MSI RG54SE

Wireless 11g Broadband Router

User Manual

Hiermit erklärt *Micro Star International CO., LTD* dass sich dieses Produkt in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet.
Die Konformitätserklärung kann auf folgender website eingesehen werden:
http://www.msi-technology.de/support/dl_man.php?Prod_Typ=9

Hereby, *Micro Star International CO., LTD* declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
The respective Declaration of conformity can be found online:
http://www.msi-technology.de/support/dl_man.php?Prod_Typ=9

IEEE 802.11b/g 2.4 GHz operation
Europe: Frequencies: 2.400 – 2.4835 GHz

France: Frequencies: 2.4465– 2.4835 GHz, channels 10, 11, 12, 13
BANDE DE FREQUENCES DES 2.4GHZ
La décision N° 02-1008 en date du 31 octobre 2002 autorise l'utilisation d'une partie de la bande de fréquences 2400-2483,5 MHz pour les réseaux locaux radioélectriques (RLAN) comme suit :
L'utilisation de la bande 2400-2446,5 MHz est autorisée à l'intérieur des bâtiments avec une puissance isotrope rayonnée équivalente (PIRE) limitée à 10 mW et que l'utilisation de la bande 2446,5-2483,5 MHz est autorisée à l'intérieur des bâtiments avec une PIRE limitée à 100 mW. L'utilisation en extérieur est soumise à demande d'autorisation sur la bande de fréquences de 2446,5-2483,5 MHz avec une puissance limitée à 100mW.

Notified Countries:
Germany, UK, Netherlands, Belgium, Norway, Sweden, Denmark, Finland, France, Italy, Spain, Austria, Iceland, Ireland, Portugal, Greece, Luxemburg and Switzerland

Bestimmungsgemäße Verwendung:
Dieses Produkt integriert als Teil der Produktausstattung eine WLAN-Komponente.
Die WLAN-Komponente verbindet Computer über eine Funkverbindung . Es kann auch eine Funkverbindung zu anderen geeigneten WLAN-Geräten hergestellt werden.

Prescribed use:
This product integrates a WLAN-device.
The WLAN-device sets up a radio link between to computer. In addition it is possible to link the WLAN device to any other WLAN device which stick to the IEEE 802.11b/g requirements.

Hinweise zur Reichweite:
Der Abstand zwischen Sender und Empfänger (von einem WLAN-Gerät zu einem anderen WLAN-Gerät) hängt stark von der Einsatzumgebung ab. Wände, Betonboden (Eisen), beschichtete Fensterscheiben, Fahrzeug-Karosserie, etc..
Weitere Beeinflussungen:
- Hochfrequenzaussendungen jeder Art
- Gebäude, Bäume, etc.
- Heizkörper, Stahlbeton, etc.
- offen betriebene Computer, etc.
- Mikrowellenherde, etc,

Die Kommunikation zwischen unterschiedlichen WLAN-Geräten ist von der jeweiligen Software und dem entsprechenden Versionsstand abhängig

Operating range:
The transmission range between different WLAN devices varies depending the specific environment. Walls, concrete floor (iron), laminated windows, vehicle-body, etc..
More electromagnetic interferences:
- high frequency emission of any kind,
- Buildings, trees, etc.
- Heaters, ferroconcrete, etc.
- open computer systems, etc.
- Microwave oven, etc,

Communication (exchange data) is dependent on the software of the WLAN devices.

FCC Caution

1. The 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.

2. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
3. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
4. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

Copyright Notice

Trademarks

Important Safety Precautions

Always read and follow these basic safety precautions carefully when handling any piece of electronic component.

1. Keep this User Manual for future reference.
2. Keep this equipment away from humidity.
3. Lay this equipment on a reliable flat surface before setting it up.
4. The openings on the enclosure are for air convection hence protects the equipment from overheating.
5. All cautions and warnings on the equipment should be noted.
6. Never pour any liquid into the opening that could damage or cause electrical shock.
7. If any of the following situations arises, get the equipment checked by a service personnel:
   - Liquid has penetrated into the equipment
   - The equipment has been exposed to moisture
   - The equipment has not work well or you can not get it work according to User Manual
   - The equipment has dropped and damaged
   - If the equipment has obvious sign of breakage
8. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT UNCONDITIONED, STORAGE TEMPERATURE ABOVE 60°C OR BELOW -20°C, IT MAY DAMAGE THE EQUIPMENT.

Table of Contents

Revision History

DATE	REVISION OF USER'S MANUAL	FIRMWARE
2005/12/30	First release (Version 1.0)	V1.2.7.G

Terminology

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
CCK	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SNR	Signal to Noise Ratio
SSID	Service Set Identification
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play
VPN	Virtual Private Network
WDS	Wireless Distribution System

WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Introduction

The Wireless 11g Broadband Router is an affordable IEEE 802.11b/g wireless LAN broadband router solution; setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN.

This document describes the steps required for the initial IP address assign and other WLAN router configuration. The description includes the implementation of the above steps.

1.1 Package contents

The package of the Wireless 11g Broadband Router includes the following items,

- ✓ The Wireless 11g Broadband Router
- ✓ The AC to DC power adapter
- ✓ The Documentation CD
- ✓ 1.8M RJ-45 Cable Line

1.2 Product Specifications

Product Name	RG54SE Wireless 11g Broadband Router
Standard	802.11b/g(Wireless), 802.3(10BaseT), 802.3u(100BaseT)
Data Transfer Rate	54Mbps(Wireless), 100Mbps(Ethernet)
Modulation Method	CCK(802.11b), OFDM(802.11g)
Frequency Band	2.4GHz – 2.497GJz ISM Band, DSSS
RF Output Power	CCK< 17 dBm, OFDM< 13.5 dBm
Receiver Sensitivity	802.11b -80 dBm@8%, 802.11g -68 dBm@5%
Operation Range	30 to 280 meters (depend on surrounding)
Antenna	SMA Detachable Antenna
LED	Power, Active (WLAN), Act/Link (Ethernet)
Security	64 bit/ 128 bit WEP, WPA, WPA2, port filtering, IP filtering, MAC filtering, port forwarding and DMZ hosting
LAN interface	One 10/100BaseT with RJ45 connector (WAN) Four 10/100BaseT with RJ45 connectors (LAN)
Power Consumption	7.5V DC Power Adapter
Operating Temperature	0 ~ 50^{o}C ambient temperature
Storage Temperature	-20 ~ 70^{o}C ambient temperature
Humidity	5 to 90 % maximum (non-condensing)
Dimension	137 x 96 x 35 mm

1.3 Product Features

- Complies with IEEE 802.11b/g standard for 2.4GHz Wireless LAN.
- Supports 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption function to protect the wireless data transmission.
- Supports IEEE 802.1x Authentication.
- Support Wi-Fi Protected Access Authentication with Radius and Pre-Shared Key mode.
- Supports Inter-Access Point Protocol (IAPP).
- Supports Wireless Distribution System (WDS).
- Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports DHCP client for Ethernet WAN interface auto IP address assignment.
- Supports PPPoE on Ethernet WAN interface.
- Supports clone MAC address function.
- Supports firewall security with port filtering, IP filtering, MAC filtering, port forwarding, trigger port and DMZ hosting functions.
- Supports WEB based management and configuration.
- Supports PPTP Client on Ethernet WAN interface.
- Supports UPNP for automatic Internet access.
- Supports Dynamic DNS service.
- Supports NTP client service.
- Supports Log table and remote Log service.
- Support Setup Wizard mode.

1.4 Front Panel Description

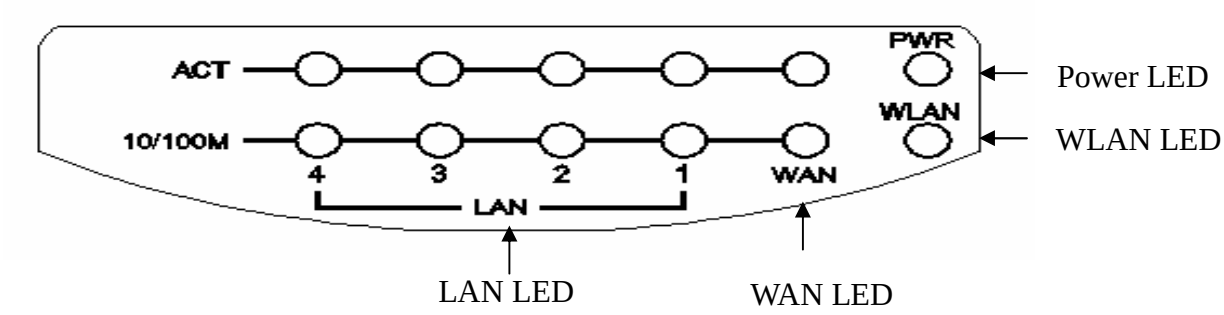


Figure 1 –Wireless Broadband Router Front Panel

LED Indicator	State	Description
1. Power LED	On	The Wireless Broadband Router is powered on.
	Off	The Wireless Broadband Router is powered off.
2. WLAN LED	Flashing	Data is transmitting or receiving on the antenna.
	Off	No data is transmitting or receiving on the antenna.
3. WAN LED ACT	Flashing	Data is transmitting or receiving on the WAN interface.
	Off	No data is transmitting or receiving on the WAN interface.
10/100M	On	Connection speed is 100Mbps on WAN interface.
	Off	Connection speed is 10Mbps on WAN interface.
4. LAN LED ACT	Flashing	Data is transmitting or receiving on the LAN interface.
	Off	No data is transmitting or receiving on the LAN interface.
10/100M	On	Connection speed is 100Mbps on LAN interface.
	Off	Connection speed is 10Mbps on LAN interface.

1.5 Rear Panel Description

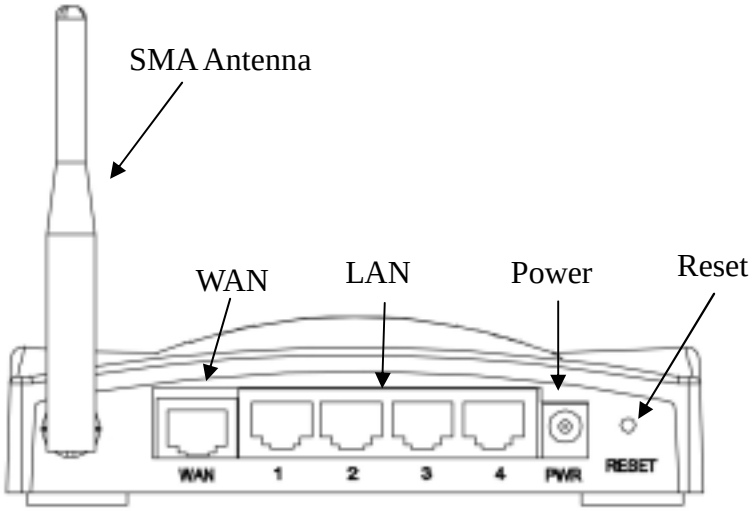


Figure 2 – Wireless Broadband Router Rear Panel (SMA Antenna)

Interfaces	Description
1. Antenna	The Wireless LAN Antenna.(Figure 2)
2. Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.
3. WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
4. LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
5. Power	The power jack allows an external DC +7.5 V power supply connection. The external AC to DC adaptor provide adaptive power requirement to the Wireless Broadband Router.

2 Installation

2.1 Hardware Installation

Step 1: Place the Wireless Broadband Router to the best optimum transmission location. The best transmission location for your Wireless Broadband Router is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.

Step 2: Connect the Wireless Broadband Router to your wired network. Connect the Ethernet WAN interface of Wireless Broadband Router by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.

Step 3: Supply DC power to the Wireless Broadband Router. Use only the AC/DC power adapter supplied with the Wireless Broadband Router; it may occur damage by using a different type of power adapter.

The hardware installation finished.

2.2 Software Installation

- There are no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 3 for software configuration.

Notice: It will take about 50 seconds to complete the boot up sequence after powered on the Wireless Broadband Router; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.

3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The Wireless Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address**: *192.168.1.254***
Default IP subnet mask**: *255.255.255.0***
WEB login User Name**: *admin***
WEB login Password**: *admin***

3.1 Prepare your PC to configure the Wireless Broadband Router

For OS of Microsoft Windows 95/ 98/ Me:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
   Note: Windows Me users may not see the Network control panel. If so, *select* **View all Control Panel options** on the left side of the window
2. Move mouse and double-click the right button on ***Network*** icon. The ***Network*** window will appear.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK and reboot your PC after completes the IP parameters setting.

For OS of Microsoft Windows 2000, XP:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control***

Panel window will appear.

2. Move mouse and double-click the right button on ***Network and Dial-up Connections*** icon. Move mouse and double-click the ***Local Area Connection*** icon. The ***Local Area Connection*** window will appear. Click ***Properties*** button in the ***Local Area Connection*** window.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to completes the IP parameters setting.

For OS of Microsoft Windows NT:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network*** icon. The ***Network*** window will appear. Click ***Protocol*** tab from the ***Network*** window.
3. Check the installed list of ***Network Protocol*** window. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to complete the IP parameters setting.

