

300Mbps Wireless-N Broadband Router User Manual

V1.4

2010-07-06

Certification

FCC CE

FCC Statement

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

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

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

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment 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.

Caution!

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment

Package Contents

The following items should be found in your package:

- 300Mbps Wireless-N Broadband Router
- Power adapter
- Quick Installation Guide
- CD

Make sure that the package contains above items. If any of the above items is missing or damaged, please contact the store you bought this product from.

Contents

1. INTRODUCTION	5
1.1. PRODUCT OVERVIEW	5
1.2. MAIN FEATURES	5
1.3. SUPPORTING STANDARD AND PROTOCOL	5
1.4. WORKING ENVIRONMENT	6
2. HARDWARE INSTALLATION.....	7
2.1. SYSTEM REQUIREMENT	7
2.2. PANEL	7
2.3. RESTORE TO FACTORY CONFIGURATION	9
2.4. HARDWARE INSTALLATION PROCEDURES	9
3. LOGIN.....	11
3.1. CONFIGURE COMPUTER.....	11
3.1.1. Windows 98/Me	11
3.1.2. Windows 2000	11
3.1.3. Windows XP	14
3.1.4. Windows Vista	17
3.2. CHECKING CONNECTION WITH THE ROUTER.....	21
3.3. LOGIN	22
4. SYSTEM CONFIGURATION	25
4.1. CONVENIENT SETUP	25
4.1.1. DHCP user (Cable Modem).....	25
4.1.2. PPPoE user (ADSL).....	26
4.1.3. Static User.....	27
4.1.4. Wireless Configuration.....	27
4.2. SYSTEM INFORMATION.....	28
4.2.1. Internet Access Info.....	28
4.2.2. LAN Info.....	29
4.2.3. Primary AP Info	30
4.2.4. System Info	30
4.2.5. Statistics Info	31
4.3. SYSTEM LOG	31
4.3.1. System Log	31
4.3.2. Connection Logs.....	32
4.4. INTERNET SETUP.....	32
4.4.1. DHCP User (Cable Modem).....	32
4.4.2. PPPoE user (ADSL).....	34
4.4.3. Static user.....	35
4.5. WIRELESS MANAGEMENT	36
4.5.1. Wireless Basic	36

4.5.2.	<i>Security</i>	37
4.5.2.1.	NONE	38
4.5.2.2.	WEP	38
4.5.2.3.	WPA-PSK	39
4.5.2.4.	WPA2-PSK	39
4.5.2.5.	WPA/WPA2-PSK	40
4.5.3.	WDS	40
4.5.4.	<i>Host Filter</i>	41
4.5.5.	<i>Host List</i>	42
4.5.6.	<i>Site Survey</i>	42
4.5.7.	WPS.....	43
4.5.8.	<i>Advanced</i>	45
4.6.	SECURITY	46
4.6.1.	<i>MAC Filter</i>	46
4.6.2.	<i>Internet Access Control</i>	47
4.6.3.	<i>DNS Filter</i>	48
4.7.	LAN SETUP	49
4.7.1.	<i>LAN IP address</i>	49
4.7.2.	<i>DHCP Server</i>	50
4.7.3.	<i>DHCP Client Info</i>	50
4.8.	APPLICATIONS AND GAMING.....	50
4.8.1.	<i>Virtual Server</i>	51
4.8.2.	DMZ.....	52
4.8.3.	UPNP	52
4.8.4.	<i>Port Trigger</i>	53
4.9.	APPLICATION GATEWAY	53
4.10.	DDNS.....	54
4.11.	ROUTING.....	54
4.12.	SYSTEM MANAGEMENT.....	55
4.12.1.	<i>Password setup</i>	55
4.12.2.	<i>Web setup</i>	56
4.12.3.	<i>Upgrade</i>	56
4.12.4.	<i>Reboot</i>	56
4.12.5.	<i>Restore</i>	56
4.12.6.	WOL.....	57
4.12.7.	<i>System time</i>	57
5.	FAQ	58

1. Introduction

1.1. Product Overview

The 300Mbps Wireless-N Broadband Router is dedicated to Small Office/Home Office (SOHO) Wireless network solution. It is 4 in 1 network device, which combines wireless access point, firewall, 4-port Switch and the NAT-Router. It provides up to 300Mbps data transmission rate in 2.4GHz frequency, complies with IEEE 802.11n, IEEE 802.11g and IEEE802.11b and backwards compatible with all IEEE 802.11n/g/b devices. And the router also supports wireless LAN up to 128-bit WEP, WPA/WPA2 encryption security. The 300Mbps Wireless-N Broadband Router also provides WEB and Remote Management and system log so that network administrators can manage and monitor the network in real time.

The 300Mbps Wireless-N Broadband Router also provides a hardware WPS (Wi-Fi protected setup) button, which helps you setup a secure wireless network in a snap. The button lets you activate the wireless protection easily

1.2. Main Features

- Comply with IEEE802.11n/g/b, IEEE802.3 10Base-T, IEEE802.3u 100Base-TX standards
- Provides up to 6 times the transmission rate and double the range of 802.11g products
- Supports 64/128-bit WEP, WPA and WPA2 wireless security mode
- WPS (PIN/PBC) enabled
- MIMO technology enabled
- Support DHCP Client, PPPoE Client, Static IP, PPTP
- Support multi-wireless mode: AP, WDS, AP+WDS, repeater, client
- Support MAC filtering, IP access control, DNS filter
- Support FTP, PPTP and L2TP pass through
- Support UPNP (universal plug and play)
- Upgradeable firmware for future functions
- Support WMM
- Support DMZ

1.3. Supporting Standard and Protocol

- IEEE 802.11b/g/n
- IEEE 802.11e
- IEEE 802.11h,
- IEEE 802.11k
- IEEE 802.11i
- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX

1.4. Working Environment

Temperature

- 0° to 40° C (operating)
- -40° to 70° C (storage)

Humidity

- 10% to 90 % non-condensing (operating)
- 5% to 90% non-condensing (storage)

Power

- DC 9V

2. Hardware Installation

2.1. System Requirement

Minimum Requirements:

- Broadband (DSL/Cable) modem and service with Ethernet port
- 802.11n b/g/n wireless adapter or Ethernet adapter and cable for each computer
- Internet Explorer® 5.0, Firefox® 2.0 or Safari® 1.4 or higher

2.2. Panel

Front panel



Figure 2-1

LED	Function	
PWR	ON	Power on
	Off	Power off
WPS	Flashing slowly	WPS is running
	OFF	WPS is not running

SYS	ON and Off	Abnormal
	Flashing	Normal
WLAN	Flashing	Wireless data transmitting
	Off	Wireless off
WAN	On	WAN Connection normal
	Flashing	Data transmitting
	Off	WAN Connection abnormal
LAN	On	LAN Connection normal
	Flashing	Data transmitting
	Off	LAN Connection abnormal

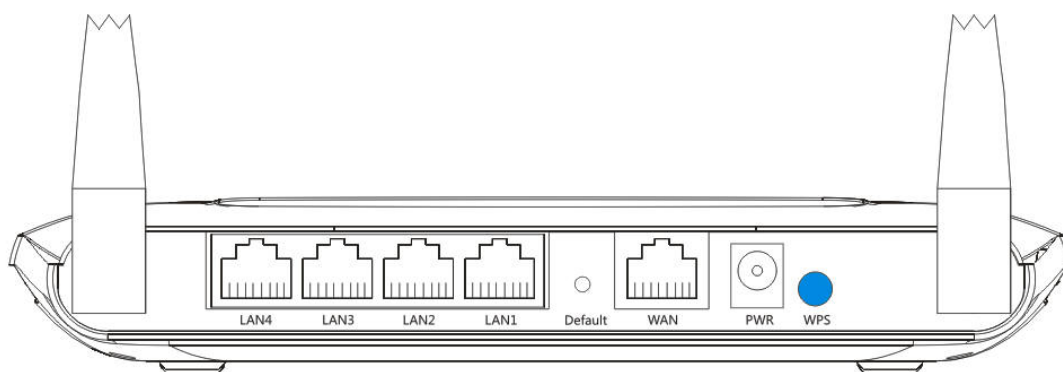
Rear panel

Figure 2-2

Description	Function
PWR port	Connect to Power adapter, please don't use the unknown power adapter, otherwise your device may be damaged.
LAN port	Connect with computer NIC or Ethernet device
WAN port	Internet access
Default	Restore settings
WPS	Press the WPS button until the WPS LED flashing slowing. The WPS LED will be off when finish negotiation with

	network card, it will also be off if the negotiation between router and network card is failed after 2minutes
Antenna	

2.3. Restore to factory configuration

If the router ever freezes in a setting change process or if you can't access it because you can't remember the IP you have given it or other problem, you may have to utilize the default button on the back of the router to put it back to factory settings. You have to press and hold this button for a few seconds (2-6s) with a pencil when it is working, then release and it will restore settings to the factory configuration.

The other way to restore factory settings is through the same user interface used in setup. Click on 'System management' - 'Restore', and click on the 'Restore' button.

