

Wireless-N Broadband AP / Router

User's Manual

Version 1.3

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The WRTR-501(FCC ID: RYK-WRTR501) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise without the prior writing of the publisher.

JULY 2007

Contents

1. Introduction	4
2. Safety Notification	5
3. Hardware Installation	6
4. How to Configuring the 11n Router	9
4.1 Setup – Basic Setup	10
4.2 Setup – DDNS	14
4.3 Setup – MAC Address Clone	16
4.4 Wireless – Basic Wireless Settings	17
4.5 Wireless – Wireless Security	19
4.6 Wireless – Wireless MAC Filter	20
4.7 Wireless – Advanced Wireless Settings	21
4.8 Wireless – Wireless WDS Settings	23
4.9 Security – VPN Passthrough	24
4.10 Access Restrictions – Internet Access Policy	25
4.11 Application & Gaming – Port Range Forwarding	27
4.12 Application & Gaming – Port Range Triggering	28
4.13 Application & Gaming – DMZ	29
4.14 Administration – Management	30
4.15 Administration – Log	32
4.16 Administration – Diagnostics	33
4.17 Administration – Factory Defaults	34
4.18 Administration – Firmware Upgrade	35
4.19 Status – Router	36
4.20 Status – Local Network	38
4.21 Status – Wireless Network	39
5. Troubleshooting – Q & A	40

1. Introduction

Thank you for purchasing your Wireless 802.11n AP Router.

This user guide will assist you with the installation procedure.

The package you have received should contain the following items:

- Wireless 802.11n AP Router
- Quick Installation Guide
- User Manual CD-ROM
- 3 Detachable Antennas
- Universal AC/DC Power Adapter
- RJ-45 Network Cable
- Warranty Card

Note: if anything is missing, please contact your vendor

2. Safety Notification

Your Wireless AP Router should be placed in a safe and secure location. To ensure proper operation, please keep the unit away from water and other damaging elements. Please read the user manual thoroughly before you install the device.

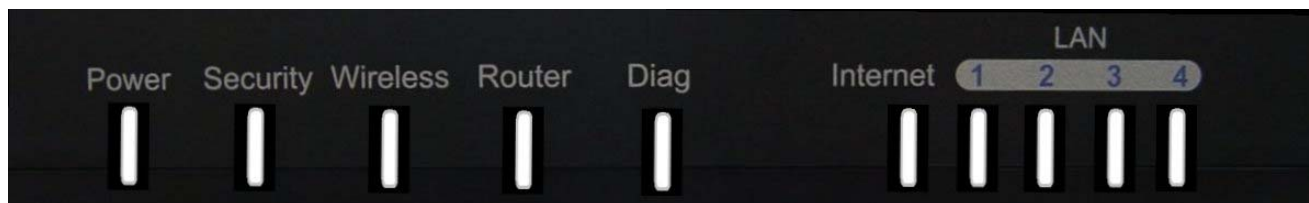
The device should only be repaired by authorized and qualified engineer.

- Please do not try to open or repair the device yourself.
- Do not place the device in a damp or humid location, i.e. a bathroom.
- The device should be placed in a sheltered and non-slip location within a temperature range of +5 to +40 Celsius degree.
- Please do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

3. Hardware Installation

Front Panel

The front panel provides LED's for device status. Refer to the following table for the meaning of each feature.



Power	Green - When turn on the power, this led light.
Wireless	Green - When wireless is available, this led lights. And When transmit/receive the data, this led is blinking
LAN1-LAN4, WAN	Green - When link is established, these leds light. And when transmit or receive the data, these led is blinking.
Security	Orange - While WPS function is working after WPS switch is pushed and, this led is blinking
DIAG	Red - This led is blinking during the FW update or when system is abnormal Firmware defines the action.
Router	Green - When Router is working as "Bridge", this LED light

Rear Panel

The rear panel features 4 LAN ports, 1 WAN port and Reset button. Refer to the following table for the meaning of each feature.



Power	The POWER port is where you will connect the power adapter.
WAN	The WAN port is where you will connect your broadband Internet connection.
LAN 1,2,3,4	These ports (1, 2, 3, 4) connect the Router to your networked PCs and other Ethernet network devices.
RESET Button	The RESET button can restore device to factory default settings by press this button for approx. 10 seconds during device power on status.
Router Mode Switch	Switch router or access point mode

AP Router Default Settings

User	
Password	admin
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
RF ESSID	MIMO
Channel	6
Radio Band	Wide (Full speed to 300Mbps)
Mode	BGN Mixed
Encryption	Disabled
WPS Function	Enabled
DHCP Server	Enabled

Hardware Installation for Connection to Your Broadband Modem

1. Power off your network devices.
2. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your wireless devices.
3. Adjust the antennas. Normally, higher location of your Router will get better performance.
4. Using a standard Ethernet network cable, connect the Router's Internet port to your broadband modem.
5. Connect your network PCs or Ethernet devices to the Router's LAN ports using standard Ethernet network cable.
6. Connect the AC power adapter to the Router's Power port. Then connect the other end to an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter may cause product damage.
7. The Hardware installation is complete; please refer to the following content for Router configuration.

4. How to Configuring the 11n Router

TURN ON POWER SUPPLY

Quick power cycle would cause system corruption. When power on, be careful not to shut down in about 5 seconds, because data is writing to the flash.

START UP & LOGIN

In order to configure the Wireless 11n Router, you must use web browser and manually input `http://192.168.1.1` into the Address box and press Enter. The Main Page will appear.



In order to configure the Wireless 11n Router, you must input the password into the **Password** box and leave blank on the **User Name** box. The default password is "**admin**".

Once you have logged-in as administrator, it is a good idea to change the administrator password to ensure a secure protection to the Wireless 11n Router. The Security Settings section described later in this manual describes how to change the password.

Once you have input the correct password and logged-in, the screen will change to the Setup page screen.

4.1 Setup – Basic Setup

MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER

To change the configuration, use Internet Explorer (IE) or Netscape Communicator to connect the WEB management 192.168.1.1.

This following screen contains all of the Router's basic setup functions.

The screenshot shows the MIMO Wireless GN router's basic setup web interface. The interface is divided into several sections:

- Setup:** Includes tabs for Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Below these are sub-tabs for Basic Setup, DDNS, and MAC Address Clone.
- Internet Setup:** Internet Connection Type is set to "Automatic Configuration - DHCP".
- Optional Settings (required by some Internet Service Providers):** Host Name and Domain Name are empty text boxes. MTU is set to "Auto" and Size is "1500".
- Network Setup:** Router IP Local IP Address is "192.168.1.1" and Subnet Mask is "255.255.255.0".
- DHCP Server Settings:** DHCP Server is "Enabled". Start IP Address is "192.168.1.100", Maximum Number of Users is "50", IP Address Range is "192.168.1.100 ~ 149", Client Lease Time is "1440" minutes. Static DNS 1, 2, 3, and WINS are all set to "0".
- Time Setting:** Time Zone is "(GMT-12:00) Kwajalein". A checkbox "Automatically adjust clock for daylight saving changes." is checked.

At the bottom right, there are "Save Settings" and "Cancel Changes" buttons.

Most users will be able to configure the AP Router and get it working properly using the settings on this screen. Some Internet Service Providers (ISPs) will require that you enter broadband specific information into this device, such as User Name, Password, IP Address, Default Gateway Address, or DNS IP Address for Internet access. This information can be obtained from your ISP, if required.

