. Choices are **64-bit** and **128-bit**. Select **128-bit** for higher security.

Key Format – Specify how you want to enter the keys. Select **Hex** to enter hexadecimal format (that starts with 0x). Select **ASCII** to enter alphanumerical characters (a-z, A-Z, 0-9) for the keys.

Default Tx Key – Select the default key to encrypt data before transmitting.

Encryption Key 1 .. 4 – If you select **64-bit** in the **Key Length** field, enter 10 hexadecimal or 5 ASCII characters. If you select **128-bit** in the **Key Length** field, enter 26 hexadecimal or 13 ASCII characters.

Note: As you enter the keys, an asterisk "*" displays for each character you enter.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Close – Click **Close** to close this screen.

Note: All unsaved changes will be lost.

Reset – Click **Reset** to undo the changes.

• Wireless: Security: WPA/ WPA2/ WPA2 Mix

WPA (WiFi Protected Access) is a subset of IEEE802.11i and provides better data encryption over WEP and optional authentication. WPA2 (WiFi Protected Access 2), also known as IEEE 802.11i, has improved data encryption and user authentication compared to WPA. For AES, WPA2 uses a 256-bit block data encryption.

Wireless Security Setup

This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys can prevent any unauthorized access to your wireless network.

Encryption:

 Use 802.1x Authentication WEP 64bits WEP 128bits
WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)
WPA Cipher Suite: TKIP AES
WPA2 Cipher Suite: TKIP AES
Pre-Shared Key Format:
Pre-Shared Key:
 Enable
Pre-Authentication
Authentication RADIUS Server: Port IP address
 Password

Note: When encryption WEP is selected, you must set WEP key value.

Encryption – Select **WPA**, **WPA2** or **WPA2 Mix** (for both WPA and WPA2).

Use 802.1x Authentication – Select this option to enable IEEE 802.1x for user authentication.

WPA Authentication Mode – Specify the authentication mode to use.

- Select **Enterprise (RADIUS)** if you have an external RADIUS (Remote Authentication Dial-In User Service) server to authenticate a user.
- Select **Personal (Pre-Shared Key)** if you do not have a RADIUS server. All wireless devices in the same wireless network must use the same pre-shared key.

WPA/ WPA2 Cipher Suite – Specify an encryption method to use.

- Select **TKIP** (Temporal Key Integrity Protocol) that uses a stronger encryption algorithm and protects against hackers with MIC (Message Integrity Check).
- Select **AES** (Advanced Encryption System) that uses symmetric 128-bit block data encryption.

Pre-Shared Key Format – Specify how you want to enter the keys. Select **Hex** to enter hexadecimal format (that starts with 0x). Select **ASCII** to enter alphanumeric characters (a-z, A-Z, 0-9) for the keys.

Pre-Shared Key – Enter between 8 to 32 characters for the pre-shared key.

Note: All wireless devices in the same wireless network must use the same pre-shared key.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Wireless: Wireless Access Control

Use the Wireless Access Control to set the Wireless-G Router to allow or block wireless access based on a computer's MAC address. This allows you to restrict wireless access and increase security.

Click **Wireless > Wireless Access Control** to display the configuration screen as shown.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses in the access control list will be able to connect to your Wireless-G Router. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect to the Wireless-G Router.

Wireless Access Control Mode:

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Wireless Access Control Mode – Set the access control action to apply on the specified computer(s).

- Select **Allow Listed** to grant wireless access to only the computer(s) with the specified MAC address(es). Computers with MAC address not listed are blocked wireless access to the Wireless-G Router.
- Select **Deny Listed** to block wireless access to the computer(s) with the specified MAC address(es). Computers with MAC addresses not listed below are allowed wireless access.
- Select **Disable** to deactivate wireless access control. This allows all computers wireless access to the Wireless-G Router.

MAC Address – Enter the MAC address of a computer on which you want to restrict wireless access. For example, 0023f6378a1.

Comment – Enter a description for this access control rule.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Current Access Control List – This table displays the current wireless access control settings on the Wireless-G Router.

MAC Address – This field displays the MAC address of the computer to which this access control setting applies.

Comment – This field displays the description for this access control setting.

Select – Select this option to delete the MAC filter.

Delete Selected – Click **Delete Selected** to delete the selected access control setting(s). When you click this button, a warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all access control setting(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the Select check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

Example: Allow Wireless Access on a Computer

The following figure shows an example where the Wireless-G Router allows wireless access from a computer with the MAC address of 00:02:3f:63:78:a1. All other computers are not allowed to access the Wireless-G Router over the wireless interface.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses in the access control list will be able to connect to your Wireless-G Router. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect to the Wireless-G Router.

Wireless Access Control Mode:

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Wireless: WDS (Wireless Distributed System)

The WDS screen is applicable when you set the Wireless-G Router to operate in WDS mode in the Wireless Basic Settings screen. WDS allows the Wireless-G Router to act as a bridge to connect to other wireless routers in bridge mode. This allows two LAN networks to communicate to each other wirelessly. To participate in a WDS, wireless routers must be set to operate in bridge mode with the same channel and know each other's MAC address. If applicable, they must also use the same security settings. Click **Wireless > WDS** to display the configuration screen as shown.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of all other APs which you want to communicate with in the table and then check enable WDS.