2.4. Hardware Installation Procedures

The procedures to install the 300Mbps Wireless-N Broadband Router please refer to the following picture

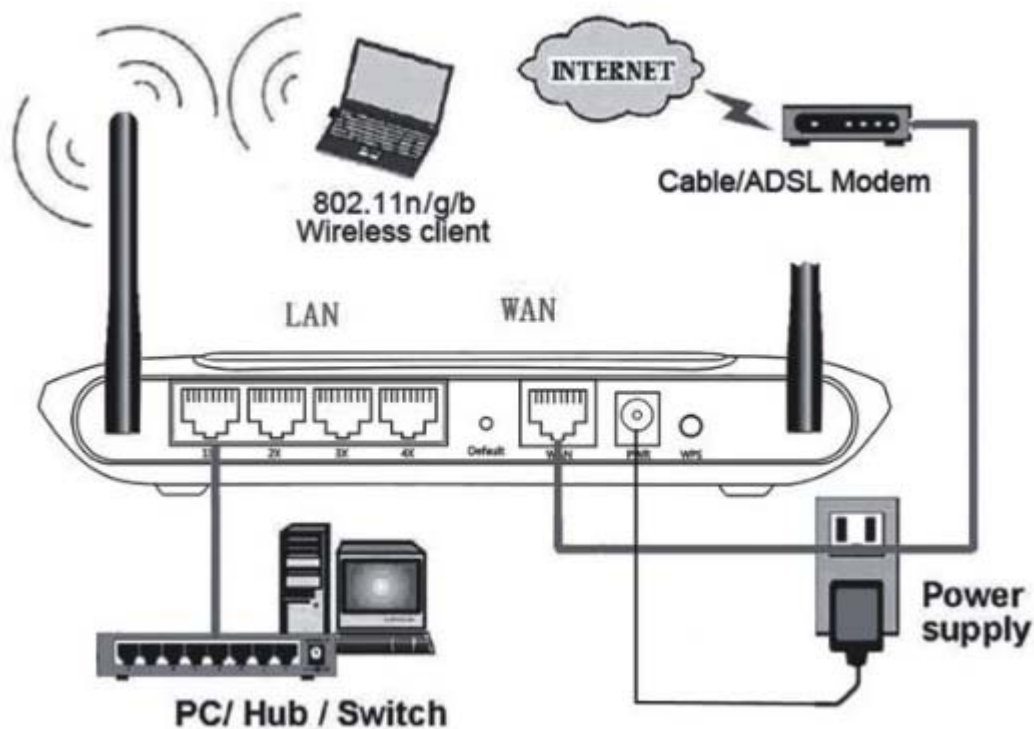


Figure 2-3

- Attach one end of an Ethernet cable to your computer's Ethernet port, and the other end to

one of the LAN ports of your router.

- Connect another Ethernet cable from your Cable/DSL modem to the WAN port of your router.
- Connect the single DC output connector of the power adapter to the power jack on the back of the router and plug the Power Adapter into an AC outlet.

3. Login

You can manage the 300Mbps Wireless-N Broadband Router through the Web browser- based configuration utility. To configure the device via Web browser, at least one properly configured computer must be connected to the device via Ethernet or wireless network. The Router 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 enabled by default.

3.1. Configure computer

3.1.1. Windows 98/Me

1. Go to **Start → Settings → Control Panel**.
2. Find and double-click the Network icon. The Network dialog box appears.
3. Click the Configuration label and ensure that you have network card.
4. Select TCP/IP. If TCP/IP appears more than once, please select the item that has an arrow “→” pointing to the network card installed on your computer. **DO NOT** choose the instance of TCP/IP with the words “Dial Up Adapter” beside it.
5. Click Properties. The TCP/IP Properties dialog box appears.
6. Ensure the Obtain IP Address Automatically is checked.
7. From the WINS Configuration dialog box, Ensure that Disable WINS Resolution is checked.
8. From the Gateway dialog box, remove all entries from the Installed gateways by selecting them and clicking Remove.
9. From the DNS Configuration dialog box, remove all entries from the DNS Server Search Order box by selecting them and clicking Remove. Remove all entries from the Domain Suffix Search Order box by selecting them and clicking Remove. Click Disable DNS.
10. Click OK, back to Network Configuration dialog box
11. Click OK, if prompted to restart, click YES.

3.1.2. Windows 2000

Please follow the steps below to setup your computer:

1. Go to **Start → Settings → Control Panel**



Figure 3-1

2. Double click the icon Network and Dial-up Connections
3. Highlight the icon Local Area Connection, right click your mouse, and click Properties

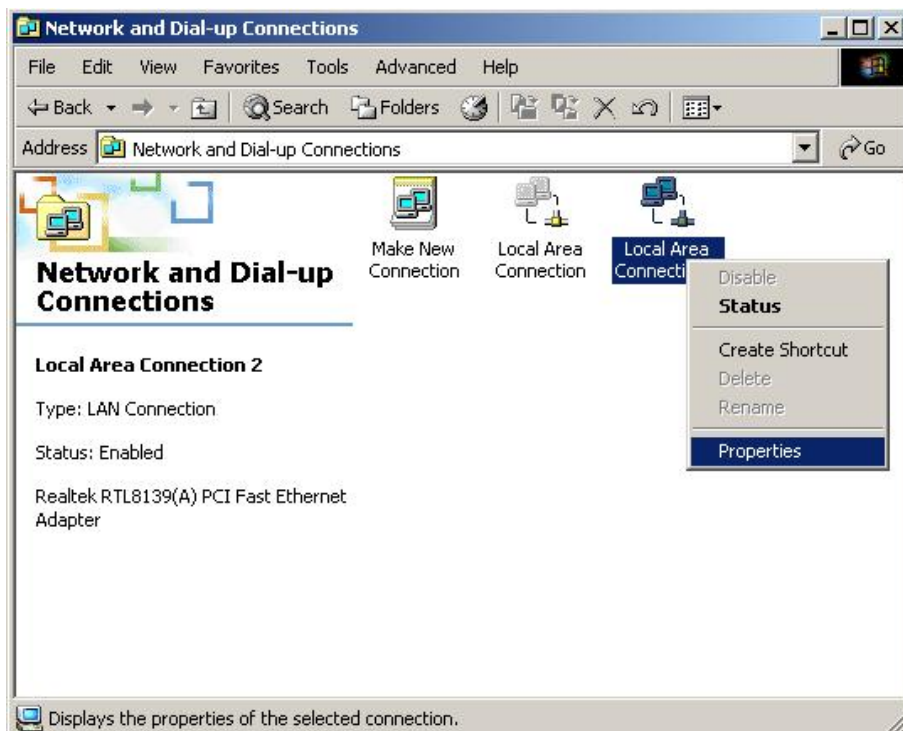


Figure 3-2

4. Highlight Internet Protocol (TCP/IP), and then press Properties button



Figure 3-3

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

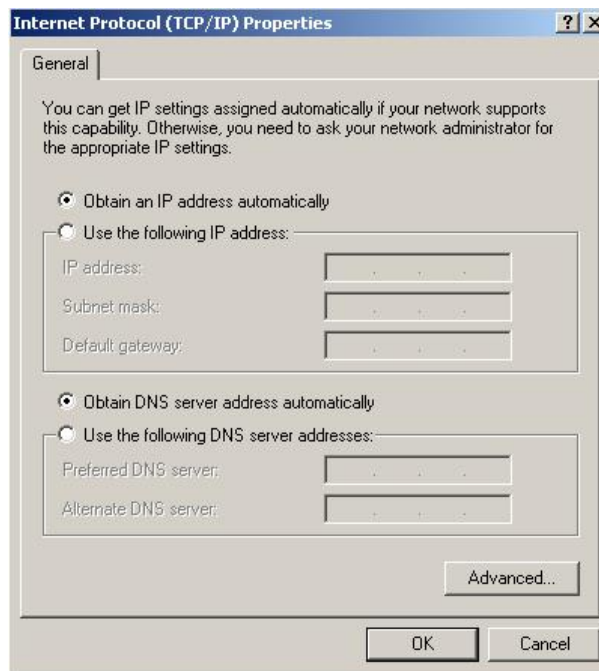


Figure 3-4

6. Press OK to close the Local Area Connection Properties window



Figure 3-5

3.1.3. Windows XP

Please follow the steps below to setup your computer:

1. Go to Start → Settings → Control Panel
2. Click Network and Internet Connections

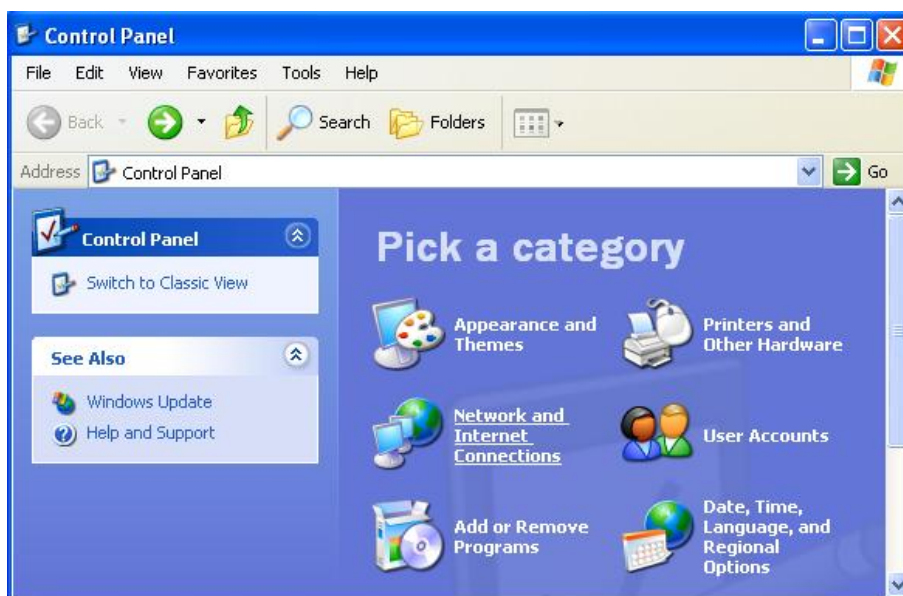


Figure 3-6

3. Click Network Connections



Figure 3-7

4. Highlight the icon Local Area Connection, right click your mouse, and click Properties

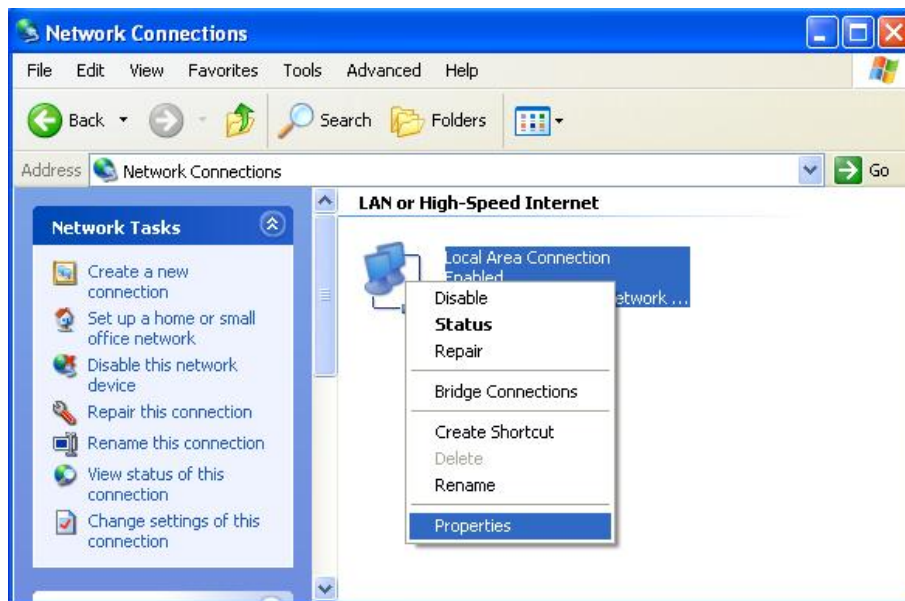


Figure 3-8

5. Highlight Internet Protocol (TCP/IP), and then press Properties button

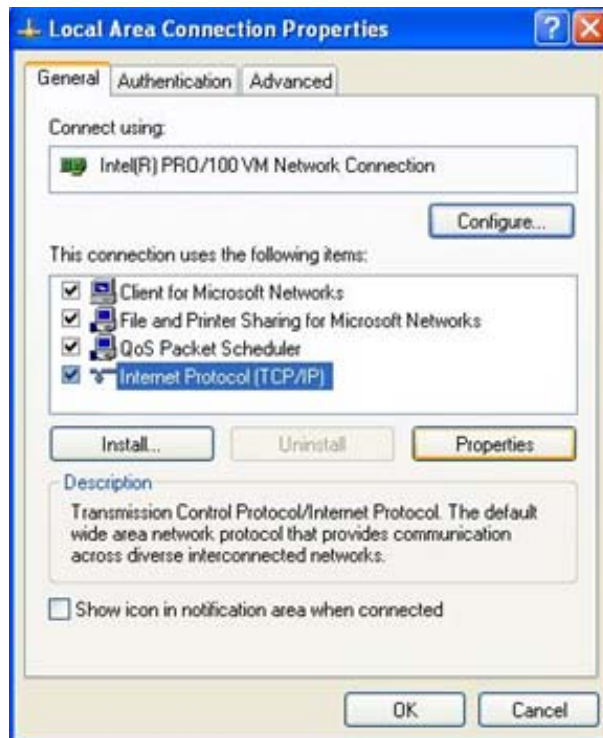


Figure 3-9

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

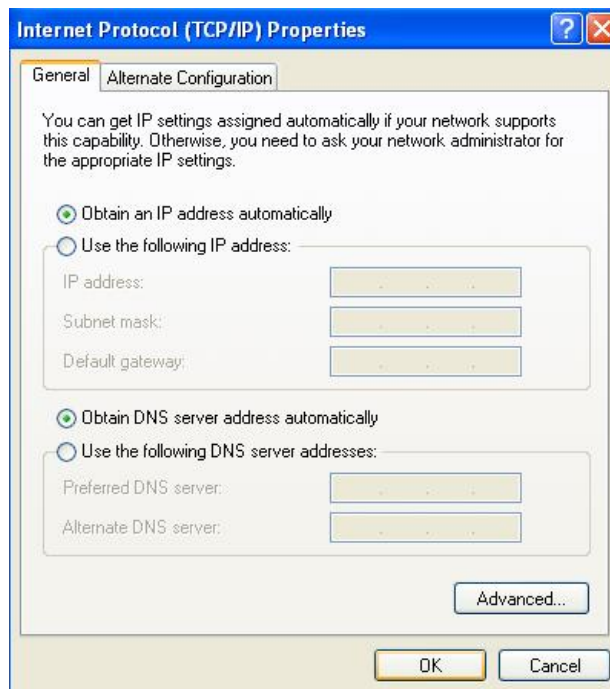


Figure 3-10

7. Press OK to close the Local Area Connection Properties window



Figure 3-11

3.1.4. Windows Vista

Please follow the steps below to setup your computer:

1. Go to Start → Settings → Control Panel
2. Click Network and Sharing Center

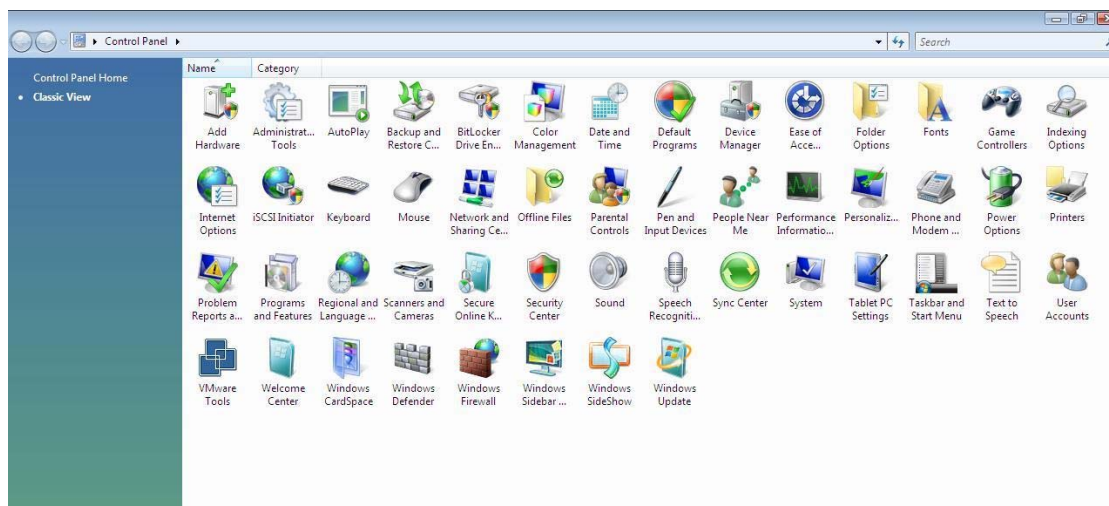


Figure 3-12

3. Click Manage Network Connections

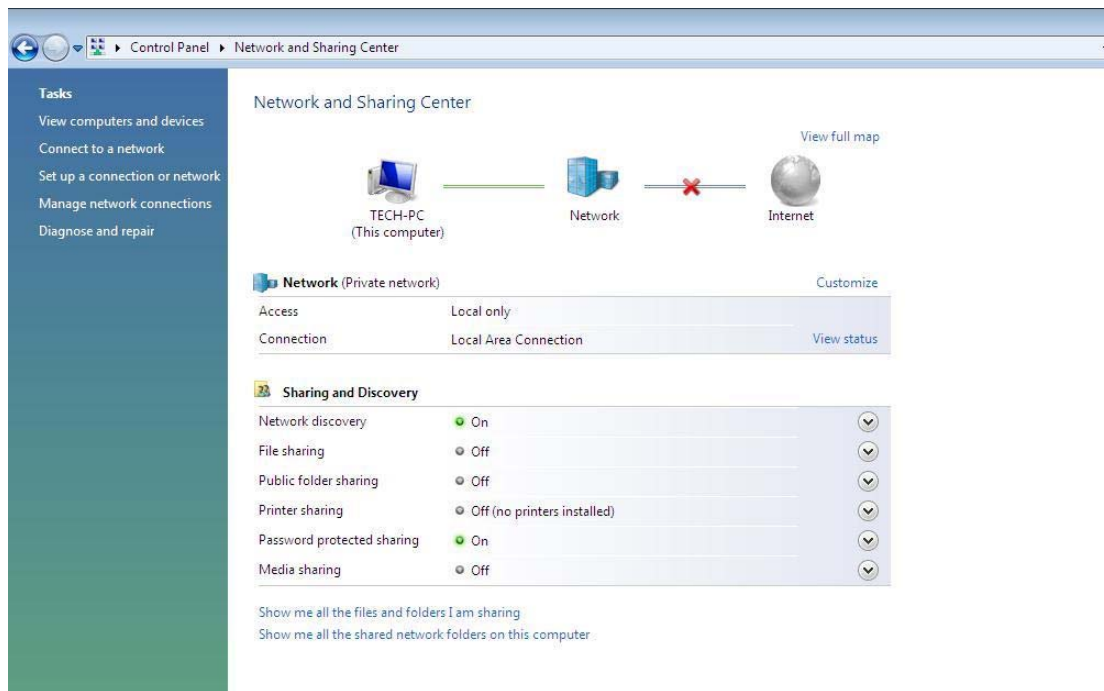


Figure 3-13

4. Highlight the icon Local Area Connection, right click your mouse, and click Properties

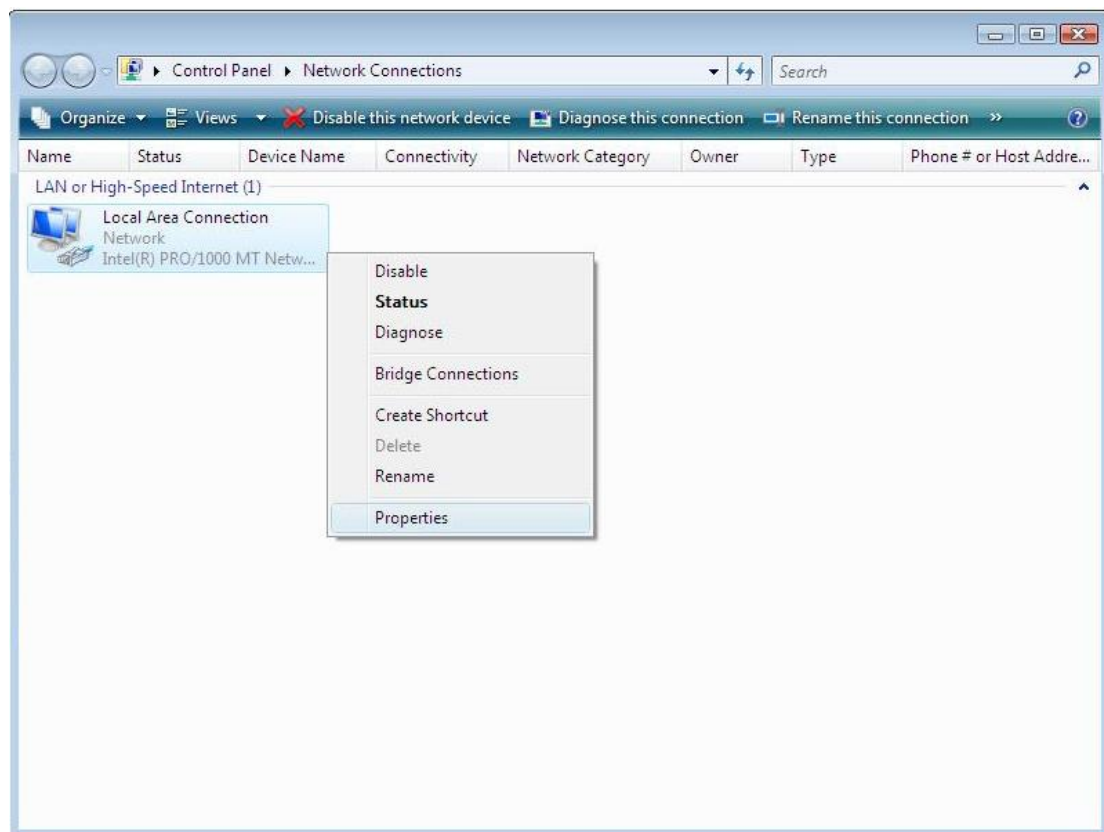


Figure 3-14

5. Highlight Internet Protocol Version 4 (TCP/IP) and then press Properties button

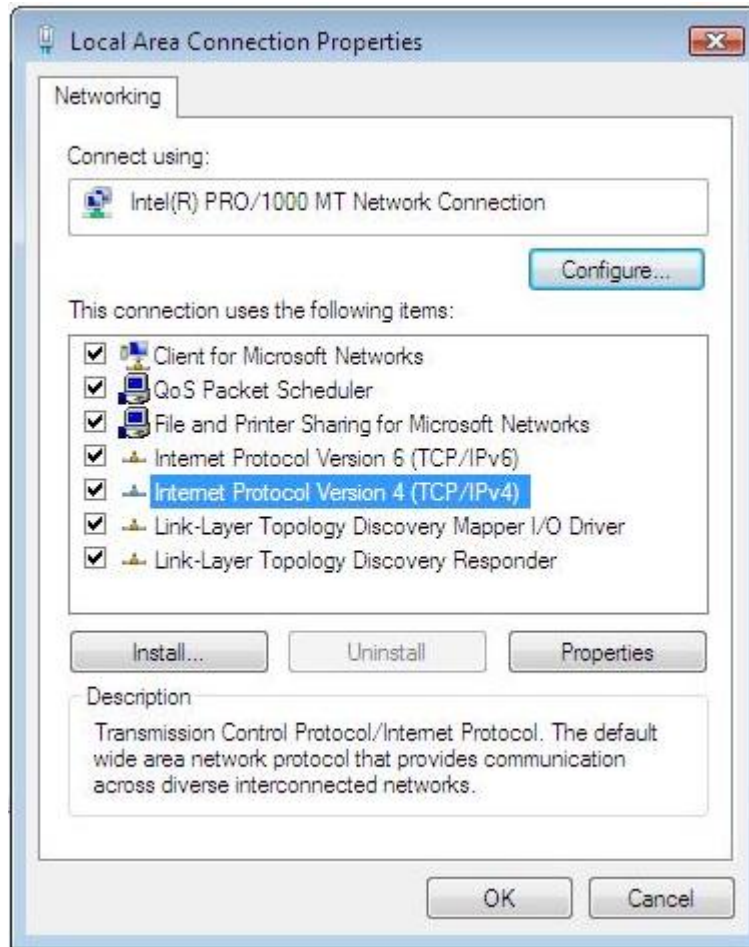


Figure 3-15

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

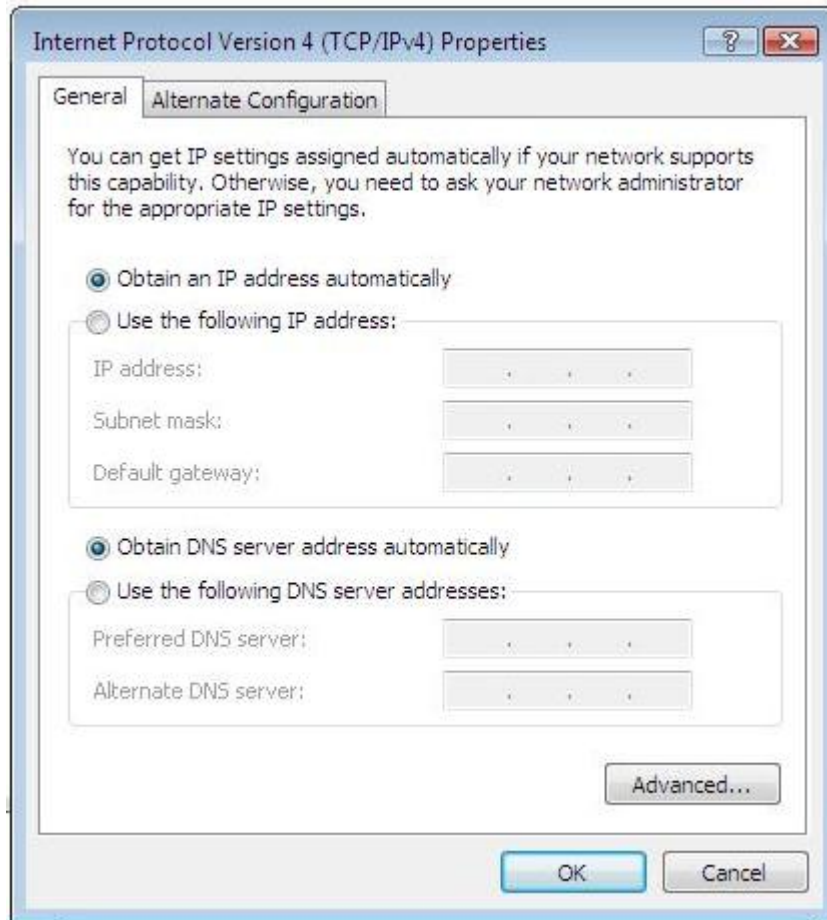


Figure 3-16

7. Press OK to close the Local Area Connection Properties window

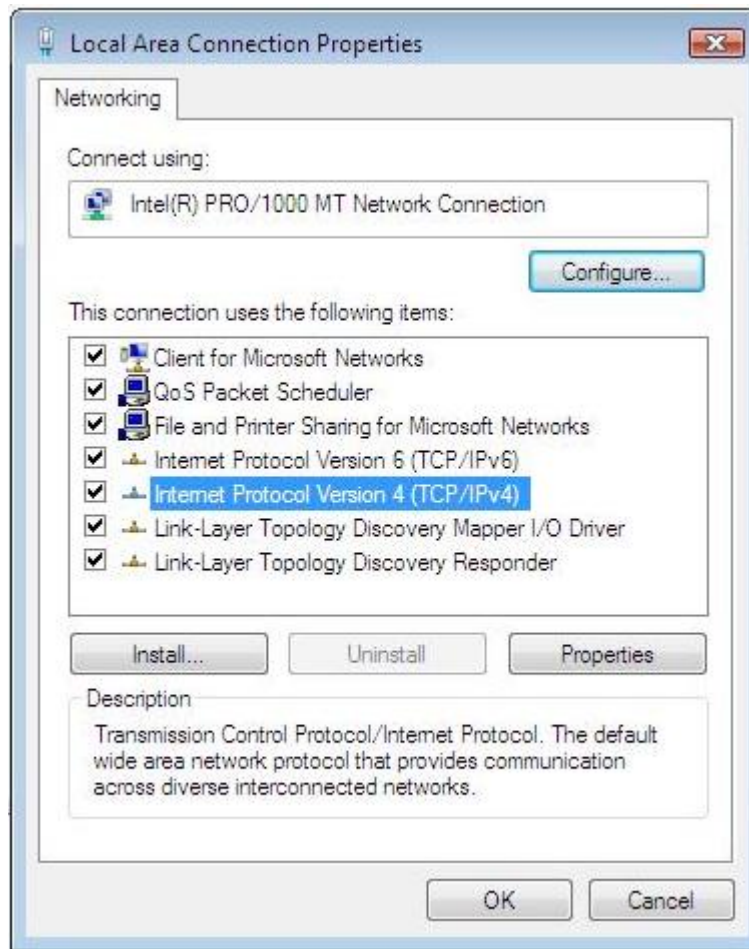


Figure 3-17

3.2. Checking 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 300Mbps wireless-N 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:

```
C:\Documents and Settings\admin>ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

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:

```
C:\Documents and Settings\admin>ping 192.168.1.1
```

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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

In order to make the whole network operate successfully, it is necessary to configure the 300Mbps wireless-N Broadband Router through your computer has a WEB browser installed.

Please follow up the steps listed below.

3.3. Login

➤ Open a web browser (Safari, Internet Explorer, etc.) on the computer you have just connected to the router, type `http://192.168.1.1` in the address bar, and press enter

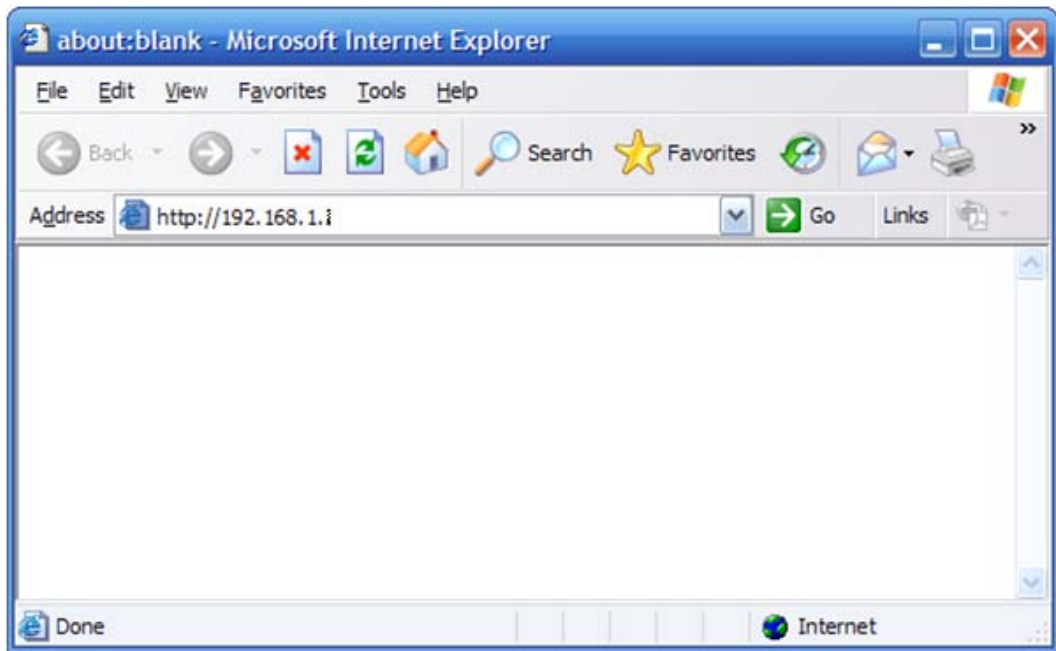


Figure 3-18

- In the pop-up window, enter the user name **guest** and password **guest** and then click OK

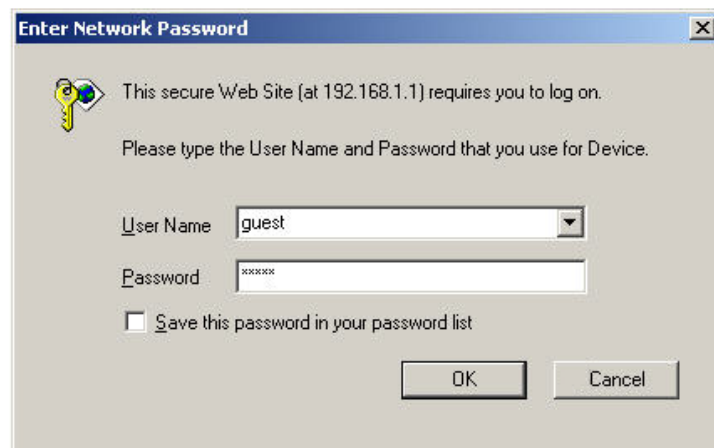


Figure 3-19

- Login successfully and the home page appears, the left navigation bar shows the main options to configure the system, the right screen is the summary information for viewing the configurations.

Convenient Setup

- Convenient Setup
- System Information
- System Log
- Internet Setup
- Wireless Management
- Security Setup
 - Access Control
- LAN Setup
- Applications & Game
- Application Gateway
- DDNS
- Routing
- System Management

Convenient Setup

☒ **DHCP user (Cable Modem)**

☐ **PPPoE user (ADSL)**

☐ **Static User**

Dynamic IP address access

Wireless Configuration

Wireless Status ☒ Enable ☐ Disable

Network Name(SSID)

Save

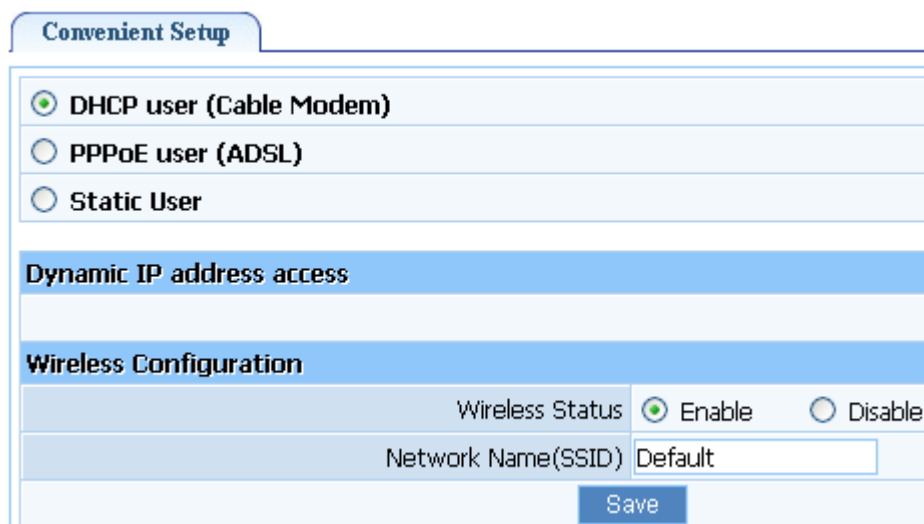
Figure 3-20

4. System configuration

4.1. Convenient Setup

Providing you the convenient and simplest method for configure the router, the purpose of this item is to provide an easy way for you to use it and configure your router to access the Internet quickly; including “DHCP”, “PPPoE”, “Static IP” and “Wireless Configuration”. This is the most convenient tool for you to configure router.

4.1.1. DHCP user (Cable Modem)



The screenshot shows the 'Convenient Setup' web interface. At the top, there is a tab labeled 'Convenient Setup'. Below the tab, there are three radio button options: 'DHCP user (Cable Modem)' (selected), 'PPPoE user (ADSL)', and 'Static User'. Below these options, there is a section titled 'Dynamic IP address access'. Further down, there is a section titled 'Wireless Configuration'. In this section, the 'Wireless Status' is set to 'Enable' (selected) and 'Disable' (unselected). The 'Network Name (SSID)' is set to 'Default'. At the bottom right of the 'Wireless Configuration' section, there is a 'Save' button.

Figure 4-1

After select this item, you will obtain an IP address from your ISP automatically, those ISP who supply Cable modem always use DHCP technology.

4.1.2. PPPoE user (ADSL)

Convenient Setup

☐ DHCP user (Cable Modem)

☒ PPPoE user (ADSL)

☐ Static User

PPPoE Client Access

PPPoE Username

PPPoE Password

Wireless Configuration

Wireless Status ☒ Enable ☐ Disable

Network Name(SSID)

Save

Figure 4-2

If your ISP provides you the PPPoE service (all ISP with DSL transaction will supply this service, such as the most popular ADSL technique), please select this item. In the “Convenient configuration” You can input your PPPoE username and password to access the Internet.

- PPPoE Username: Input PPPoE username provided by ISP
- PPPoE Password: Input PPPoE password provided by ISP.

4.1.3. Static User

Convenient Setup

☐ DHCP user (Cable Modem)
☐ PPPoE user (ADSL)
☒ **Static User**

Static IP address access

WAN IP address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS	
Secondary DNS	

Wireless Configuration

Wireless Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Name(SSID)	Default

Save

Figure 4-3

This item should only be used when users use a static IP address to access Internet, you should input your “WAN IP address”, “subnet mask”, “default gateway” and “DNS server (domain name server)” according to the information provided by your ISP. And every IP address should be input in appropriate IP field, a IP address only divided into four IP octets by sign“.” is acceptable.

- WAN IP address: The IP address that your Internet access into
- Subnet mask: Specify a Subnet Mask for your WAN segment
- Default gateway: It is provided by your ISP
- Primary DNS: DNS server is used for resolve domain name. Your ISP will provides you with at least one DNS IP address, input IP address of your DNS server in this field
- Secondary DNS: Input IP address of backup DNS server, or you can leave this field blank.

4.1.4. Wireless Configuration

You can choose “Enable” or “Disable” to enable or disable the wireless function. The default setting is “enable”. If you chose the “Disable” status, the router will become a wired broadband router without wireless function, so be careful when you choose this status.

- **SSID:** SSID (Service Set Identifier) is your wireless network's 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. Make sure all points in the wireless network have the same SSID. For added security, you should change the default SSID to a unique name.

4.2. System information

This page indicate current status of the router, including “Internet Access Info”, ”LAN Info”, “Primary AP Info”, “System Info” and “statistics info”. This item is used for monitor the current status of router for administrator, and also supplies help information about judge working situation of router

4.2.1. Internet Access Info

Internet Access Info	LAN Info	Primary AP Info	System Info	Statistics Info
Connection Type: DHCP				
Physical Address: 00:08:10:00:02:20				
IP Address: 0.0.0.0				
Subnet Mask: 0.0.0.0				
Default Gateway: 0.0.0.0				
Primary DNS:				
Secondary DNS:				
MTU : 1496				
Connect				
Current version: APR-R3A4-V1.3.05EN(2T2R),2009.12.01.17:30.				
Refresh				

Figure 4-4

This feature provides running status information of the WAN port (the port connect to the Internet)

- **Connection Type:** Display router’s current connection type, it should be one of “PPPoE”, “DHCP”, “Static IP”, depending on what kind of connection type your ISP provides.
- **Physical Address:** The physical address of WAN port, this is a unique address assigned by manufacturer.
- **IP Address:** The IP address you obtained after connect to the Internet, if you haven’t connected to the Internet yet, this field is 0.0.0.0.
- **Subnet Mask:** The Subnet mask you obtained after connect to the Internet, if you haven’t

connected to Internet yet, this field is 0.0.0.0

- **Default Gateway:** The IP address of Default gateway you obtained after connect to the Internet, if you haven't connected to Internet yet, this field is 0.0.0.0.
- **Primary DNS:** The DNS server translates domain or website names into IP address.
- **Secondary DNS:** display IP address of a backup DNS server
- **MTU:** The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Most DSL users should use the value 1492. You can set MTU manually, and you should leave this value in the 1200 to 1500 range. If the value you set is not in accord with the value ISP provide, it may causes some problems, such as fail to send Email, or fail to browse website. So if that happen, you can contact your ISP for more information and correct your router's MTU value
- **Current version:** The version information of your current firmware

4.2.2. LAN Info

Internet Access Info	LAN Info	Primary AP Info	System Info	Statistics Info
Physical Address:		00:08:10:00:02:1f		
IP Address:		192.168.1.1		
Subnet Mask:		255.255.255.0		
DHCP Server:		ON		
DHCP Server Start IP:		192.168.1.2		
DHCP Server End IP:		192.168.1.63		

Figure 4-5

This item provides information about router's LAN port, display LAN port's physical address, IP address and current situation of DHCP server.

4.2.3. Primary AP Info

Internet Access Info	LAN Info	Primary AP Info	System Info	Statistics Info
Wireless Status:		On		
Number of Wireless Client:		1		
Wireless Mode:		AP		
Channel:		channel6		
SSID:		Default		
Wireless Interface MAC Address:		00:08:10:00:02:21		
SSID Broadcasting:		on		
Security Mode:		None		

Figure 4-6

This item provides current running information of Primary AP

- **Wireless status:** Display wireless interface status is enabled or not
- **Number of Wireless Client:** Display the current number of wireless stations associated with router
- **Wireless Mode:** Current wireless mode of wireless router
- **Channel:** Display current channel of your wireless router.
- **SSID:** SSID (Service Set Identifier) is your wireless network's name shared among all points in a wireless network.
- **Wireless Interface MAC Address:** The MAC address used for wireless communication
- **SSID Broadcasting:** You can select “enable” or “disable” to enable or disable the broadcast SSID function. If the setting of this field is disable, wireless client can't obtain this SSID to login in, then user have to input the SSID value manually
- **Security Mode:** Display whether your security wireless function have been applied

4.2.4. System Info

Internet Access Info	LAN Info	Primary AP Info	System Info	Statistics Info
System Uptime:		0 Days 0 hours 21 minutes 6 seconds		
CPU Usage:		1.6%		
Memory Usage:		7%		
Firmware Version:		APR-R3A4-V1.3.05EN(2T2R),2009.12.01.17:30.		
<div>Refresh</div>				

Figure 4-7

This item provides current running information of System

4.2.5. Statistics Info

Internet Access Info LAN Info Primary AP Info System Info Statistics Info				
Type	Sending Packets	Receiving Packets	Sending data (Kbytes)	Receiving data(KBytes)
LAN	2459	2820	392	354
WAN	57	0	32	0
WLAN	6534	77193	2297	9104
Refresh				

Figure 4-8

This item provides statistics information about the bits router sends and received

4.3. System log

4.3.1. System Log





System Logs Connection Logs		
Items show in every single page 10 Apply		
<div>     </div> 1 Total1Pages		
No.	Time	Descript
1	Nov 19 08:26:38	klogd started: BusyBox v1.00-pre8 (2009.10.01-20:30+0000)
2	Nov 19 08:26:38	RTL8192SE driver version 1.17 (2009-11-02)
3	Nov 19 08:26:42	wlan0: A wireless client is associated - 00:00:00:00:00:3F
4	Nov 19 08:26:42	wlan0: A wireless client is associated - 00:00:00:00:00:3F
5	Nov 19 08:28:03	wlan0: A wireless client is associated - 00:1C:BF:6D:37:93
6	Nov 19 08:28:03	wlan0: A wireless client is associated - 00:1C:BF:6D:37:93
7	Nov 19 08:28:17	wlan0: A wireless client is deauthenticated - 00:1C:BF:6D:37:93
8	Nov 19 08:47:52	wlan0: A STA is expired - 00:00:00:00:00:3F
Del All		

Figure 4-9