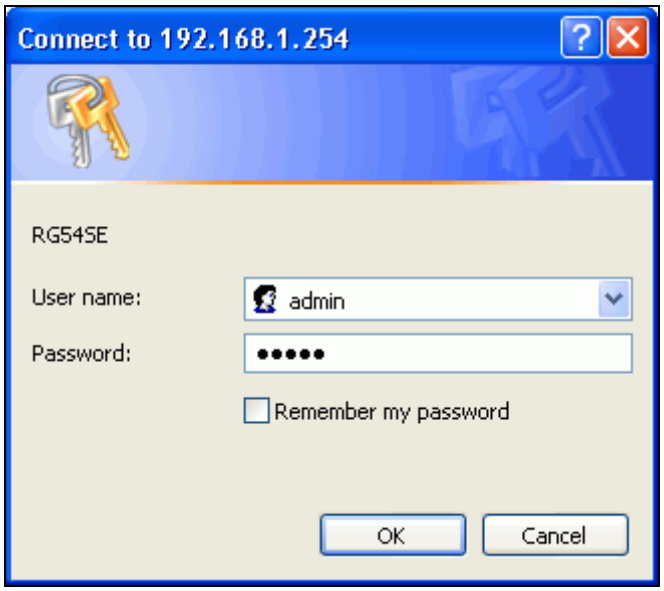
3.2 Connect to the Wireless Broadband Router

Open a WEB browser, i.e. Microsoft Internet Explorer, enter 192.168.1.254 on the URL to connect the Wireless Broadband Router.

3.3 Management and configuration on the Welcome Page

3.3.1 Login

User input **User name/Password** to login web configuration page.

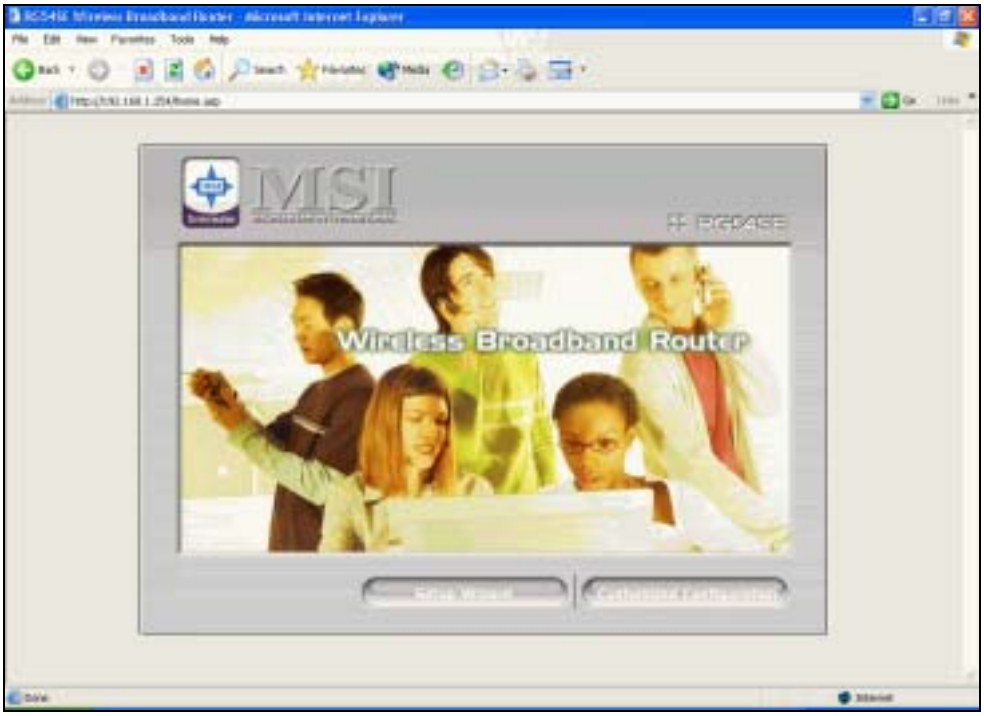


Screen snapshot – Login

Item	Description
User name	admin
Password	admin

3.3.2 Welcome Page

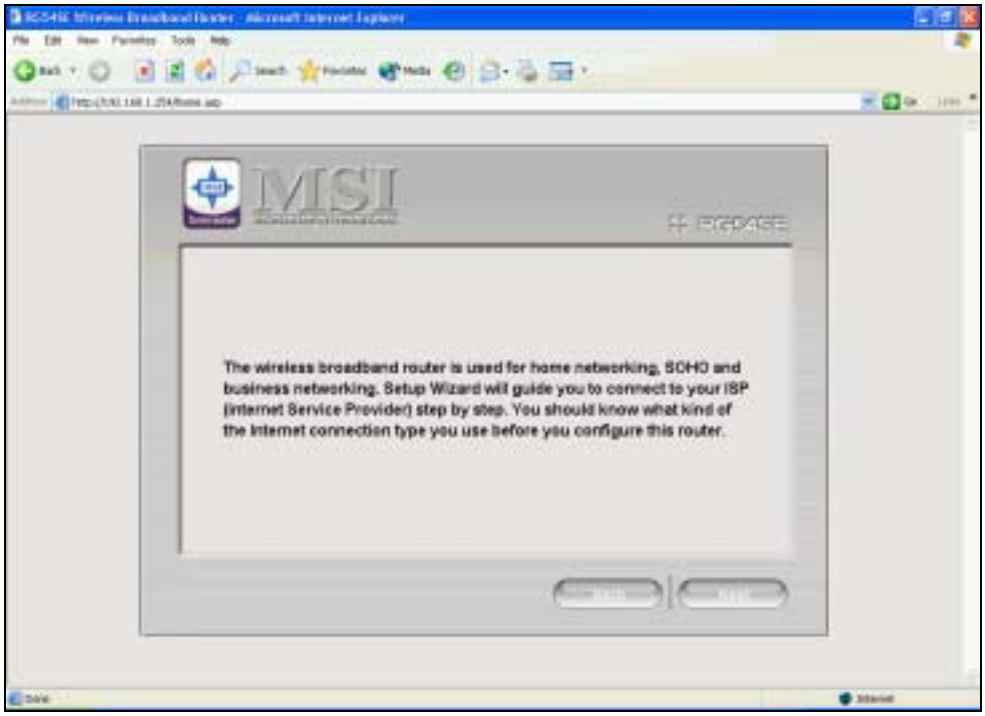
This page guides you to configure wireless broadband router via **Setup Wizard** or **Customized Configuration**.



Screen snapshot – Welcome

3.3.3 Setup Wizard

3.3.3.1 Descriptions



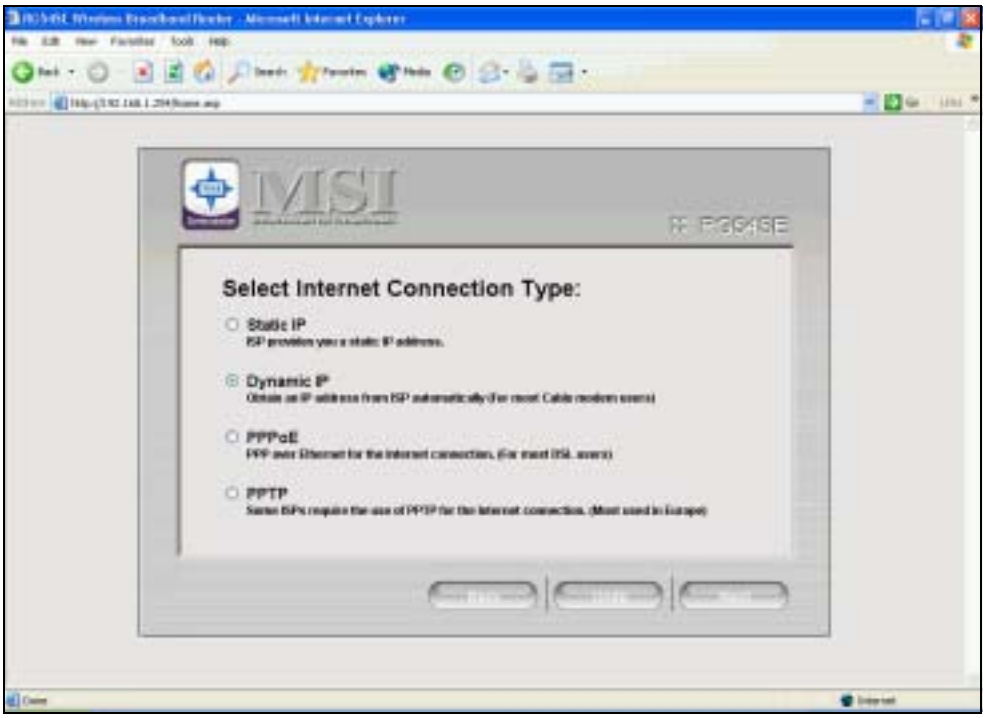
Screen snapshot – Descriptions of Setup Wizard

Item	Description

Next	Go to next step.
Back	Back to previous step.

3.3.3.2 Internet Connection

This page is to choose internet connection of you ISP provided.

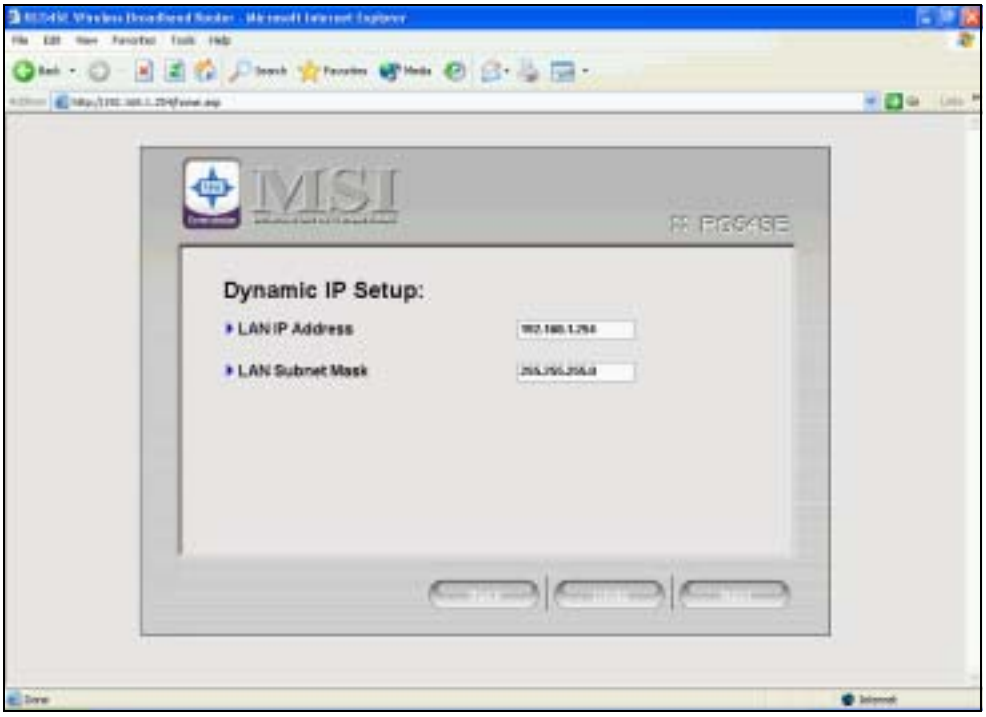


Screen snapshot – Internet Connection

Item	Description
Internet Connection	There are Static IP, Dynamic IP, PPPoE and PPTP connections
Next	Go to next step.
Undo	Select previous setting.
Back	Back to previous step.

3.3.3.3 Dynamic IP Setup

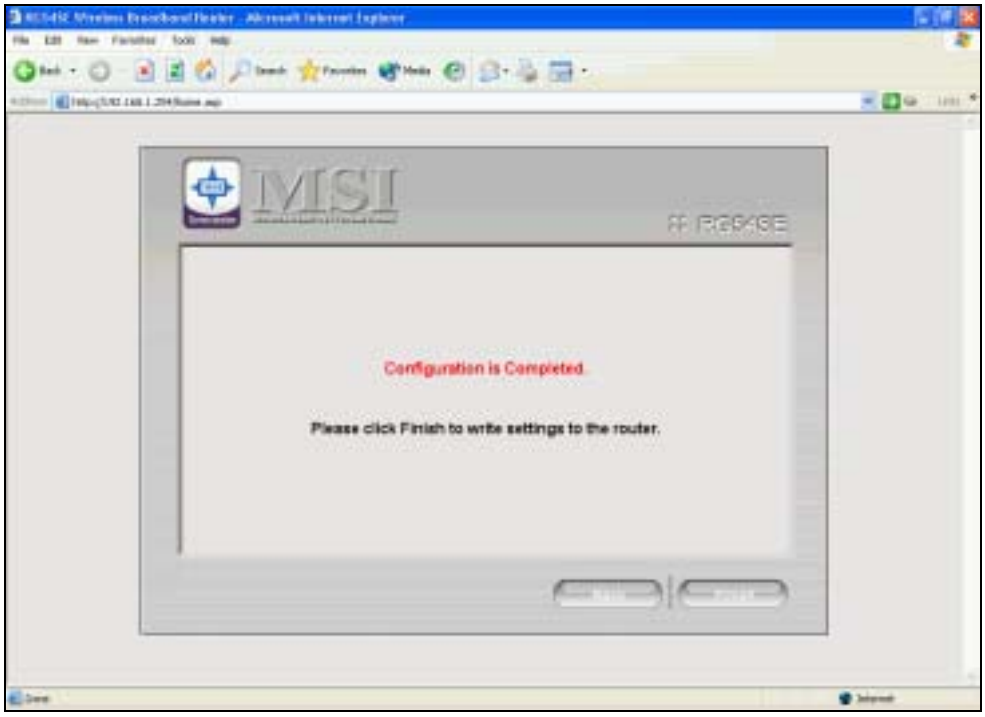
Step1 - This page is used to change WAN/LAN/DNS configuration.



