802.11g Wireless Broadband Router

WRT-416

User's Manual

Copyright

Copyright © 2007 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.
PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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

1. Reorient or relocate the receiving antenna.

2. Increase the separation between the equipment and receiver.

3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance. (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation e re set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC rad uency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all

times to ensure the safe use of the equipment.

EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

Potential Restrictive Use

France: Only channels 10,11,12 and 13

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET Wireless Broadband Router

Model: WRT-416

Rev: 1.0 (October, 2007)
Part No. EM-WRT416

Table of Contents

Chapter 1 Introduction 6
1.1 Package Content 6
1.2 System Requirement 6
1.3 Features 6
1.4 Wireless Performance 7
Chapter 2 Hardware Installation 8
2.1 Hardware Connection 8
2.2 LED Indicators 8
2.3 Back View 9
Chapter 3 Configuring Local Networking 10
3.1 Setting up TCP/IP 10
3.1.1 Windows 2000 10
3.1.2 Windows XP/2003 13
3.2 Additional Settings for Wireless Client 16
3.3 Checking PC's IP and Connection with the Router 17
Chapter 4 Web Configuration 19
4.1 Status 20
4.1.1 System Status 20
4.1.2 Statistics 22
4.2 WAN Setup 23
4.2.1 Dynamic IP Address 24
4.2.2 PPPoE 24
4.2.3 Static IP 25
4.2.4 PPTP 27
4.2.5 L2TP 28
4.3 LAN Setup 28
4.3.1 LAN Setup 28
4.3.2 DHCP IP Address Reserving 29
4.3.3 DHCP Info 29
4.4 Wireless 30
4.4.1 Basic Settings 30
4.4.2 Security 31
4.4.3 Filter List 34
4.4.4 WDS 35
4.4.5 Advanced 36
4.4.6 Association Table 36
4.5 Routing 37
4.6 NAT 37
4.6.1 DMZ Host Setup 38
4.6.2 FTP Private Port 39
4.6.3 Virtual Server Setup 39
4.6.4 Port Trigger 40
4.7 Fire Wall 40
4.7.1 MAC Filtering 40
4.7.2 Access Control 41
4.7.3 URL Filtering 42
4.7.4 Ping 43
4.8 DDNS 44
4.9 MISC 44
4.9.1 Login ID & Password Setup 44
4.9.2 Remote Mgmt 45

4.9.3 UPnP Setup 45
4.9.4 System Time Setup 46
4.9.5 WAN Link Status & Setup 46
4.9.6 Restore Default / Restart System 46
4.9.7 Firmware Upgrade 46
Appendix Ⅰ: Specification 47

Chapter 1 Introduction

Thank you for purchasing WRT-410. This device features the latest innovation wireless technology making the wireless networking world happened. This manual guides you on how to install and properly use the WRT-410 in order to take full advantage of its features.

1.1 Package Content

- One WRT-416
- One dipole antenna
- One Ethernet cable
- One AC Power Adapter
- One User's Manual CD
- One Quick Installation Guide

Note:	If any of the above items are missing, contact your supplier as soon as possible.

1.2 System Requirement

- Cable/ADSL modem and an Internet access account for Internet connection
- One computer with 10/100Base-T Ethernet card and TCP/IP protocol installed for initial setup
- Internet Explorer 5.0 or higher for Web configuration
- 802.11g or 802.11b compliant wireless adapters (for wireless connection)

1.3 Features

- 2.4GHz ISM band, unlicensed operation
- Supports WEP / WPA Personal / WPA2 Personal
- Dual-standard capability: 802.11g and 802.11b compliant
- Supports DHCP server
- Web Configuration provide a user friendly interface for the user to configure through web browser
- Supports UPnP (Universal Plug and Play)
- Supports MAC / URL Filter
- Supports DDNS, virtual server and DMZ
- Build-in 4 -port switch
- Provides Setup Wizard for the user to configure easily in the first time

1.4 Wireless Performance

The following information will help you utilizing the wireless performance, and operating coverage of WRT-416.

1. **Site selection**
   To avoid interferences, please locate WRT-416 and wireless clients away from transformers, microwave ovens, heavy-duty motors, refrigerators, fluorescent lights, and other industrial equipments. Keep the number of walls, or ceilings between AP and clients as few as possible; otherwise the signal strength may be seriously reduced. Place WRT-416 in open space or add additional Access Point as needed to improve the coverage.
2. **Environmental factors**
   The wireless network is easily affected by many environmental factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operating range of WRT-416 in a specific location without testing.
3. **Antenna adjustment**
   The bundled antenna of WRT-416 is adjustable. Firstly install the antenna pointing straight up, then smoothly adjust it if the radio signal strength is poor. But the signal reception is definitely weak in some certain areas, such as location right down the antenna.
   Moreover, the original antenna of WRT-416 can be replaced with other external antennas to extend the coverage. Please check the specification of the antenna you want to use, and make sure it can be used on WRT-416.
4. **WLAN type**
   If WRT-416 is installed in an 802.11b and 802.11g mixed WLAN, its performance will reduced significantly. Because every 802.11g OFDM packet needs to be preceded by an RTS-CTS or CTS packet exchange that can be recognized by legacy 802.11b devices. This additional overhead lowers the speed. If there are no 802.11b devices connected, or if connections to all 802.11b devices are denied so that WRT-416 can operate in 11g-only mode, then its data rate should actually 54Mbps

Chapter 2 Hardware Installation

Before you proceed with the installation, it is necessary that you have enough information about the WRT-416.

2.1 Hardware Connection

1. Locate an optimum location for the WRT-416. The best place for your WRT-416 is usually at the center of your wireless network, with line of sight to all of your mobile stations.
2. Connect the power adapter to the receptor at the rear panel of the WRT-416, and plug the other end of the power adapter to a wall outlet or power strip. The Power LED will light up to indicate proper operation.
3. Power off the ADSL / Cable modem first. Connect ADSL/Cable Modem to the WAN port on WRT-416. Use the cable supplied with your modem. If no cable was supplied with your modem, please use a RJ-45 Ethernet cable. After the Ethernet cable is securely connected, power on the ADSL / Cable modem. The WAN LED will light up to indicate proper connection.
4. Use an Ethernet cable to connect one of the LAN ports on the WRT-416 and the computer you are using to configure the router. The corresponding LAN LED will light up to indicate proper connection. The LAN ports on the WRT-416 are Auto-MDI/MDIX; thus, you can use a straight or crossover Ethernet cable freely.
5. Adjust the antennas of WRT-416. Try to adjust them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.

Note: ONLY use the power adapter supplied with the WRT-416. Otherwise, the product may be damaged.

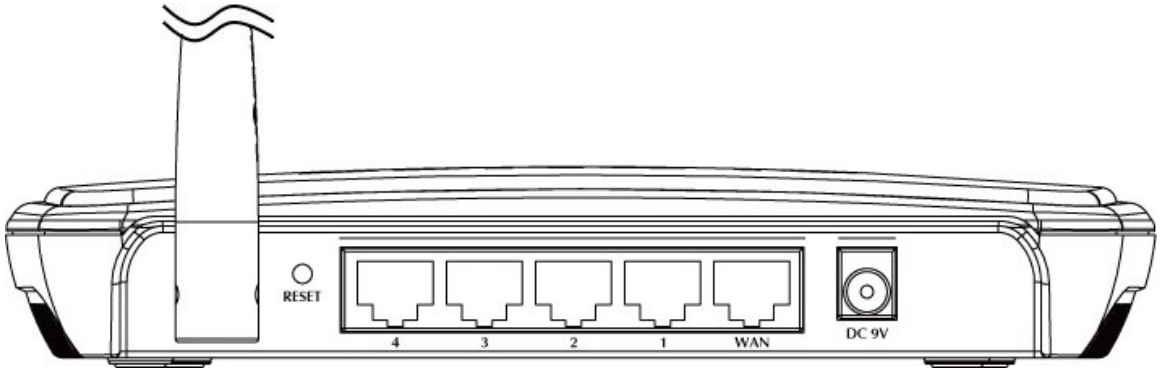
Note: If you want to reset WRT-416 to default settings, press and hold the Reset button over 5 seconds. And then wait for 10 seconds for WRT-416 restart.

2.2 LED Indicators

LED		STATE	MEANING
PWR/SYS		Green	Device power on
WAN		Green	WAN link status is on
		Blinking Green	WAN activity
LAN	**1**	Green	Link is established
		Blinking Green	Packets are transmitting or receiving
	2	Green	Link is established
		Blinking Green	Packets are transmitting or receiving

	3	Green	Link is established
		Blinking Green	Packets are transmitting or receiving
	4	Green	Link is established
		Blinking Green	Packets are transmitting or receiving

2.3 Back View



Power (DC 9V): The receptacle where you plug in the power adapter.

WAN: Connect your modem to your router using this port with your supplied Ethernet cable. This is the only port you can use for this procedure. This enables your router to access the Internet. The port supports 10/100 Mbps as well as straight-through and crossover Ethernet cables.

LAN Ports 1-4: These four ports connect the router to your LAN or home network using Ethernet cables. This enables communication among clients, such as PCs, on the network. The LAN ports support either 10-BASE-T or 100-BASE-T transmission speeds as well as straight-through and crossover Ethernet cables. Any of these four ports can also serve as an uplink port to other network devices, such as another router or switch, which allows you to extend your network.

Reset button: Resets your router or resets the router to the default login settings.
To reset the AP to the factory defaults, press and hold the Reset button for more than five seconds. This clears the AP's user settings, including User ID, Password, IP Address, and Subnet mask. (Warning: your original configurations will be replaced with the factory default settings).

Antenna: The antenna used for wireless connections. You are able to rotate the antenna to gain the best signal reception.

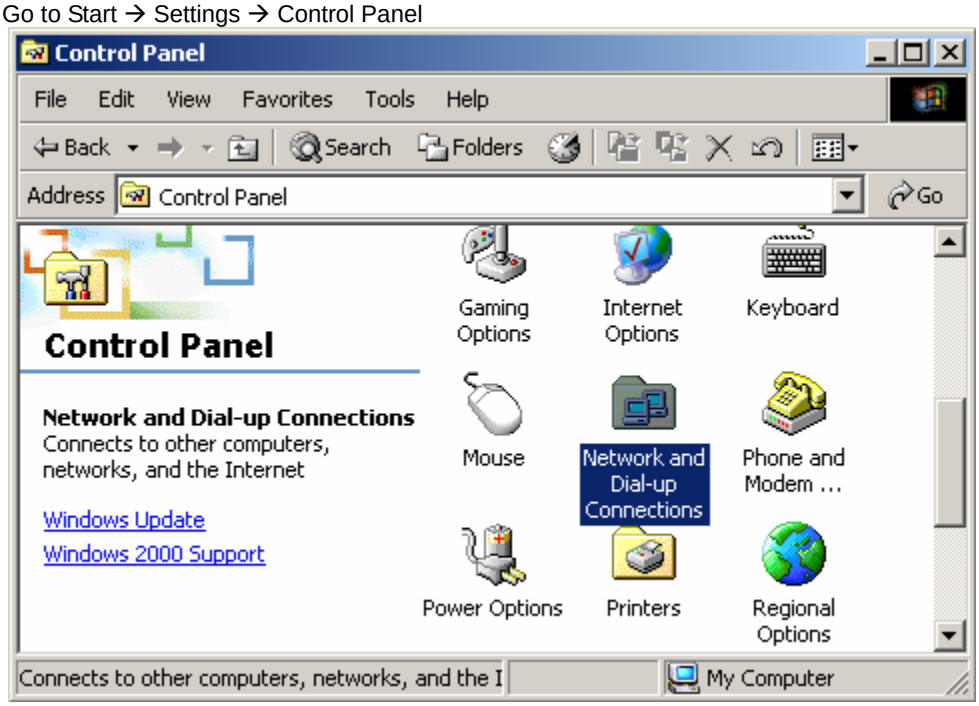
Chapter 3 Configuring Local Networking

You can manage the WRT-416 through the Web browser. To configure the device via Web browser, at least one properly configured computer must be connected to the device via Ethernet (recommended) or wireless network. The WRT-416 is configured with the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0 and its DHCP server is disabled by default.

3.1 Setting up TCP/IP

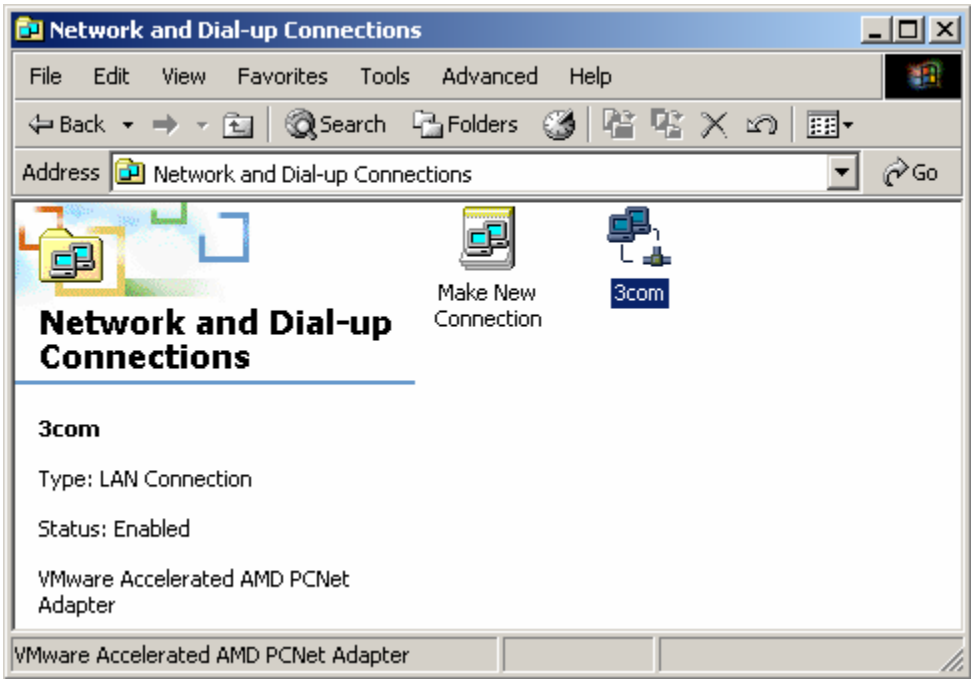
3.1.1 Windows 2000

Step 1: Go to Start → Settings → Control Panel

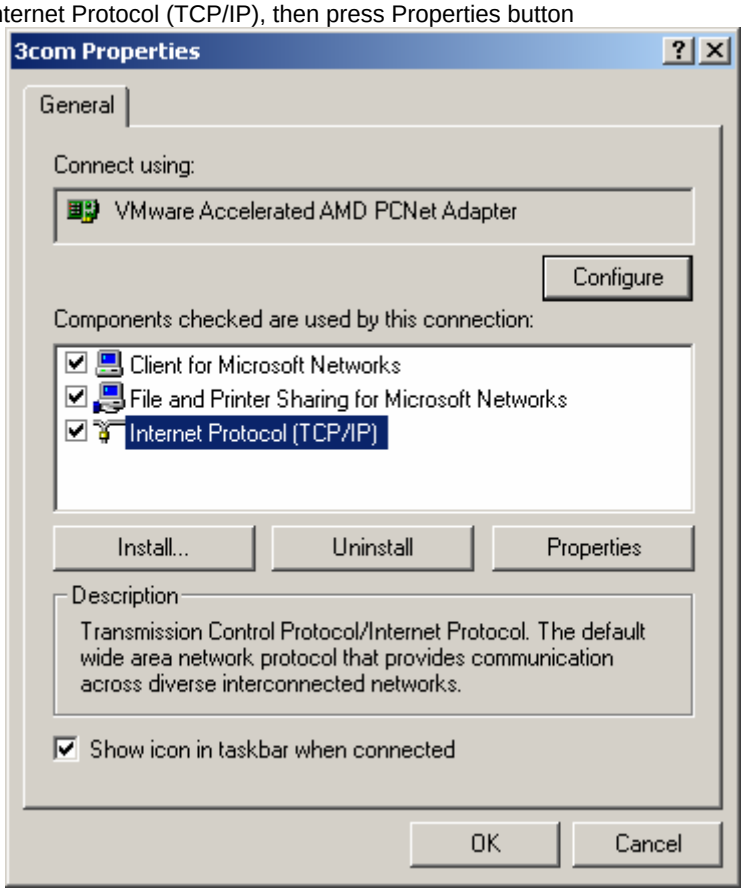


Step 2: Double click the icon Network and Dial-up Connections.