Enable WDS

Add WDS AP: MAC Address Comment

Current WDS AP List:

MAC Address	Comment	Select
-------------	---------	--------

Enable WDS – Select this option to activate this feature.

Add WDS AP – Enter the MAC address of another wireless device participating in this WDS. For example, 0023f6378a1.

Comment – Enter a description for this setting.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Set Security – Click **Set Security** to display a screen to configure WDS security settings.

Current WDS AP List – This table displays the list of wireless APs participating in this WDS.

MAC Address – This field displays the MAC address of the wireless AP in this WDS.

Comment – This field displays the description for this setting.

Select – Select this option to delete the wireless AP.

Delete Selected – Click **Delete Selected** to delete the selected wireless AP(s). When you click this button, a warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all wireless AP(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the **Select** check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

Wireless: WDS: Set Security

You can set the security settings for the WDS in the **WDS Security Setup** screen.

Note: You must set the same encryption method and key in the same WDS.

Encryption – Select the encryption method in this field.

WEP Key Format – Specify how you want to enter the keys. Select **Hex** to enter hexadecimal format (that starts with 0x). Select **ASCII** to enter alphanumerical characters (a-z, A-Z, 0-9) for the keys.

WEP Key – If you select **64-bit** in the **Key Length** field, enter 10 hexadecimal or 5 ASCII characters. If you select **128-bit** in the **Key Length** field, enter 26 hexadecimal or 13 ASCII characters.

Note: As you enter the keys, an asterisk "*" displays for each character you enter.

Pre-Shared Key Format – Specify how you want to enter the keys. Select **Hex** to enter hexadecimal format (that starts with 0x). Select **ASCII** to enter alphanumerical characters (a-z, A-Z, 0-9) for the keys.

Pre-Shared Key – Enter between 8 to 32 characters for the pre-shared key.

Note :All wireless devices in the same wireless network must use the same pre-shared key.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Close – Click **Close** to close this screen.

Note: All unsaved changes will be lost.

Firewall

Firewall: IP Filtering

Use the **IP Filtering** screen to limit Internet access on computers based on the IP addresses and protocol types. This is useful to restrict Internet access usage and providing network security. Click **Firewall > IP Filtering** to display the configuration screen as shown.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address: **Protocol:** **Comment:**

Current Filter Table:

Local IP Address	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> <input type="button" value="Help"/>			

Enable IP Filtering – Select this option to activate this feature.

Local IP Address – Enter the IP address of a computer on which you want to restrict access. For example, 0023f6378a1.

Protocol – Select a protocol type for the application. Choices are **UDP**, **TCP** or **Both**.

Comment – Enter a description for this IP filter.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Current Filter Table – This table displays the current IP filter settings on the Wireless-G Router.

Local IP Address – This field displays the IP address of the computer to which this IP filter applies.

Comment – This field displays the description for this IP filter.

Select – Select this option to delete the IP filter.

Delete Selected – Click **Delete Selected** to delete the selected IP filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all IP filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the **Select** check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

Example: Restricting Internet Access on a Computer

This following example sets the Wireless-G Router to block Internet access from the computer with an IP address of 192.168.1.120.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address: Protocol: Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
------------------	----------	---------	--------

Firewall: Port Filtering

The **Port Filtering** feature allows you to restrict Internet access based on the application protocol and port number(s). You can control Internet access usage (for example, block peer-to-peer applications) and increase network security. Click **Firewall > Port Filtering** to display the configuration screen as shown.

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: - Protocol: Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
------------	----------	---------	--------

Enable Port Filtering – Select this option to activate this feature.

Port Range – Specify the service port number range in the fields provided. To specify one port number, enter the same service port number in both fields.

Protocol – Select a protocol type for the application. Choices are **UDP**, **TCP** or **Both**.

Comment – Enter a description for this port filtering rule.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Current Filter Table – This table displays the current port filter settings on the Wireless-G Router.

MAC Address – This field displays the MAC address of the computer to which this MAC filter applies.

Comment – This field displays the description for this port filter.

Select – Select this option to delete the port filter.

Delete Selected – Click **Delete Selected** to delete the selected port filter(s). When you click this button, a Selected warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all port filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the **Select** check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

Example: Blocking FTP File Transfer

The following example sets the Wireless-G Router to block users from using FTP (File Transfer Protocol) to transfer files over the Internet.

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: 20 - 21 **Protocol:** Both **Comment:**

NoFTP

Apply Changes

Reset

Current Filter Table:

Port Range	Protocol	Comment	Select
------------	----------	---------	--------

Delete Selected

Delete All

Reset

Help

Firewall: MAC Filtering

Use the **MAC Filtering** screen to limit Internet access on computers behind the Wireless-G Router. This is useful to restrict Internet access usage and providing network security. Click **Firewall > MAC Filtering** to display the configuration screen as shown.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering

MAC Address:

Comment:

Apply Changes

Reset

Current Filter Table:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

Help

Enable MAC Filtering – Select this option to activate this feature.

MAC Address – Enter the MAC address of a computer on which you want to restrict access. For example, 0023f6378a1.

Comment – Enter a description for this MAC filtering rule.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Current Filter Table – This table displays the current MAC filter settings on the Wireless-G Router.

MAC Address – This field displays the MAC address of the computer to which this MAC filter applies.

Comment – This field displays the description for this MAC filter.

Select – Select this option to delete the MAC filter.