Screen snapshot – Dynamic IP Setup

Item	Description
LAN IP Address	Default is 192.168.1.254. User can change it.
LAN Subnet Mask	Default is 255.255.255.0. User can change it.
Next	Go to next step.
Undo	Select previous setting.
Back	Back to previous step.

Step2 - This page is to finish Dynamic IP setup wizard and wait for settings successful message.

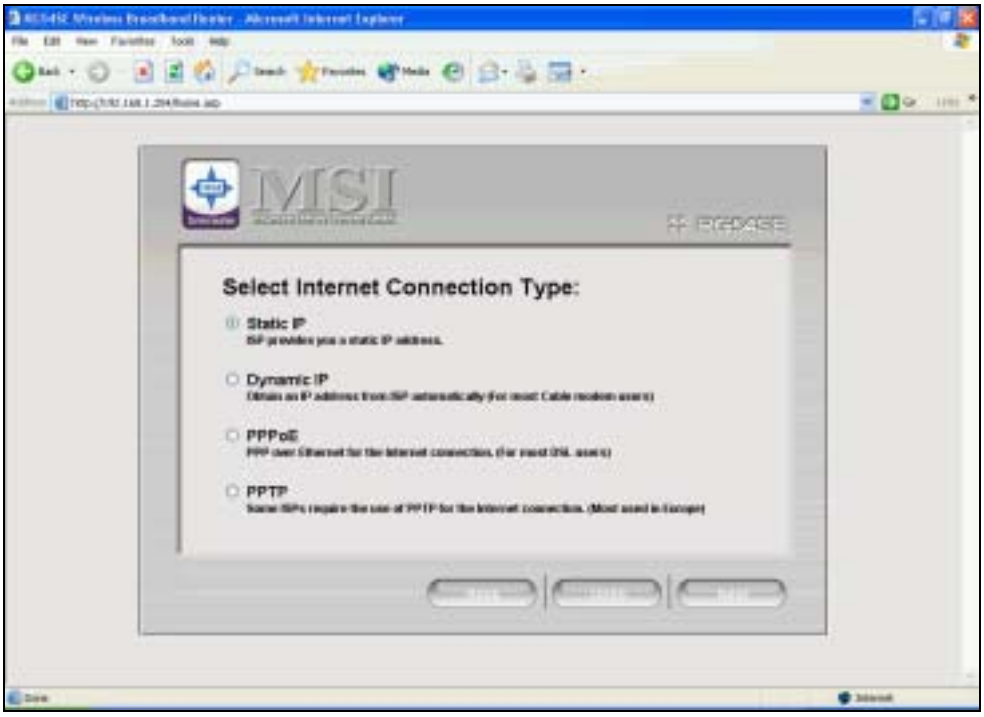


Screen snapshot – Finish Dynamic IP setup

Item	Description
Finish	Go to next step.
Back	Back to previous step.

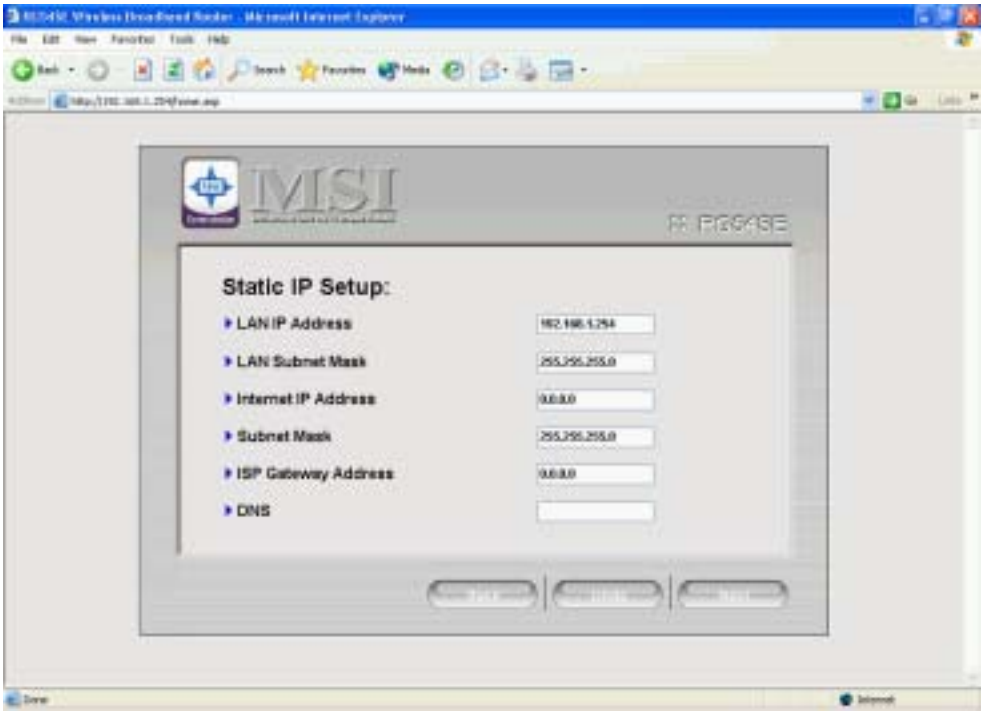
3.3.3.4 Static IP Setup

Step1- This page is used to choose which type connection type you applied.



Screen snapshot – Choose Static IP Connection

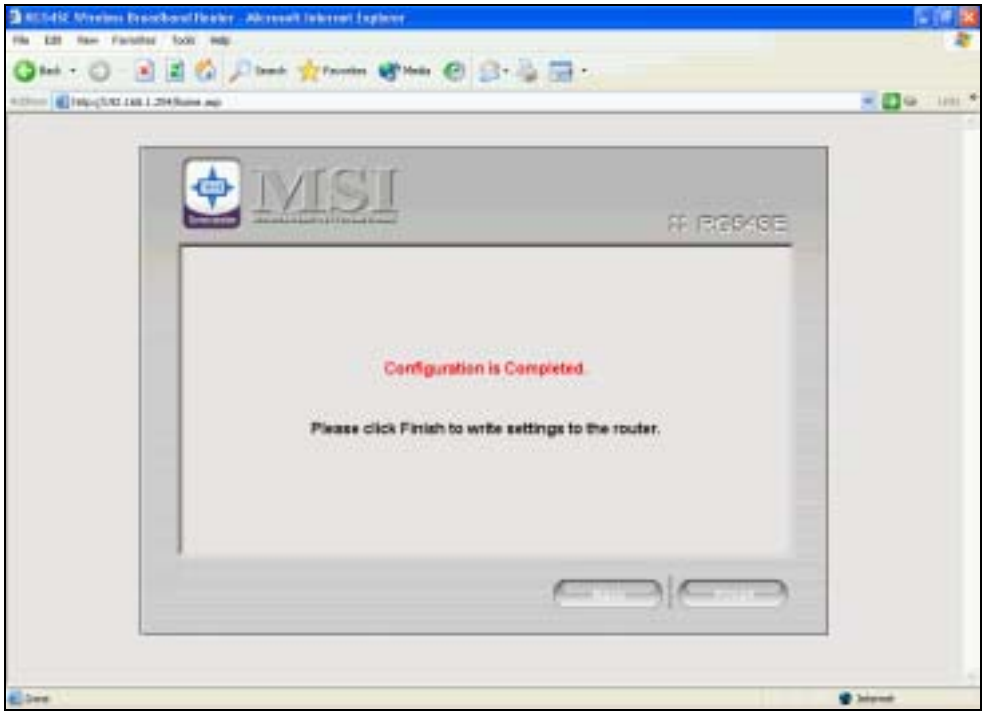
Step2 - This page is used to change WAN/LAN/DNS configuration.



Screen snapshot – Static IP Setup

Item	Description
LAN IP Address	Default is 192.168.1.254. User can change it.
LAN Subnet Mask	Default is 255.255.255.0. User can change it.
Internet IP Address	User input the IP address that ISP provided.
Subnet Mask	User input the subnet mask that ISP provided.
ISP Gateway Address	User input the gateway that ISP provided.
DNS	User input DNS info that ISP provided.
Next	Go to next step.
Undo	Select previous setting.
Back	Back to previous step.

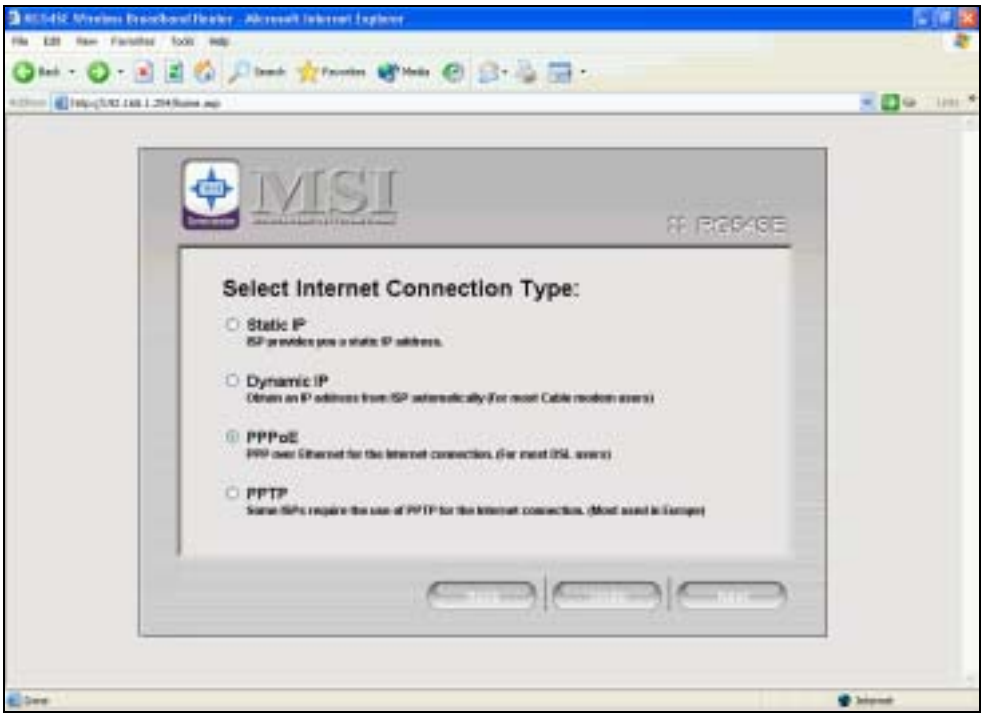
Step3 - This page is to finish Static IP setup wizard and wait for settings successful message.



Screen snapshot – Finish Static IP setup

3.3.3.5 PPPoE Setup

Step1- This page is used to choose which type connection type you applied.



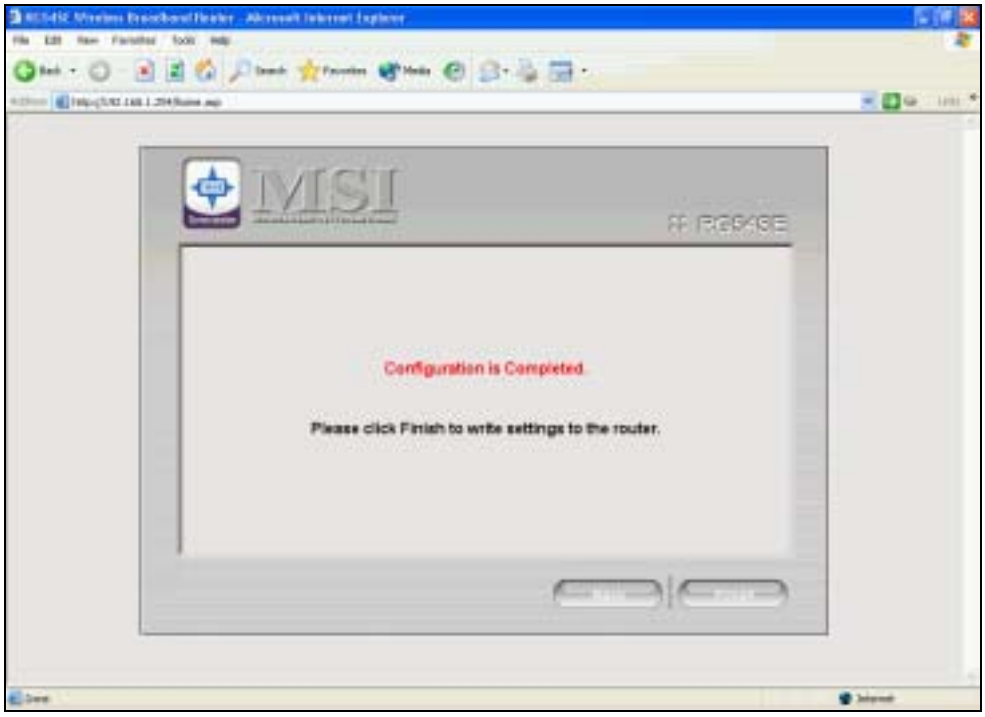
Screen snapshot – Choose PPPoE Connection

Step2 - This page is used to change WAN/LAN/DNS configuration.