Examine system logs. You can configure items shown in one Page, the default is 10

4.3.2. Connection Logs





System Logs		Connection Logs	
Items show in every single page		<input type="text" value="10"/>	<input type="button" value="Apply"/>
		<div></div> <input type="text" value="1"/> <input type="button" value="v"/> Total5Pages	
No.	Time	Descript	
1	2009-11-19 08:26:41	DHCP:DHCP Server enable!	
2	2009-11-19 08:26:42	DHCP:Recv REQUEST!	
3	2009-11-19 08:26:42	DHCP:Recv DISCOVER!	
4	2009-11-19 08:26:44	DHCP:Will get IP address:192.168.1.2	
5	2009-11-19 08:26:46	DHCP:Will get IP address:192.168.1.3	
6	2009-11-19 08:26:49	DHCP: Client enable!	
7	2009-11-19 08:26:53	DHCP:Send DISCOVER Packet!	
8	2009-11-19 08:26:57	DHCP:Not recv OFFER Packet!	
9	2009-11-19 08:28:01	DHCP:Send DISCOVER Packet!	
10	2009-11-19 08:28:05	DHCP:Not recv OFFER Packet!	
<input type="button" value="Del All"/>			

Figure 4-10

Examine connection logs. You can configure items shown in one Page, the default is 10

4.4. Internet Setup

The purpose of this item is to provide an easy way for you to use it and configure your router to access the Internet quickly

4.4.1. DHCP User (Cable Modem)

After select this item, you will obtain an IP address from your ISP automatically, those ISP who supply Cable modem always use DHCP

Internet Setup

☒ **DHCP user (Cable Modem)**

☐ **PPPoE user (ADSL)**

☐ **Static user**

Clone MAC address	00:08:10:00:02:20	Clone MAC address
Default MAC address	00:08:10:00:02:20	Default MAC address
MTU	1496	
Primary DNS		
Secondary DNS		
Save		

Figure 4-11

- **Clone MAC address:** The WAN port of router has a unique MAC address assigned by manufacturer; it called as “Default MAC”. The “Clone MAC” is used for some special situations; For example, ISP only allows certain MAC address to access the Internet, thus you can modify your WAN port’s MAC address in accord with the requirement of ISP, avoiding ISP’s detection
- **MTU:** The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Most DSL users should use the value 1492. You can set MTU manually, and you should leave this value in the 1200 to 1500 range. If the value you set is not in accord with the value ISP provide, it may causes some problems, such as fail to send Email, or fail to browse website. So if that happened, you can contact your ISP for more information and correct your router’s MTU value
- **Primary DNS:** DNS server is used for resolve domain name. Your ISP will provide you with at least one DNS IP address, input IP address of your DNS server in this field
- **Secondary DNS:** Input IP address of backup DNS server or you can leave this field blank

4.4.2. PPPoE user (ADSL)

Internet Setup

☐ DHCP user (Cable Modem)
☒ **PPPoE user (ADSL)**
☐ Static user

PPPoE Username	<input type="text"/>
PPPoE Password	<input type="password"/>
Clone MAC address	<input type="text" value="00:08:10:00:02:20"/> <input type="button" value="Clone MAC address"/>
Default MAC address	<input type="text" value="00:08:10:00:02:20"/> <input type="button" value="Default MAC address"/>
MTU	<input type="text" value="1492"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

☒ Connect to Internet automatically (Default)
☐ Auto disconnect when idle, time out ,After (1-30) minutes, if no found the access request then auto-break off!
☐ Connect to Internet manually

Figure 4-12

If your ISP provides you the PPPoE service (all ISP with DSL transaction will supply this service, such as the most popular ADSL technique), please select this item. In the “Convenient Setup” You can input your PPPoE username and password to access the Internet

- PPPoE username: Input PPPoE username provided by ISP
- PPPoE Password: Input PPPoE password provided by ISP
- Default MAC Address: The MAC address of WAN port, this is a fixed, unique address assigned by manufacturer
- MTU: The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Most DSL users should use the value 1492. You can set MTU manually, and you should leave this value in the 1200 to 1500 range. If the value you set is not in accord with the value ISP provide, it may causes some problems, such as fail to send Email, or fail to browse website. So if that happened, you can contact your ISP for more information and correct your router’s MTU value
- Primary DNS: DNS server is used for resolve domain name. Your ISP will provide you with at least one DNS IP address, input IP address of your DNS server in this field
- Secondary DNS: Input IP address of backup DNS server, or you can leave this field blank

You can select three modes: connect to Internet automatically (Default), auto disconnect when idle or time out, connect to Internet manually

- Connect to Internet automatically (default): it is suitable for connect to Internet without recording time. It connects automatically when the power is on, when it is disconnected it will redial again
- Auto disconnect when idle, time out: it is suitable for connect to Internet that need to record time. It doesn't connect to Internet when the power is on, only when there is access request it will connect automatically. When there is no access request in set time (1-30 minutes) it will disconnect
- Connect to Internet manually: it is suitable for those whose access method is controlled by administrator who knows password. It doesn't connect to Internet when the power is on, only when you connect or disconnect manually

4.4.3. Static user

The screenshot shows the 'Internet Setup' page with the 'Static user' option selected. The configuration fields are as follows:

Internet Setup	
<input type="radio"/> DHCP user (Cable Modem) <input type="radio"/> PPPoE user (ADSL) <input checked="" type="radio"/> Static user	
WAN IP address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Clone MAC address	00:08:10:00:02:20 Clone MAC address
Default MAC address	00:08:10:00:02:20 Default MAC address
MTU	1500
Primary DNS	
Secondary DNS	
<input type="button" value="Save"/>	

Figure 4-13

This should be used only you are connecting through a static IP address. You should input your “WAN IP address”, “subnet mask”, “default gateway” and “DNS server (domain name server)” according to the information provided by your ISP. And IP address input should be filled in appropriate IP field, a IP address only divided into four IP octets by sign.” is acceptable

- WAN IP address: The IP address that your Internet access into
- Subnet mask: Specify a Subnet Mask for your WAN segment

- Default gateway: It is provided by your ISP
- Clone MAC address: The WAN port of router has a unique MAC address assigned by manufacturer; it called as “Default MAC”. The “Clone MAC” is used for some special situations; For example, ISP only allows certain MAC address to access the Internet, thus you can modify your WAN port’s MAC address in accord with the requirement of ISP, avoiding ISP’s detection
- MTU: The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Most DSL users should use the value 1492. You can set MTU manually, and you should leave this value in the 1200 to 1500 range. If the value you set is not in accord with the value ISP provide, it may causes some problems, such as fail to send Email, or fail to browse website. So if that happened, you can contact your ISP for more information and correct your router’s MTU value
- Primary DNS: DNS server is used for resolve domain name. Your ISP will provides you with at least one DNS IP address, input IP address of your DNS server in this field
- Secondary DNS: Input IP address of backup DNS server, or you can leave this field blank.

4.5. Wireless management

It contains the following parts: Basic, Security, WDS, host filter, Host List, Site Survey, WPS, Advanced

4.5.1. Wireless Basic

Basic	Security	WDS	Host Filter	Host List	Site Survey	WPS	Advanced
Basic							
Wireless Network Status		<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Radio Band		802.11b+g+n					
Radio Mode		Access Point					
SSID		Default					
SSID Broadcasting		<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Channel Width		<input checked="" type="radio"/> 20MHZ <input type="radio"/> 40MHZ					
Region		ETSI					
Channel		Channel 6					
Save							

Figure 4-14

Providing basic configuration items for wireless router users, including “wireless network

status”, “Radio Band”, “Radio Mode”, “SSID”, “SSID broadcasting”, “Channel width”, “Channel sideband”, “Region” and “Channel” several basic configuration items.

- Wireless network status: You can choose “enable” or “disable” to enable or disable the “Wireless Network Status”, if what you choose is “Disable”, the AP function of wireless router will be turned off
- Radio band: You can select the wireless standards running on your network, if you have Wireless-N, and Wireless-B/G devices in your network, keep the default setting, 802.11b+g+n
- Radio mode: You can select radio mode of wireless router, it contains Access Point, Client, AP+WDS and WDS. The default setting is AP mode
- SSID: The default is Default
- SSID Broadcasting: You can select “enable” or “disable” to enable or disable the broadcast SSID function, If the setting of this field is disable, wireless client can’t obtain this SSID to login in, then user have to input the SSID value manually
- Channel width: This switch allows you to set Router's wireless bandwidth. 20MHz: In this mode you can get low bandwidth, little interference and slow rate. 40MHz: In this mode you can get high bandwidth, high interference and rapid rate. Use only when you have a pure router, draft 802.11n wireless network
- Channel sideband: It controls your wireless router use higher or lower channel when working on 40MHz
- Region: please select the region where you live in
- Channel: In 20MHz, you can select one channel from 1 to 13 manually, and in 40MHz, you can select one channel from 1 to 9 or 5 to 13, which provides a choice of avoiding interference

4.5.2. Security

The item allows you to encrypt your wireless communication, and you can also protect your wireless network from unauthorized user access. It supplies “None”, “WEP”, “WPA-PSK”, “WPA2-PSK” and “WPA/WPA2-PSK” five different encryption modes.

4.5.2.1. NONE

The screenshot shows the 'AP Security Setup' page. At the top, there are tabs: Basic, Security, WDS, Host Filter, Host List, Site Survey, WPS, and Advanced. The 'Security' tab is selected. Below the tabs, the 'Authentication Type' is set to 'None' in a dropdown menu. At the bottom right, there is a 'Save' button.