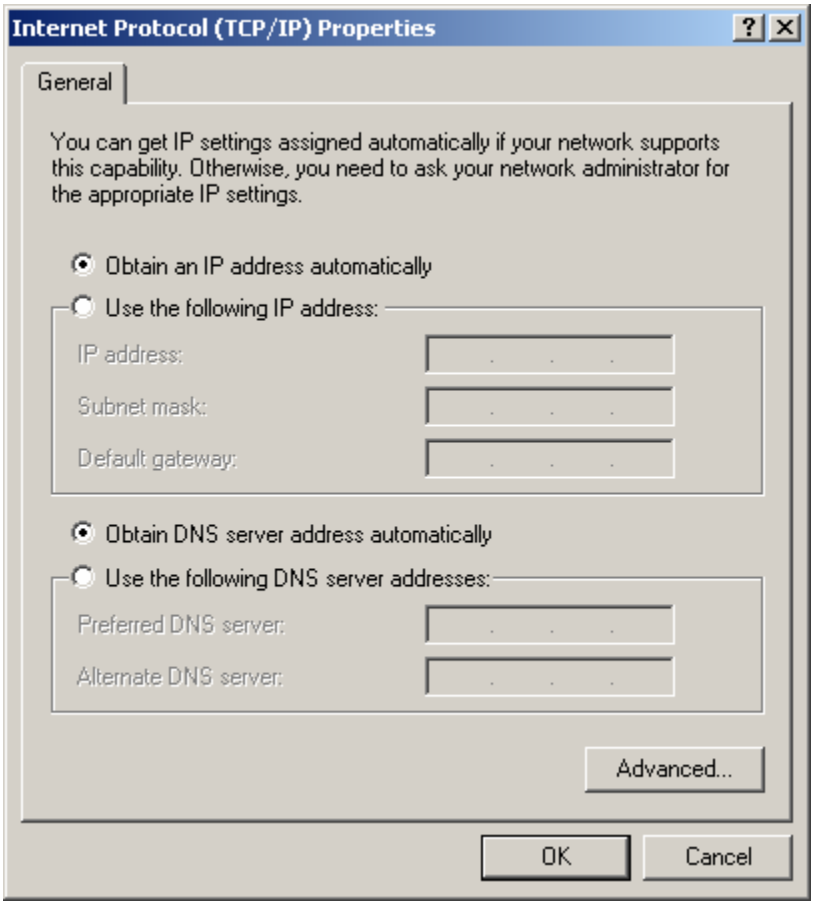
Step 3: Highlight the icon Local Area Connection, right click your mouse, Click Properties



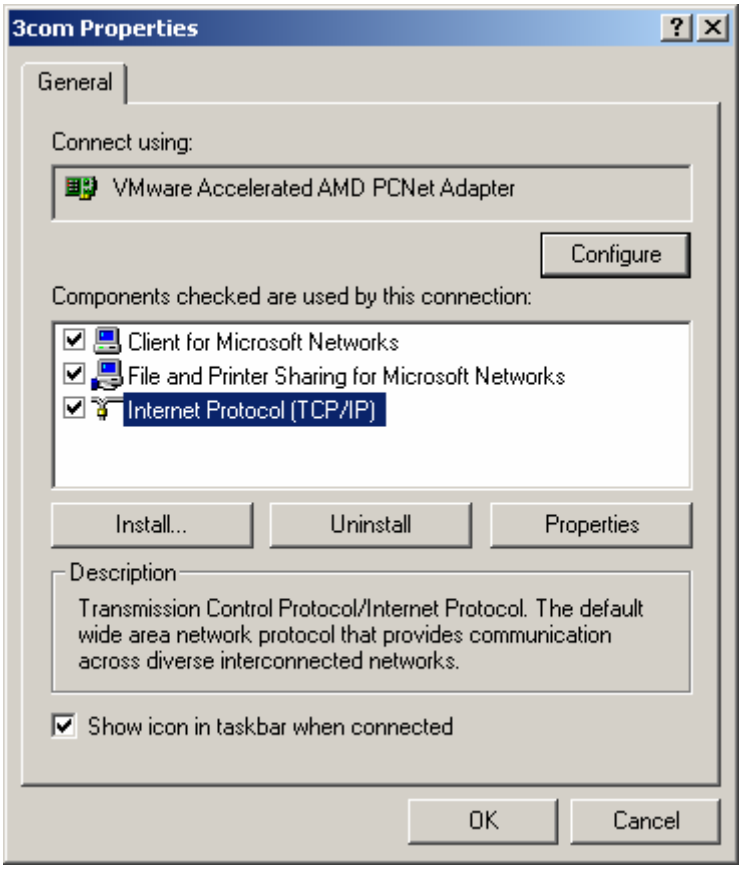
Step 4: Highlight Internet Protocol (TCP/IP), then press Properties button



Step 5: Choose Obtain an IP address automatically and Obtain DNS Server Address automatically, and then press OK to close the Internet Protocol (TCP/IP) Properties window.



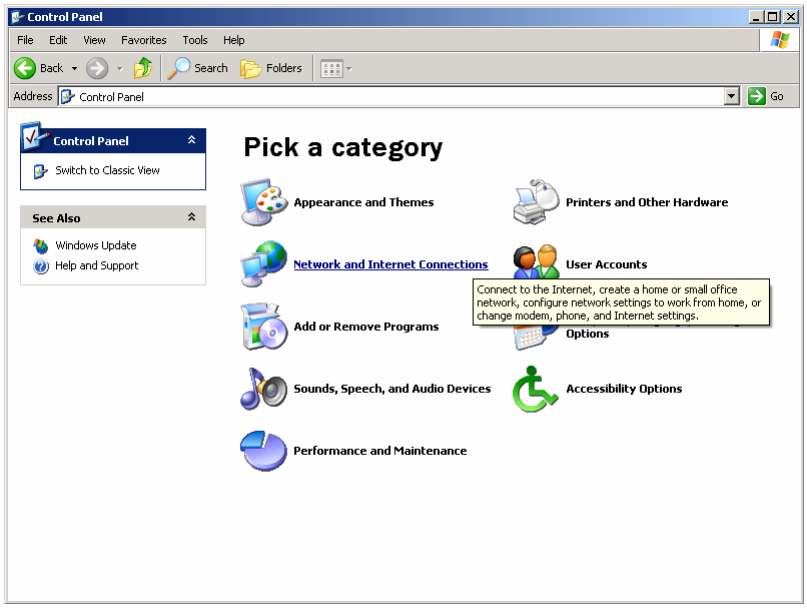
Step 6: Press OK to close the Local Area Connection Properties window



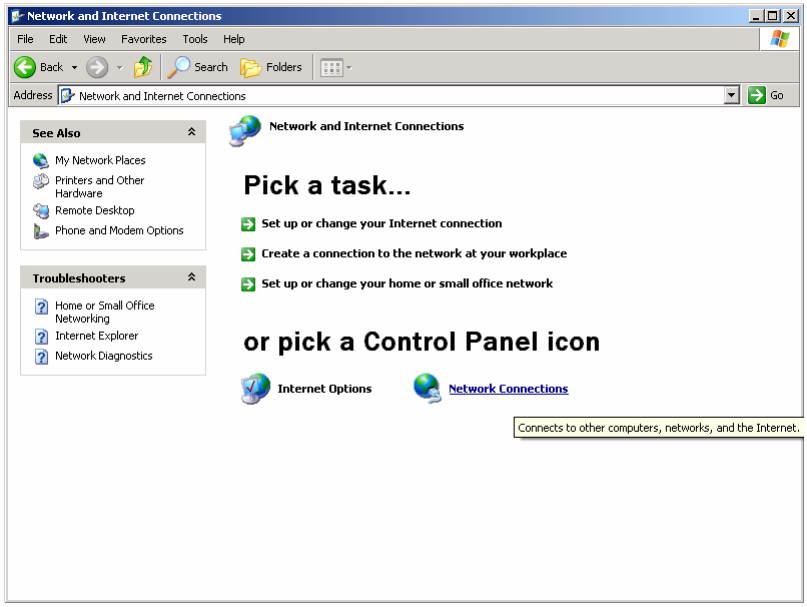
3.1.2 Windows XP/2003

Step 1: Go to Start → Settings → Control Panel

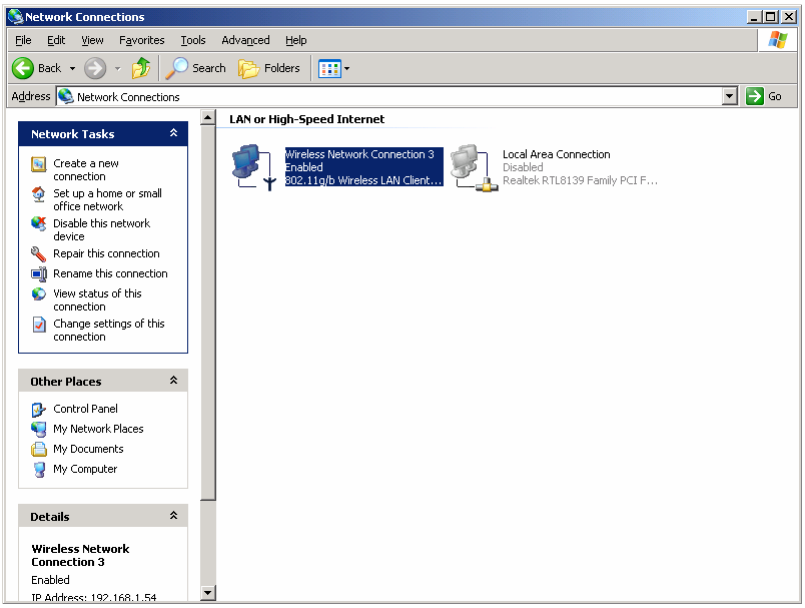
Step 2: Click Network and Internet Connections



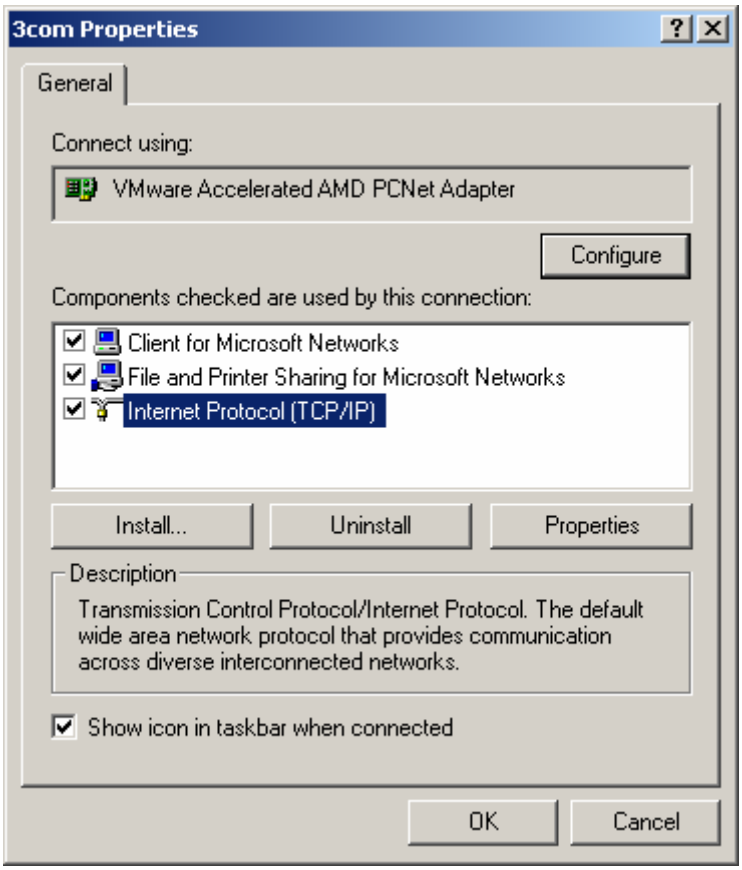
Step 3: Click Network Connections



Step 4: Highlight the icon Local Area Connection, right click your mouse, Click Properties

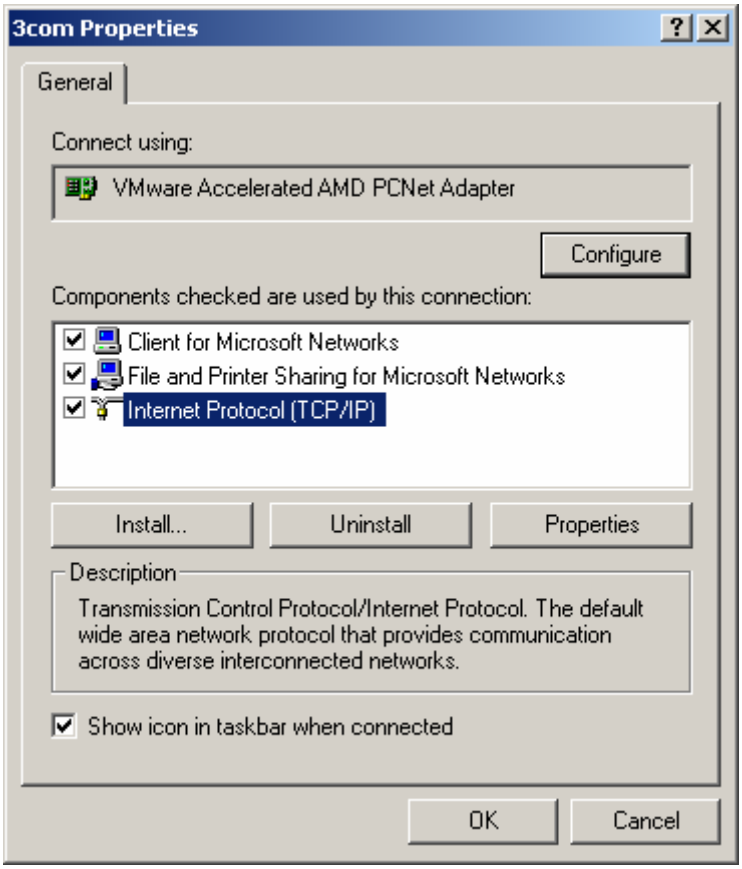


Step 5: Highlight Internet Protocol (TCP/IP), then press Properties button



Step 6: Choose Obtain an IP address automatically and Obtain DNS Server address automatically, and then press OK to close the Internet Protocol (TCP/IP) Properties window.

Step 7: Press OK to close the Local Area Connection Properties window



3.2 Additional Settings for Wireless Client

If you chose to access the router via a wireless client, also verify the following:

Step 1: Make sure your PC is equipped with 802.11g or 802.11b wireless adapter and has appropriate WLAN card driver/utility and TCP/IP installed.

Step 2: Set the wireless adapter to use appropriate TCP/IP settings as described in previous section.

Step 3: Launch the wireless adapter's provided utility and verify that your wireless client is configured with these settings:

- Operation Mode: Infrastructure
- SSID: default
- Authentication: Disabled
- Encryption: Off
- Radio Band: 802.11B/G

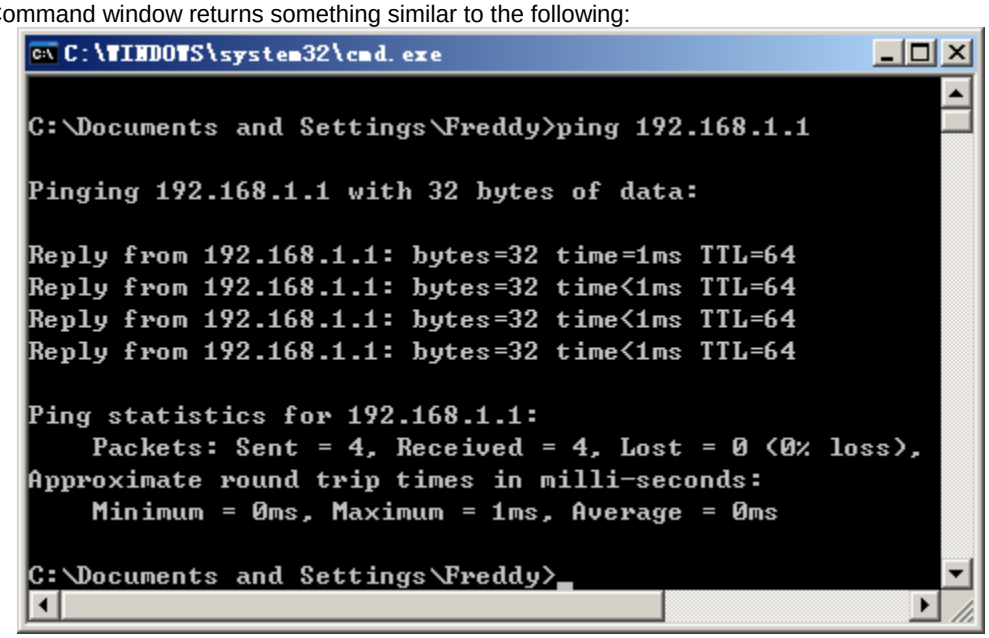
⚠	If you only finished the wireless settings and didn't configure the wireless adapter's TCP/IP settings, even your link status indicates a successful connection with the AP. This connection applies to the "physical" network layer only. Your wireless adapter cannot communicate with the AP. Make sure to set the TCP/IP properties as described in this previous section.