Internet Setup

Internet Connection Type:

◆ Automatic Configuration – DHCP

This is default connection type. If your ISP supports DHCP assigning dynamic IP address then please select this type.

◆ **Static IP**

If you are required to use a fixed IP address to connect to the Internet, then select **Static IP**.
Internet IP Address: This is the Router's WAN IP address. Usually it will provide by your ISP, and need to input here.

Subnet Mask: This is the Router's Subnet Mask. Usually it will provide by your ISP, and need to input here.

Default Gateway: This is the Router's Gateway Address. Usually it will provide by your ISP, and need to input here.

DNS (1-3): Your ISP will provide you at least one DNS Server IP Address and need to input here.

◆ **PPPoE**

PPPoE (Point-to-Point Protocol over Ethernet) is one of Internet connections type. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE type. If yes, you will have to enable **PPPoE**.

User Name and Password: Enter the User Name and Password provided by your ISP.

Connect on Demand: The Max Idle Time means the Router will disconnect the Internet connection if there is no any traffic through this Router during a specified period of time. If your Internet connection has been terminated due to over this idle time, the Connect on Demand option will trigger the Router to automatically re-establish your connection as soon as you try to access the Internet again.

Keep Alive: The Redial Period means the Router will periodically check your Internet connection by Redial Period time. If the connection is disconnected, then the Router will redial automatically for your connection.

◆ **PPTP**

Point-to-Point Tunneling Protocol (PPTP), is one of VPN tunnel that can use to encrypt data and prevent the unauthorized viewing of confidential data that is transmitted across public networks.

Internet IP Address and Subnet Mask: This is the Router's IP Address and Subnet Mask. If your Internet connection requires a Static IP address, then your ISP will provide you a Static IP Address and Subnet Mask for input here.

Default Gateway: Your ISP will provide you with the Gateway IP Address.

User Name and Password: This is PPTP login User Name and Password. Your ISP will provide you such information for input here.

Keep Alive: The Redial Period means the Router will periodically check your Internet connection by Redial Period time. If the connection is disconnected, then the Router will redial automatically for your connection.

These types can be selected from the Internet Connection Type drop-down menu. The information required and available features with minor different that depend on what kinds of connection type you select.

Optional Settings

Your ISP may require these settings. If your ISP would provide such information, please note to specify them into your device.

Host Name and Domain Name: These fields allow you to input a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select **Manual** if you want to manually enter the largest packet size that will be transmitted. The recommended size, entered in the *Size* field, is 1500. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, please select the default setting--**Auto**.

Network Setup

The Network Setup section changes the Router's local network settings.

Router IP

IP Address and Subnet Mask. This is Router's LAN IP Address and Subnet Mask. The default IP Address is **192.168.1.1** and the default Subnet Mask is **255.255.255.0**.

DHCP Server Settings

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, you must make sure there is no other DHCP server on your network. If you disable the Router's DHCP server function, you must configure the IP Address, Subnet Mask, and DNS for each network computer (note that each IP Address must be unique).

DHCP Server: DHCP is enabled by factory default. If you already have a DHCP server on your network or you do not want a DHCP server, then select **Disable** from the options.

Assign Static DHCP: The function can enable DHCP server to assign a same IP address for an appointed PC. If you want a PC to be assigned the same IP address every time when it reboots, then click the **Assign Static IP** button.

How to set a PC as Static DHCP client

On the *Static DHCP Client List* screen, enter the static local IP address in the *Assign this IP* field, and enter the MAC address of the PC in the *To this MAC* field. Then click the **Enabled** checkbox. When you have finished your entries, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel your changes. To exit this screen, click the **Close** button.

How to set a DHCP client as Static DHCP client

Click the **DHCP Client Table** button can see a list of DHCP client. On the *DHCP Client Table*, you will see a list of DHCP clients with the following information: Client Names, Interfaces, IP Addresses, and MAC Addresses. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. If you want to add any of the DHCP clients to the Static DHCP Client List, then click the **Save to Static DHCP Client List** checkbox and then click the **Save Settings** button. Click the **Cancel Changes** button to cancel your changes. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

Start IP Address: Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Starting IP Address is **192.168.1.100**.

Maximum Number of Users: Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The absolute maximum is 253 - possible if 192.168.1.1 is your starting IP address. The default is **50**.

IP Address Range: The range of DHCP addresses. This range is according to the setting of Maximum Number of Users.

Client Lease Time: The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. Once the leased time is up, the user will get a new dynamic IP address automatically. The default is 0 minutes, which means one day.

Static DNS 1-3: The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to utilize another, enter that IP Address in one of these fields. You can enter up to 3 DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS: The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Time Settings

Change the time zone in which your network functions from this pull-down menu. Click the checkbox if you want the Router to automatically adjust for daylight savings time.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**.

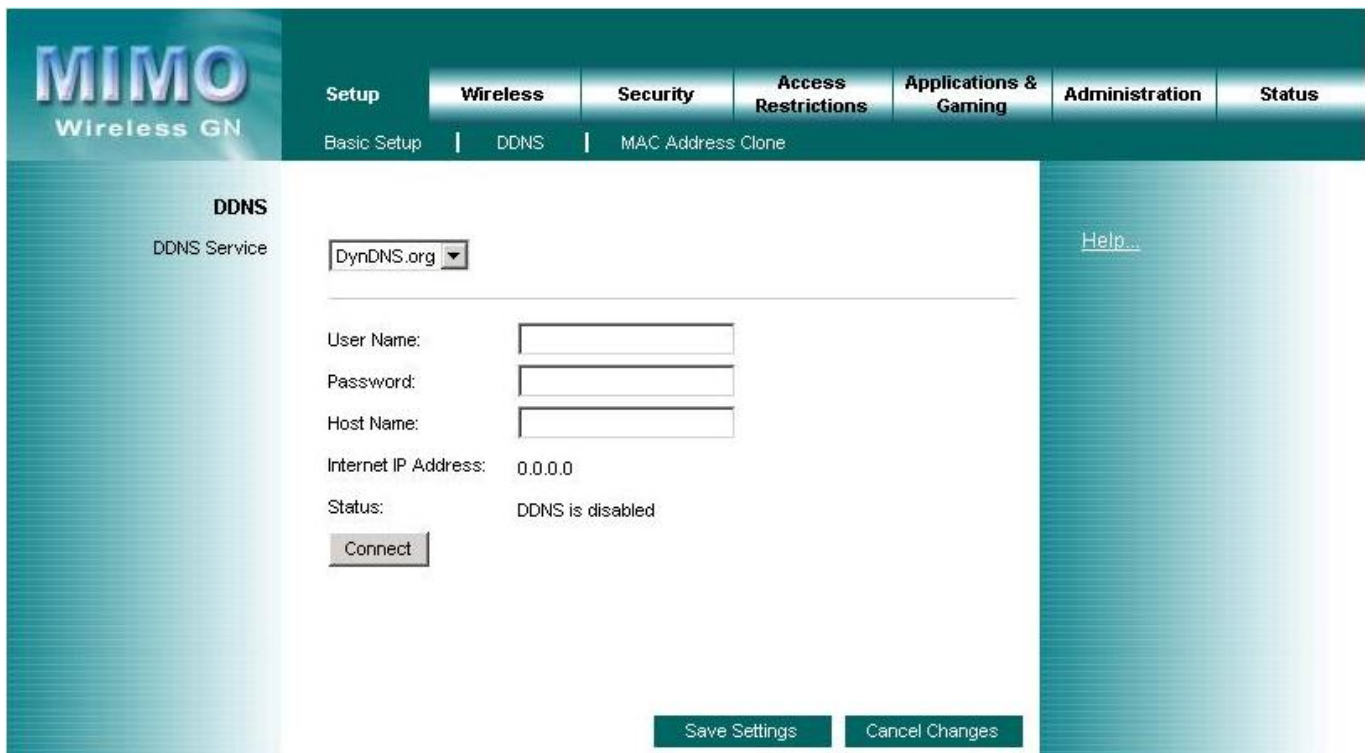
4.2 Setup – DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before using this feature, you need to sign up for DDNS service with one of two DDNS service providers, DynDNS.org or TZO.