Delete Selected – Click **Delete Selected** to delete the selected MAC filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all MAC filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the **Select** check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

Example: Restricting Internet Access on a Computer

The following example blocks Internet access on a computer with a MAC address of 00:02:3F:63:78:A1.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering

MAC Address: 00023f6378a1

Comment: Block web surfing

Apply Changes

Reset

Current Filter Table:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

Help

Firewall: URL Filtering

URL Filtering allows you to restrict access based on the web site address. Click **Firewall > URL Filtering** to display the configuration screen.

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Enable URL Filtering

URL Address:

Current Filter Table:

URL Address	Select

Enable URL Filtering – Select this option to activate this feature.

URL Address – Enter the web site address to which you want to restrict access. For example, http://xxx.com.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Current Filter Table – This table displays the current MAC filter settings on the Wireless-G Router.

URL Address – This field displays the address of the web site to which this filter applies.

Select – Select this option to delete the MAC filter.

Delete Selected – Click **Delete Selected** to delete the selected MAC filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all MAC filter(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the **Select** check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

VPN Settings

A VPN (Virtual Private Network) allows you to set up a secure connection over the Internet to a remote location without the cost of a leased line. With VPN, data is encrypted before sending over the Internet to the remote site. This technique of secure communication is known as tunneling. The Wireless-G Router supports IPSec (Internet Protocol Security) VPN. IPSec VPN secures data transferred over the IP layer. In order to establish VPN tunnels, you must set the same VPN rule and security settings on the Wireless-G Router and the remote VPN gateway.

VPN Settings: VPN Setup

You can enable the VPN feature and configure general VPN settings in the **VPN Setup** screen. Click **VPN Settings > VPN Setup** to display the configuration screen.

VPN Setup

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

Enable IPSec VPN
 Enable NAT Traversal

Current VPN Connection Table: WAN IP:0.0.0.0

#	Name	Active	Local Address	Remote Address	Remote Gateway	Status
1	Example	Y	192.168.1.0/24	10.10.10.0/24	10.10.10.254	Disconnected
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-	-	-	-
10	-	-	-	-	-	-

Enable IPSec VPN – Select this option to activate this feature.

Enable NAT Traversal – Select this option to set up VPN connection over NAT-enabled devices.

Generate RSA Key – Click **Generate RSA Key** to set the Wireless-G Router to automatically create a new RSA key for VPN communication.

Show RSA Public Key – Click **Show RSA Public Key** to display the public RSA key in a separate screen.

Current VPN Connection Table – This tables the current VPN tunnels configured on the Wireless-G Router.

WAN IP – This field displays the WAN IP address of the Wireless-G Router.

– This field displays the index number.

Name – This field displays the descriptive name for the VPN tunnel.

Active – This field indicates whether the VPN tunnel is enabled or not.

Local Address – This field displays the IP address and subnet mask of the local network/device.

Remote Address – This field displays the IP address and subnet mask of the remote VPN location.

Remote Gateway – This field displays the IP address of the remote VPN gateway.

Status – This field displays whether this VPN tunnel is up (**Connected**) or not (**Disconnected**).

Edit – Click **Edit** to configure the selected VPN tunnel.

Delete – Click **Delete** to remove the selected VPN tunnel.

Refresh – Click **Refresh** to update this screen.

Help – Click **Help** to display on-line help information in a pop-up screen.

Configuring a VPN Tunnel

To configure a VPN tunnel, select an entry in the **Current VPN Connection Table** list and click **Edit**.

VPN Setup

Enable Tunnel 2

Connection Name:

Auth Type:

Local Site:

Local IP Address/Network

Local Subnet Mask

Remote Site:

Remote Secure Gateway

Remote IP Address/Network

Remote Subnet Mask

Local/Peer ID:

Local ID Type

Local ID

Remote ID Type

Remote ID

Key Management: IKE

Connection Type

ESP (Encryption Algorithm)

(Authentication Algorithm)

PreShared Key

Remote RSA Key

Status

Enable Tunnel 1 – Select this option to activate this VPN rule.

Connection Name – Enter a descriptive name for identification purposes.

Auth Type – Specify an authentication type. Choices are **PSK** (Pre-Shared Key) and **RSA** (an authentication method that requires a digital certificate).

Local Site – Select whether to allow one local host or any computer in a network to initiate a VPN connection to the remote location.

Local IP Address/ Network – Enter the IP address for the local host/network in dotted decimal notation. For example, 192.168.1.10.

Local Subnet Mask – Enter the subnet mask for the local host/network. For example, 255.255.255.0.

Remote Site – Specify the destination of the outgoing VPN traffic.

Remote Secure Gateway – Enter the IP address of the remote VPN gateway with which the Wireless-G Router sets up a VPN connection.

Remote IP Address/ Network – Enter the destination IP address of the remote host/network. For example, 192.168.1.10.

Remote Subnet Mask – Enter the subnet mask for the remote host/network. For example, 255.255.255.0.

Local/Peer ID – Configure the fields below to set the ID type and content to identify the local and remote VPN endpoints.

Local ID Type – Select the ID type the Wireless-G Router uses. Choices are **IP**, **DNS** or **Email**.

Local ID – Specify the ID to identify the Wireless-G Router.

- If you select **IP** in the **Local ID Type** field, the Wireless-G Router uses the IP address you specify in the **Local IP Address/Network** as the local ID.
- If you select **DNS** in the **Local ID Type** field, enter a domain name.
- If you select **Email** in the **Local ID Type** field, enter an email address.