3.3 Checking PC's IP and Connection with the Router

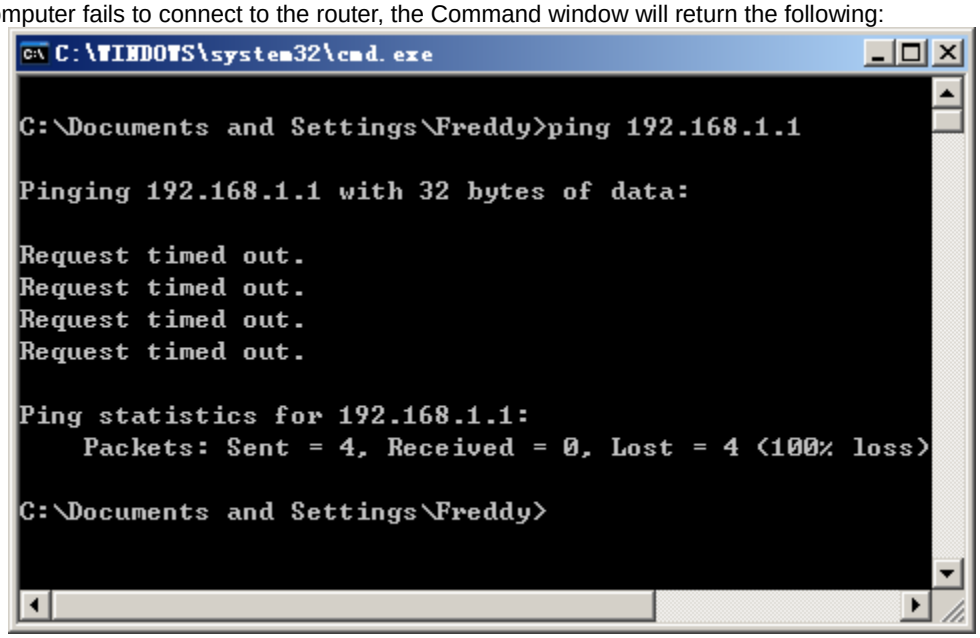
After configuring the TCP/IP protocol, use the ping command to verify if the computer can communicate with the Router. To execute the ping command, open the DOS window and PING the IP address of the Wireless Broadband Router at the DOS prompt:

- For Windows 98/Me: Start -> Run. Type **"command"** and click OK.
- For Windows 2000/XP: Start -> Run. Type **"cmd"** and click OK.

At the DOS prompt, type the following command:
If the Command window returns something similar to the following:



Then the connection between the router and your computer has been successfully established.
If the computer fails to connect to the router, the Command window will return the following:



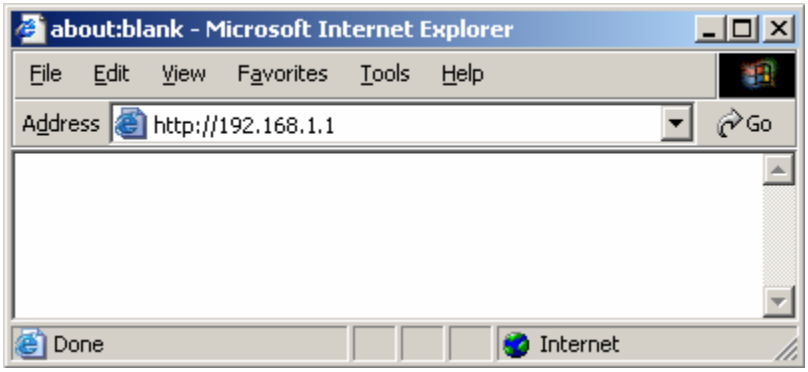
Verify your computer's network settings are correct and check the cable connection between the router and the computer.

Chapter 4 Web Configuration

Web configuration provides a user-friendly graphical user interface (web pages) to manage your WRT-416. An AP with an assigned IP address (e.g. http://192.168.1.1) will allow you to monitor and configure (via web browser e.g., MS Internet Explorer or Netscape).

1. Open your web browser.

2. Enter WRT-416 IP address (default IP address is http://192.168.1.1) into the address field of the web browser. Please also make sure your PC's IP address is in the same IP range with WRT-416.



If the router's LAN port has been changed with new IP address, enter the new IP address instead.

3. A User Name and Password dialog box will appear. Please enter your User Name and Password here. The User Name and Password are "guest" by default. Click "OK" the management page.

Don't forget to change the Password in configuration's Authentication to ensure the security. When first configuring your router, it is recommended that you have an Ethernet cable connected to the router. Performing the INITIAL configuration using a wireless connection is not secure and is not recommended. After you have finished the initial configuration of the router, your connection will be secure and you can safely use either a wired or wireless connection.

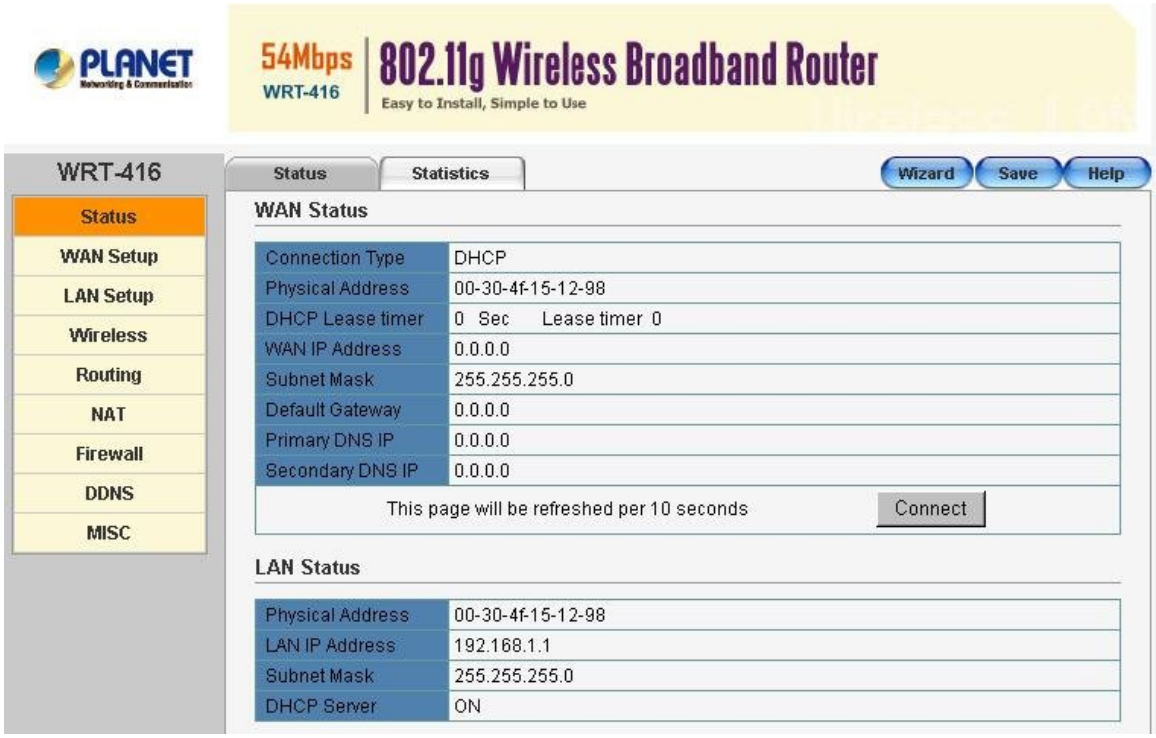
On every page of the Wireless Router, the left navigation bar shows the main options to configure the system. In the right navigation screen is the summary of system status for viewing the configurations. You can usually get context sensitive help by clicking on the Help link at the top right of the page.

To apply any settings you've altered on any page, click the Save button. Otherwise you change settings would be lost after the Router reboot.

4.1 Status

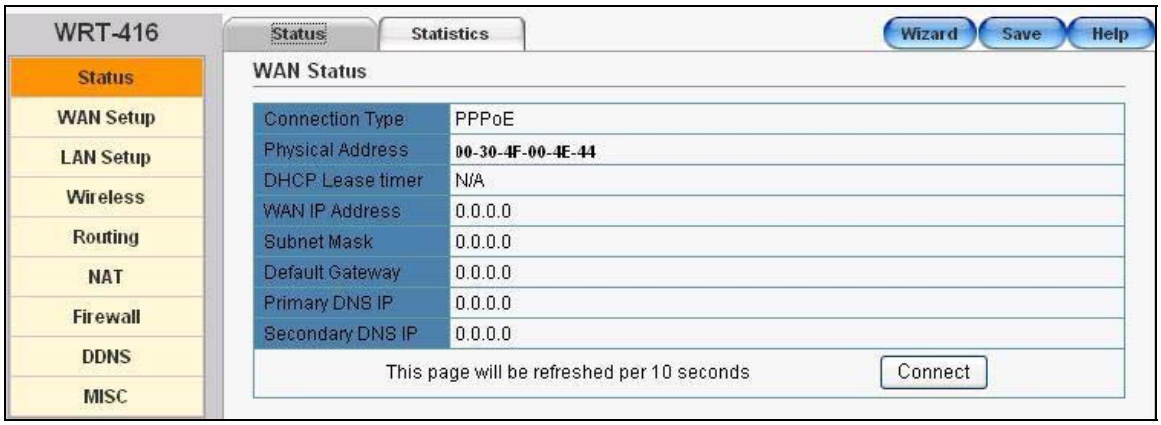
4.1.1 System Status

This page shows most of the basic configuration parameters of the Router. It is the first page shown after login.

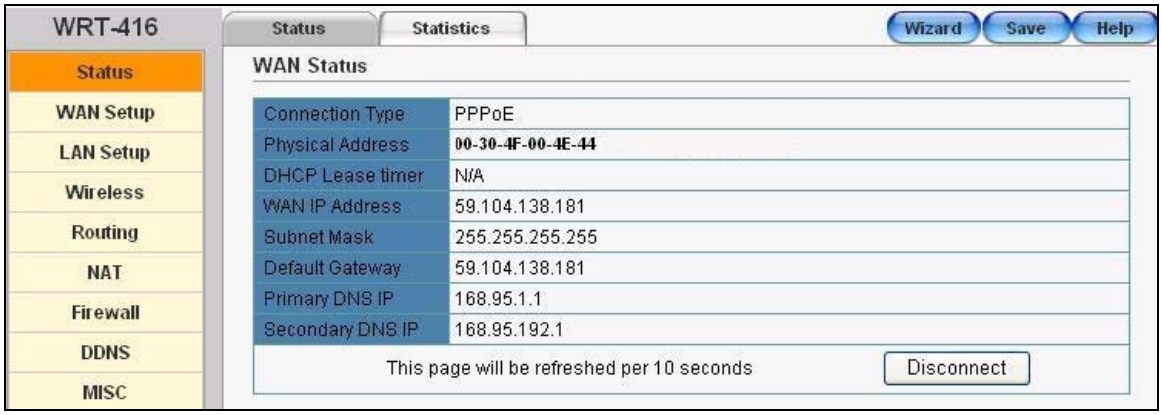


- **WAN Status:** This section shows the WAN interface parameters of the wireless router. This includes information such as:
  Connection type (DHCP, PPPoE or Static IP)
  The MAC address of WAN interface
  IP/Subnet Mask
  Default Gateway
  Primary DNS
  Backup DNS

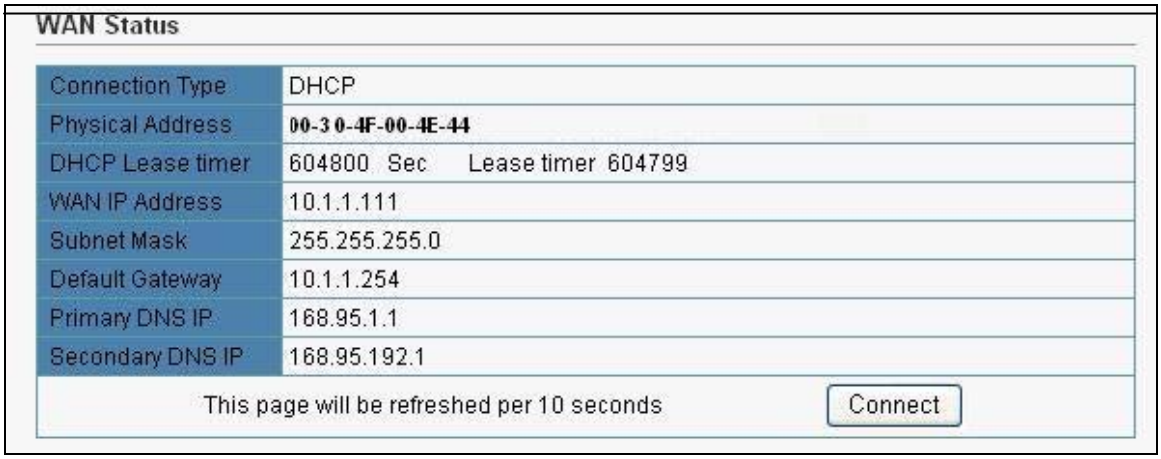
  PPPoE: In PPPoE mode, if you want to start a connection, click on the “Connect” button to build a PPPoE session.



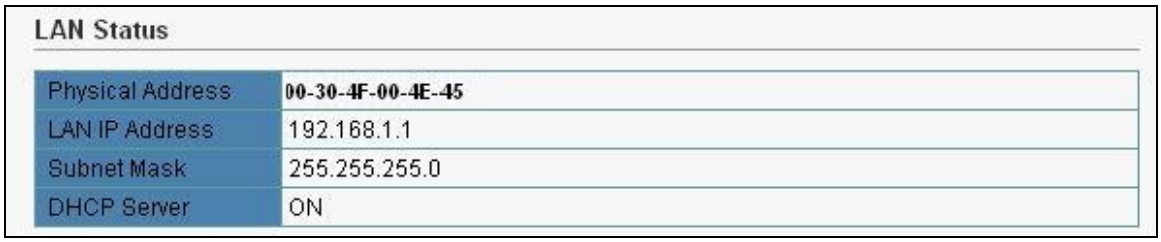
To terminate the connection, click on the “Disconnect” button.



DHCP: In DHCP mode, press "Disconnect" button to release IP address and press "Connect" button to renew IP address.