DynDNS service

To enable DDNS Service using DynDNS.org, follow these instructions:

1. On the *DDNS* screen, select **DynDNS.org** from the *DDNS Service Provider* drop-down menu.
2. Sign up for DynDNS service at www.dyndns.org for applying one DDNS account. Write down your account information.
3. Complete the *User Name*, *Password*, and *Host Name* fields.
4. Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.



The screenshot shows the DDNS configuration interface for a MIMO Wireless GN router. The page has a teal header with the MIMO logo and navigation tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Under the Wireless tab, there are sub-tabs for Basic Setup, DDNS, and MAC Address Clone. The DDNS section is active, showing a dropdown menu for 'DDNS Service' set to 'DynDNS.org'. Below this are input fields for 'User Name', 'Password', and 'Host Name'. The 'Internet IP Address' is set to '0.0.0.0' and the 'Status' is 'DDNS is disabled'. A 'Connect' button is located below the status. At the bottom of the page, there are 'Save Settings' and 'Cancel Changes' buttons. A 'Help...' link is visible on the right side of the page.

TZO service

To enable DDNS Service using TZO, follow these instructions:

1. On the *DDNS* screen, select **TZO.com** from the *DDNS Service Provider* drop-down menu.
2. Sign up for a free, 30-day trial of TZO service at www.tzo.com/order.html . Write down your account information.
3. Complete the *Email Address*, *TZO Password Key*, and *Domain Name* fields.
4. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel unsaved changes.

The screenshot shows the MIMO Wireless GN web interface. At the top, there is a navigation bar with tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Below this, there are sub-tabs for Basic Setup, DDNS, and MAC Address Clone. The main content area is titled 'DDNS' and 'DDNS Service'. It features a dropdown menu for 'DDNS Service Provider' set to 'TZO.com'. Below this are input fields for 'E-mail Address', 'TZO Password', and 'Domain Name'. The 'Internet IP Address' is displayed as '0.0.0.0'. The 'Status' is 'DDNS is disabled'. There is a 'Connect' button and a 'Help...' link. At the bottom right, there are 'Save Settings' and 'Cancel Changes' buttons.

Internet IP Address: The Router's current Internet IP Address is displayed here.

Status: The status of the DDNS service connection is displayed here.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.3 Setup – MAC Address Clone

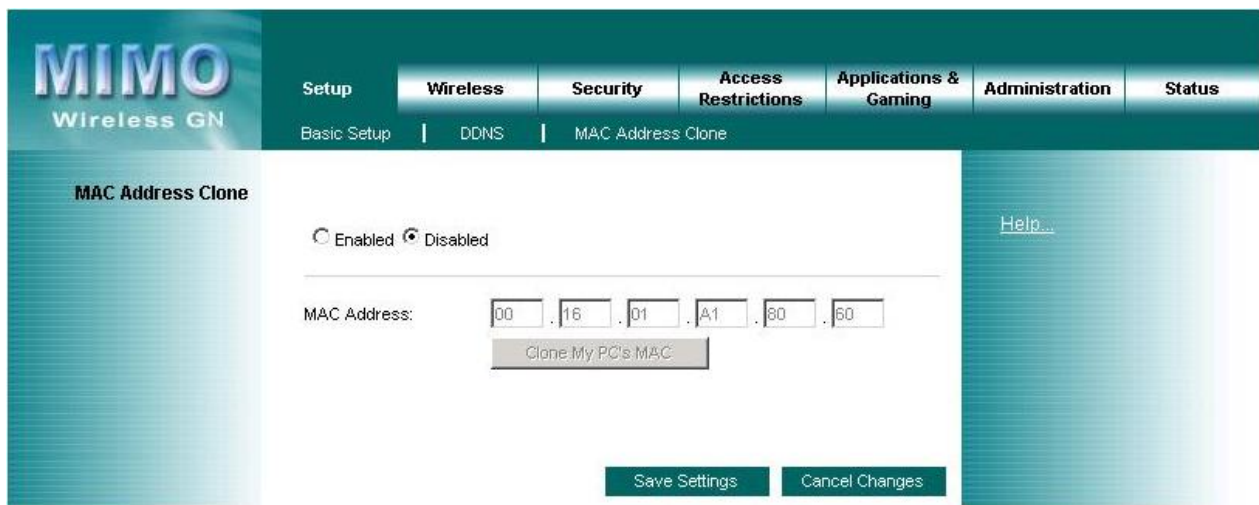
A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

MAC Address Clone

Enabled/Disabled: To have the MAC Address cloned, select **Enabled**.

MAC Address: Enter the MAC Address registered with your ISP here.

Clone My PC's MAC: Clicking this button will clone the MAC address of the PC you are currently using.



The screenshot shows the MIMO Wireless GN web interface. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. Under 'Setup', there are sub-menus for 'Basic Setup', 'DDNS', and 'MAC Address Clone'. The 'MAC Address Clone' page is active, showing radio buttons for 'Enabled' and 'Disabled' (with 'Disabled' selected). Below this is a 'MAC Address' field with six input boxes containing '00', '16', '01', 'A1', '80', and '60'. A 'Clone My PC's MAC' button is positioned below the MAC address field. At the bottom of the page are 'Save Settings' and 'Cancel Changes' buttons. A 'Help...' link is visible on the right side of the page.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.4 Wireless – Basic Wireless Settings

Wireless Network

Wireless Settings

If you are using a Wireless-B, Wireless-G, Wireless-N, Wireless B+G, or Wireless BGN network then the following settings that you may need to configure.

Wireless: You can enable or disable the wireless function.

Network Mode: From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **B/G Mixed**. If you have only 802.11g devices, select **Wireless-G Only**. If you have only 802.11b devices, select **Wireless-B Only**. If you have only 802.11n devices, select **Wireless-N Only**. If you have both 802.11n and 802.11g and 802.11b devices in your network, select **Wireless-BGN**. If you do not have any 802.11g and 802.11b devices in your network, select **Disabled**.

Network Name (SSID): The service set identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. You shall have selected the same SSID for all the APs that will be communicating with mobile wireless stations.

Radio Band: This argument is related to the bandwidth. 20MHz Channel could reach 150 Mbps, and 40 MHz could reach 300 Mbps.

Channel: Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must broadcast on the same channel in order to communicate.

Ext Channel: When 40MHz has been selected with Band Width, two channels of Control Channel and Extension Channel are used.

SSID Broadcast: When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

WPS: WPS function is an easy-to-use encryption to keep wireless connection safe and the default setting, **Enabled**, is to enable it. If you do not want to enable the WPS function, then select **Disabled**.