Remote ID Type – Select the ID type the remote VPN endpoint uses. Choices are **IP**, **DNS** or **Email**.

Remote ID – Specify the ID to identify the remote VPN gateway.

- If you select **IP** in the **Remote ID Type** field, the Wireless-G Router uses the IP address you specify in the **Remote IP Address/Network** as the peer ID.
- If you select **DNS** in the **Remote ID Type** field, enter a domain name.
- If you select **Email** in the **Remote ID Type** field, enter an email address.

Key Management

IKE – Select this option to set the Wireless-G Router to automatically generate the encryption keys for the VPN tunnel. Clear this option to manually set the authentication and encryption keys.

Advanced – This button is applicable when you select **IKE**. Click **Advanced** to configure IKE authentication and encryption settings.

Connection Type – Select Initiator to set the Wireless-G Router is to initiate a VPN connection to the remote VPN gateway. Select Responder to set the Wireless-G Router to allow VPN connection from a remote location.

Connect – This button is applicable when you select **Responder** in the **Connection Type** field. Click **Connect** to establish a VPN connection to the remote location.

Disconnect – This button is applicable when you select **Initiator** in the **Connection Type** field and the connection is up. Click **Disconnect** to terminate the VPN connection.

ESP – Set the fields below to configure ESP (Encapsulating Security Payload) settings.

(Encryption Algorithm) – Specify the encryption algorithm for this VPN rule. Choices are **3DES** and **AES128** (faster). Select **NULL** to set up phase 2 tunnel (for key exchange) without encryption.

(Authentication Algorithm) – Specify the encryption algorithm for this VPN rule. Choices are **MD5** and **SHA1** (more secure).

PreShared Key – This field displays when you select **IKE**. Enter the pre-shared key for IKE authentication. The key length varies depending on the authentication algorithm.

- For **MD5**, enter 16 characters for the key.
- For **SHA1**, enter 20 characters for the key.

Remote RSA Key – This field displays when you select **IKE**. Enter the public RSA key of the remote VPN gateway to authenticate with a certificate.

Status – This field displays whether this VPN tunnel is up (**Connected**) or not (**Disconnected**).

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to clear the settings in the fields.

Refresh – Click **Refresh** to update this screen.

Back – Click **Back** to return to the main VPN setup screen.

Help – Click **Help** to display on-line help information in a pop-up screen.

Advanced VPN Settings for IKE

To configure phase 1 and phase 2 IKE security settings for a VPN rule, click **Advanced** in the **Edit** screen. There are two phases for an IKE negotiation before a VPN tunnel is established. During phase 1 negotiation, two VPN devices exchange security parameters (such as the authentication and encryption algorithms, etc.). After phase 1 negotiation, an SA (Security Association) is created. The SA is then used for phase 2 negotiation where the security keys are exchanged.

Advanced VPN Setting for IKE

This page is used to provide advanced setting for IKE mode

Tunnel 1

Phase 1:

Negotiation Mode: Main mode

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Key Group: DH5(modp1536)

Key Life Time: 3600

Phase 2:

Active Protocol: ESP

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Key Life Time: 28800

Encapsulation: Tunnel mode

Perfect Forward Secrecy (PFS): ON

Ok Cancel Help

Done

Phase 1 – Set the fields for phase 1 negotiation.

Negotiation Mode – For negotiation, the Wireless-G Router uses **Main mode** that also encrypts the ID type and content (you specify in the **VPN Setup – Edit** screen) for maximum security.

Encryption Algorithm – Specify the encryption algorithm for this VPN rule. Choices are **3DES** and **AES128** (faster).

Authentication Algorithm – Specify the authentication algorithm for this VPN rule. Choices are **MD5** and **SHA1** (more secure).

Key Group – Select the Diffie-Hellman (DH) encryption protocol to generate a secret key. Choices are **DH1(modp768)**, **DH2(modp1024)** and **DH5(modp1536)**. The higher the group number, the higher the security.

Key Life Time – Specify the time (in seconds) before the Wireless-G Router updates the key with the remote VPN gateway. A short key life time increases security as it forces the two VPN gateways to update the keys regularly. However, during the key update process, the VPN tunnel(s) will be disrupted temporarily.

Phase 2 – Set the fields for phase 2 negotiation.

Active Protocol – The Wireless-G Router uses ESP (Encapsulating Security Payload) to maintain an SA.

Encryption Algorithm – Specify the encryption algorithm for this VPN rule. Choices are **3DES** and **AES128** (faster). Select **NULL** to set up phase 2 tunnel (for key exchange) without encryption.

Authentication Algorithm – Specify the encryption algorithm for this VPN rule. Choices are **MD5** and **SHA1** (more secure).

Key Life Time – Specify the time (in seconds) before the Wireless-G Router updates the key with the remote VPN gateway. A short key life time increases security as it forces the two VPN gateways to update the keys regularly. However, during the key update process, the VPN tunnel(s) will be disrupted temporary.

Encapsulation – The Wireless-G Router uses Tunnel mode to encapsulate the entire IP packet to transmit it securely.

Perfect Forward Secrecy (PFS) – Select **ON** to activate this feature. This sets the Wireless-G Router and the remote VPN gateway to use different keys every time. Same keys are not used twice. Enable this feature for maximum security. Select **NONE** to disable this feature for faster SA setup in exchange for less data security.