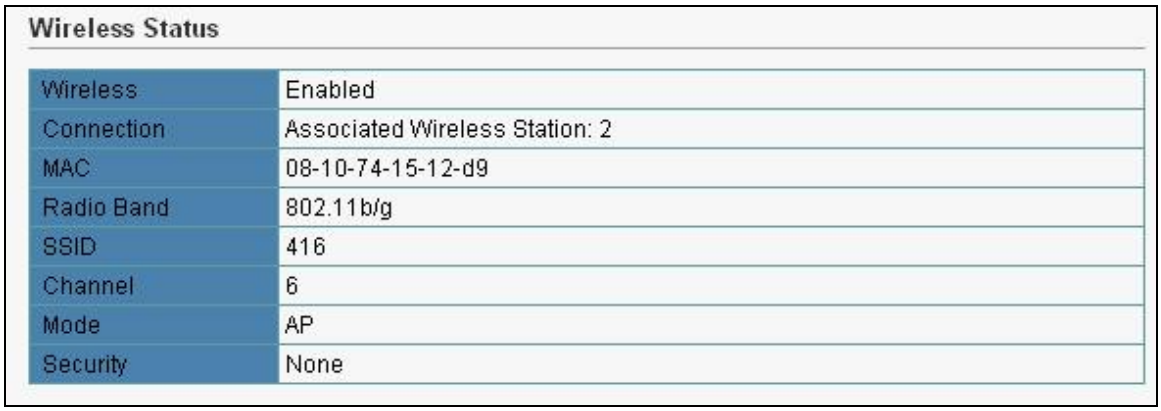
- **LAN Status:** This section shows the LAN interface parameters of the wireless router. This includes information such as:
  The MAC address of LAN interface
  IP/Subnet Mask
  DHCP Server status



LAN Status

Physical Address	00-30-4F-00-4E-45
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	ON

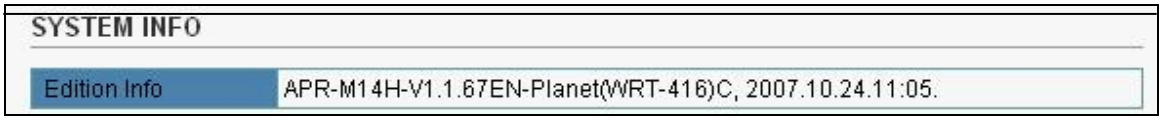
- **Wireless Status:** This section shows the WLAN interface parameters of the wireless router. This includes information such as:
  Wireless status
  Connection status
  The MAC address of WLAN interface
  Radio Band
  SSID
  Channel number
  Security mode



Wireless Status

Wireless	Enabled
Connection	Associated Wireless Station: 2
MAC	08-10-74-15-12-d9
Radio Band	802.11b/g
SSID	416
Channel	6
Mode	AP
Security	None

- **System Information:** This section shows the installed version of the firmware of the WRT-416.

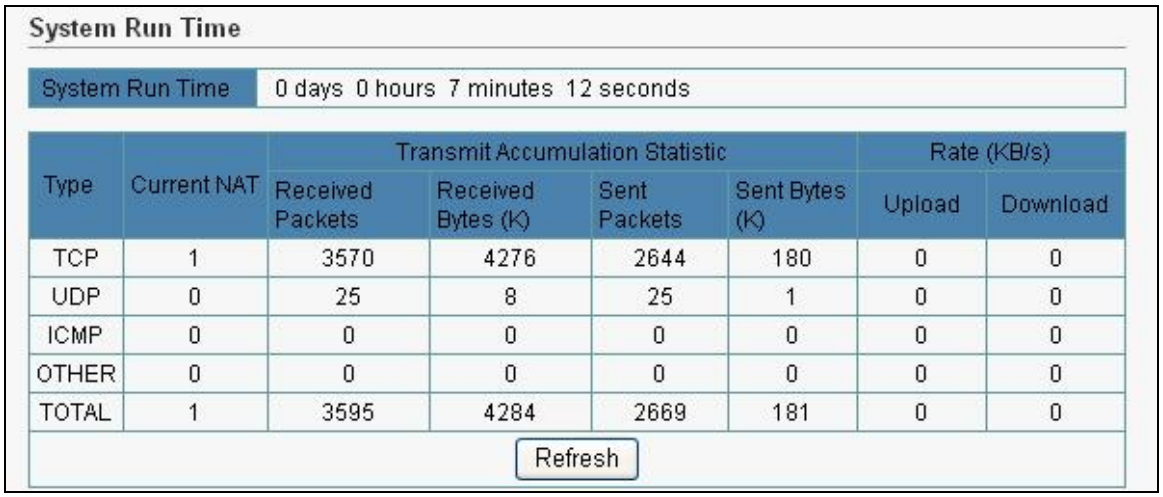


SYSTEM INFO

Edition Info	APR-M14H-V1.1.67EN-Planet(WRT-416)C, 2007.10.24.11:05.

4.1.2 Statistics

The statistics tab contains following items for monitoring network traffic between interface of types external (WAN) and internal (LAN and WLAN), and display System Run Time.



System Run Time

System Run Time	0 days 0 hours 7 minutes 12 seconds

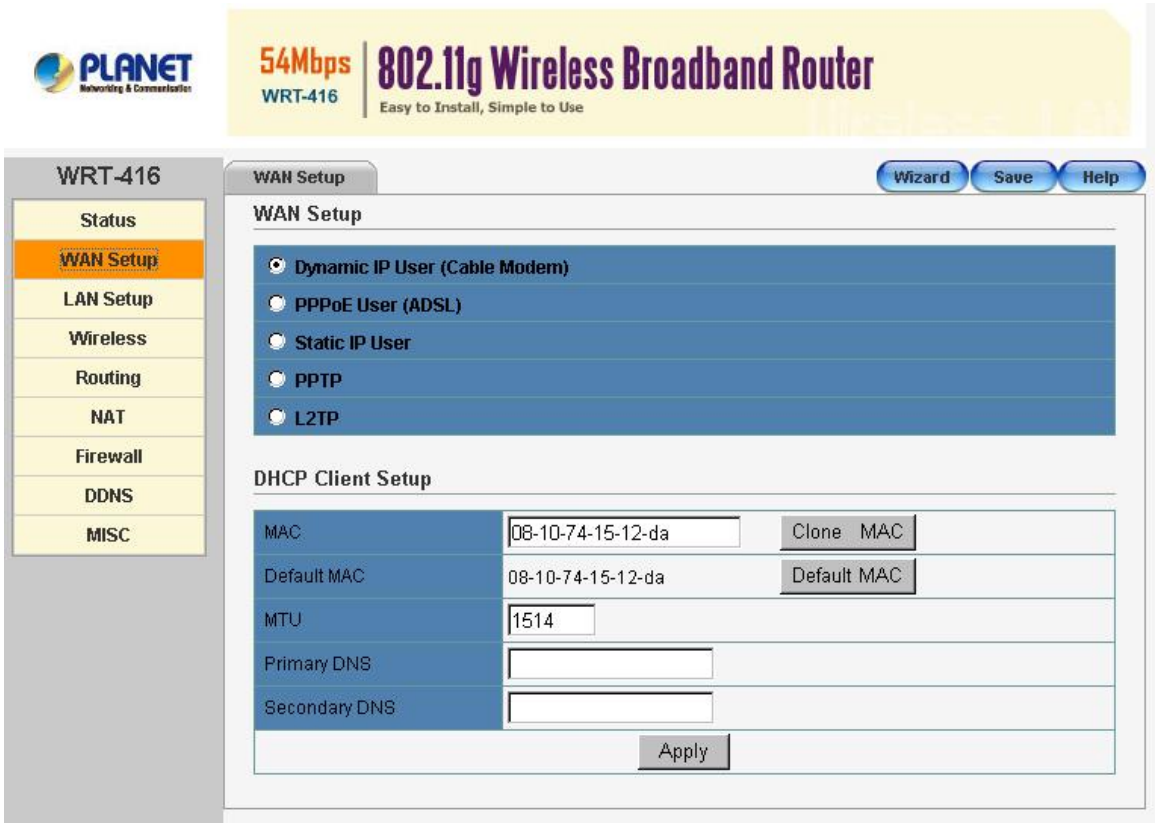
Type	Current NAT	Transmit Accumulation Statistic				Rate (KB/s)	
		Received Packets	Received Bytes (K)	Sent Packets	Sent Bytes (K)	Upload	Download
TCP	1	3570	4276	2644	180	0	0
UDP	0	25	8	25	1	0	0
ICMP	0	0	0	0	0	0	0
OTHER	0	0	0	0	0	0	0
TOTAL	1	3595	4284	2669	181	0	0

Refresh

- **System Run Time:** Display the active duration since system start up.
- **Statistics:** You can monitor current sent & received packets counters of wireless and Ethernet networks .To see the latest information, click “Refresh” button.

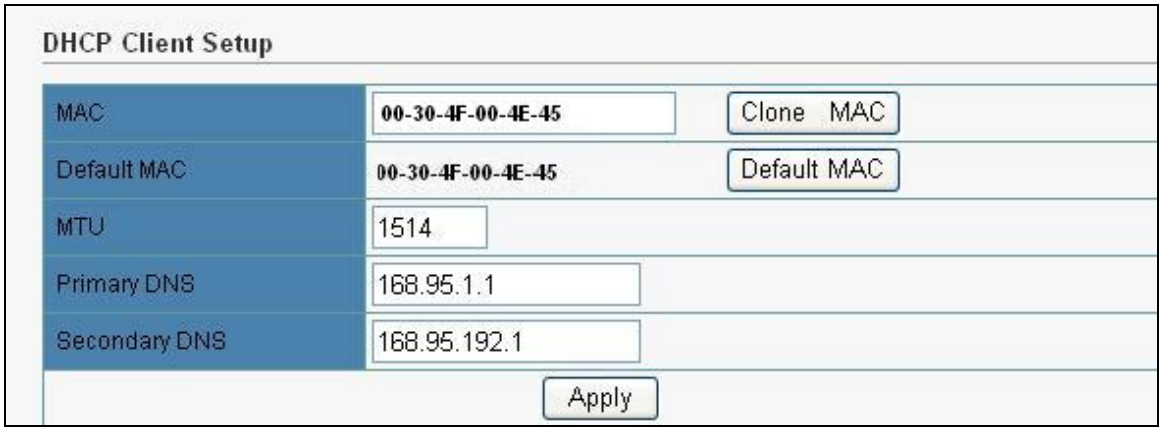
4.2 WAN Setup

The WAN Setup screen allows you to specify the Internet type. Select the appropriate connection mode according to your ISP (Internet Service Provider).



4.2.1 Dynamic IP Address

This is the default setting for the router. DHCP is most commonly used for cable modem connections. There is no configuration necessary for this setting because the ISP will automatically supply the information. Choose this type while Cable mode is used.

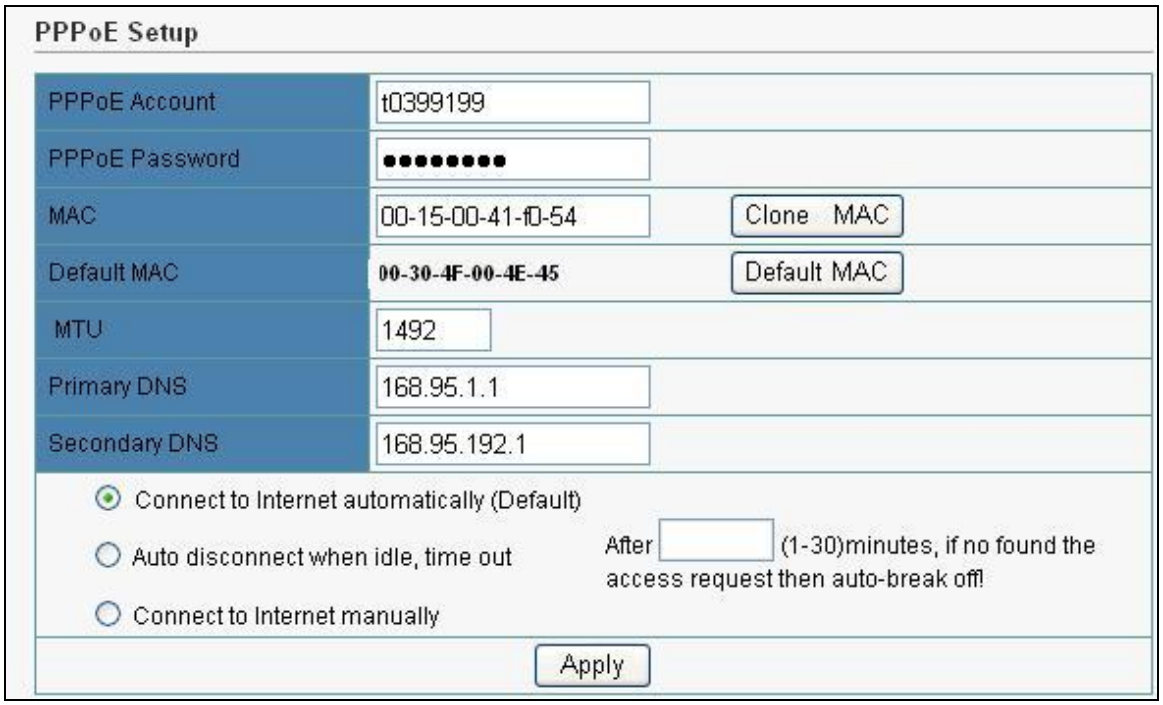


- **Clone MAC**: Your ISP may require a particular MAC address in order for you to connect to the Internet only. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in your PC's MAC address in this section to replace the WAN MAC address of WRT-416 (you have to be using that PC for the Clone MAC Address button to work).
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The recommended size, entered in the Size field, is 1496. You should leave this value in the 1200 to 1500 range.
- **DNS**: Check "DNS" and enter the IP address to specify DNS server for LAN DHCP server.

Click "Apply" to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

4.2.2 PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to obtain all necessary information.



- **PPPoE Account**: Enter the User Name provided by your ISP for the PPPoE connection
- **PPPoE Password**: Enter the Password provided by your ISP for the PPPoE connection
- **Clone MAC**: Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The default value of MTU is 1492 and use 1300 while the line condition is bad.
- **DNS**: Check "DNS" and enter the IP address to specify DNS server for LAN DHCP server.
- **Connection Type**: Select your PPPoE connection from these options:

  Connect to Internet automatically: This feature will keep your Internet connection always alive. The Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to Auto Connect.

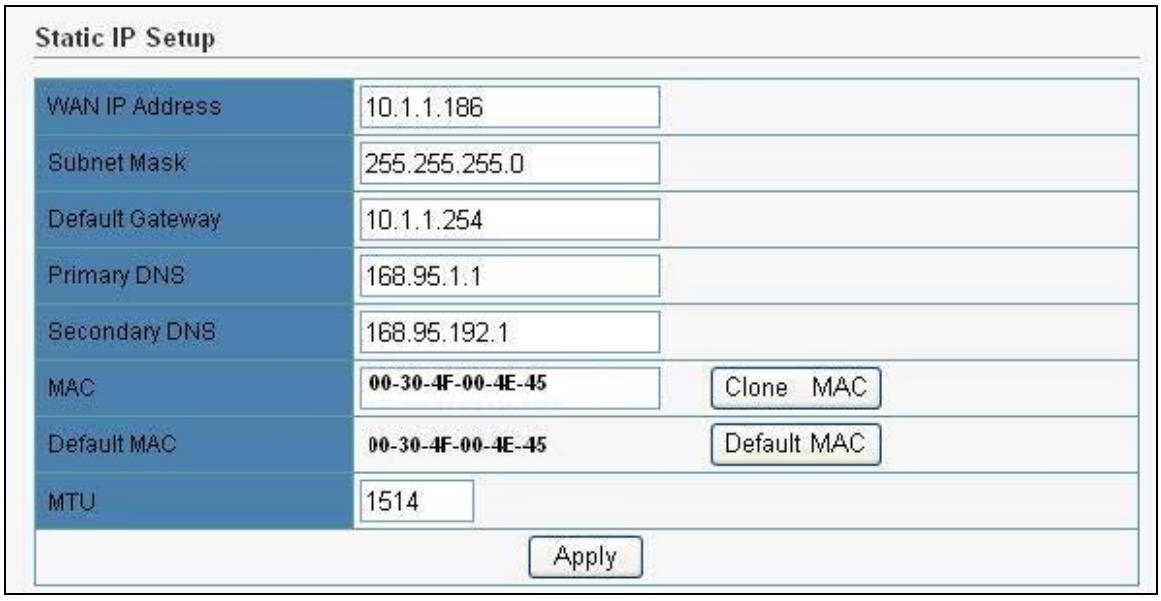
  Auto disconnect when idle, time out: If enabled, the router will trigger a PPPoE session for connection to the Internet if any client PC on your WLAN/LAN sends out a request for Internet access. However, the router automatically disconnects the PPPoE session after the WAN connection has been idle for the amount of time you specified in the timeout box. If your Internet account is billed based on the amount of time of your Internet connection, you probably want to enable this option and enter an idle time value best suitable for your network. To use this option, click the radio button next to Connect on demand.

  Connect to Internet manually: The router will connect to Internet while click the "Connect" button on the Web. And the WAN connection will disconnect. If you click "Disconnect" manually from the Web user interface. The router will not auto-connect to the Internet. To use this option, click the radio button next to Connect on demand.