PIN Code of client: Type the client's PIN code here then click "Connect" button then you could start WPS connection

MIMO
Wireless GN

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings | Wireless WDS Settings

Basic Wireless Settings

Wireless: Enabled Disabled

Network Mode: Wireless-N Only

Network Name(SSID): spur

Radio Band: Wide - 40MHz Channel

Channel: 6 - 2.437GHz

Ext Channel: 2

SSID Broadcast: Enabled Disabled

WPS: Enabled Disabled

PIN Code of client:

[Help...](#)

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.5 Wireless – Wireless Security

The Wireless Security settings configure the security of your wireless network. There are three wireless security mode options supported by the Router: WEP, WPA-Personal(WPA-PSK), and WPA-Enterprise(WPA), WPA2-Personal(WPA2-PSK), and WPA2-Enterprise(WPA2). WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.

Wireless Security

The security options are the same and independent for your Wireless-B and Wireless-G networks. You can use different wireless security methods for your networks; however, within each network (Wireless-B or Wireless-G), all devices must use the same security method and settings.

Security Mode:

WEP: WEP is a basic encryption method; select a level of WEP encryption, **40/64-bit** or **128-bit**. If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button. If you want to enter the WEP key manually, then enter it in the *WEP Key 1-4* field(s). To indicate which WEP key to use, select the appropriate *TX Key* number.

WPA-Personal(WPA-PSK), WPA2-Personal(WPA2-PSK):

This method offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of encryption method you want to use, **TKIP** or **AES**. Enter the Passphrase, which can have 8 to 63 characters. Then enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

WPA-Enterprise(WPA), WPA2-Enterprise(WPA2)

This option features a WPA-Personal used in coordination with a RADIUS server that uses either EAP-TLS or PEAP as its authentication method. (This should only be used when a RADIUS server is connected to the Router.) First, select the type of encryption method you want to use, **TKIP** or **AES**. Enter the RADIUS servers IP address and port number, along with the authentication key shared by the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

802.1x: It designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standard. 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. This central authority is commonly called RADIUS Server.



Change these settings as described here and click the Save Settings button to apply your changes or Cancel Changes. **Changes**. For additional information, click **Help**.

4.6 Wireless – Wireless MAC Filter

This function allows administrator to have access control by enter MAC address of wireless devices which transmitting within your wireless network.

Wireless MAC Filter

Access Restrictions

This policy can effectively control each wireless device using the wireless network. Enable this function to filter wireless devices by MAC Address, either permitting or blocking access. If you do not want to filter users by MAC Address, select **Disabled**.

Prevent PCs listed below from accessing the wireless network: Select this option will block selected wireless client by MAC address.

Permit PCs listed below to access the wireless network: Select this option will permit selected wireless client by MAC Address.

Wireless Client List

Wireless Client List: Click the **Wireless Client MAC List** button to display a list of wireless clients by MAC Address. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, MAC Address. If you want to add any of the wireless clients to the Wireless MAC Filter List, then click the **On the List** checkbox and then click the **Save Settings** button. Click the **Cancel Changes** button to cancel your changes. To view the most updated information, click the **Refresh** button. To exit this screen, click the **Close** button.

MIMO Wireless GN

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | **Wireless MAC Filter** | Advanced Wireless Settings | Wireless WDS Settings

Wireless MAC Filter

Enabled Disabled

Access Restriction

Prevent PCs listed below from accessing the wireless network.

Permit PCs listed below to access the wireless network.

MAC Address Filter List

Wireless Client Table

MAC 1:	<input type="text" value="00:00:00:00:00:00"/>	MAC 9:	<input type="text" value="00:00:00:00:00:00"/>
MAC 2:	<input type="text" value="00:00:00:00:00:00"/>	MAC 10:	<input type="text" value="00:00:00:00:00:00"/>
MAC 3:	<input type="text" value="00:00:00:00:00:00"/>	MAC 11:	<input type="text" value="00:00:00:00:00:00"/>
MAC 4:	<input type="text" value="00:00:00:00:00:00"/>	MAC 12:	<input type="text" value="00:00:00:00:00:00"/>
MAC 5:	<input type="text" value="00:00:00:00:00:00"/>	MAC 13:	<input type="text" value="00:00:00:00:00:00"/>
MAC 6:	<input type="text" value="00:00:00:00:00:00"/>	MAC 14:	<input type="text" value="00:00:00:00:00:00"/>
MAC 7:	<input type="text" value="00:00:00:00:00:00"/>	MAC 15:	<input type="text" value="00:00:00:00:00:00"/>
MAC 8:	<input type="text" value="00:00:00:00:00:00"/>	MAC 16:	<input type="text" value="00:00:00:00:00:00"/>

Save Settings | Cancel Changes

Help...

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.7 Wireless – Advanced Wireless Settings

This section provides Router's advanced wireless settings. These settings should be adjusted carefully. Any improper settings will affect the Router's wireless performance.

Advanced Wireless

Frame Burst Mode

Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Enabled**.

AP Isolation

This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, click **Enabled**. AP Isolation is **disabled** by default.

Authentication Type

The default is set to **Auto (Default)**, allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Basic Rate

The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate

The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto (Default)** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto (Default)**.

Transmission Power (Transmit Power Control)

The greater the transmission power used, the larger the area a wireless network covers. To minimize the likelihood of eavesdropping by unauthorized wireless users, do not use more transmission power than necessary to cover the range needed by your wireless network. Try using the Router at different levels of transmission power, and determine how much power is needed to reach the wireless client, such as a PC or access point, that is farthest from the Router. Then select the appropriate level, **Full (Default)**, **Half**, **Quarter**, **Eighth**, or **Min**, from the drop-down menu. The default is **Full (Default)**.

CTS Protection Mode

CTS (Clear-To-Send) Protection Mode should be set to **Auto (Default)**. The Router will automatically use CTS Protection Mode when your Wireless-G products are experiencing severe

problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance. If you do not want to use CTS Protection Mode at all, select **Disabled**.

Beacon Interval

The default value is **100**. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

DTIM Interval

This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold

This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold

Should you encounter inconsistent data flow, only minor reduction of the default value, **2312**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2312**.

The screenshot shows the 'Advanced Wireless' settings page in a web interface. The page has a navigation bar with tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Below the navigation bar, there are sub-tabs for Basic Wireless Settings, Wireless Security, Wireless MAC Filter, Advanced Wireless Settings, and Wireless WDS Settings. The main content area is titled 'Advanced Wireless' and contains the following settings:

- Frame Burst Mode: Enabled Disabled (Default: Enabled)
- AP Isolation: Enabled Disabled (Default: Disabled)
- Authentication Type: Auto (Default: Auto)
- Basic Rate: Default (Default: Default)
- Transmission Rate: Auto (Default: Auto)
- Transmission Power: Full (Default: Full)
- CTS Protection Mode: Disabled (Default: Auto)
- Beacon Interval: 100 (Default: 100, Milliseconds, Range: 20~1000)
- DTIM Interval: 1 (Default: 1, Range: 1 - 255)
- Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
- RTS Threshold: 2312 (Default: 2312, Range: 256 - 2346)

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'. A 'Help...' link is also visible on the right side of the page.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.8 Wireless – Wireless WDS Settings

WDS (Wireless Distribution System) is comprised of a bridging and/or a repeater mode. Wireless bridging is where the WDS APs communicate only with each other to bridge together two separate networks. Wireless repeating is where the WDS APs rebroadcasts the received signals to extend reach and range.