Screen snapshot – PPPoE Setup

Item	Description
LAN IP Address	Default is 192.168.1.254. User can change it.
LAN Subnet Mask	Default is 255.255.255.0. User can change it.
User Name	User input the user name that ISP provided.
Password	User input the password ISP provided.
DNS Mode	User chooses DNS mode that ISP provided.
	■ Auto
	■ Manual – Input the DNS server IP address.
Next	Go to next step.
Undo	Select previous setting.
Back	Back to previous step.

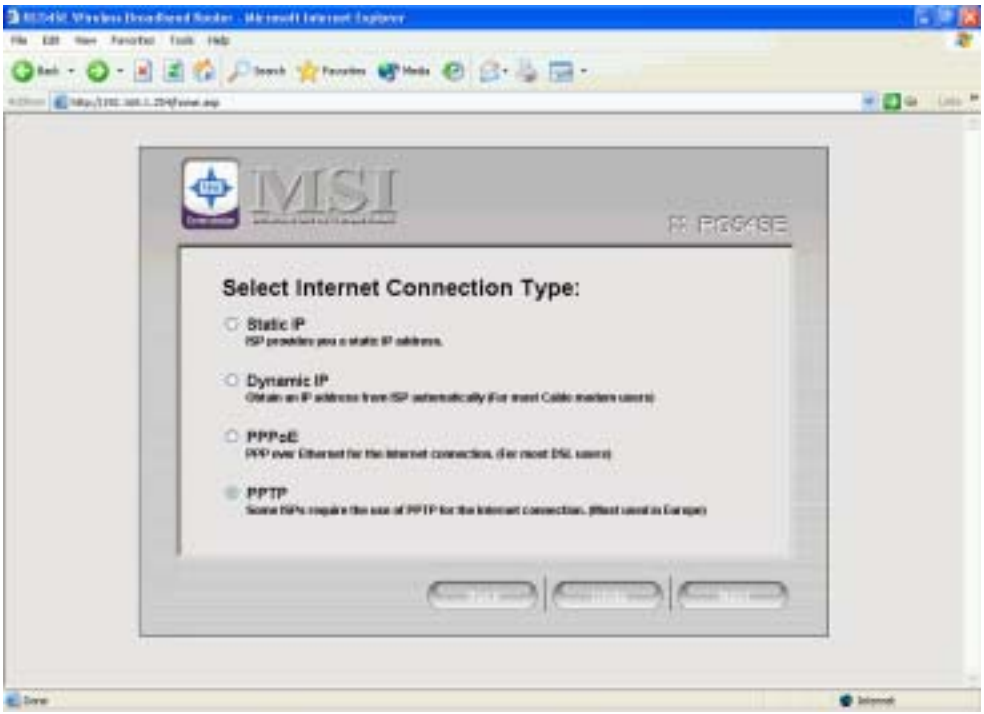
Step3 - This page is to finish PPPoE setup wizard and wait for settings successful message.



Screen snapshot – Finish PPPoE setup

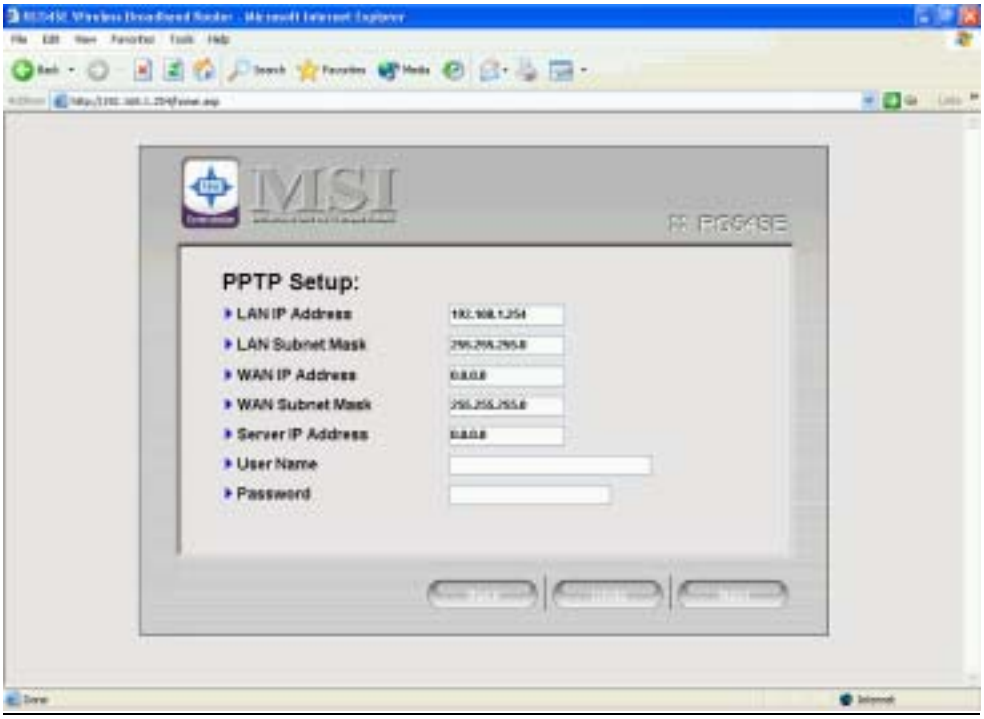
3.3.3.6 PPTP Setup

Step1- This page is used to choose which type connection type you applied.



Screen snapshot – Choose PPTP Connection

Step2 - This page is used to change WAN/LAN/DNS configuration.

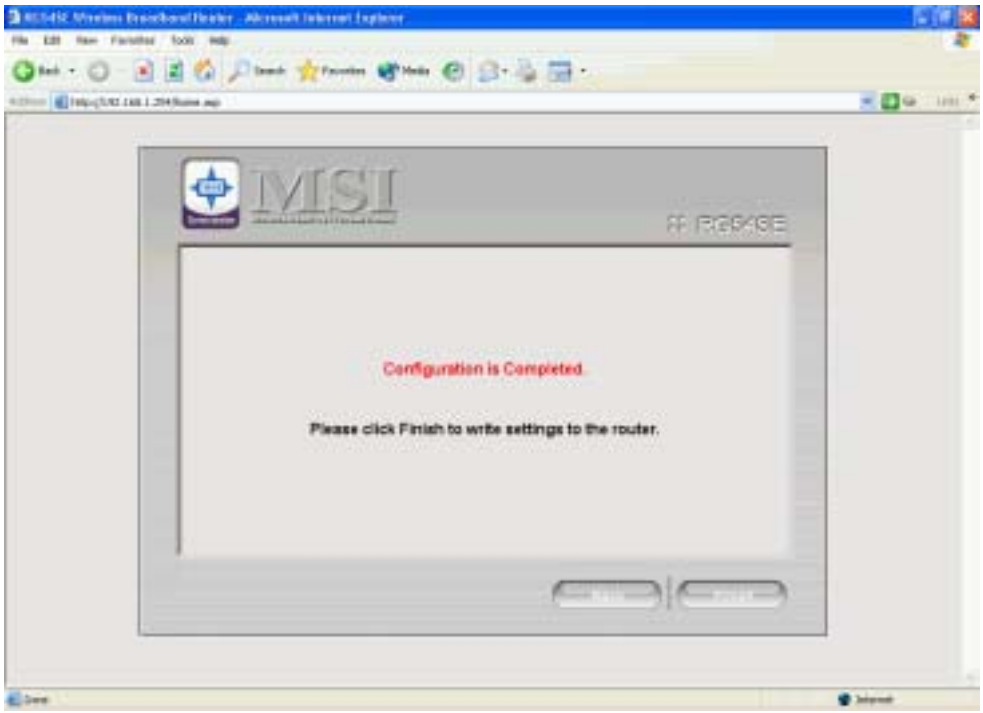


Screen snapshot – PPTP Setup

Item	Description
LAN IP Address	Default is 192.168.1.254. User can change it.
LAN Subnet Mask	Default is 255.255.255.0. User can change it.
WAN IP Address	User input WAN ip address that ISP provided.
WAN Subnet Mask	User input WAN subnet mask that ISP provided.
Server IP Address	User input PPTP server ip address that ISP provided.
User Name	User input the user name that ISP provided.
Password	User input the password ISP provided.
Next	Go to next step.
Undo	Select previous setting.
Back	Back to previous step.

Screen snapshot – PPTP Setup

Step3 - This page is to finish PPTP setup wizard and wait for settings successful message.

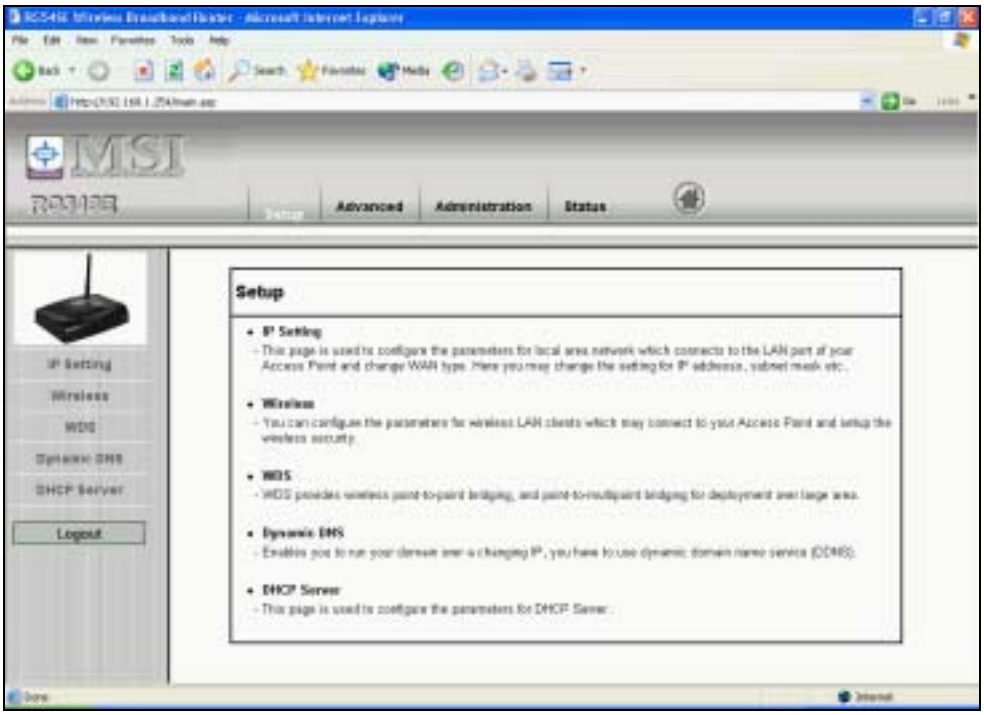


Screen snapshot – Finish PPTP setup

3.3.4 Customized Configuration

3.3.4.1 Setup Main Page

This page is used to show the descriptions of each feature in Setup group.



Screen snapshot – Setup Main Page

- IP Setting

Screen snapshot – IP Setting

Item	Description
LAN IP Address	Fill in the IP address of LAN interfaces.
LAN Subnet Mask	Fill in the subnet mask of LAN interfaces.
WAN Type	Display current WAN connection type and support

	Change button to redirect to WAN Setting page.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the *Undo* button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of IP Setting.

- IP Setting – WAN Setting – DHCP Client

Screen snapshot – DHCP client

Item	Description
WAN Access Type	Click to select DHCP Client support on WAN Setting for IP address assigned automatically from a DHCP server.
DNS Mode	Click Auto/Manual. If choose Manual, input at least DNS info in DNS1/2/3.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
UPNP	Click to Enable/Disable UPNP function.

Web Server Access on WAN	Click to Enable/Disable web configuration from WAN side.
WAN Echo Reply	Click to Enable/Disable WAN ICMP response.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Close	Back to IP Setting page.
Help	Click *Help* button to redirect to help page of WAN Connection Setting.

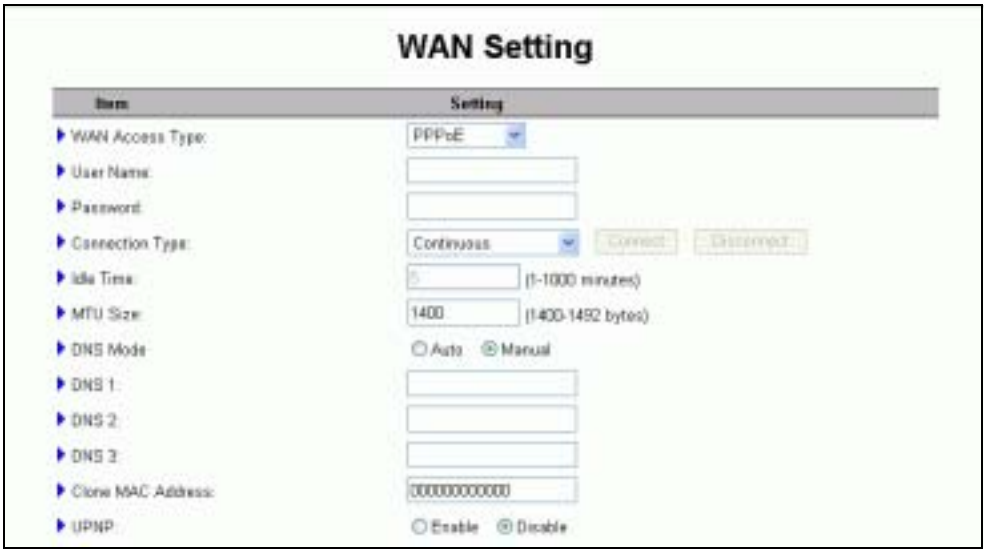
- IP Setting –WAN Setting – Static IP

Screen snapshot – Static IP

Item	Description
WAN Access Type	Click to select Static IP support on WAN interface. There is IP address, subnet mask and default gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface, fill

	in the default gateway for WAN interface out going data packets.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
PNP	Click to Enable/Disable UPNP function.
Web Server Access on WAN	Click to Enable/Disable web configuration from WAN side.
WAN Echo Reply	Click to Enable/Disable WAN ICMP response.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Close	Back to IP Setting page.
Help	Click *Help* button to redirect to help page of WAN Connection Setting.