OK – Click **OK** to save the settings

Cancel – Click **Cancel** to reset the fields.

Help – Click **Help** to display on-line help information in a pop-up screen.

Generating RSA Key

In addition to using a pre-shared key for security, you can set the Wireless-G Router to automatically create a new RSA key for VPN communication. In the VPN Setup screen, click the **Generate RSA Key** button.

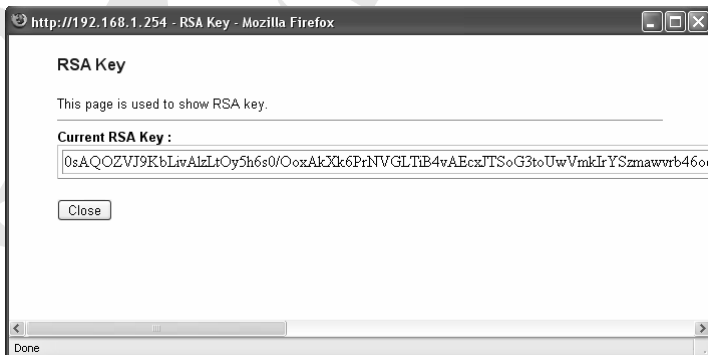
Note: This process may take up to 2 minutes. Do NOT turn off the Wireless-G Router.

After the RSA key is generated, a screen display as shown. Click **OK** to return to the main **VPN Setup** screen.

Change setting successfully!

OK

To display the public RSA key on the Wireless-G Router, click **Show RSA Public Key** button in the **VPN Setup** screen.



Advanced

Advanced: Port Forwarding

Use the **Port Forwarding** screen to forward service requests to the computer(s) behind the Wireless-G Router. This allows you to set up web servers, FTP servers or special applications that require Internet access (such as video conferencing or online gaming). Click **Advanced > Port Forwarding** to display the configuration screen as shown.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

IP Address:

Protocol: Port Range: -

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>	<input type="button" value="Reset"/>	<input type="button" value="Help"/>	

Enable Port Forwarding – Select this option to activate this feature.

IP Address – Enter the IP address of the computer to which the service requests are forwarded. For example, 192.168.1.100.

Note: You must set the computer to use a static (or fixed) IP address.

Protocol – Select a protocol type for the application. Choices are **UDP**, **TCP** or **Both**.

Port Range – Specify the service port number range in the fields provided. To specify one port number, enter the same service port number in both fields.

Comment – Enter a description for this application.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Current Port Forwarding Table – This table displays the current port forwarding settings on the Wireless-G Router.

Local IP Address – This field displays the IP address of the computer to which to forward the specified service requests.

Protocol – This field displays the protocol type used for the application.

Port Range – This field displays a port number or a range of port numbers the Wireless-G Router forwards.

Comment – This field displays the description for the setting.

Select – Select this option to delete the port forwarding rule.

Delete Selected – Click **Delete Selected** to delete the selected port forwarding rule(s). When you click this button, a warning screen displays. Click **OK** to continue.

Delete All – Click **Delete All** to remove all port forwarding rule(s). When you click this button, a warning screen displays. Click **OK** to continue.

Reset – Click **Reset** to clear the Select check box(es).

Help – Click **Help** to display on-line help information in a pop-up screen.

Example: Forwarding HTTP Requests

This section shows you how to configure the **Port Forwarding** screen to forward HTTP (or web) requests. In this example, you want to set the Wireless-G Router to forward all service requests on port 80 to a server computer with a fixed IP address of 192.168.1.10.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

IP Address: 192.168.1.10

Protocol: Both Port Range: 80 - 80

Comment: Web

Apply Changes Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
------------------	----------	------------	---------	--------

Delete Selected Delete All Reset Help

Advanced: DMZ

The Demilitarized Zone (DMZ) feature on the Wireless-G Router enables you to play computer games or use special applications (such as video conferencing) over the Internet on a LAN computer. The DMZ function exposes just the one computer to the Internet without compromising the security for other LAN computers. Click **Advanced > DMZ** to display the configuration screen as shown.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Enable DMZ

DMZ Host IP Address:

Apply Changes Reset Help

Enable DMZ – Select this option to activate this feature.

DMZ Host IP Address – Enter the IP address of the computer you want to expose to the Internet. For example, 192.168.1.100.

Note: You must set the computer to use a static (or fixed) IP address.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Advanced: Dynamic DNS

You can configure Dynamic Domain Name System (DDNS) settings on the Wireless-G Router. DDNS allows you to assign fixed domain name to a dynamic IP address. This is useful when you want to set up a web server, FTP server or other publicly accessible servers on your computer. Before you enable and use DDNS, you must sign up for DDNS service with a service provider (such as <http://www.dyndns.org>). Click **Advanced** > **Dynamic DNS** to display the configuration screen.

Dynamic DNS Settings

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider:

Domain Name:

User Name/Email:

Password/Key:

*Note: For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)
For DynDNS, you can create your DynDNS account [here](#)*

Enable DDNS – Select this option to activate this feature.

Service Provider – Select the DDNS service provider with which you have set up an account.

Domain Name – Enter the domain name (or URL) assigned to you by the DDNS service provider.

User Name/Email – Enter the account user name or the email address that you use to sign up for the service.

Password/Key – Enter the password or key for the user name above.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Management

Management: Status

View current device status in the Wireless-G Router Status screen. Click **Management > Status**.