Click "Apply" to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

4.2.3 Static IP

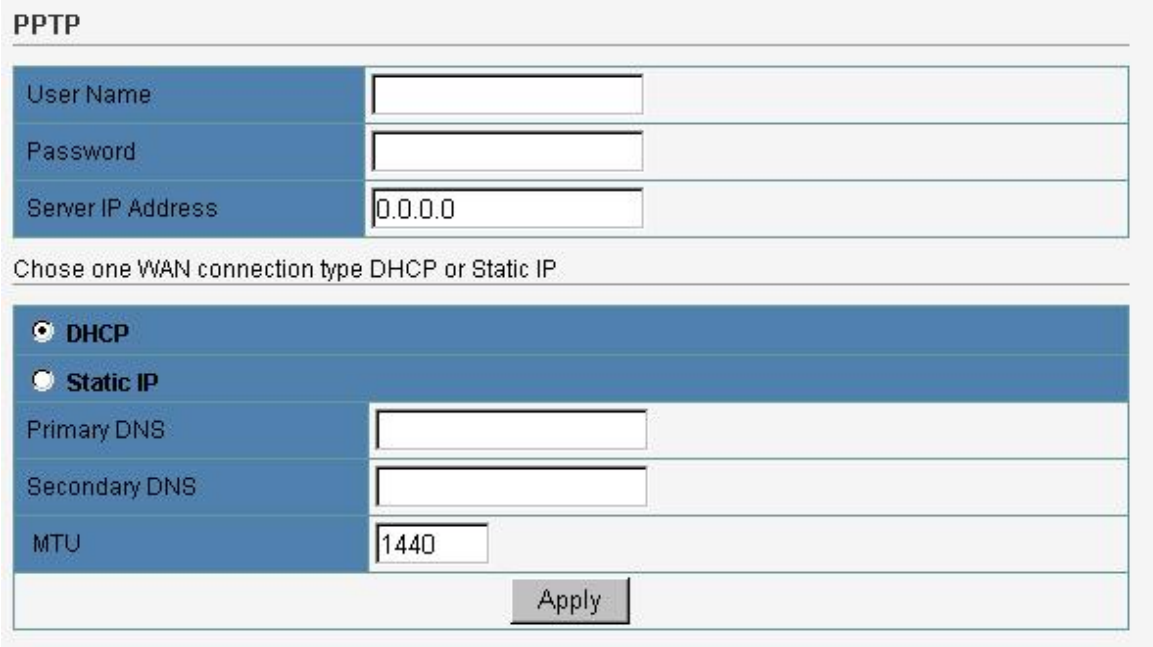
If you are required to use a permanent IP address to connect to the Internet, select Static IP.



- **WAN IP Address**: This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.
- **Subnet Mask**: This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- **Default Gateway**: Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.
- **Physical Address Clone**: Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The recommended size, entered in the Size field, is 1496. You should leave this value in the 1200 to 1500 range.
- **DNS**: Check "DNS" and enter the IP address to specify DNS server for LAN DHCP server.

Click "Apply" to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

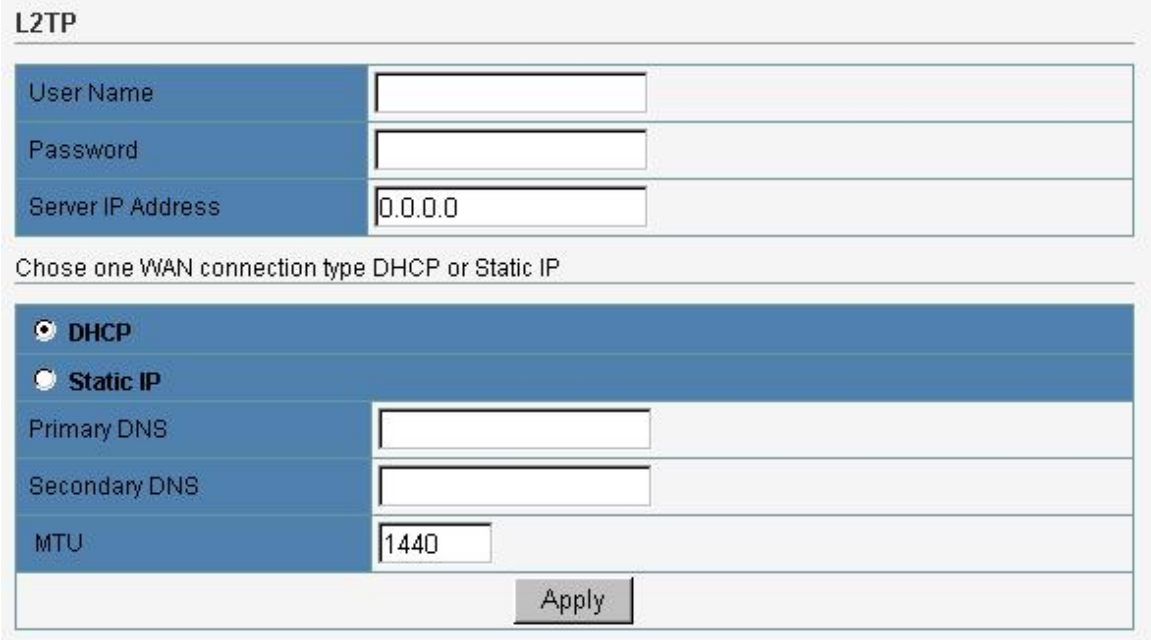
4.2.4 PPTP



- **User Name:** Type your PPTP account.
- **Password:** Type your PPTP password.
- **Server IP Address:** Type the IP address of server which offers Internet service. Your ISP will provide you with this information.
- **DHCP / Static IP:** Select the IP assignment method.
- **IP Address:** Type the IP address which your ISP provides.
- **Subnet Mask:** Type the Subnet Mask which your ISP provides.
- **Gateway:** Type the IP address of Gateway which your ISP provides.
- **Primary/Secondary DNS:** Type the IP address of DNS server which your ISP provides.
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The recommended size, entered in the Size field, is 1440.

Click “Apply” to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

4.2.5 L2TP



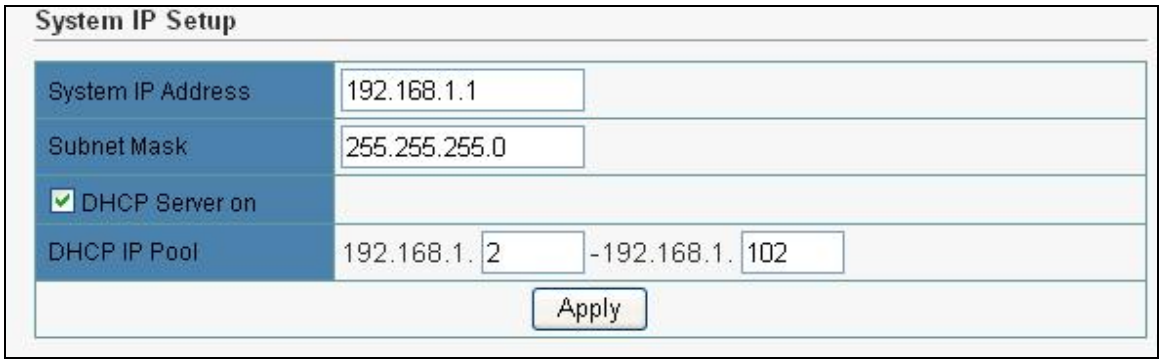
- **User Name:** Type your L2TP account.
- **Password:** Type your L2TP password.
- **Server IP Address:** Type the IP address of server which offers Internet service. Your ISP will provide you with this information.
- **DHCP / Static IP:** Select the IP assignment method.
- **IP Address:** Type the IP address which your ISP provides.
- **Subnet Mask:** Type the Subnet Mask which your ISP provides.
- **Gateway:** Type the IP address of Gateway which your ISP provides.
- **Primary/Secondary DNS:** Type the IP address of DNS server which your ISP provides.
- **MTU**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The recommended size, entered in the Size field, is 1440.

Click “Apply” to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

4.3 LAN Setup

4.3.1 LAN Setup

The Wireless Broadband Router communicates with the wired/wireless clients through its LAN port. The LAN configuration page allows you to define the private IP address and DHCP server settings over the LAN interface.



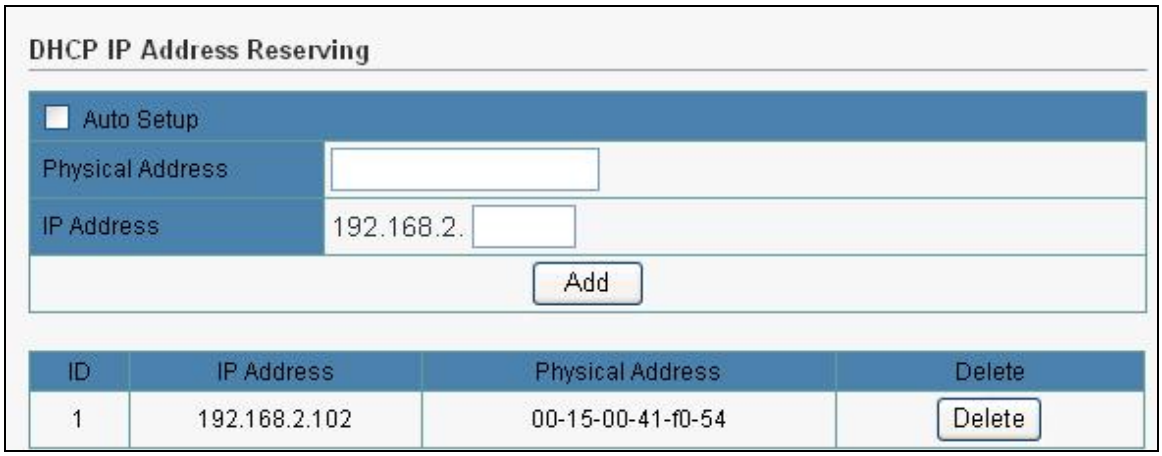
- I**P Address/Subnet Mask**: Enter the IP address and subnet mask for the Wireless Broadband Router LAN port. All local wired/wireless devices communicate with the device through this port. By default, the IP address and subnet mask of the LAN port is 192.168.1.1 and 255.255.255.0 respectively.
- **DHCP Server**: The DHCP server can be ON or OFF in this screen. If you choose to set this device as a DHCP server, it will assign IP addresses to its clients. The DHCP pool range is also changeable.

Click “Apply” when you have finished the configuration above. And the wireless router will be automatically restarted if you change the LAN IP address.

If you change the private IP address and apply the changes, the PC from which you configure the router will lose the communication to the router. To reconnect, you will need to renew the IP address of the PC or change to an IP address compatible with the new LAN port IP address.

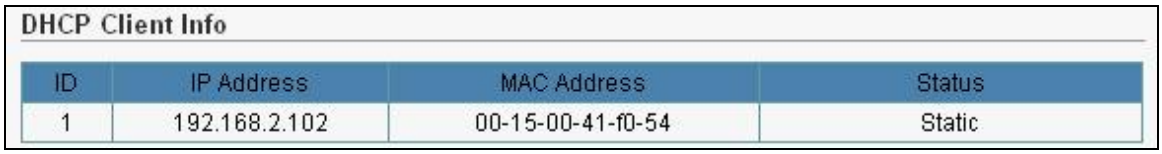
4.3.2 DHCP IP Address Reserving

Set the IP address you want to reserve for specified station here.



4.3.3 DHCP Info

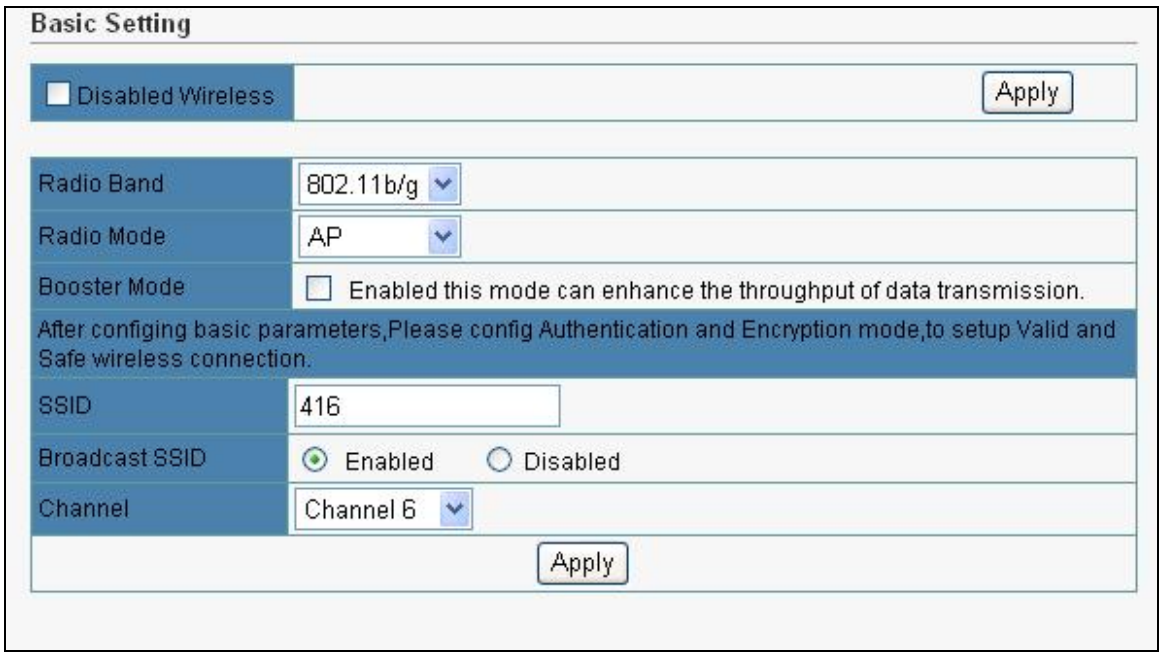
You can View all the pc which connect to the Wireless Router by DHCP here.



4.4 Wireless

The WRT-416 implements Access Point capability, which connects wireless clients to a wired LAN. It allows wireless stations to access network resources and share the broadband Internet connection.

4.4.1 Basic Settings



- **Radio Band**: The default setting is mixed mode [802.11B/G]. If you do not know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11G if you have only 11G card. If you have only 802.11 B card, then select 802.11B.
- **Radio Mode**: The Route has 3 modes: AP, WDS, AP+WDS. If WDS or AP+WDS is selected, please go to WDS tab to complete related settings.
- **Booster Mode**: Enabled this mode can enhance the throughput of data transmission.
- **SSID**: The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (default) to a unique name.
- **Channel**: Select the channel used for wireless communication. There are 11 overlapping channels. Channels 1, 6 and 11are non-overlapping. The default is channel 6.

Click “Apply” when you have finished the configuration above.

Please setup authentication and Encryption mode to setup Valid and Safe wireless connection after setting Basic Wireless parameters.

4.4.2 Security

This wireless router provides complete wireless LAN security functions; include WEP, WPA with pre-shared key and WPA2 with pre-shared key. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

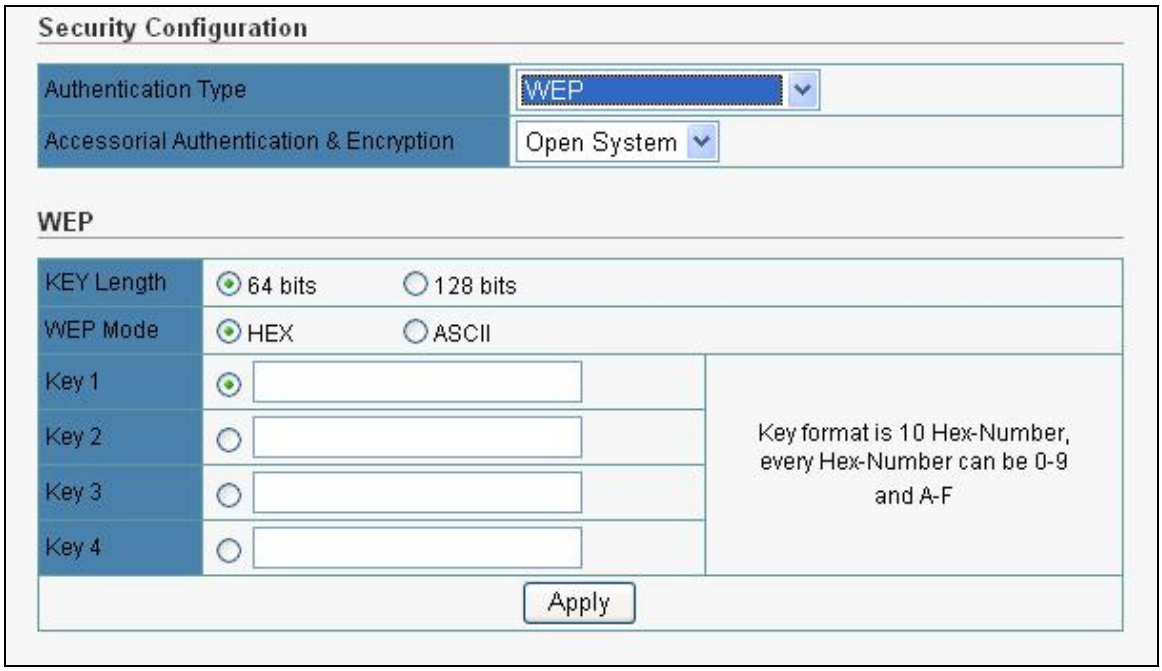
4.4.2.1 None

Transmit data without encryption and authentication. This is the default option.