- IP Setting –WAN Setting – PPPoE



Screen snapshot – PPPoE-1

Item	Description

WAN Access Type	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
User Name	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Password	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Connection Type	Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select. ***Continuous*** connection type means to setup the connection through PPPoE protocol whenever this Wireless Broadband Router is powered on. ***Connect on Demand*** connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set. ***Manual*** connection type means to setup the connection through the PPPoE protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.
Idle Time	If you select the ***PPPoE*** and ***Connect on Demand*** connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
DNS Mode	Click Auto/Manual. If choose Manual, input at least DNS info in DNS1/2/3.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.

UPNP	Click to Enable/Disable UPNP function.
Web Server Access on WAN	Click to Enable/Disable web configuration from WAN side.
WAN Echo Reply	Click to Enable/Disable WAN ICMP response.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the *Undo* button to abort change and recover the previous configuration setting.
Close	Back to IP Setting page.
Help	Click *Help* button to redirect to help page of WAN Connection Setting.

- IP Setting –WAN Setting – PPTP

Screen snapshot – PPTP-1

Screen snapshot – PPTP-2

Item	Description
WAN Access Type	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router a VPN connection.
IP Address	If you select the PPTP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill in the subnet mask for it.
Server IP Address	Enter the IP address of the PPTP Server.
User Name	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Password	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400.
DNS Mode	Click Auto/Manual. If choose Manual, input at least DNS info in DNS1/2/3.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.

Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
UPNP	Click to Enable/Disable UPNP function.
Web Server Access on WAN	Click to Enable/Disable web configuration from WAN side.
WAN Echo Reply	Click to Enable/Disable WAN ICMP response.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the *Undo* button to abort change and recover the previous configuration setting.
Close	Back to IP Setting page.
Help	Click *Help* button to redirect to help page of WAN Connection Setting.

- Wireless

Screen snapshot – Wireless

Item	Description
Band	Display current band setting.
Mode	Click to select the AP / WDS / AP+WDS wireless mode.
SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Number	Select the wireless communication channel from

	pull-down menu.
Security	Display current WLAN security status and support Change button to redirect to WLAN Security page.
Associated Clients	Click the ***Show Active Clients*** button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of Wireless.

- Wireless – WLAN Security

Screen snapshot – WLAN Security

Item	Description
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed
Use 802.1x Authentication	Click checkbox to use 802.1x via RADIUS Sever authentication.

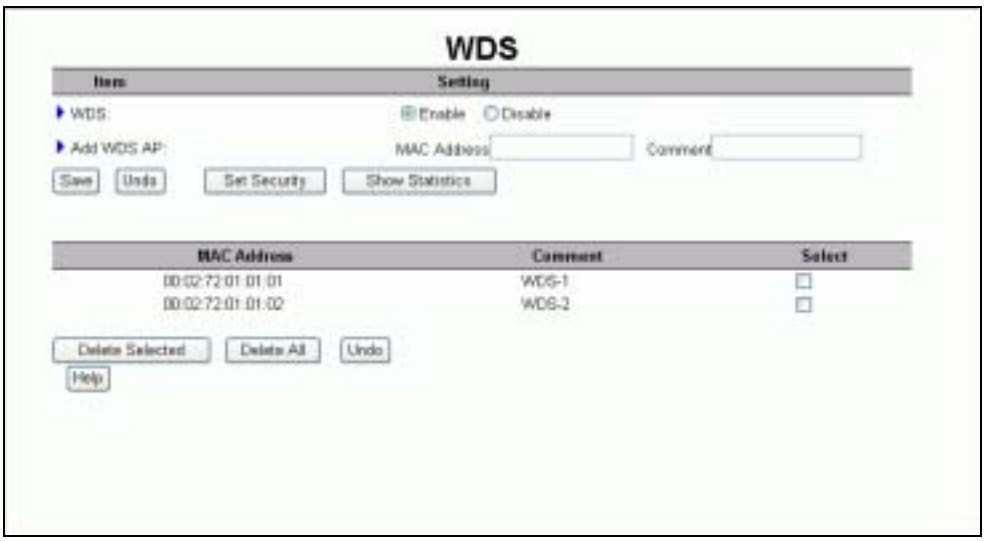
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). **[WPA, Personal(Pre-Shared Key) only]**
Pre-Shared Key	Fill in the key value. **[WPA, Personal(Pre-Shared Key) only]**
Pre-Authentication	Click to Enable/Disable Pre-Authentication. **[WPA2/WPA2 Mixed only, Enterprise only]**
Authentication RADIUS Server	Set the IP address, port and login password information of authentication RADIUS sever.
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Close	Back to Wireless page.
Help	Click *Help* button to redirect to help page of WLAN Security.

- WLAN Security - WEP

Screen snapshot – Wireless WEP Key Setup

Item	Description
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Default Tx Key	Set the default secret key for WEP security function. Value can be chose between 1 and 4.
Encryption Key 1	Secret key 1 of WEP security encryption function.
Encryption Key 2	Secret key 2 of WEP security encryption function.
Encryption Key 3	Secret key 3 of WEP security encryption function.
Encryption Key 4	Secret key 4 of WEP security encryption function.
Save	Click the ***Save*** button to complete the new configuration setting.
Close	Click to back to Wireless page.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.

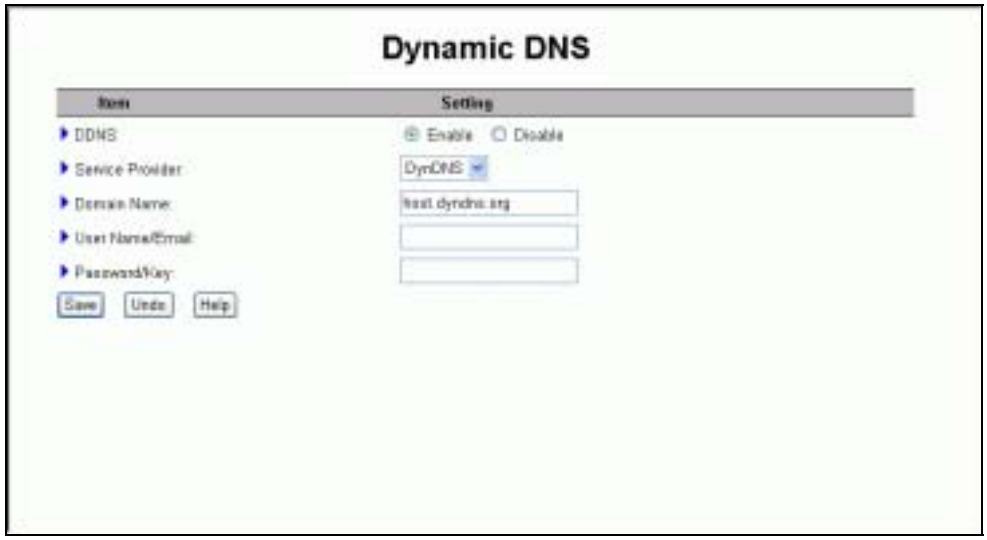
- WDS



Screen snapshot – WDS

Item	Description
Enable WDS	Click the Enable/Disable wireless distribution system.
MAC Address	Fill in the MAC address of AP to register the wireless distribution system access capability.
Comment	Fill in the comment tag for the registered AP.
Save	Click the *Save* button to register the AP to new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Set Security	Click button to configure wireless security like ***WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES)*** or ***None***
Show Statistics	It shows the TX, RX packets, rate statistics
Delete Selected	Click to *Delete Selected* clients that will be removed from the wireless distribution system.
Delete All	Click to *Delete All* the registered APs from the wireless distribution system allowed list.
Undo	Click the *Undo* button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of WDS.

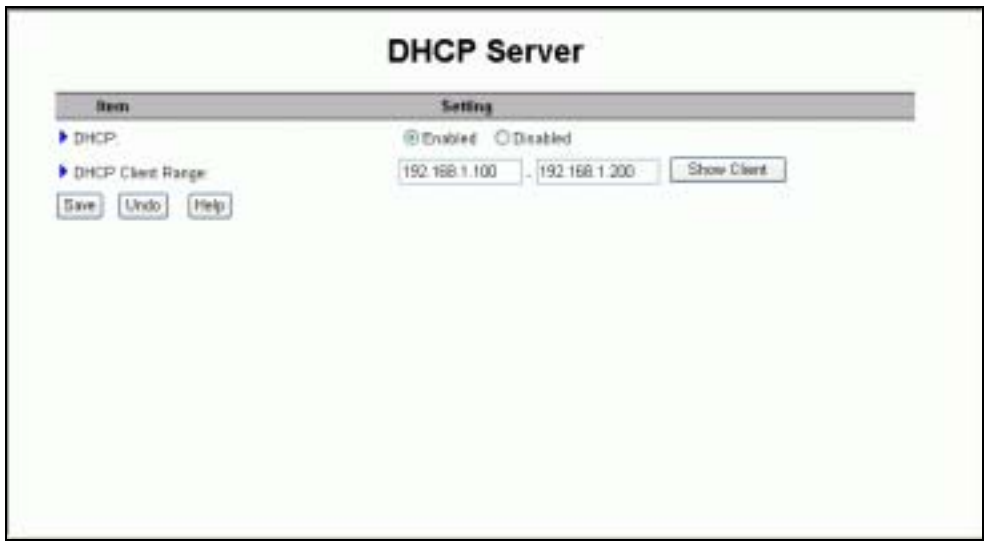
- Dynamic DNS



Screen snapshot – Dynamic DNS

Item	Description
DDNS	Click Enable/Disable ***DDNS*** service.
Service Provider	Click the drop down menu to pickup the service provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Save	Click the ***Save*** button to save the enable DDNS service.
Undo	Click the *Undo* button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of Dynamic DNS.

- DHCP Server



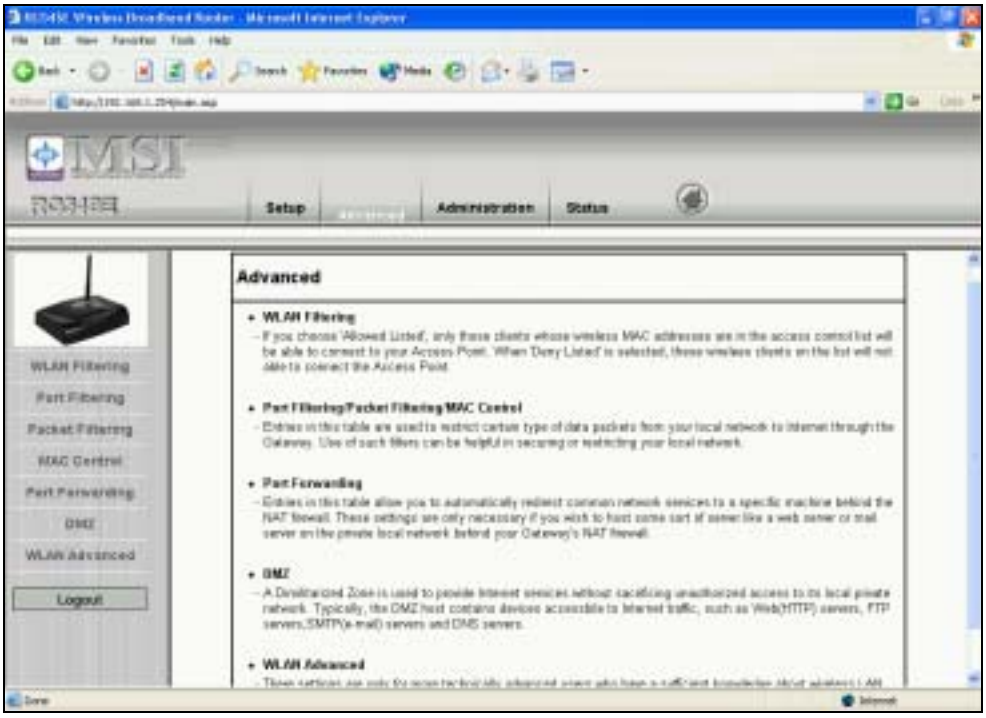
Screen snapshot – DHCP Server

Item	Description
DHCP	Click to Enable/Disable DHCP Server.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Show Client	Click to open the Active DHCP Client Table window that shows the active clients with their assigned IP address, MAC address and time expired information. **[Server**

	mode only]
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of DHCP server.

3.3.4.2 Advanced Main Page

This page is used to show the descriptions of each feature in Advanced group.