Wireless-G Router Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:54m:24s
Firmware Version	v1.4.0.3
Wireless Configuration	
Mode	WDS
Band	802.11 B/G
SSID	
Channel Number	11
Encryption	Disabled
BSSID	00:08:a1:aa:04:62
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Enabled
MAC Address	00:08:a1:aa:04:62
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:08:a1:aa:04:61



Help

System

Uptime – This field displays the time that elapsed since the Wireless-G Router last reboots.

Firmware Version – This field displays the current firmware version number.

Wireless Configuration

Mode – This field displays the wireless operating mode on the Wireless-G Router.

Band – This field displays the wireless protocol the Wireless-G Router uses.

SSID – This field displays the unique name for the wireless network.

Channel Number – This field displays the operating frequency the Wireless-G Router uses.

Encryption – This field displays whether data encryption is activated for the wireless interface.

BSSID – This field displays the ID (or MAC address) of the wireless interface.

Associated Clients – This field displays the number of wireless computers currently connected to the Wireless-G Router.

TCP/IP Configuration

Attained IP Protocol – This field displays the IP addressing type on the LAN interface.

IP Address – This field displays the LAN IP address.

Subnet Mask – This field displays the subnet mask associated with the IP address above.

Default Gateway – This field displays the IP address of the gateway device.

DHCP Server – This field displays whether DHCP server is activated on the Wireless-G Router.

MAC Address – This field displays MAC address of the LAN Interface.

WAN Configuration

Attained IP Protocol – This field displays the IP addressing type on the WAN interface.

IP Address – This field displays the WAN IP address.

Subnet Mask – This field displays the subnet mask associated with the IP address above.

Default Gateway – This field displays the IP address of the gateway device.

MAC Address – This field displays MAC address of the WAN Interface.

Help – Click **Help** to display on-line help information in a pop-up screen.

Management: DHCP Settings

The **DHCP Settings** screen allows you to set the Dynamic Host Configuration Protocol (DHCP) server settings on the Wireless-G Router. A DHCP server automatically assigns an IP address to each connected computer on the network. You must configure the computers to automatically receive an IP address from the DHCP server (the Wireless-G Router) and make sure there is no other DHCP server(s) on the same network. Click **Management > DHCP Settings** to display the configuration screen.

DHCP Settings

This page is used to configure the parameters for local area network which connects to the LAN port of your Wireless-G Router. Here you may change the setting for DHCP.

Enable DHCP Server

DHCP Client Range: -

Domain Name:

Dynamic DHCP Client List

IP Address	MAC Address	Time Expired(s)
None	----	----

Enable DHCP Server – Select this option set the Wireless-G Router to act as a DHCP server providing IP address(es) to connected computers. Click this option to disable this feature. You must then set up a DHCP server on the network or assign the computers fixed IP addresses.

DHCP Client Range – Specify the range of the IP address pool to assign the computers.

Note: *The DHCP client IP addresses you specify here must be in the same subnet as the LAN interface on the Wireless-G Router. When you change the LAN IP address in the LAN Interface screen, these fields are automatically updated to be in the same subnet.*

Apply – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Dynamic DHCP Client IP – This table displays the information of the DHCP client(s) that is assigned an IP address from the Wireless-G Router.

IP Address – This field displays the IP address assigned to a DHCP client.

MAC Address – This field displays the MAC address of the DHCP client.

Time Expired(s) – This field displays the time(s) the DHCP client is allowed to use the IP address. After the time expires, the DHCP client must obtain a new IP address from the Wireless-G Router again.

Refresh – Click **Refresh** to update this table.

Help – Click **Help** to display on-line help information in a pop-up screen.

Management: Time Zone Settings

You can set the system time on the Wireless-G Router using the following methods:

- manually.
 - automatically update using NTP (Network Time Protocol) through a time server.
- Setting the device system time is recommended to display the correct time for the event logs. In the WebGUI, click **Management > Time Zone Settings** to display the configuration screen.

Time Zone Settings

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :

Enable NTP client update

NTP server :

(Manual IP Setting)

Current Time – These fields displays the current system time. To manually change the system time, change the corresponding fields.

Time Zone Select – Select the time zone of the geographical location in which the Wireless-G Router is installed.

Enable NTP client update – Select this option to set the Wireless-G Router as an NTP client to automatically update the system date and time from a time server on the network. Then specify a time server below. Clear this check box to disable this feature. In this case, logs will not show the correct system time.

NTP Servers – Select a pre-defined time server. To manually specify a time server, enter the IP address in dotted decimal notation. For example, 10.10.10.1.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Refresh – Click **Refresh** to set the Wireless-G Router to re-synchronize the system time with a time server.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Management: Password

The default administrative login name is **root** and the default password is **1234**. It is recommended you change the default login password after the first login.

Password Setup

This page is used to set the account to access the web server of Wireless-G Router. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

User Name – The default user name is **root**. Specify a new user name. Enter a name between 1 to 30 alphanumeric characters. If you don't want to change the default user name, enter **root**.

Note: The user name is case sensitive. If you leave this field blank, login authentication will be disabled. That means you don't need to enter a user name and password to log into the WebGUI for management. This is NOT recommended.

New Password – Enter the new password. The password can be between 1 and 30 alphanumeric characters.

Note: The password is case sensitive.