Figure 4-15

“None” means do not encrypt wireless data

4.5.2.2. WEP

The screenshot shows the 'AP Security Setup' page with the 'Authentication Type' set to 'WEP'. Below this, there is a section titled 'WEP' with a red warning message: 'WPS enable, please not use wep!'. Under this section, there are two rows of settings: 'Key Length' with radio buttons for '64 bits' (selected) and '128 bits'; and 'Key Mode' with radio buttons for 'HEX' (selected) and 'ASCII'. Below these is a text input field for the 'Key'. At the bottom right, there is a 'Save' button.

Figure 4-16

- **Key Length:** There are two basic levels of WEP encryption, 64 bits and 128 bits, the more bits password have, the better security wireless network is, at the same time the speed of wireless is more slower.
- **Key Mode:** If you select WEP to encrypt your data, choose the bits of password, it should be 64 bits or 128 bits. Then choose the format of password; it should be HEX or ASCII. The valid character for HEX format should be numbers from 0 to 9 and letters from A to F. HEX support mixed letter and number mode. And ASCII supports all characters that in keyboard
- **Key Length description:** when you select 64bits, you need to input 10 chars for HEX and 5 chars for ASCII, and when you select 128bits, you need to input 26 chars for HEX and 13 chars for ASCII

Note: when the WPS is enabled, please not use WEP

4.5.2.3. WPA-PSK

The screenshot shows the 'AP Security Setup' page with the 'Security' tab selected. The 'Authentication Type' is set to 'WPA-PSK'. Under the 'Pre-Shared Key' section, 'Encryption Type' has radio buttons for TKIP (selected), AES, and TKIP & AES. 'Key Mode' has radio buttons for HEX and ASCII (selected). There is an empty text field for 'Key' and a text field for 'Key Renewal (60-86400 seconds)' containing the value '86400'. A 'Save' button is at the bottom right.

Figure 4-17

- Encryption type: You can select the algorithm you want to use, TKIP, AES or TKIP&AES. TKIP means “Temporal Key Integrity Protocol”, which incorporates Message Integrity Code (MIC) to provide protection against hackers. AES, means “Advanced Encryption System”, which utilizes a symmetric 128-Bit block data
- Key Renewal: you can configure the renewal time between 60 to 86400 seconds
- Key Length description: you need to input 8 to 63 ASCII characters no matter which type you select

4.5.2.4. WPA2-PSK

The screenshot shows the 'AP Security Setup' page with the 'Security' tab selected. The 'Authentication Type' is set to 'WPA2-PSK'. Under the 'Pre-Shared Key' section, 'Encryption Type' has radio buttons for TKIP (selected), AES, and TKIP & AES. 'Key Mode' has radio buttons for HEX and ASCII (selected). There is an empty text field for 'Key' and a text field for 'Key Renewal (60-86400 seconds)' containing the value '86400'. A 'Save' button is at the bottom right.

Figure 4-18

The WPA2-PSK is similar to WPA-PSK and with stronger encryption method than WPA-PSK, using WPA2-PSK; you should input password (leave this value in the range of 8 to 63

characters) and key renewal time (leave this value in the range of 60 to 86400 seconds).

4.5.2.5. WPA/WPA2-PSK

The screenshot shows the 'WPA/WPA2-PSK' configuration page. At the top, there are tabs: Basic, Security, WDS, Host Filter, Host List, Site Survey, WPS, and Advanced. The 'WPA/WPA2-PSK' tab is selected. Below the tabs, there is a section titled 'AP Security Setup'. Under this section, the 'Authentication Type' is set to 'WPA/WPA2-PSK'. Below this, there is a section titled 'Pre-Shared Key'. Under this section, the 'Encryption Type' has three radio buttons: TKIP (selected), AES, and TKIP & AES. The 'Key Mode' has two radio buttons: HEX and ASCII (selected). There is a text input field for the 'Key'. Below that, there is a text input field for 'Key Renewal (60-86400 seconds)' with the value '86400'. At the bottom right of the section is a 'Save' button.

Figure 4-19

This item mixed WPA-PSK and WPA2-PSK mode, which provides higher security level; you can configure it according with WPA-PSK or WPA2-PSK

4.5.3. WDS

The screenshot shows the 'WDS Setup' page. At the top, there are tabs: Basic, Security, WDS, Host Filter, Host List, Site Survey, WPS, and Advanced. The 'WDS' tab is selected. Below the tabs, there is a section titled 'WDS Setup:'. Under this section, there are two text input fields: 'WDS Name:' and 'WDS MAC Address:'. To the right of the 'WDS Name:' field is an 'AP Scan' button. Below the 'WDS MAC Address:' field is an 'Add' button. At the bottom of the section, there is a table with the following columns: ID, WDS Name, WDS MAC Address, and Del. Above the table, there is a text input field for 'Items show in every single page' with the value '3', an 'Apply' button, and a 'Total 0 Pages' indicator.

Figure 4-20

If you have selected WDS or AP+WDS mode in **Wireless Basic-Radio Mode**, please do the following configurations

- WDS Name: Give a description of your wireless bridge to tell apart
- WDS MAC Address: If the current working mode is “WDS” or “AP+WDS”, then you need to configure wireless bridge configuration. Enter MAC address of remote access point, at the same time the remote access point also need to configure to “WDS” or “AP+WDS” mode

- AP Scan: it may search some remote AP, then you can select the wireless Bridge MAC here. Click connect, it will be filled into the WDS MAC address automatically
- Current WDS Information: It illustrates basic information of all wireless bridge that in connection status, you may delete unnecessary bridge.

E.g.: If you want setup WDS connection between the AP that the MAC address is 00-22-4f-cc-ae-f5 (we call it AP1) and the AP that the MAC address is 00-22-4f-bc-af-5d (we call it AP2), please follow the next steps:

1. Select **radio mode** is WDS in **wireless management-basic** of AP1
2. Input WDS name (e.g.: default), input MAC address of AP2 (00-22-4f-bc-af-5d), click add, then the record named default will appears in WDS list
3. We can also select **radio mode** is WDS in **wireless management-basic** of AP2
4. Input WDS name (e.g.: Default), input MAC address of AP1 (00-22-4f-cc-ae-f5), click add, then the record named Default will appears in WDS list

Note: Before you setup WDS connection, please make sure that AP1 and AP2 is in the same network, that is if the IP address of AP1 is 192.168.1.1, then the IP address of AP2 should be 192.168.1.x (1<x<255,e.g.: x=8)

4.5.4. Host Filter

You can filter wireless users by enabling this function; thus unauthorized users cannot access the network.

Figure 4-21

- Wireless Access Control Status: the default is disable. To disable “Wireless Access Control Status”, keep the default setting “Disable”

Please select “enable” if you want to configure Wireless Access Control, then you can follow the following steps to set:

1. Add MAC address you want to control in the “MAC address” field (the format is ****_**_**_**_**_****), then click “Add” button, and you will see the MAC address has displayed in the MAC list.
2. There are two items supplied, “Permit wireless connection for MAC address listed (others are Denied)” and “Deny wireless connection for MAC address listed (others are Permitted)”, Select the item you want, and click “Save” button

4.5.7. WPS

Wi-Fi Protect Setup (WPS) function can let you create a safety network easily. You can through 'PIN Input Config (PIN)' or 'Push Button (PBC)' to encrypt your network. This router also provides WPS button, you only need to push the WPS button in this router and the wireless network card that support WPS function, then the router will be encrypted to WPA2-AES mode automatically

Note:

If you have configured encryption mode in your router, then when you use this WPS function, please configure the authentication type to None, then it will be encrypted to WPA2-AES mode automatically. If you don't want to change your authentication type, then when you use this function, the router will be encrypted to the mode that you have configured.

WPS Settings			
WPS Status	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
AP PIN Code	66170099	Generated PI	
Save			
WPS PIN Settings			
Wireless Host PIN Code	<input type="text"/>		
Connect			
WPS PBC Settings			
Connect			
WPS Configuration			
Security Mode	Authentication Type	Key Format	Key
None			

Figure 4-24

- WPS Status: you can use this function to setup the wireless connection between this router and wireless network card. The default is Enable.
- AP PIN Code: this code can mark a wireless product
- Generated PI: generate a new PIN code
- Wireless Host PIN Code: input the PIN of wireless network card that support WPS function. Click connect, when it connect successfully, it will be encrypted to WPA2-PSK
- WPS PBC settings: Click connect, when it connect successfully, it will be encrypted to WPA2-PSK
- WPS Configuration: display the encryption information

WPS can connect the wireless adapter and the router in a safe way. If you have a wireless

network card which has WPS button, you may set up a safe network via the following methods

Method 1:

- Push the WPS button in the Router until the WPS LED is flashing several times
- Push the WPS button in the wireless network card for about 3-5seconds
- The safe connection will be established automatically

Method 2:

- Input the PIN code of the adapter's WPS page into the router's WPS configure page, then click 'connect'



Figure 4-25

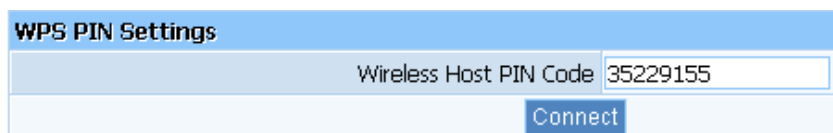


Figure 4-26

- Push the 'PIN Input Config (PIN)' in the Wi-Fi protect setup of the adapter

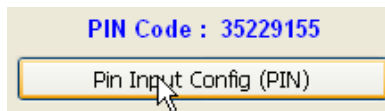


Figure 4-27

- Select this router in the pop-up window, then click 'Select'
- The connection between the adapter and the router is be established automatically.

Method 3:

- Select 'Input PIN from AP' in WI-FI protect setup page, input PIN of the router, then click 'PIN Input Config (PIN)'

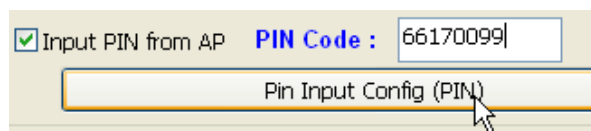


Figure 4-28

- Select this router in the pop-up window, then click 'Select'
- The connection between the adapter and the router is be established automatically.

Remark

If there is more than one AP in the PBC mode when you use the method 1, there will be session overlap. Please using method 2/3 or wait for a while push the button again.

4.5.8. Advanced

Basic		Security		WDS		Host Filter		Host List		Site Survey		WPS		Advanced	
Advance Setup															