Screen snapshot – Advanced Main Page

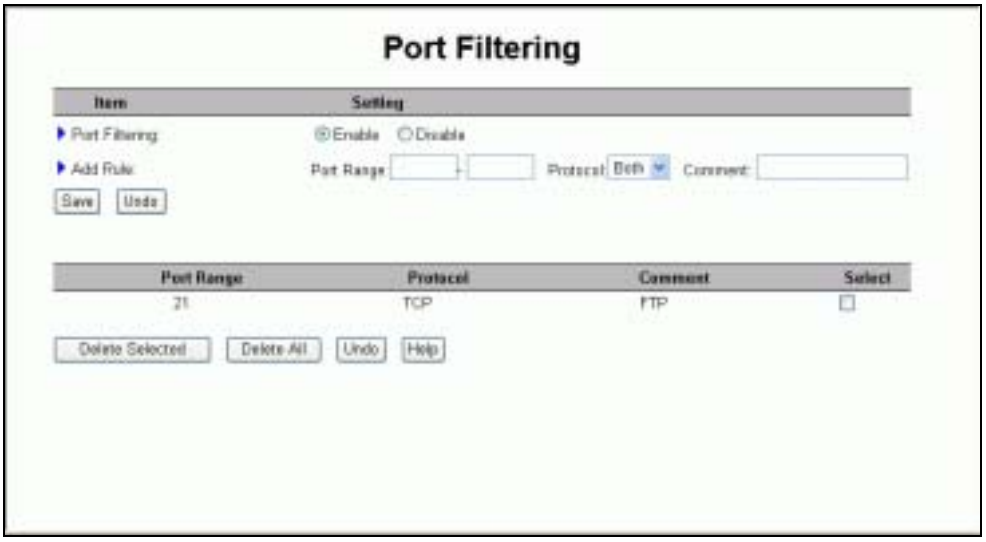
- WLAN Filtering

Screen snapshot – WLAN Filtering

Item	Description
Wireless Access Control Mode	Click the ***Disabled***, ***Allow Listed*** or ***Deny Listed*** of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this Wireless Broadband Router.
MAC Address	Fill in the MAC address of client to register this Wireless Broadband Router access capability.
Comment	Fill in the comment tag for the registered client.
Save	Click the ***Save*** button to register the client to new configuration setting.
Undo	Click the *Undo* button to abort change and recover the previous configuration setting.
Current Access Control List	It shows the registered clients that are allowed to link to this Wireless Broadband Router.
Delete Selected	Click to delete the selected clients that will be access right removed from this Wireless Broadband Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.

Help	Click *Help* button to redirect to help page of WLAN Filtering.

- Port Filtering

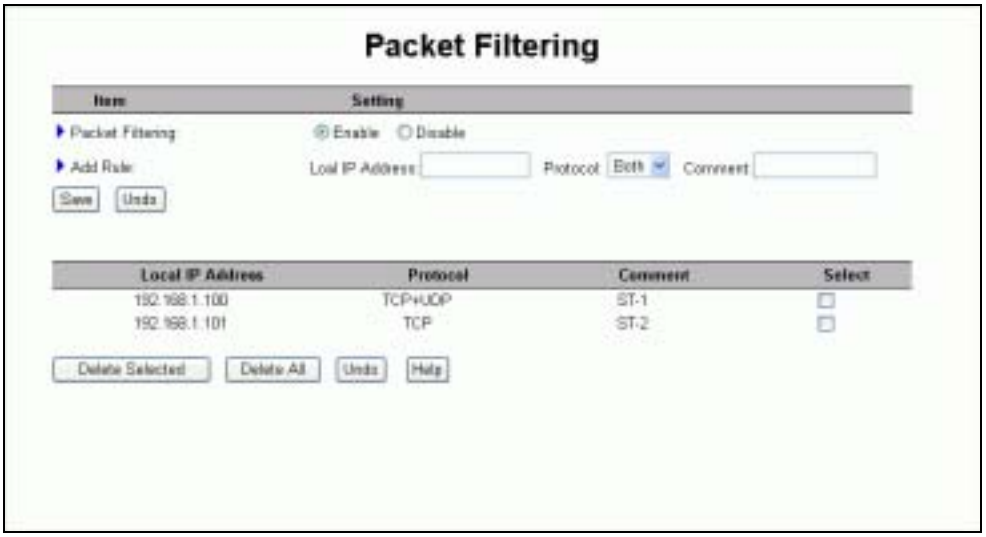


Screen snapshot – Port Filtering

Item	Description
Port Filtering	Click to Enable/Disable the port filtering security function.
Port Range Protocol Comments	To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the ports.
Save	Click the ***Save*** button to register the ports to port filtering list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Undo	Click the ***Undo*** button to abort change and recover the

	previous configuration setting.
Help	Click *Help* button to redirect to help page of Port Filtering.

- Packet Filtering



Screen snapshot – Packet Filtering

Item	Description
Packet Filtering	Click to Enable/Disable the Packer filtering security function.
Local IP Address Protocol Comments	To restrict data transmission from local network on certain IP addresses, fill in the IP address and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the IP address.
Save	Click the ***Save*** button to register the IP address to Packet filtering list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be removed from the IP-filtering list.

Delete All	Click to delete all the registered entries from the IP-filtering list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of Packet Filtering.

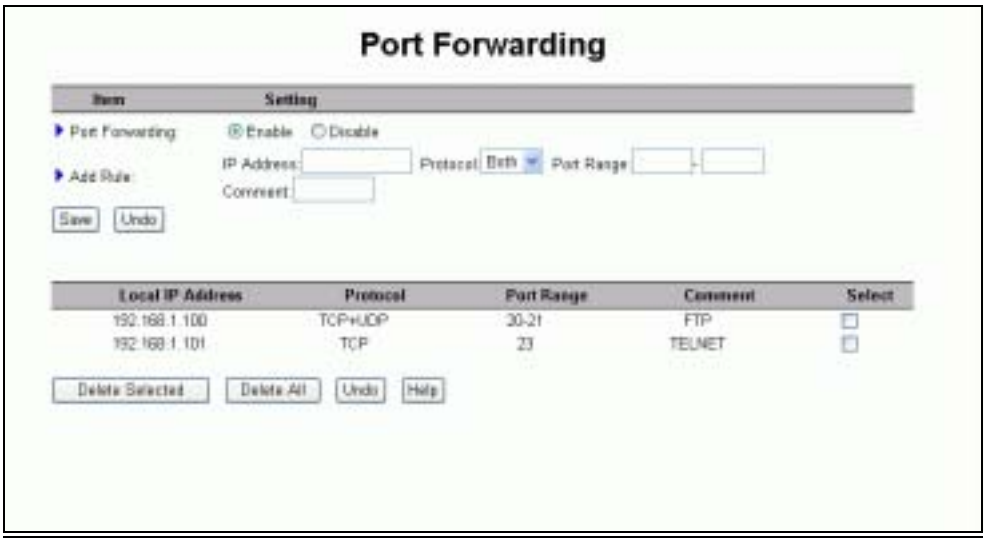
- MAC Control

Screen snapshot – MAC Control

Item	Description
MAC Control	Click Enable/Disable the MAC Control security function.
MAC Address Comments	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it. ***Comments*** let you know about whys to restrict data from the MAC address.
Save	Click the ***Save*** button to register the MAC address to MAC Control list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be removed from the MAC-filtering list.

Delete All	Click to delete all the registered entries from the MAC-filtering list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of MAC Control.

- Port Forwarding

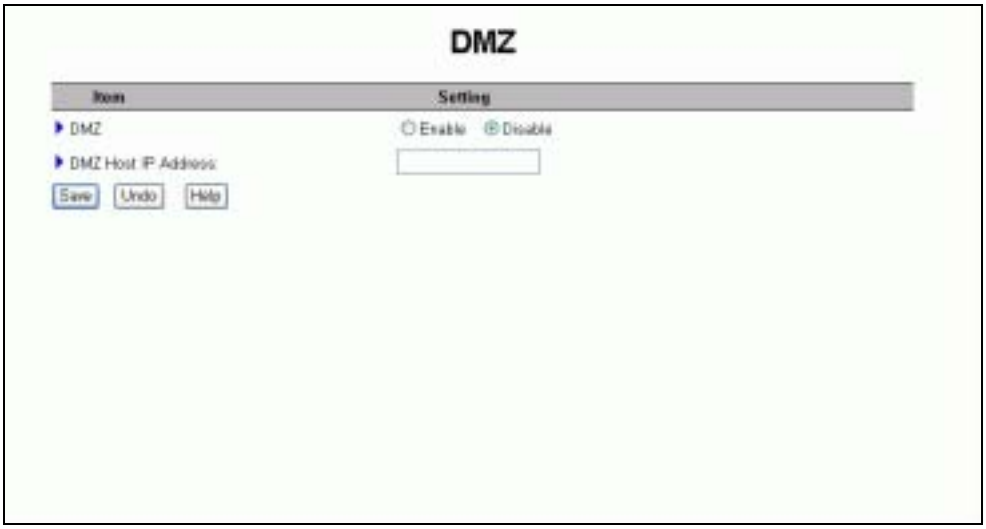


Screen snapshot – Port Forwarding

Item	Description
Port Forwarding	Click to Enable/Disable the Port Forwarding security function.
IP Address Protocol Port Range Comment	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address, protocol, port range and your comments. The ***Protocol*** can be TCP, UDP or Both. The ***Port Range*** for data transmission. ***Comments*** let you know about whys to allow data packets forward to the IP address and port number.
Save	Click the ***Save Changes*** button to register the IP address

	and port number to Port forwarding list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address and port number that will be removed from the port-forwarding list.
Delete All	Click to delete all the registered entries from the port-forwarding list.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of Port Forwarding.

- DMZ

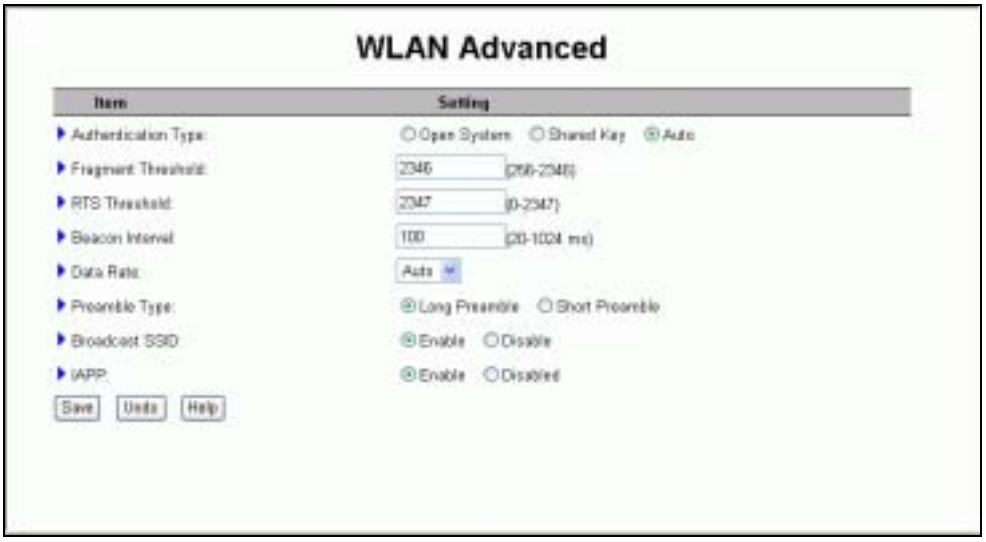


Screen snapshot – DMZ

Item	Description
DMZ	Click to Enable/Disable the DMZ function.
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.
Save	Click the ***Save*** button to register the IP address of DMZ host.
Undo	Click the ***Undo*** button to abort change and recover the

	previous configuration setting.
Help	Click *Help* button to redirect to help page of DMZ.

- WLAN Advanced



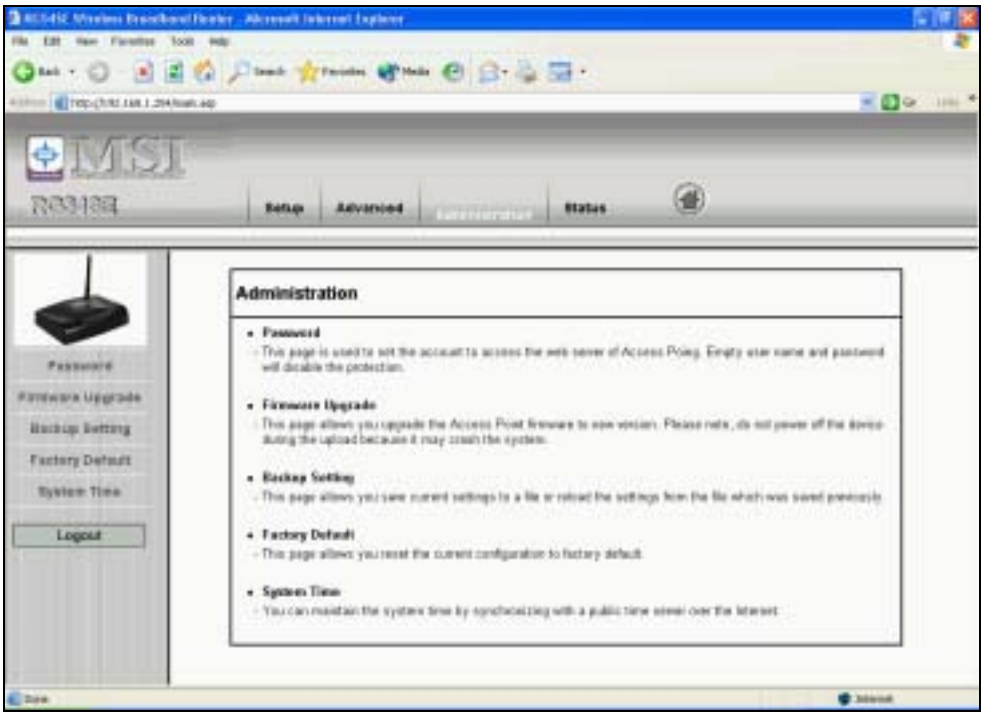
Screen snapshot – WLAN Advanced

Item	Description
Authentication Type	Click to select the authentication type in ***Open System***, ***Shared Key*** or ***Auto*** selection.
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes.
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes.
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 11M, 5.5M, 2M or 1Mbps(11b) 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M (11g).
Preamble Type	Click to select the ***Long Preamble*** or ***Short Preamble*** support on the wireless data packet transmission.
Broadcast SSID	Click to enable or disable the SSID broadcast function.