Confirm Password – Enter the new password again for confirmation.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Reset – Click **Reset** to undo the changes.

Help – Click **Help** to display on-line help information in a pop-up screen.

Management: Firmware Upgrade

The firmware on the Wireless-G Router is upgraded through the WebGUI. Follow the steps below.

Note: Make sure you upgrade the correct firmware to the device. Upgrading a wrong firmware to the device may render it useless.

1. Download the latest firmware version from the product web site.
2. In the WebGUI, click **Management > Firmware Upgrade** to display the screen as shown.
3. Specify the location and name of the firmware in the **Select File** field or click **Browse** to locate it.
4. Click **Upload** to start the firmware upgrade process.

Upgrade Firmware

This page allows you to upgrade the Wireless-G Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

Note: Do NOT turn off during the firmware upgrade process. Doing so may render your device useless.

5. After the firmware upgrade process is successful, the screen displays as shown. Click **OK**. The Wireless-G Router automatically restarts to make the changes take effect.

Update successfully (size = 1943355 bytes)!

Please wait a while for rebooting...

Management: Remote Management

By default, the Wireless-G Router blocks WebGUI access from the WAN port for management. You can set the Wireless-G Router to allow easy remote management.

1. Click **Management > Remote Management**.
2. Select the **Enable Web Server Access on WAN** option.
3. Click **Apply Changes** to restart the Wireless-G Router to make the changes take effect.

Remote Management

This page allows you to configure and managed from the WAN side of your Wireless-G Router.

- Enable Web Server Access on WAN
- Enable Ping Access on WAN

Enable Web Server Access on WAN – If you want to control the Wireless-G Router across the internet, you must enable this feature, check the box.

Enable Ping Access on WAN – If you don't want the Wireless-G Router to response the ping packet from WAN, you must disable this feature, uncheck the box.

Management: Save/Restore Settings

Use the **Save/Restore Settings** screen to back up the device settings, restore configuration or reset the Wireless-G Router back to the factory default settings.

Save/Reload Settings

This page allows you to save current settings to a file or reload the settings from the file which was saved previously. Besides, you may reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

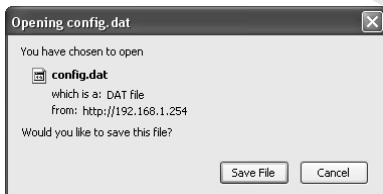
Reset Settings to Default:

- **Save/Restore Settings: Save Current Configuration**

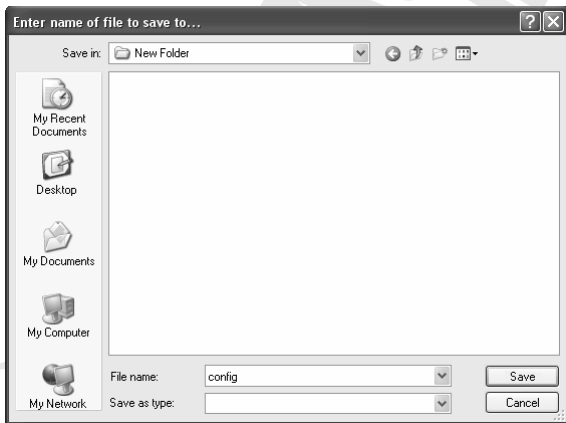
You can back up the device configuration information to a file on your computer. This is recommended after you have complete settings on the Wireless-G Router and that it is fully operable for your network.

Follow the steps below to back up a copy of the device configuration.

1. In the WebGUI, click **Management > Save/Restore Settings**.
2. Click **Save...**
3. A **File Download** screen displays as shown. Click **Save**.



4. A **Save as** screen displays. Specify the location and name for the file. Click **Save** to start the configuration backup process.



5. After the configuration backup process is complete, a **Download complete** message displays.

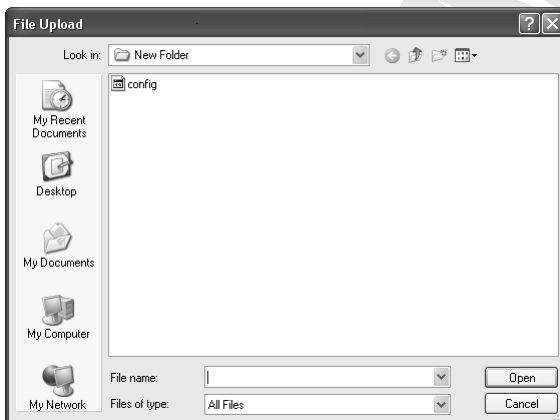


- **Save/Restore Settings: Restore Configuration**

You can use the **Save/Restore Settings** screen to restore the device settings to a previous backup configuration.

Note: Restoring settings erases all current configuration on the Wireless-G Router. Do NOT turn off the device during the file transfer process. Doing so may render your device useless.

1. In the WebGUI, click **Management > Save/Restore Settings**.
2. In the **Load Settings from File** field, specify the location and file name of a previously backed up file. Click **Browse...** to locate it.
3. A **Choose file** screen displays. Select a backup configuration file and click **Open**.

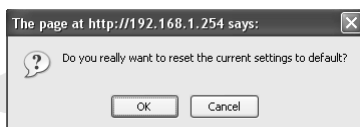


4. Click **Upload** to start the file transfer process.
5. After the process is successful, the screen displays as shown. Click **OK**.

Update successfully!