If you select none, any data will be transmitted without Encryption and any station can access the wireless router.

4.4.2.2 WEP

WEP (Wired Equivalent Privacy) is an encryption method used to protect your wireless data communications. WEP uses a combination of 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission.



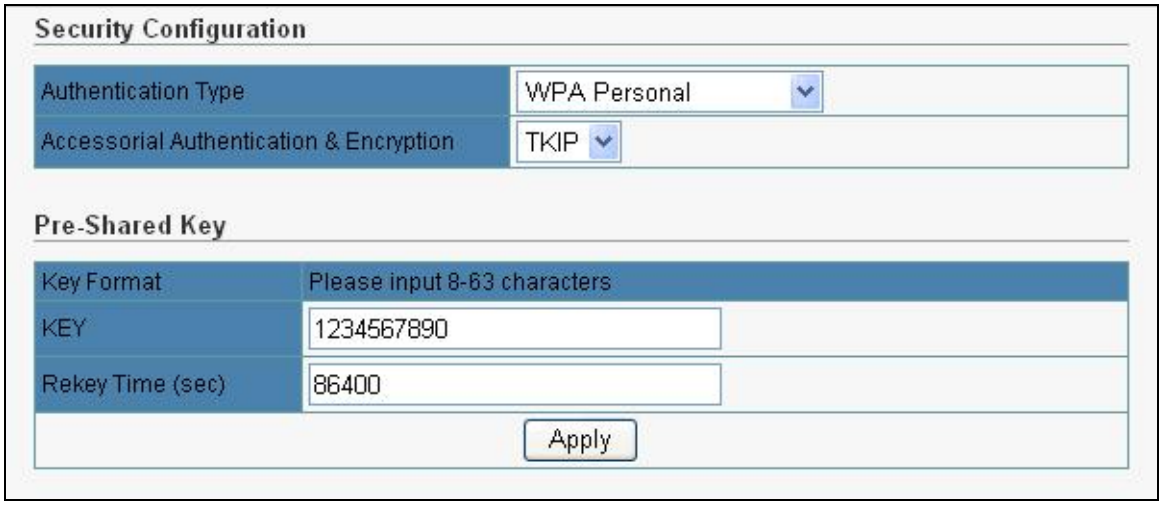
- **Open-System**: No authentication is used. But uses WEP encrypt data packets.
- **Share-keys**: Authentication is a process in which the AP validates whether the wireless client is qualified to access the AP's service. You must enable WEP function and define your WEP keys. The keys are used both to authenticate wireless clients and encrypt outgoing data.
- **Auto-Select**: It can detect Wireless Client authentication information, and automatically choose Open-System or Share-Keys mode to communicate with client. When use Auto-Select mode, you must setup WEP keys which are used by authentication system.
- **WEP Length**: Selects 64-bit or 128-bit WEP encryption. Be sure that the key length setting in the AP shall be the same as in wireless clients, or the communication will not work.
- **WEP Mode**: You may select to select ASCII Characters or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.
- **Default Key**: The Key selected here must match the key selected in the client. For example, if you select Key 1 here you have to select Key 1 for the client. The default is 1.
- **Key 1~4**: Enter one to four WEP keys in either ASCII or Hexadecimal format. You can use 64 bits or 128 bits as the encryption algorithm.
  Enter one to four WEP keys in either ASCII or Hexadecimal format. You can use 64 bits or 128 bits as the encryption algorithm.
  Note that when using Hexadecimal format, only digits 0-9 and letters A-F, a-f are allowed. Valid key length for each encryption type is as below:

Key Length	HEX Format	ASCII Format
64 Bit	10 hexadecimal digits	5 ASCII characters
128 Bit	26 hexadecimal digits	13 ASCII characters

Click "Apply" at the bottom of the screen to save the above configurations.

4.4.2.3 WPA Personal

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP and AES to change the encryption key frequently. This can improve security very much.

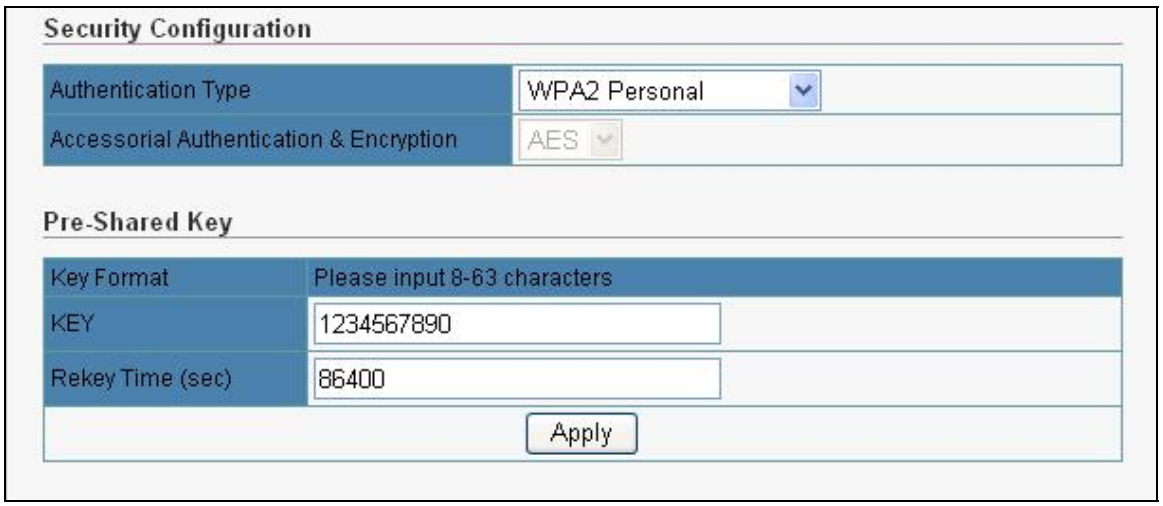


- **TKIP**: Temporal Key Integrity Protocol (TKIP) utilizes a stronger encryption algorithm and includes Message Integrity Code (MIC) to provide protection against hackers.
- **AES**: Advanced Encryption System (AES) utilizes a symmetric 128-Bit block data encryption. It's the strongest encryption currently available.
- **WPA Pass Phrase**: The WPA Pass Phrase is used to authenticate and encrypt data transmitted in the wireless network. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Rekey Time (sec)**: Specifies the timer the WPA key must changes. The change is done automatically between the server and the client. The default value is 86400.

Click "Apply" at the bottom of the screen to save the above configurations.

4.4.2.4 WPA2 Personal

The WPA2 is a stronger version of WPA. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses AES to change the encryption key frequently. This can improve security very much.



- **AES**: Advanced Encryption System (AES) utilizes a symmetric 128-Bit block data encryption. It's the

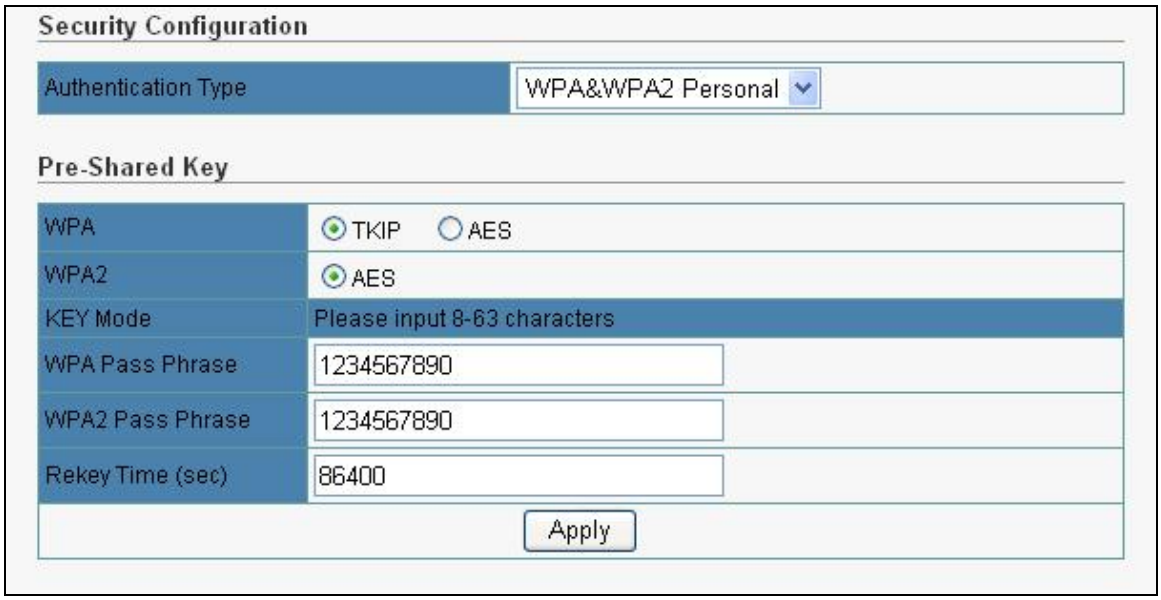
strongest encryption currently available.

- **WPA2 Personal** : The WPA Pass Phrase is used to authenticate and encrypt data transmitted in the wireless network. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Rekey Time (sec)**: Specifies the timer the WPA key must changes. The change is done automatically between the server and the client. The default value is 86400.

Click “Apply” at the bottom of the screen to save the above configurations.

4.4.2.5 WPA&WPA2 Personal

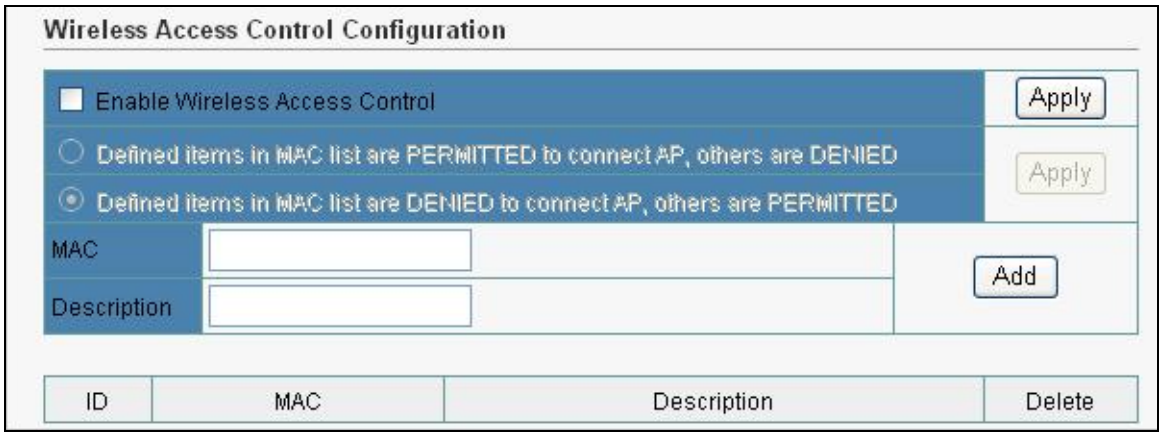
Auto-Select WPA/WPA2 can detect Wireless Client authentication information, and automatically choose WPA or WPA2 mode to communicate with client. Operation is the same as WPA or WPA2.



Click “Apply” at the bottom of the screen to save the above configurations.

4.4.3 Filter List

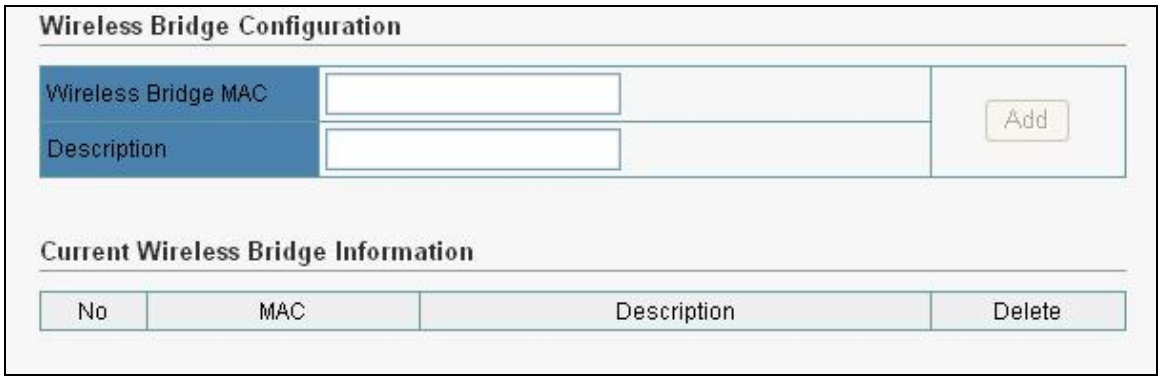
This Wireless router has the capability to control the wireless client access based on the MAC address of the wireless client. The user has the flexibility to customize your own control policy based on these options:



- **Enable Wireless Access Control**: To enable Wireless MAC Filter, select the checkbox in front of "Enable Wireless Access Control", then click the "Apply " button. The default is "disable".
- You can choose a default operation for your factual security or management consideration:
  Defined items in MAC list are PERMIT to connect AP, others are DENIED.
  Defined items in MAC list are DENIED to connect AP, others are PERMIT.
  Click "Apply" when you have selected,
- **MAC**: Enter the MAC Address of a station.
- **Description**: Enter the Comment of station.
- Click "Add", then this wireless station will be added into the" Current Access Control List" below.
- If you want to remove some MAC address, select them from the list and then click "Delete ".

4.4.4 WDS

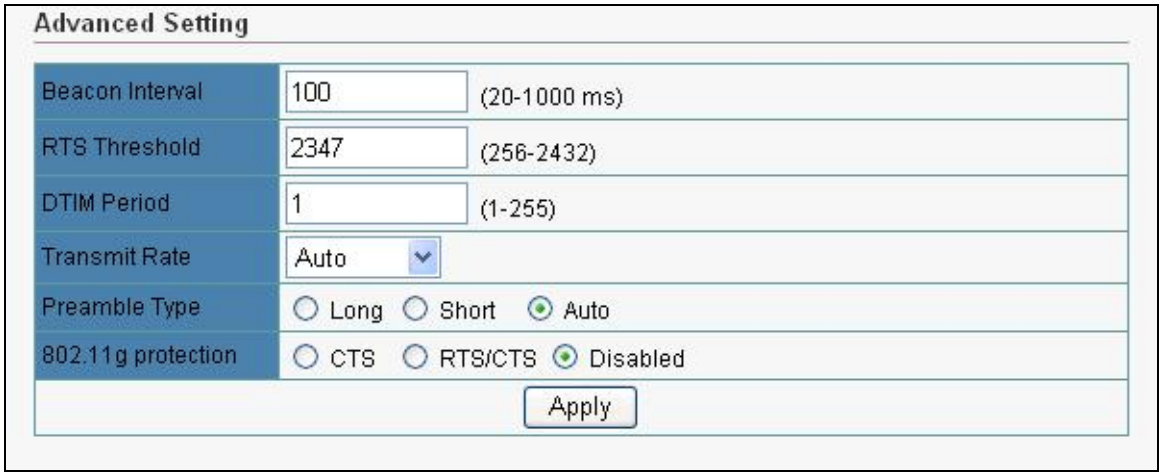
You can set the wireless Bridge MAC here. This mode is used to connect two or more WRT-416 or WAP-4036 wirelessly.



- **Wireless Bridge MAC:** If the operating mode of your WRT-416 is "WDS" or "AP+WDS", you should have a setting in Wireless Bridge MAC. Enter the MAC address of target access point. Moreover, the target access point must be "WDS" or "AP+WDS" as well.
- **Description:** Enter the Comment of station.
- **Current Wireless Bridge Information:** You can see the basic information of all wireless bridge devices. And you can delete any wireless bridge in the list.