Advanced Wireless

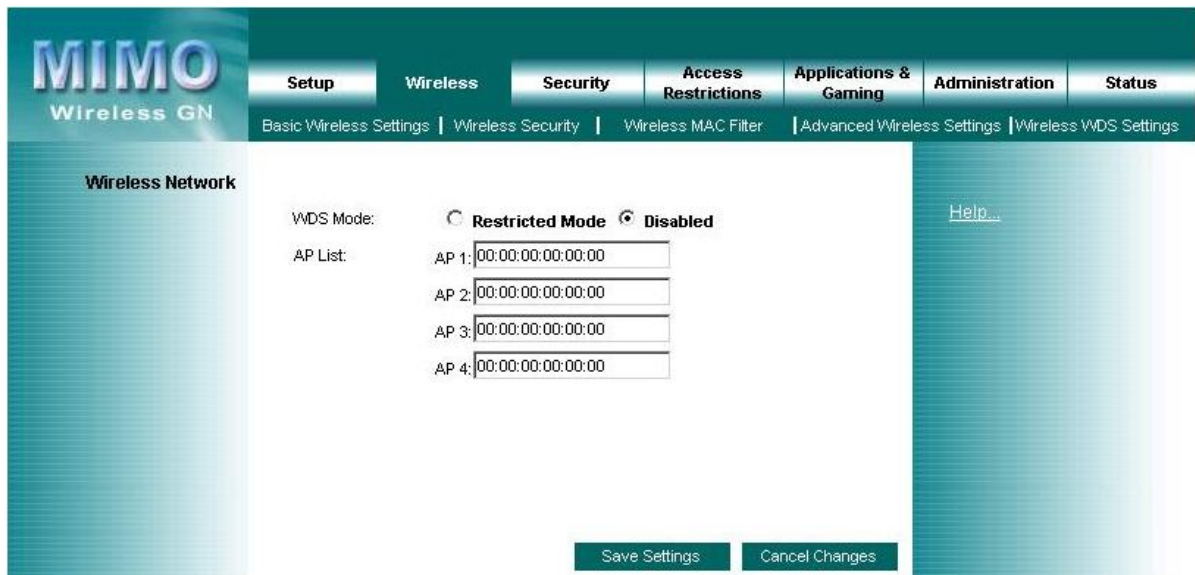
WDS Mode:

Restricted Mode - It's working as a repeater.

Disabled - WDS function disabled.

AP List:

You can type Mac address which you would like to connect.



The screenshot displays the 'Wireless WDS Settings' page in the MIMO Wireless GN web interface. The page has a teal header with navigation tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Under the 'Wireless' tab, there are sub-tabs: Basic Wireless Settings, Wireless Security, Wireless MAC Filter, Advanced Wireless Settings, and Wireless WDS Settings. The main content area is titled 'Wireless Network' and contains the following settings:

- WDS Mode:** Two radio buttons are present: 'Restricted Mode' (unselected) and 'Disabled' (selected).
- AP List:** Four text input fields labeled 'AP 1' through 'AP 4', each containing the default MAC address '00:00:00:00:00:00'.

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'. A 'Help...' link is visible on the right side of the page.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.9 Security – VPN Passthrough

VPN Passthrough

This Router provides VPN Pass through function for LAN client behind the Router to build VPN tunnels for secure the network. Use the settings on this tab to allow VPN tunnels using IPSec, L2TP, or PPTP protocols to pass through the Router's firewall.

IPSec Passthrough: Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass-Through is enabled by default. To disable IPSec Passthrough, select **Disabled**.

L2TP Passthrough: Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled**.

PPTP Passthrough: Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default. To disable PPTP Passthrough, select **Disabled**.



Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.10 Access Restrictions – Internet Access Policy

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated applications, websites, and inbound traffic during specific days and times.

Internet Access Policy

Access Policy

Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete This Policy** button. To view all the policies, click the **Summary** button.

On the *Summary* screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled) to view. To delete a policy, click its **Delete** button. Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. To return to the Internet Access Policy tab, click the **Close** button.

To create an Internet Access policy:

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. Select a number from the *Access Policy* drop-down menu.
4. Enter a Policy Name in the field provided.
5. To enable this policy, click **Enabled**.
6. Click the **Edit List** button to select which PCs will be affected by the policy. The *Internet Access PCs List* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP
7. Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.
8. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
9. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
10. You can also block access by URL address by entering it in the *Website Blocking by URL* Address field or by Keyword by entering it in the *Website Blocking by Keyword* field. Click the **>>** button to add a selection to the Blocked Applications list.
11. You can filter access to various applications accessed over the Internet, such as FTP or telnet, by selecting up to three applications from the drop-down menus under *Applications*. If the application you want to block is not listed or you want to edit an application's settings,

then create a new one by entering an Application Name, Port Range, and Protocol. Then, click **Add**.

MIMO Wireless GN

Setup Wireless Security **Access Restrictions** Applications Gaming Administration Status

Internet Access Policy

Access Policy: 1() [Help...](#)

Enter Policy Name:

Status: Enabled Disabled

(This Policy applies only to PCs on the List.)

Deny Allow
Internet access during selected days and hours.

Days: Everyday Sun Mon Tue Wed Thu Fri Sat

Times: 24 Hours 00 : 00 ~ 00 : 00

URL 1: URL 2:
URL 3: URL 4:

Keyword 1: Keyword 2:
Keyword 3: Keyword 4:

Note: Only three applications can be blocked per policy.

Applications	Blocked List
DNS [53~53]	<input type="text"/>
HTTP [80~80]	
HTTPS [443~443]	
FTP [21~21]	
POP3 [110~110]	
IMAP [143~143]	
SMTP [25~25]	
NNTP [119~119]	
SNMP [161~161]	

Application Name:
Port Range: ~
Protocol:

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.11 Application & Gaming – Port Range Forwarding

The *Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Before using forwarding, you should assign static IP addresses to the designated PCs.

Port Range Forwarding

To forward a service from local network, please fill in the relevant information on each field.

Application Name

In this field, enter the name you wish to give the application.

Start/End

This is the port range. Enter the port number or range of external ports used by the server or Internet application. Check with the software documentation of the Internet application for more information.

Protocol

Select the protocol(s) used for this application, **TCP** and/or **UDP**.

To IP Address

For each application, enter the IP address of the PC running the specific application.

Enabled

Click the **Enabled** checkbox to enable port forwarding for the relevant application.

MIMO Wireless GN

Setup | Wireless | Security | Access Restrictions | **Applications & Gaming** | Administration | Status

Port Range Forwarding | Port Range Triggering | DMZ

Port Range Forwarding

Application Name

Start ~ End Port	Protocol	To IP address	Enabled
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1.0	<input type="checkbox"/>

Help...

Save Settings | Cancel Changes

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.12 Application & Gaming – Port Range Triggering

The *Port Range Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Port Range Triggering

Application Name: Enter the application name of the trigger.

Triggered Range: For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number of the Triggered Range.

Forwarded Range: For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

Enabled: Click the **Enabled** checkbox to enable port range triggering for the relevant application.

Application Name	Triggered Range	Forwarded Range	Enabled
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/>

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.13 Application & Gaming – DMZ

The DMZ feature allows one network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function

DMZ

To expose one PC, select **Enabled**.

Internet Source IP Address: If you want to allow any Internet IP address to access the exposed computer, select **Any IP Address**. If you want to allow a specific IP address or range of IP addresses to access the exposed computer, select the second option and enter the IP address or range of IP addresses in the fields provided.