OK

6. The Wireless-G Router automatically restarts to make the changes take effect. Wait until the reboot process is finished before accessing the device again.
- **Save/Restore Settings: Reset**
Resetting the device erases all custom settings.
 1. To reset the Wireless-G Router back to the factory default settings, click **Reset** in the **Save/Restore Settings** screen.
 2. A warning screen displays. Click **OK**.



3. The Wireless-G Router automatically restarts to make the changes take effect. Wait until the reboot process is finished before accessing the device again.

Management: System Restart

Use the **System Restart** screen to reboot the Wireless-G Router without disconnecting the power source.

Follow the steps below to restart the Wireless-G Router through the WebGUI.

1. Click **Management > System Restart** to display the screen as shown.
2. Click **Apply Changes**.

Note: Restarting the device erases all unsaved changes.

System Restart

This page is used to restart device.

Do you want to restart ?

3. The screen displays as shown. Click **OK**.

Please wait a while for rebooting...

4. Wait until the Wireless-G Router finishes restarting before accessing it again.

Event Log

Use the **Event Log** screen to view logs and set log settings. By default, the Wireless-G Router records logs of all management and traffic activities. You can use the logs to monitor network traffic or troubleshooting.

Event Log

This page can be used to set remote log server and show the system log.

Enable Log
 system all **wireless**
 Enable Remote Log **Log Server IP Address:**

```

Oday 01:00:42 device wlan0 left promiscuous mode
Oday 01:00:42 br0: port 1(eth0) entering disabled state
Oday 01:00:42 device eth0 left promiscuous mode
Oday 01:00:42 device eth0 entered promiscuous mode
Oday 01:00:42 eth0:phy is 8305
Oday 01:00:42 device wlan0 entered promiscuous mode
Oday 01:00:42 br0: port 2(wlan0) entering listening state
Oday 01:00:42 br0: port 1(eth0) entering listening state
Oday 01:00:42 br0: port 2(wlan0) entering learning state
Oday 01:00:42 br0: port 2(wlan0) entering forwarding state
Oday 01:00:42 br0: topology change detected, propagating
Oday 01:00:42 br0: port 1(eth0) entering learning state
Oday 01:00:42 br0: port 1(eth0) entering forwarding state
Oday 01:00:42 br0: topology change detected, propagating
Oday 01:00:47 eth1:phy is 8305

```


Enable Log – Select this option to activate system logging.

System all – Select this option to record all log types.

Wireless – Select this option to record wireless related logs.

Enable Remote Log – Select this option to record and store logs to a remote syslog server.

Log Server Address – When you select **Enable Remote Log**, specify the IP address of the remote syslog server. Enter the IP address in dotted decimal notation. For example, 192.168.1.100.

Apply Changes – Click **Apply Changes** to save the changes. The Wireless-G Router will reboot to make the changes take effect.

Refresh – Click **Refresh** to update this screen.

Clear – Click **Clear** to delete all log entries.

Help – Click **Help** to display on-line help information in a pop-up screen.

Troubleshooting

If the router is not function properly, first check this session for simple troubleshooting before contacting your Internet service provider (ISP) for support.

Using LEDs to Diagnose Problems

The **LEDs** are useful aides for finding possible problem causes.

Power LED

The **POWER LED** on the front panel does not light up.:

1. Make sure that the power adaptor is connected to the router and plugged in to an appropriate power source. Use only the supplied power adaptor;
2. Check that the router and the power source are both turned on and the router is receiving sufficient power;
3. Turn the router off and on;
4. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

LAN LED

The **LAN LED** on the front panel does not light up:

1. Check the Ethernet cable connections between your router and the computer or hub;
2. Check for faulty Ethernet cables;
3. Make sure your computer's Ethernet card is working properly;
4. If these steps fail to correct the problem, contact your local distributor for assistance.

WAN LED

The **WAN LED** on the front panel does not light up:

1. Check the Ethernet cable connections between your router and ISP's access device;
2. Check that the ISP's access device is turned on and receiving sufficient power;

Problems with the Web Interface

I cannot access the web Interface:

1. Make sure you are using the correct IP address of the router. Check the IP address of the router;
2. Your computer's and the router's IP addresses must be on the same subnet for LAN access;
3. If you changed the router's LAN IP address, then enter the new one as the URL;
4. Remove any filters in LAN or WAN that block web service.

Problems with the Login Username and Password

I forgot my login username and/or password:

1. The default username is "**root**". The default password is "**1234**". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing;
2. Press the RESET button for 10-12 seconds, and then release it - the defaults have been restored and the router restarts;

Problems with LAN Interface

I cannot access the router from the LAN or ping any computer on the LAN:

1. Check the Ethernet LEDs on the front panel. A LAN LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting;
2. Make sure that the IP address and the subnet mask is consistent between the router and the workstation.

Problems with the Internet Access

I cannot access the Internet:

1. Make sure the router is turned on and connected to the network;
2. If the WAN LED is off, refer to Section **WAN LED** of this troubleshooting;
3. Verify your WAN settings;
4. Make sure you entered the correct user name and password;
5. For wireless stations, check that both the router and wireless station(s) are using the same ESSID, channel and encryption keys (if encryption is activated).

Internet connection disconnects:

1. If you use PPPoE, check the idle time-out setting;
2. Contact your ISP.

If you have any troubles to configure or setup this Wireless-G Router, please feel free to contact us.