4.4.5 Advanced

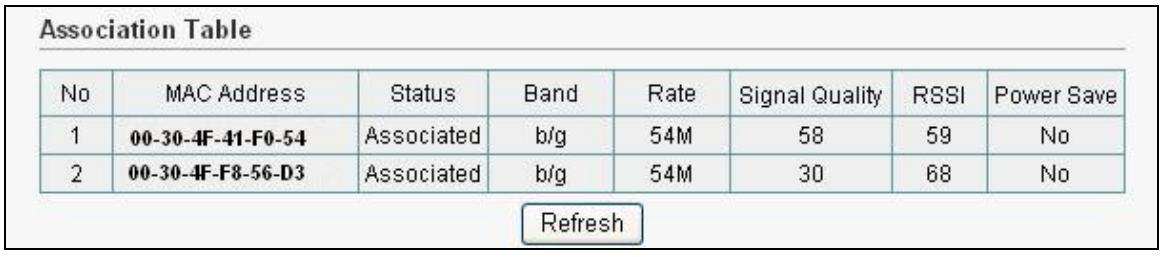
This tab is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.



- **Beacon Interval**: This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the wireless router to keep the network synchronized. A beacon includes the wireless LAN service area, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM). The default value is 100.
- **RTS Threshold**: This value should remain at its default setting of 2,347. Should you encounter inconsistent data flow, only minor modifications are recommended.
- **DTIM Interval**: This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.
- **Transmit Rate**: The "Transmit Rate "is the data packets limitation this wireless router can transmit, The wireless router will use the highest possible selected transmission rate to transmit the data packets. The default value is Auto.
- **Preamble Type**: It defines the length of CRC block in the frames during the wireless Communication. "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability

4.4.6 Association Table

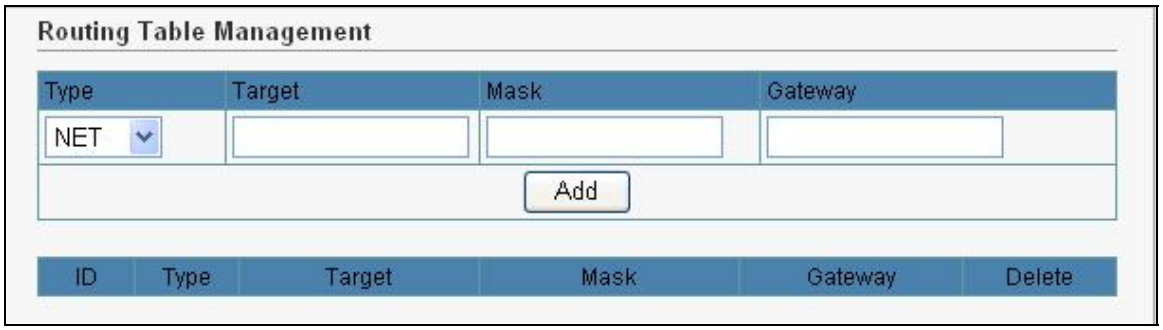
You can see the status of all active wireless stations that are connecting to the wireless router.



- To see the latest information, click Refresh button.

4.5 Routing

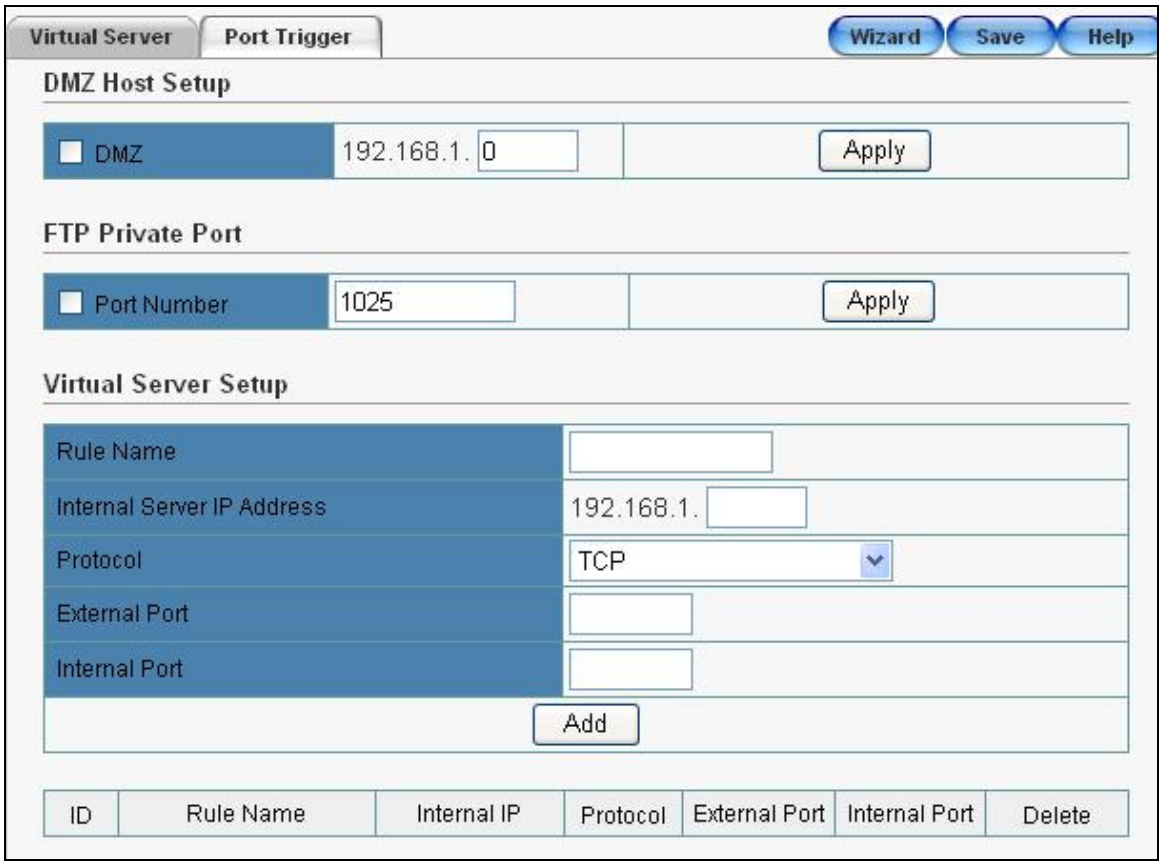
If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.



- **Type / Target / Mask / Gateway**: Fill in these fields required by this Static Routing function.
- **Add**: Fill in the all of the setting to be added and click "Add", then this Special Application setting will be added into the "Current Routing Table" below.
- **Current Routing Table**: This display shows the valid routing paths in Broadband Router. User can view the information about current routing paths
- If you want to remove some route entries from the “Current Routing Table ", select the Route entry you want to remove in the table and then click "Delete ".

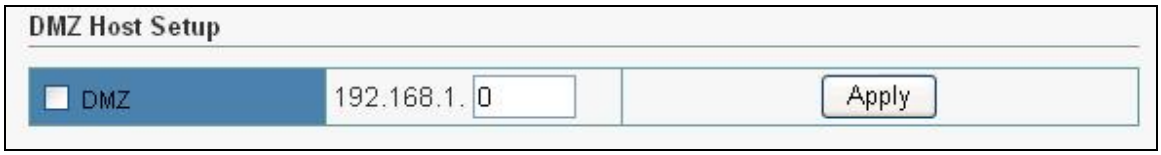
4.6 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP.



4.6.1 DMZ Host Setup

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, you can place this client to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.



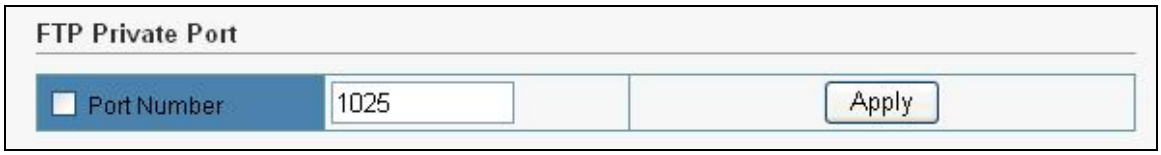
- **DMZ :** Enable/disable DMZ
- **DMZ Host:** Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above, you need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

Click “Apply” at the bottom of the screen to save the DMZ configurations.

If there is a conflict between the Virtual Server and the DMZ setting, then Virtual Server function will have priority over the DMZ function.

4.6.2 FTP Private Port

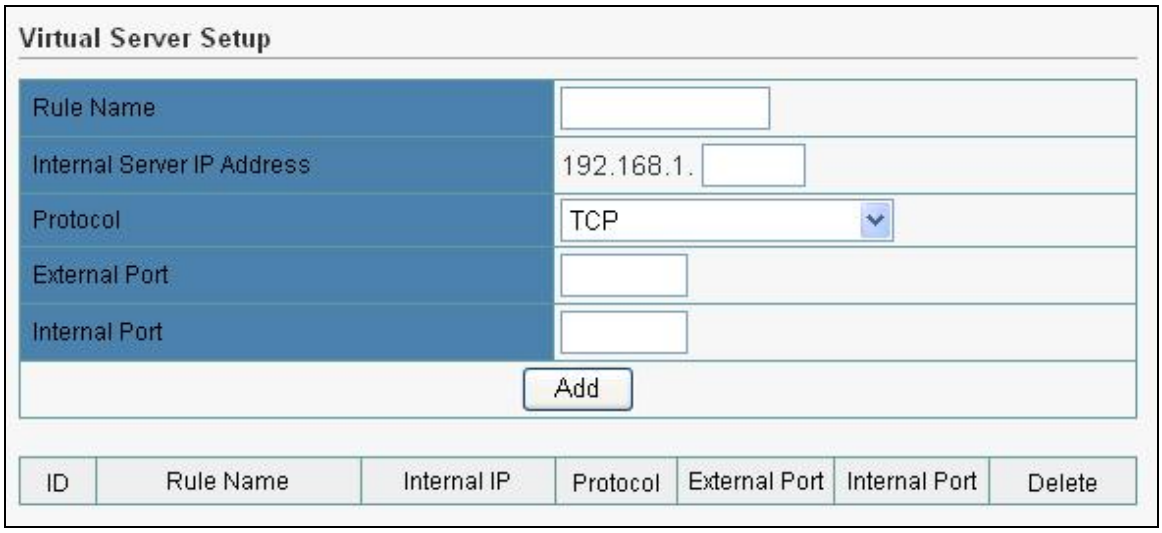
FTP private port enables user to setup FTP server which is not using the standard port 21.



- Check port number and enter the number and then press the "Apply" button to setup Private FTP port. The default Value is 1025.

4.6.3 Virtual Server Setup

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.). Computers use port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a specified LAN private IP address and its service port number.



- **Rule Name**: Define a name for this rule. It's just a string.
- **Internal Server IP**: Enter the host IP address to which the packet will be forwarded. The virtual server can be set easily by setting the internal server IP address only. You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
- **Protocol**: Chose TCP/UDP type for the packet you want to forward. If the rule existed in predefined virtual server rule, you can choose the rule.
- **External Port**: Enter the port number (The value's range is 1 to 65535) from which the packet will be on WAN.
- **Internal Port**: Enter the port number to which the packet will be forwarded on LAN
- Press "Add" button after enter the all fields to add the rule.
- Check to select the rule and press "Delete" to delete the rule.

ID	Rule Name	Internal IP	Protocol	External Port	Internal Port	Delete
1	TEST	192.168.1.100	TCP	21	21	Delete

4.6.4 Port Trigger

Port Trigger set the port you want used for some special use.

Port Triggering

Predefined Trigger Rules	Select one of the predefined rules
Rule Name	
Trigger Protocol	TCP
Trigger Port	-
Forward Protocol	TCP
Forward Port	

Add

ID	Rule Name	Trigger Condition	Forward Condition	Delete
1	WarCraft	tcp:6112	tcp:6112	Delete

- **Rule Name**: Define a name for this rule. It's just a string.
- **Trigger Protocol**: Chose TCP/UDP type for the packet you want to trigger. If the rule existed in predefined virtual server rule, you can choose the rule.
- **Trigger Port**: Enter the port number (The value's range is 1 to 65535) from which the packet will be on WAN.
- **Forward Protocol**: Chose TCP/UDP type for the packet you want to forward. If the rule existed in predefined virtual server rule, you can choose the rule.
- **Forward Port**: Enter the port number to which the packet will be forwarded on LAN
- Press "Add" button after enter the all fields to add the rule.
- Check to select the rule and press "Delete" to delete the rule.

4.7 Fire Wall

The WRT-416 provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks.

4.7.1 MAC Filtering

This Wireless router has the capability to control the wired client access based on the MAC address of the

wired client. The user has the flexibility to customize your own control policy based on these options:

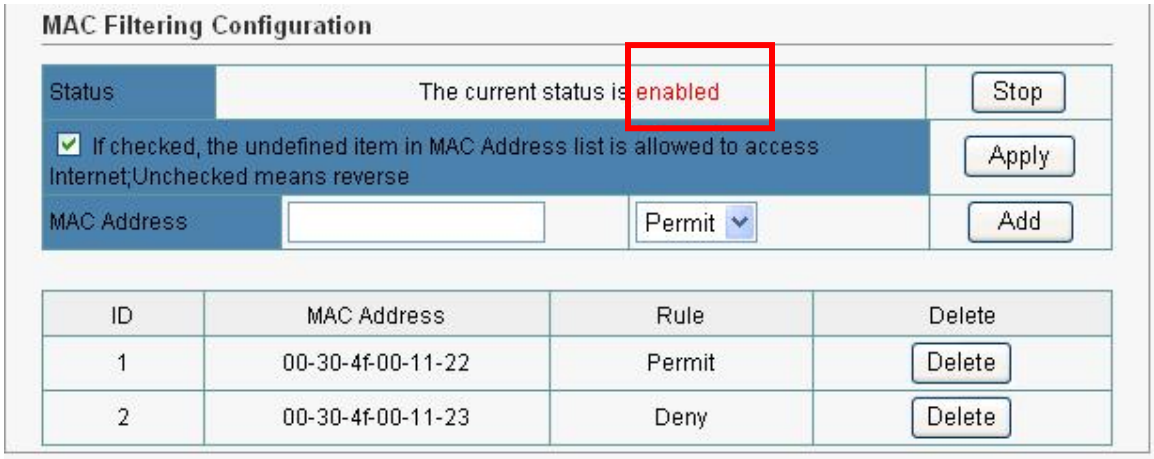


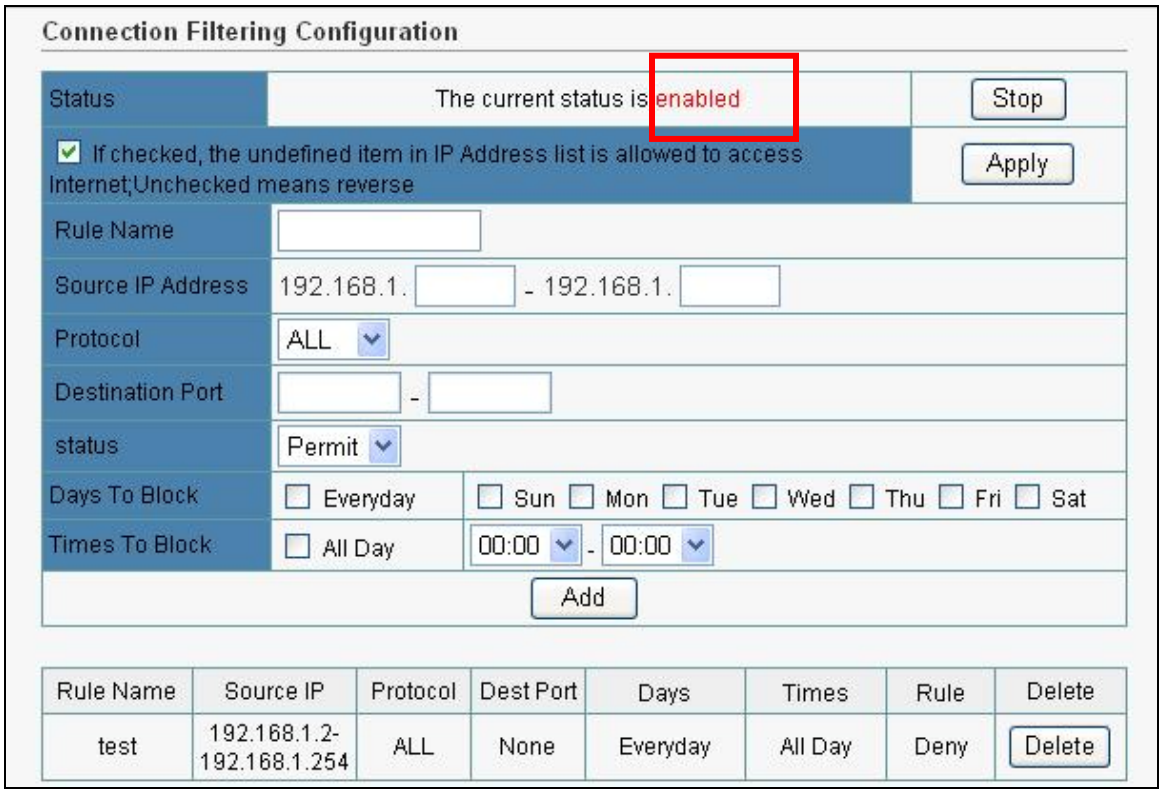
Figure 56

- **Enable MAC Filtering**: To enable MAC Filtering, click the check box. The default is “disable”.
- You can choose a default operation for your factual security or management consideration:
  - Defined items in MAC list are DENIED to access internet, others are PERMIT
  - Defined items in MAC list are PERMIT to access internet, others are DENIED

  Click “Apply” when you have selected,
- **MAC**: Enter the MAC Address of a station.
- **Description**: Enter the Comment of station.
- Click "Add”. Then this wired station will be added into the” Current Access Control List" below.
- If you want to remove some MAC address, select the MAC address from the list and then click "Delete ".