Destination Host IP Address: Enter the IP address of the computer you want to expose.

The screenshot shows the MIMO Wireless GN web interface. The navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Under the Applications & Gaming tab, there are sub-tabs for Port Range Forwarding, Port Range Triggering, and DMZ. The DMZ page is active, showing a radio button for 'Enabled' (selected) and 'Disabled'. Below, there are two options for 'Source IP Address': 'Any IP Address' (selected) and a range selection option. The 'Destination' section has two options: 'IP Address: 192.168.1.0' (selected) and 'MAC Address: 00:00:00:00:00:00'. At the bottom are 'Save Settings' and 'Cancel Changes' buttons.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.14 Administration – Management

This section allows the network's administrator to manage specific Router functions for access and security.

Router Password

Router Password and Re-enter to Confirm: You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to Confirm field to confirm.

Remote Router Access

Remote Management: To access the Router remotely, from outside of local network, select **Enabled**.

Otherwise, keeps the default setting, **Disabled**.

Remote Upgrade: If you want to be able to upgrade the Router remotely, from outside of local network, select **Enabled**. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default setting, **Disabled**.

Allow Remote IP Address: If you want to be able to access the Router from outside with any external IP address, select **Any IP Address**. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

Remote Management Port: Enter the port number that will be open to outside access.

UPnP

Universal Plug and Play (UPnP) is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

UPnP: If you want to use UPnP, keep the default setting, **Enabled**. Otherwise, select **Disabled**.

Backup and Restore

Backup Settings: To back up the Router's configuration, click this button and follow the on-screen instructions.

Restore Settings: To restore the Router's configuration, click this button and follow the on-screen instructions.

(You must have previously backed up the Router's configuration.)

MIMO
Wireless GN

Setup | **Wireless** | **Security** | **Access Restrictions** | **Applications & Gaming** | **Administration** | **Status**

Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade

Management

Router Access: Router Password: [*****]
Re-enter to confirm: [*****]

Remote Access: Remote Management: Enabled Disabled
Allow Remote IP Address: Any IP Address
 [0] [0] [0] [0] ~ [0]

UPnP: Enabled Disabled

Backup and Restore: [Backup Configurations] [Restore Configurations]

[Save Settings] [Cancel Changes]

[Help...](#)

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.15 Administration – Log

The Router can keep logs of all traffic for your Internet connection. This feature is disabled by default. To keep activity logs, select **Enable**.

Log

To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**.

Logviewer IP Address: For a permanent record of the Router's activity logs, Logviewer software must be used.

The Log viewer saves all incoming and outgoing activity in a permanent file on your PC's hard drive. In the Logviewer IP Address field, enter the fixed IP address of the PC running the Log viewer software. The Router will now send updated logs to that PC.

View Log: When you wish to view the logs, click **View Log**. A new screen will appear. Select **Incoming Log** or **Outgoing Log** from the Type drop-down menu. The Incoming Log will display a temporary log of the Source IP Addresses and Destination Port Numbers for the incoming Internet traffic. Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed. The Outgoing Log will display a temporary log of the LAN IP Addresses, Destination URLs or IP Addresses, and Service or Port Numbers for the outgoing Internet traffic. Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.

MIMO Wireless GN

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade

Log

Enabled Disabled

Logviewer IP Address: 192 . 168 . 1 . 0

View Log

Save Settings | Cancel Changes

Help...

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes**. For additional information, click **Help**.

4.16 Administration – Diagnostics

The diagnostics function provides two ways to check Router's status of Internet connection.

Diagnostics

Ping Test

This utility verifies configurations and tests IP connectivity between two computers. Ping sends an ICMP request from the source computer, and the destination computer responds with an ICMP reply.

To IP or URL Address: Enter the IP address or URL that you want to ping.

Packet Size: Enter the size of the packet you want to use.

Times to Ping: Select the number of times you wish to ping: **5, 10, 15, or Unlimited.**

Start to Ping: Click this button to begin the test. A new screen will appear and display the test results. Click the **Close** button to return to the *Diagnostics* screen.

Traceroute Test

Traceroute function provides a trace for the route that a packet takes to destination.

To IP or URL Address: Enter the destination IP address or URL that you want to trace the routes.

Start to Tracerouter: Click this button to begin the Tracerouter. A new screen will appear and display the trace results. Click the **Close** button to return to the *Diagnostics* screen.

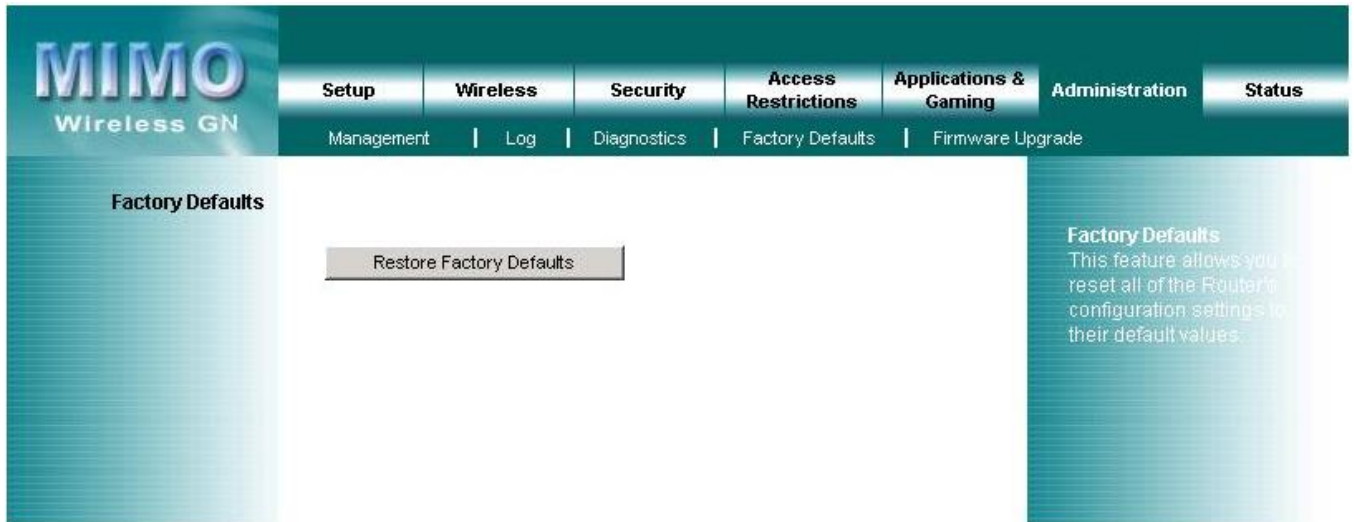
The screenshot shows the MIMO Wireless GN router's web interface. At the top, there is a navigation bar with the following tabs: Setup (Management), Wireless (Log), Security (Diagnostics), Access Restrictions (Factory Defaults), Applications & Gaming (Firmware Upgrade), Administration, and Status. The 'Diagnostics' tab is selected. Below the navigation bar, the 'Diagnostics' section is displayed. It contains two main sections: 'Ping Test' and 'Traceroute Test'. The 'Ping Test' section has three input fields: 'IP or URL Address:' (empty), 'Packet Size:' (64 bytes (32~65500)), and 'Times to Ping:' (5). Below these fields is a 'Start to Ping' button. The 'Traceroute Test' section has one input field: 'IP or URL Address:' (empty), with a 'Start to Traceroute' button below it. On the right side of the page, there is a 'Help...' link.