IAPP	Click to enable or disable the IAPP function. Refer to 4.20 What is Inter-Access Point Protocol(IAPP)?
Save	Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of WLAN Advanced.

3.3.4.3 Administration Main Page

This page is used to show the descriptions of each feature in Administration group.



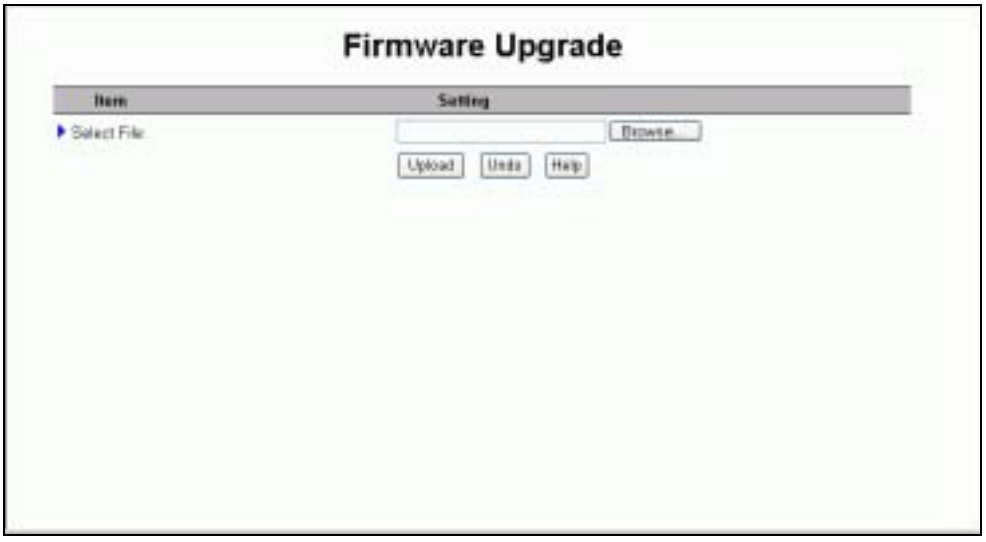
Screen snapshot – Administration Main Page

- Password

Screen snapshot – Password

Item	Description
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Save	Clear the ***User Name*** and ***Password*** fields to empty, means to apply no web management login control. Click the ***Save*** button to complete the new configuration setting.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of Password.

- Firmware Upgrade



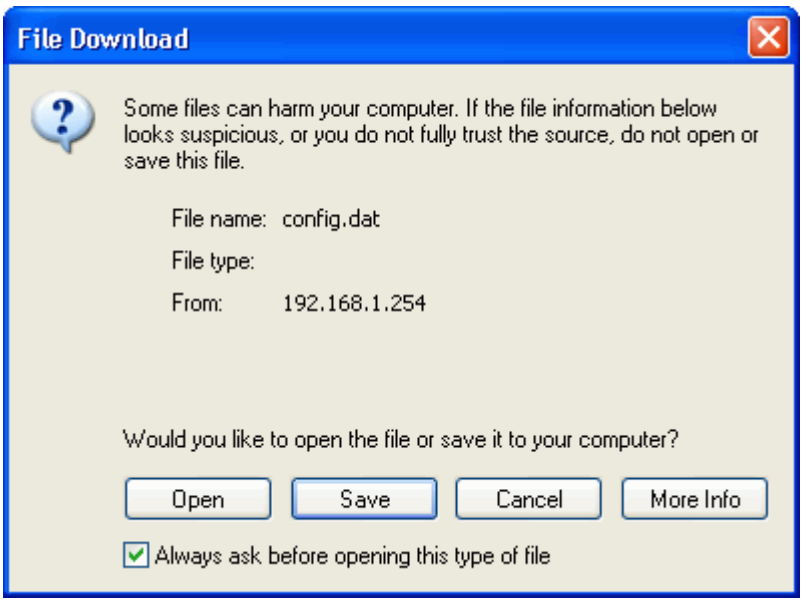
Screen snapshot – Firmware Upgrade

Item	Description
Select File	Click the ***Browse*** button to select the new version of web firmware image file.(It accepts kernel or web image)
Upload	Click the ***Upload*** button to update the selected web firmware image to the Wireless Broadband Router.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Help	Click *Help* button to redirect to help page of Firmware Upgrade.

- Backup Setting

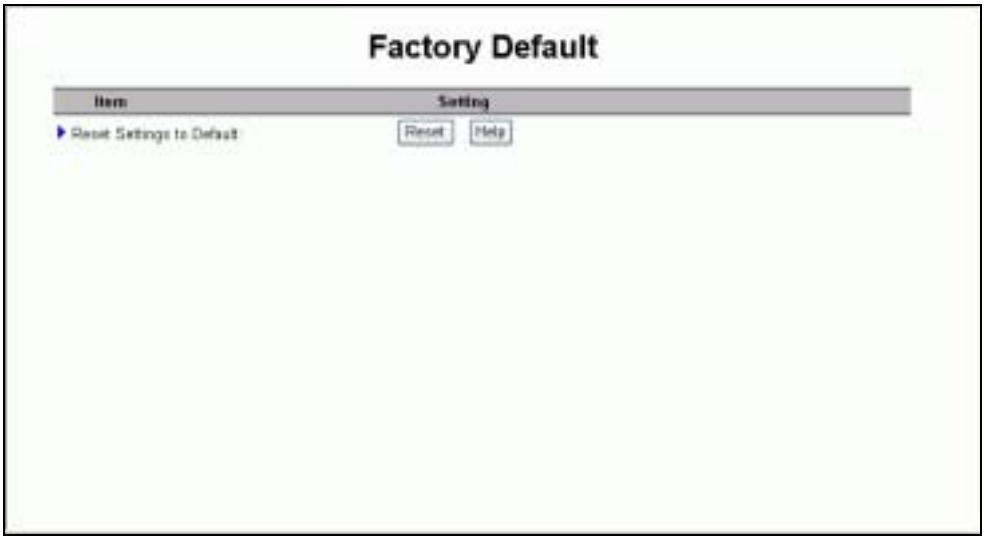
Screen snapshot – Backup Setting

Item	Description
Save Settings to File	Click the ***Save*** button to download the configuration parameters to your personal computer.
Load Settings from File	Click the ***Browse*** button to select the configuration files then click the ***Upload*** button to update the selected configuration to the Wireless Broadband Router.
Help	Click *Help* button to redirect to help page of Backup Setting.



Screen snapshot – Save Settings to File

- Factory Default



Screen snapshot – Factory Default

Item	Description
Reset Settings to Default	Click the ***Reset*** button to reset the configuration parameter to factory defaults.
Help	Click *Help* button to redirect to help page of Factory Default.

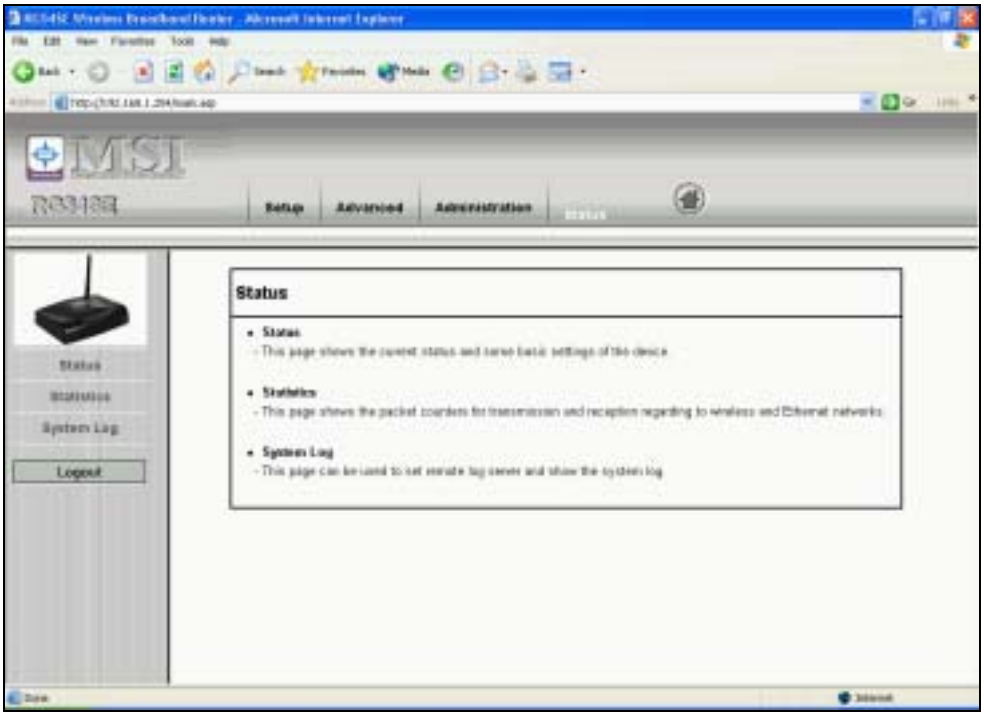
- System Time

Screen snapshot – System Time

Item	Description
Current Time	It can edit the current time stamp.
Time Zone Select	Click the time zone in your country.
NTP client update	Click to Enable/Disable NTP client update
NTP Server	Click select default or input NTP server IP address.
Save	Click the ***Save*** button to save and enable NTP client service.
Undo	Click the ***Undo*** button to abort change and recover the previous configuration setting.
Refresh	Click the refresh the current time shown on the screen.
Help	Click *Help* button to redirect to help page of System Time.

3.3.4.4 Status Main Page

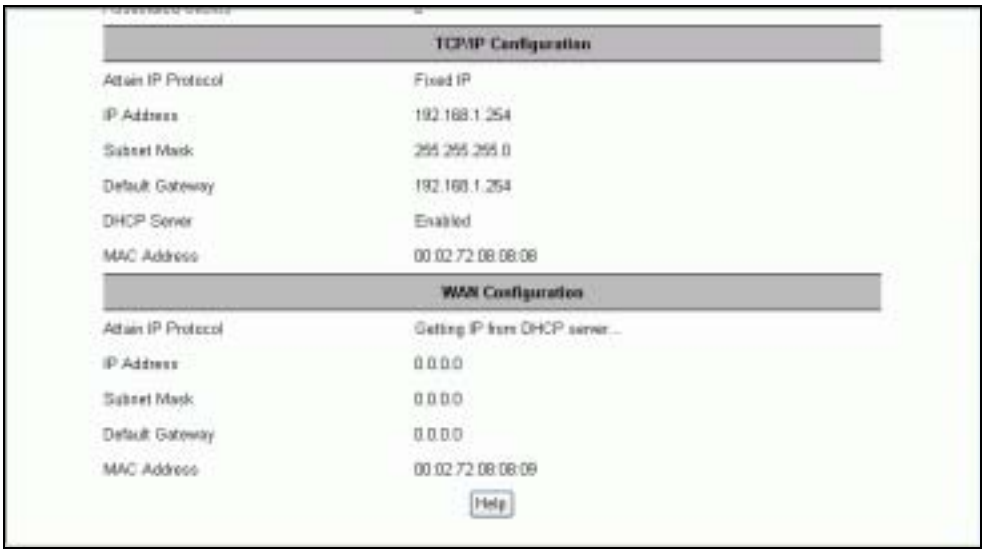
This page is used to show the descriptions of each feature in Status group.



Screen snapshot – Status Main Page

- Status

Screen snapshot – Status-1

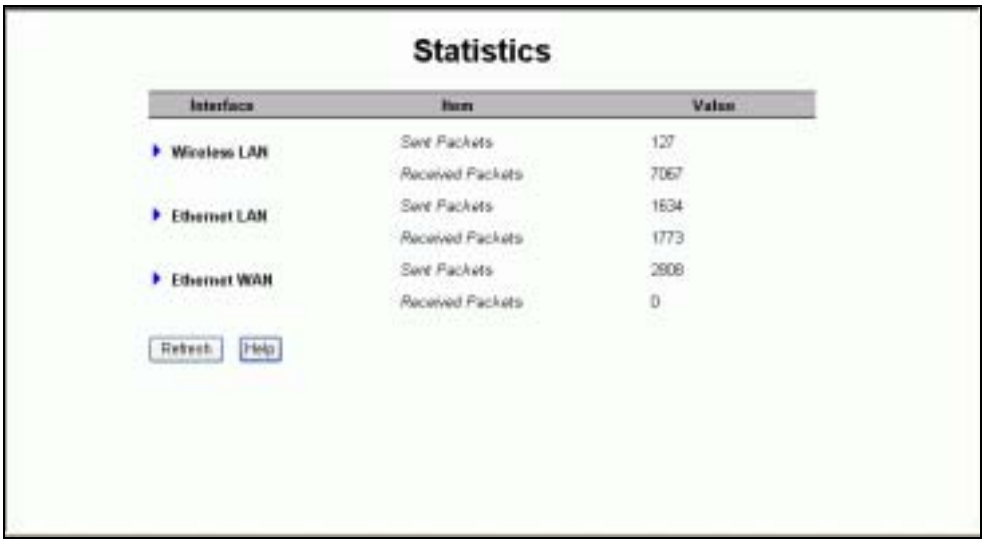


Screen snapshot – Status-2

Item	Description
System	
Uptime	It shows the duration since Wireless Broadband Router is powered on.
Firmware version	It shows the firmware version of Wireless Broadband Router.
Wireless configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this Wireless Broadband Router. The SSID is the unique name of Wireless Broadband Router and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the Wireless Broadband Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows the status of LAN IP address.