4.7.2 Access Control

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.).This is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

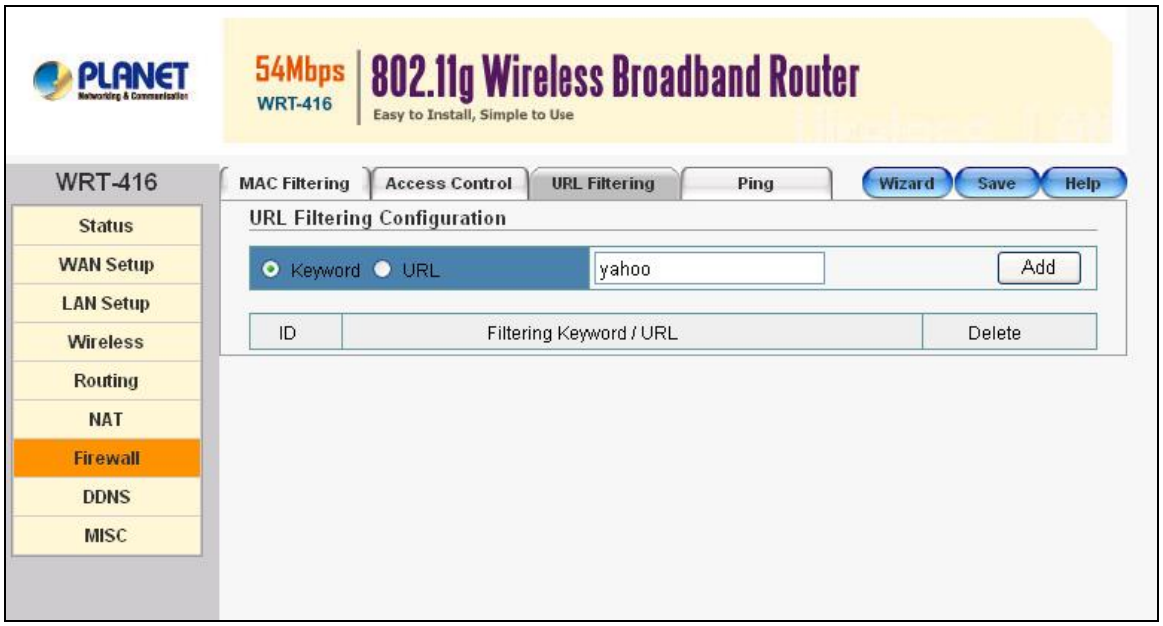


Enable Access Control: To filter the outgoing packets for security or management consideration by IP Address, either permitting or blocking access, Enable Access Control is checked.

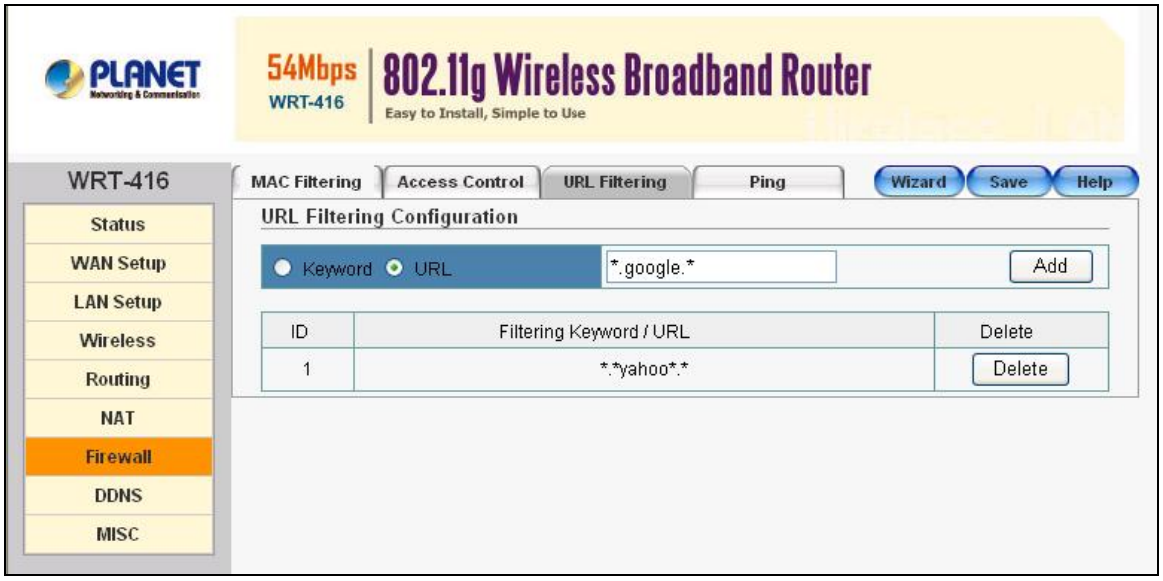
You can choose a default operation for your factual security or management consideration:
The Undefined items beside the Rule list are PERMIT to access internet DENIED to access internet.
The Undefined items beside the Rule list are DENIED to access internet DENIED to access internet.
Rule Name: Enter the rule name which you want, it is just only a string.
Source IP: Enter the IP address of a station which is you want to setting.
Predefined Applications: Chose the Predefined rule in the list to be allowed or forbade accessing Internet.
Protocol & Port: Chose protocol type (TCP/UDP) and enter the single port number or the port range to allow or forbid.
Action: You can choose the rule is be allowed or denied accessing Internet.

4.7.3 URL Filtering

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



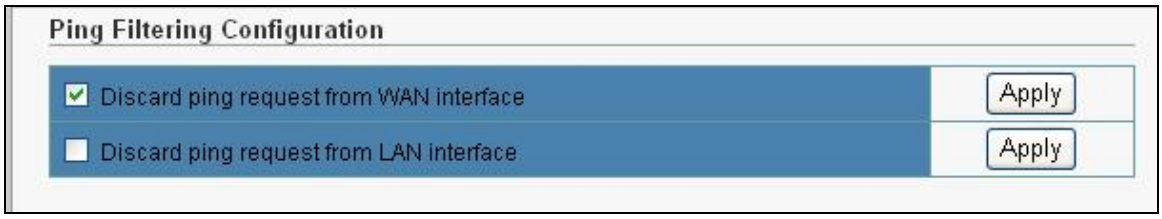
- **URLs/Keywords**: Enter the specified URL site for security or management consideration by URLs/Keywords, either permitting or blocking access.



- Press “Delete” button to delete an existing rule.

4.7.4 Ping

This page defines rules to prevent WRT-416 WAN and LAN port being scanned.



4.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers.

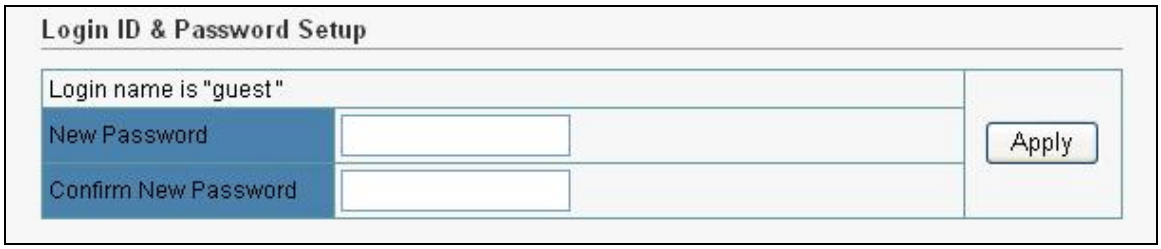
Figure 62

- **User ID/Password/Host Name**: Enter your registered domain name and your username and password for this service.
- **Information**: The status of the DDNS service connection is displayed here. To see the latest DDNS status, click Refresh button.

4.9 MISC

4.9.1 Login ID & Password Setup

In factory setting, the default password is “guest”, and that for user is also password. You can change the default password to ensure that no one can adjust your settings without permission. Every time you change your password, please record the password and keep it at a safe place.



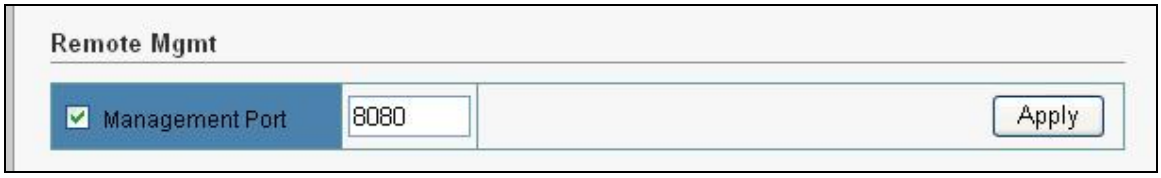
- **New Password:** Enter your new password.
- **Confirmed New Password:** Enter your new password again for verification purposes.

Click “Apply” at the bottom of the screen to change the password.

If you forget your password, you’ll have to reset the router to the factory default (Password is “guest”) with the reset button (see router’s front panel).

4.9.2 Remote Mgmt

This feature allows you to manage the Router from a remote location, via the Internet. To enable this feature, check the “Management Port” checkbox, and click the Apply button.



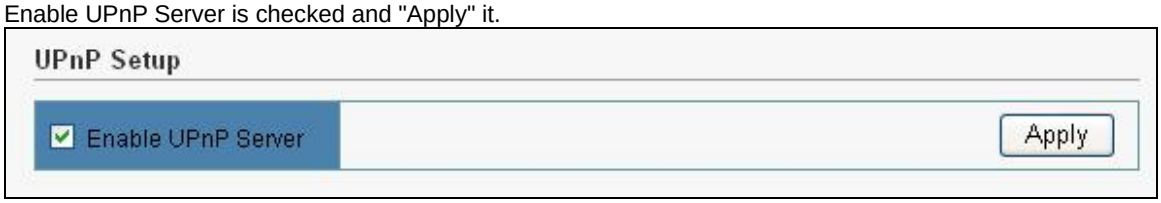
- **Management Port:** Enter the desired port number.
- Click “Apply” to change the Management Port.

When you want to access the web-based management from a remote site, enter http:// WAN IP Address:8080. (e.g:http://210.66.155.71:8080).

4.9.3 UPnP Setup

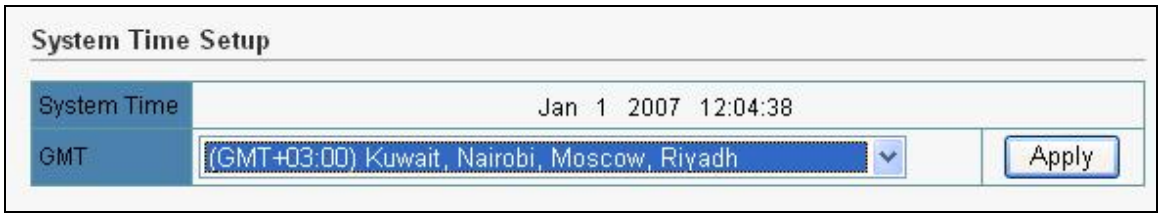
UPnP (Universal Plug and Play) is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs of all form factors.

Enable UPnP Server is checked and "Apply" it.



4.9.4 System Time Setup

The System Time Setup allows WRT-416 to allocate its time on the settings configured here.

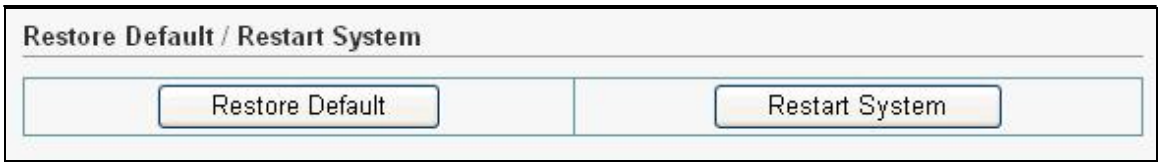


4.9.5 WAN Link Status & Setup

You can set the WAN port speed (Auto / 10M-Half / 10M-Full / 100M-Half / 100M-Full)

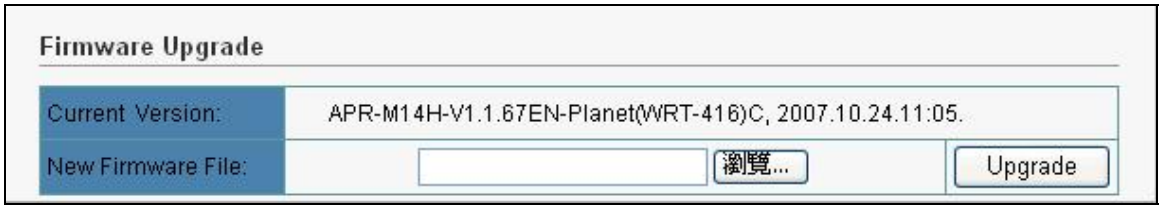
4.9.6 Restore Default / Restart System

Restore Factory Defaults -- To clear all of the AP's settings and reset them to its factory defaults.
Restart System -- reboot the AP.



4.9.7 Firmware Upgrade

To upgrade the firmware of your WRT-416, you need to save the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.



Appendix Ⅰ: Specification

Standard	IEEE 802.11b / 802.11g / IEEE 802.3 / IEEE 802.3u
Frequency Band	2.400~2.4835GHz
Transfer Rate	802.11g: 54/48/36/24/18/12/9/6Mbps 802.11b: 11/5.5/2/1Mbps
Modulation	OFDM, CCK, QPSK and BPSK
Sensitivity	● 54Mbps OFDM, 10% PER, -68dBm ● 48Mbps OFDM, 10% PER, -69dBm ● 36Mbps OFDM, 10% PER, -75dBm ● 24Mbps OFDM, 10% PER, -79dBm ● 18Mbps OFDM, 10% PER, -82dBm ● 12Mbps OFDM, 10% PER, -84dBm ● 11Mbps CCK, 8% PER, -82dBm ● 9Mbps OFDM, 10% PER, -87dBm ● 6Mbps OFDM, 10% PER, -88dBm ● 5.5Mbps CCK, 8% PER, -85dBm ● 2Mbps QPSK, 8% PER, -86dBm ● 1Mbps BPSK, 8% PER, -89dBm
Antenna	Detachable dipole antenna
Transmit Power	15dBm±2dBm
Wireless Operating Range	● Indoor- up to 328ft (100M) ● Outdoor- up to 1312ft. (400M) Note. *Environmental factors may affect actual range*
Interface	5-port RJ-45 UTP(1-WAN Port ; 4-LAN Switch Ports)
LED Indicators	6; PWR/SYS,LAN(1~4),WAN
Power	9V DC, 700mA
Temperature	0 ~ 40°C (Operating)
Humidity	5% ~ 95%, non-condensing (Operating)
Dimension	186mm*29mm*119mm
Weight	300g
Emission	FCC Class B, CE-mark