4.17 Administration – Factory Defaults

This Factory Defaults allows you to restore the Router's configuration to its factory default settings.

Factory Defaults

Restore Factory Defaults: Click this button to reset all configuration settings to their default values. Any settings you have saved will be lost when the default settings are restored.



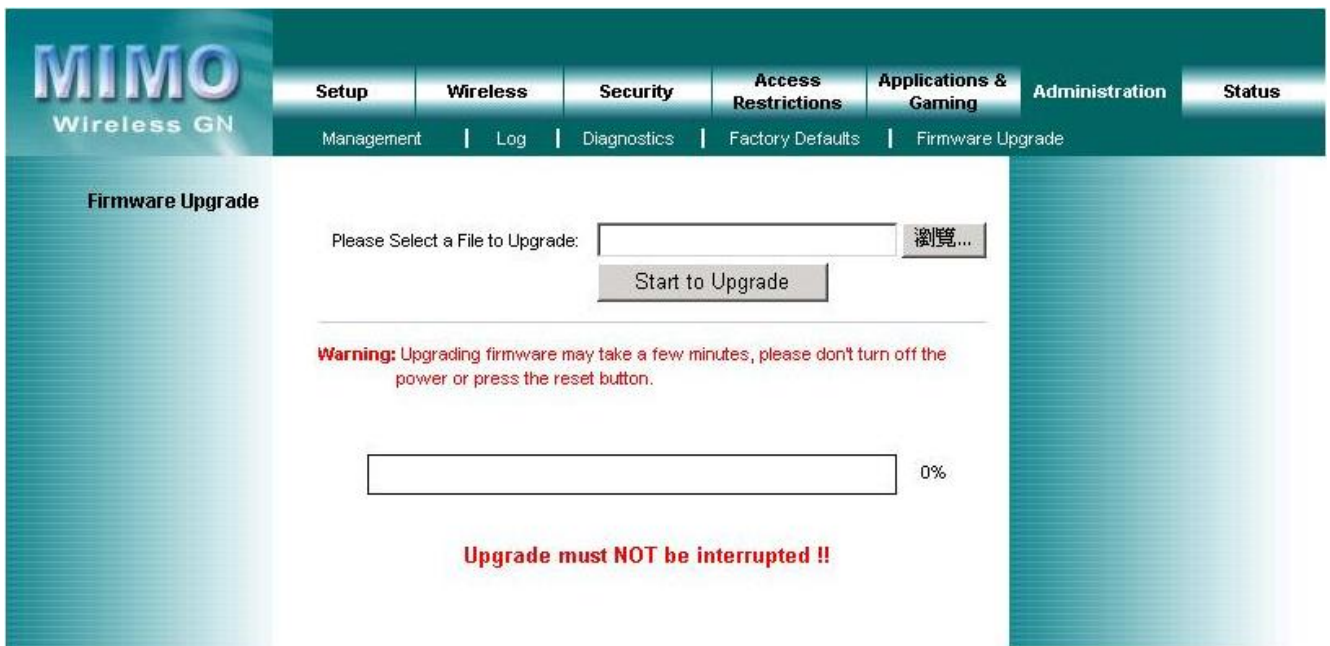
4.18 Administration – Firmware Upgrade

This Firmware Upgrade screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.

Firmware Upgrade

Please select a file to upgrade: In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Start to Upgrade: After you have selected the appropriate file, click this button for upgrade.



The screenshot shows the MIMO Wireless GN web interface for the Firmware Upgrade section. The navigation menu includes Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The Firmware Upgrade page contains a file selection field with a '瀏覽...' (Browse) button and a 'Start to Upgrade' button. A warning message states: 'Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.' Below this is a progress bar showing 0% completion. A red warning message at the bottom reads: 'Upgrade must NOT be interrupted !!'

Note: Please do not shut down the Router or PC while it is upgrading.

4.19 Status – Router

The Router screen on the Status Tab displays information about the Router and its current settings. The Internet Connection information will vary depending on the Internet Connection Type you use.

Router Information

Firmware Version: This is the Router's current firmware.

Current Time: This shows the time by the time zone you selected on the Setup Tab.

Internet MAC Address: This is the Router's MAC Address.

Host Name: If required by your ISP, it would be entered on the Setup Tab.

Domain Name: If required by your ISP, it would be entered on the Setup Tab.

Internet Connection

Connection Type: This indicates the current Internet connection type you are using.

Login Status:

The status of the connection is displayed only for a PPPoE connection. For this dial-up style connection, click the **Connect** button to click if there is no connection and you want to establish an Internet connection. When your PPPoE connection is active, you can click the **Disconnect** button to end the connection.

Internet IP Address: The Router's Internet IP Address.

Subnet Mask and Default Gateway: The Router's Subnet Mask and Default Gateway address are displayed here.

DNS1-3: The DNS (Domain Name System) IP addresses currently is used by the Router. The Router at least one DNS IP should be used for domain name resolution.

MTU: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select **Manual** if you want to manually enter the largest packet size that will be transmitted. The recommended size, entered in the *Size* field, is 1500. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, please select the default setting--**Auto**.

IP Release:

Available for a DHCP connection, click this button to release the current IP address of the device connected to the Routers Internet port.

IP Renew:

Available for a DHCP connection, click this button to replace the current IP address of the device connected to the Routers Internet port with a new IP address.

Click the **Refresh** button to update the on-screen information.

Router Information

Firmware Version: **1.0.24**
Current Time: **Thu Jan 1 03:38:21 1970 (GMT -12:00)**
Internet MAC Address: **00:16:01:A1:80:60**
Host Name:
Domain Name:

[Help...](#)

Internet Connections

Connection Type: **Automatic Configuration - DHCP**
Internet IP Address: **0.0.0.0**
Subnet Mask: **0.0.0.0**
Default Gateway: **0.0.0.0**
DNS 1: **0.0.0.0**
DNS 2: **0.0.0.0**
DNS 3: **0.0.0.0**
MTU: **Auto**

IP Address Release

IP Address Renew

Refresh

For additional information, click **Help**.

4.20 Status – Local Network

The Local Network screen on the Status Tab displays the status of your network.

Local Network

Local MAC Address: This is the Router's local MAC Address.

Router IP Address: This is the Router's local IP Address.

Subnet Mask: This is the Router's local subnet mask.