IP Address	It shows the IP address of LAN interfaces of Wireless Broadband Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of Wireless Broadband Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of Wireless Broadband Router.
WAN configuration	
Attain IP Protocol	It shows how the Wireless Broadband Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.
IP Address	It shows the IP address of WAN interface of Wireless Broadband Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of Wireless Broadband Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of Wireless Broadband Router.
Help	Click *Help* button to redirect to help page of Status.

- Statistics



Screen snapshot – Statistics

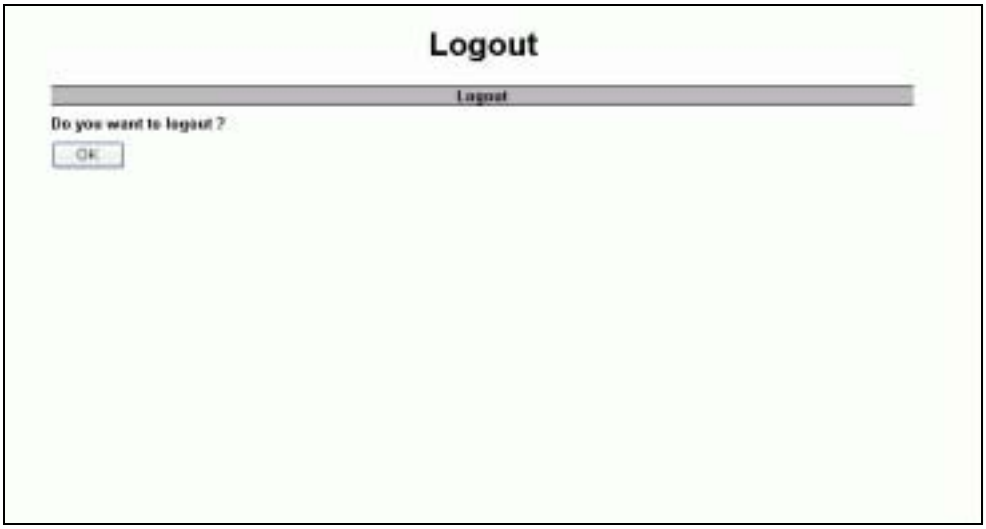
Item	Description
Wireless LAN ***Sent Packets***	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN ***Received Packets***	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN ***Sent Packets***	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet LAN interface.
Ethernet WAN ***Sent Packets***	It shows the statistic count of sent packets on the Ethernet WAN interface.
Ethernet WAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.
Help	Click *Help* button to redirect to help page of Statistics.

- System Log

Screen snapshot – System Log

Item	Description
Enable Log	Click the checkbox to enable log.
Wireless only	Only show wireless log
System all	Show all log of wireless broadband router
Enable Remote Log	Click the checkbox to enable remote log service.
Log Server IP Address	Input the remote log IP address
Save	Click the ***Save*** button to save above settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen
Help	Click *Help* button to redirect to help page of System Log.

3.3.4.5 Logout



Screen snapshot – Logout

Item	Description
OK	Click logout web configuration page.

4 Frequently Asked Questions (FAQ)

4.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
- ✓ Type in ***ipconfig /all*** then press the ***Enter*** button.

- ➢ Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

4.2 What is Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

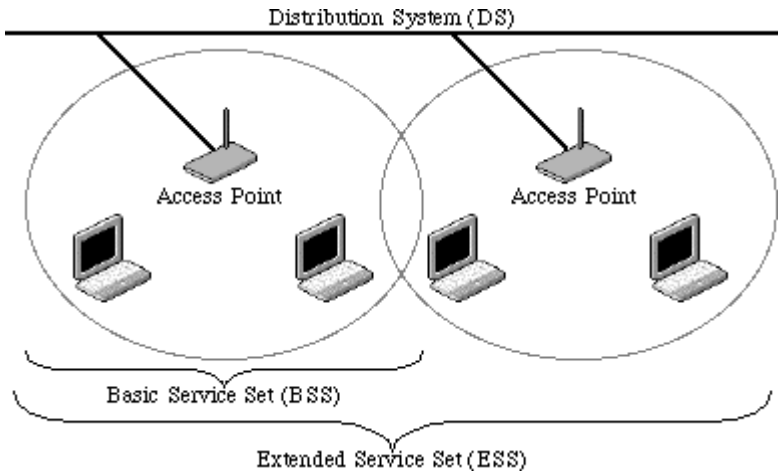
4.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

4.4 How does wireless networking work?

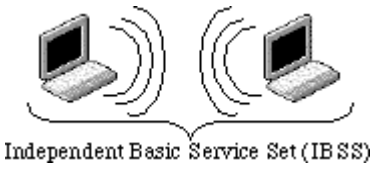
The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access

to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

4.5 What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

4.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

4.7 What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture… etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, … etc.
- ✓ Add additional WLAN Access Points if necessary.

4.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

4.9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

4.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several

fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

4.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

4.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling

stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

4.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

4.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

4.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi’s original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an

authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

4.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

4.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

4.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

4.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government’s next-generation cryptography algorithm, which will replace DES and 3DES.

4.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

4.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

4.22 What is Universal Plug and Play (UPNP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

4.23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

4.24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.
Since that all the clients will communicate outside world through the Wireless Broadband Router, so have the cloned MAC address set on the Wireless Broadband Router will solve the issue.

4.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user own the DNS server with dynamic WAN IP address.

4.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

5 Configuration Examples

5.1 Example One – PPPoE on the WAN

Sales division of Company ABC likes to establish a WLAN network to support mobile communication on sales' Notebook PCs. MIS engineer collects information and plans the Wireless Broadband Router implementation by the following configuration.

LAN configuration

IP Address	**192.168.1.254**
Subnet Mask	**255.255.255.0**

WAN configuration:

PPPoE

User Name	**H890123456**
Password	**PW192867543210**

WLAN configuration

SSID	**MSI**
Channel Number	**7**

DHCP Server configuration

DHCP Client Range	**192.168.1.100 – 192.168.1.200**

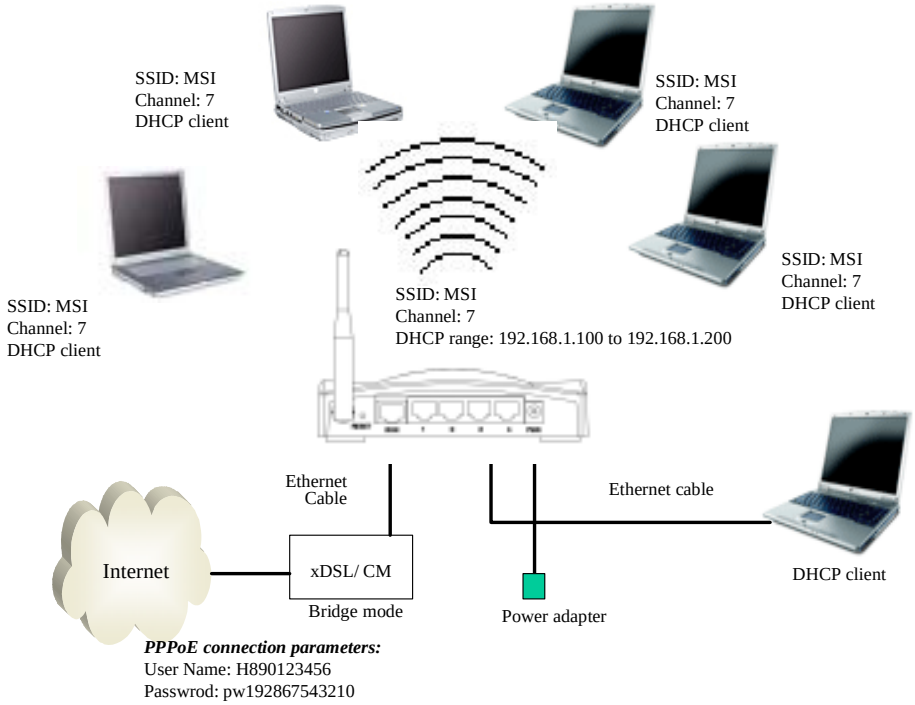


Figure 3 – Configuration Example One – PPPoE on the WAN

Configure the LAN interface:

Open IP Setting page, enter the IP Address "**192.168.1.254**", Subnet Mask "**255.255.255.0**",

Press Save button to confirm the configuration setting.

Configure the WAN interface:

Click "Change" button in "IP Setting" page, select PPPoE under WAN Access Type and enter the User Name "**H890123456"** and Password "**PW192867543210**", the password is encrypted to display on the screen.

Press Save button to confirm the configuration setting.

Configure the WLAN interface:

Open Wireless page, enter the SSID "**MSI**", Channel Number "7".

Press Save button to confirm the configuration setting.

Configure the DHCP Server

Open DHCP Server page, enable DHCP server..

Press Save button to confirm the configuration setting.

5.2 Example Two – Fixed IP on the WAN

Company ABC likes to establish a WLAN network to support mobile communication on all employees' Notebook PCs. MIS engineer collects information and plans the Wireless Broadband Router implementation by the following configuration.

LAN configuration

IP Address	**192.168.1.254**
Subnet Mask	**255.255.255.0**

WAN configuration:

Fixed IP

IP Address	**192.168.2.254**
Subnet Mask	**255.255.255.0**
Default Gateway	**192.168.2.10**
DNS Address	**168.95.1.1**

WLAN configuration

SSID	**MSI**
Channel Number	**7**

DHCP Server configuration

DHCP Client Range	**192.168.1.100 – 192.168.1.200**

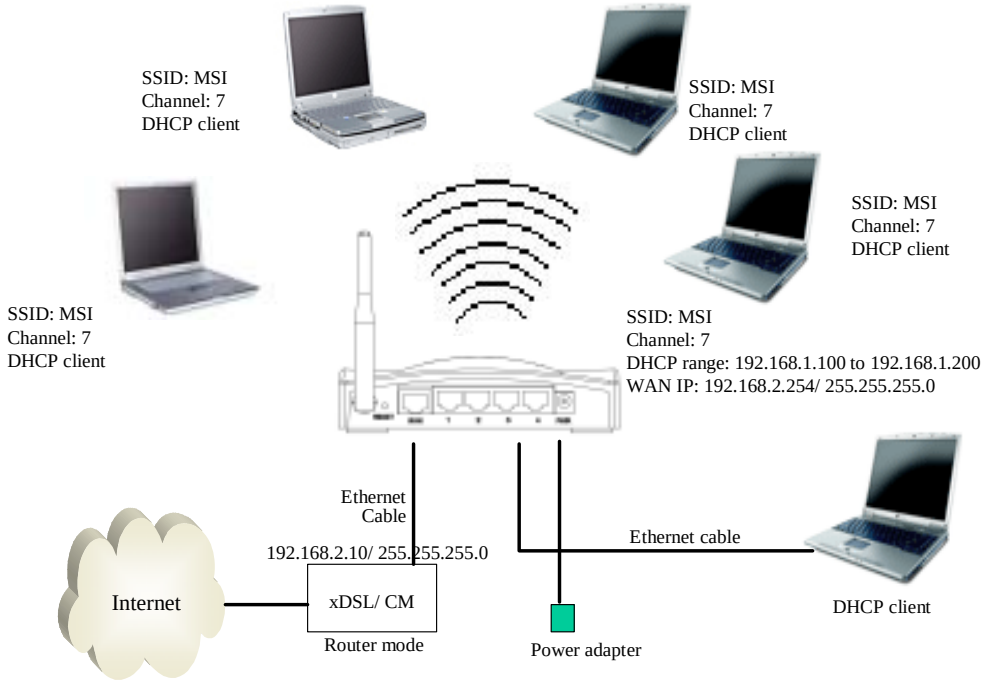


Figure 4 – Configuration Example Two – Fixed IP on the WAN

Configure the LAN interface:

Open IP Setting page, enter the IP Address "**192.168.1.254**", Subnet Mask "**255.255.255.0**"

Press Save button to confirm the configuration setting.

Configure the WAN interface:

Click "Change" button in "IP Setting" page, select "Static IP" under WAN Access Type, enter IP Address "**192.168.2.254",** subnet mask "**255.255.255.0**",

Press Save button to confirm the configuration setting.

Configure the WLAN interface:

Open "Wireless" page, enter the SSID "MSI", Channel Number "7".

Press Save button to confirm the configuration setting.

Configure the DHCP Server

Open DHCP Server page, enable DHCP server..

Press Save button to confirm the configuration setting.