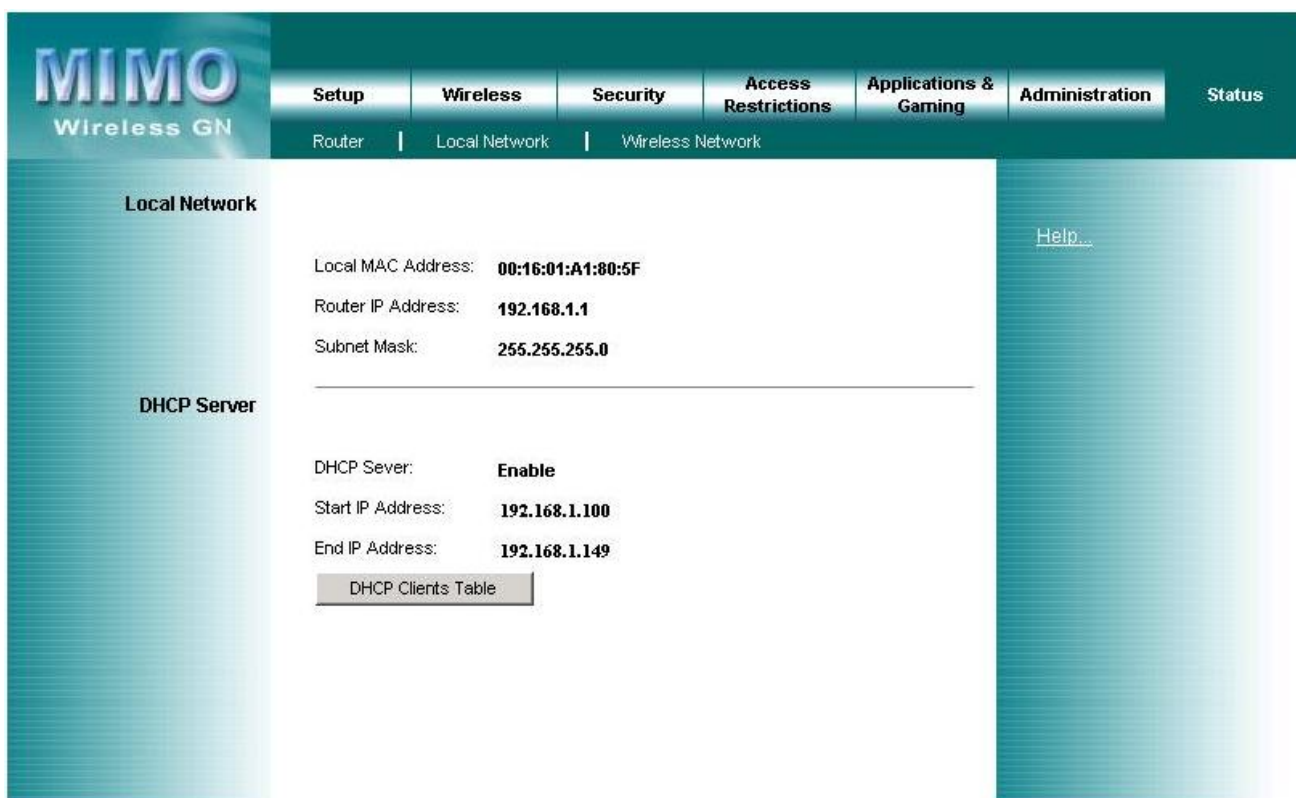
DHCP Server

DHCP Server: The Router's embedded DHCP server status.

Start IP Address: This is beginning range of assigned IP by Router's DHCP server.

End IP Address: This is end range of assigned IP by Router's DHCP server.

DHCP Client Table: Clicking this button will open a screen to show which hosts are using the Router as a DHCP server. On the DHCP Client Table screen, you will see a list of DHCP clients with the following information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the assigned IP addresses expired time. From the To Sort by drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. To remove a DHCP client from this list, click its **Delete** button. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.



The screenshot shows the MIMO Wireless GN web interface. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The 'Status' tab is active, and the 'Local Network' sub-tab is selected. The main content area is divided into two sections: 'Local Network' and 'DHCP Server'. The 'Local Network' section displays the following information: Local MAC Address: 00:16:01:A1:80:5F, Router IP Address: 192.168.1.1, and Subnet Mask: 255.255.255.0. The 'DHCP Server' section displays: DHCP Server: Enable, Start IP Address: 192.168.1.100, and End IP Address: 192.168.1.149. A button labeled 'DHCP Clients Table' is located below the DHCP Server information. A 'Help...' link is visible on the right side of the page.

For additional information, click **Help**.

4.21 Status – Wireless Network

The Wireless Network screen on the Status Tab displays the information of your Wireless networks.

Wireless Network

MAC Address: This is the Router's Wireless-G band MAC Address.

Mode: This displays the Wireless-G band network mode.

Network Name (SSID): The Wireless-G band network name.

Channel: The current G band channel you are using.

Security: This displays what type of encryption you are using.

SSID Broadcast: This displays the Router's SSID Broadcast status.



The screenshot shows the MIMO Wireless GN router's status page. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The 'Wireless' tab is selected, and the 'Wireless Network' sub-tab is active. The main content area displays the following configuration details:

MAC Address:	00:16:01:A1:80:5F
Mode:	Wireless-N Only
Network Name (SSID):	spur
Channel:	6
Security:	Disable
SSID Broadcast:	Enable

A [Help...](#) link is visible on the right side of the page.

For additional information, click **Help**.

5. Troubleshooting – Q & A

1. I'm trying to log on the Router's Web configuration page, but I do not see the login screen.

Answer:

1. Please make sure the IP address that you input on address field of IE browser is correct.
2. Make sure the physical layer connection is established. If you are using wired to connect this Router, check the relevant LAN LED whether it is lit or not.
3. On Dos Prompt screen, using " ping " command to probe this Router, check if you got reply from it.
Command: ping < Destination IP address >
4. If you have any TCP/IP setting problem, please refer to the Quick Installation Guide.

2. I need to set up a server behind my Router and make it available to the public.

Answer:

This is Router's forwarding function. Please refer to the section 4.11. Generally, using a server like a web, ftp, or mail server, you need to know what kinds of the respective port numbers they are using.

For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming).

Below is an example for how to set up a FTP server behind Router for public network access.

1. Log on the Router's web configuration page, <http://192.168.1.1> or the IP address that you have changed.
2. Select the Applications & Gaming => Port Range Forwarding tab.
3. Enter any name you want to use like "FTP service".
4. Enter the External Port range of the FTP service you are using. For example, your FTP service port range should be port 20 ~ 21.
5. Select the protocol, TCP and UDP.
6. Enter the IP address of the FTP server that locate on your local network. For example, if your FTP server's IP address is 192.168.1.10, then you should enter 10 in the address field.
7. Click the **Enabled** checkbox to enable this service then click the **Save Settings** button to apply your changes

3. I forgot my password, how to log on this Router for configuration?

Answer:

1. Reset the Router to factory default by pressing the Reset button for 10 seconds then releasing it.
2. Log on the Router's web management by <http://192.168.1.1>
Leave username blank and enter the default password **admin**.

4. How to set the Router to factory default setting.

Answer:

1. Reset the Router to factory default by pressing the Reset button for 10 seconds then releasing it.
2. After release the Reset button, the Router will get back all setting to factory default and reboot system.

3. While the reboot is complete, log on the Router's web management by default IP `http://192.168.1.1`
Leave username blank and enter the default password **admin**.

5. My SOHO AP will not turn on. No LED's light up.

Answer:

Usually it is caused by the power is not connected.
Please double check the power adapter if it connected to your Router and the other side is plugged into the power outlet. If it still has no power, please contact your reseller.

6. I can't access the AP from a wireless client.

Answer:

Generally to make the wireless client unable to access AP with following possible issues:

1. Settings are not the same among each wireless adapter.
2. Out of range.
3. IP Address is not set correctly.

Resolution:

Make sure that the mode, SSID, Channel and encryption settings are set the same on each wireless adapter. Make sure that your computer is within range and free from any strong electrical devices that may cause interference.

7. What devices cause interference?

Answer:

The Router is operating in the unlicensed 2.4 GHz band. Other devices operates in this frequency range that may cause interference include microwave ovens and 2.4 GHz portable phones. PCs or analog cellular phones do not operate at 2.4 GHz and do not cause interference. Proper placement of access points usually eliminates interference problems created by other 2.4 GHz devices.