Authentication Type		Auto <input type="button" value="v"/>													
Beacon Interval		100		(Extent:20-1000,Default:100)											
RTS Threshold		2347		(Extent:256-2347,Default:2347)											
Aggregation		AMPSDU+AMPSDU <input type="button" value="v"/>													
Fragmentation Threshold		2346		(Extent:256-2346,Default:2346)											
Transmission Rate		Auto <input type="button" value="v"/>													
ShortGi		<input checked="" type="radio"/> Enable		<input type="radio"/> Disable											
Protection		<input checked="" type="radio"/> Enable		<input type="radio"/> Disable											
Preamble Type		<input checked="" type="radio"/> Long		<input type="radio"/> Short											
WLAN Partition		<input type="radio"/> Enable		<input checked="" type="radio"/> Disable											
RF Output Power		<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%													
WMM		<input checked="" type="radio"/> Enable		<input type="radio"/> Disable											
<input type="button" value="Apply"/>															

Figure 4-29

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

- Authentication type: The default is set to “Auto”, which allows “Open System” or “Shared Key” authentication to be used. Select “Shared Key” if you only want to use “Shared Key” authentication (the sender and recipient use a WEP key for authentication)
- Beacon Interval: The interval time of this 300Mbps wireless-N Broadband Router broadcast a beacon. Beacon is used to synchronize the wireless network. The valid interval is 20-1000, the default is 100
- RTS Threshold: You can set RTS Threshold value in this field, the valid range should be 256-2347 and default value is 2347. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled
- Aggregation: You can accelerate the wireless transmission speed by enabling the aggregation function. The default is AMPDU + AMSDU
- Fragmentation Threshold: It specifies the maximum size of packet during the fragmentation of data to be transmitted
- Transmission Rate: Transmit rate indicates the transmission speed of wireless LAN access. The default setting is “Auto” and you can set this value between 1-54Mbps range
- ShortGi: You can select “Enable” or “disable” for shortgi

- Protection: Using 802.11b and 802.11g mixed mode may result in poor network performance. By enabling 802.11 protection, it will ameliorate performance of 802.11g devices in your wireless network
- Preamble Type: "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability; the default setting is "Long Preamble"
- WLAN Partition: create separate virtual network for your wireless network. When you select enable, each of your wireless client will be in his own virtual network and can't communicated with each other. If there are users who always visit your wireless network, this function may be used

4.6. Security

This feature provides security and network protection by using "MAC Filter", "Internet access control" and "DNS Filter"

4.6.1. MAC Filter

Figure 4-30

- MAC Filter Status: the default is disable. You can filter wired users by enabling this function; thus unauthorized users can not access the network
- Description: describe MAC Filter list to tell from different MAC Filter lists

- Rule: you can select permit or deny. The default is permit
- MAC address: input the MAC address that you want to control. The default format is **_**_**_**_**_**_** (e.g.: 00-22-33-da-cc-bb)

Follow the following steps to set MAC filter:

1. Enable MAC Filter, then select save.
2. Add MAC address you want to control in the “MAC address” field (the format is **_**_**_**_**_**_**), then click “Add” button, and you will see the MAC address has displayed in the MAC list.
3. There are two items supplied, “Permit wireless connection for MAC address listed (others are Denied)” and “Deny wireless connection for MAC address listed (others are Permitted)”, Select the item you want, and click “Save” button.

4.6.2. Internet Access Control

IP Filter Parameter

IP Firewall Status: ☐ Enable ☒ Disable

Default IP Firewall Rule: ☐ Deny through the router for IP address listed, others are permitted ☒ Permit through the router for IP address listed, others are denied

Save

IP Filter List Management

Description:

Rule:

Source IP Address:

Protocol and Port: -

Days To Block: ☐ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Times To Block: ☐ All Day -

Add

Items show in every single page Apply Total 0 Pages

ID	Description	Source IP	Destination Port	Protocol	Days To Block	Times To Block	Rule	Del
Del All								

Figure 4-31

- IP Firewall Status: the default is disable. The rules of “Internet access control” based on source IP, port number and protocol
- Description: describe IP Firewall list to tell from different IP Firewall lists
- Rule: you can select permit or deny. The default is permit
- Source IP address: input the source IP address that you want to control. The default

format is *.*.*.*.**(e.g: 192.168.2.3)

- Protocol and Port: If the rule has already existed in “Protocol Template”. You can select appropriate item and apply it. Or you can input protocol type and port number manually, click “add” button, then the item will displayed in the list.

Follow the following steps to set Internet Access Control:

1. You can select “enable” and click “Save” to enable “IP Firewall” function. This is only the first step, you should continued to create appropriate rules for “IP Firewall”.
2. Input description information for current access control rule in the “Description” field.
Input IP address of host you want to restrict
3. There are two items supplied, “Permit through the router for IP address listed, others are denied” and “Deny through the router for IP address listed, others are permitted”, Select the item you want, and click “Save” button
4. If you want to delete certain item on the list, select appropriate item on the list, click “delete” to delete it

4.6.3. DNS Filter

The screenshot shows the DNS Filter configuration page. At the top, there are three tabs: "MAC Filter", "Internet Access Control", and "DNS Filter". The "DNS Filter" tab is selected. Below the tabs, the page is divided into several sections:

- DNS Filter Parameter:** This section contains two rows of settings. The first row is "DNS Filter Status" with radio buttons for "Enable" and "Disable". The "Disable" button is selected. The second row is "Default DNS Filter Rule" with radio buttons for "Deny through the router for DNS Key words listed, others are Permitted" and "Permit through the router for DNS Key words listed, others are Denied". The "Permit" option is selected. Below these settings is a "Save" button.
- DNS Filter List Management:** This section contains a "Rule" dropdown menu set to "Permit", a "DNS Filter Key words" text input field, and two rows of checkboxes for "Days To Block" and "Times To Block". The "Days To Block" row has checkboxes for "Everyday" and days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). The "Times To Block" row has checkboxes for "All Day" and time range selectors (00:00 - 00:00). Below these settings is an "Add" button.
- Table and Navigation:** Below the settings is a table with columns: "ID", "DNS Filter Key words", "Days To Block", "Times To Block", "Rule", and "Del". Above the table is a navigation bar with "Items show in every single page 3", an "Apply" button, and a "Total 0 Pages" indicator. Below the table is a "Del All" button.

Figure 4-32

- DNS Filter Status: the default is disable. “DNS filter” is able to filter certain domain name such as www.sina.com
- Rule: you can select permit or deny. The default is permit
- DNS Filter Key words: Input website name or Domain name in the “DNS Key Words”

field, such as www.163.com.

Follow these steps to set DNS filter:

1. You can select “enable” and click “Save” to enable “DNS Filter” function. This is only the first step, you should continued to create appropriate rules for “DNS Filter”.
2. Input DNS Filter Key words
3. There are two items supplied, “Permit through the router for DNS Key words listed, others are denied” and “Deny through the router for DNS Key words listed, others are permitted”, Select the item you want, and click “Save” button
4. If you want to delete certain item on the list, select appropriate item on the list, click “delete” to delete it

4.7. LAN Setup

It includes LAN IP address, DHCP Server and DHCP Client Info. You can change the default IP address of LAN port by using this item, after changing IP address of LAN port, the router will restarted automatically. You can also choose enable or disable of the DHCP server, set the range of DHCP address pools

4.7.1. LAN IP address

LAN IP Address		DHCP Server	DHCP Client Info
System IP Setup			
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
			Save

Figure 4-33

The IP address of LAN port is used for access router itself by computers that connect to the router directly; here you can set IP address you need. The IP address format is like ***.**.*.**, and default IP address is 192.168.1.1, the default subnet mask is 255.255.255.0.

4.7.2. DHCP Server

DHCP Server Setup

DHCP Server Status : ☒ Enable ☐ Disable

IP Address Pool: 192.168.1.2 - 192.168.1.63

Lease Time(S): 86400

DHCP IP Address Reserving

☐ Auto Setup

Physical Address:

IP Address:

Table:

ID	IP Address	Physical Address	Del
----	------------	------------------	-----

Items show in every single page: 3 Apply Total 0 Pages

Figure 4-34

- DHCP Server Status: Keep the default setting “Enable”, so router is able to use DHCP function. If a DHCP server has already existed in the network, please select “Disable”.
- IP Address Pool: The IP Address pool is used for allocate IP address by DHCP server; The IP Address pool range is also changeable
- DHCP IP Address Reserving: reserve IP address for designed physical address host. If you want to configure a fixed IP address for some host, please input physical address and IP address, then click add

4.7.3. DHCP Client Info

DHCP Client Info

Items show in every single page: 3 Apply Total 1 Pages

ID	IP Address	MAC Address	Status
1	192.168.1.2	00:00:00:00:00:3f	Dynamic
2	192.168.1.3	00:23:ae:96:1f:1c	Dynamic

Figure 4-35

Display the state of assigned IP by DHCP Server

4.8. Applications and Gaming

This item provides configuration items and related templates about optimize games and

applications, including “Virtual service”, “DMZ setting”, “UPnP” and “Port Trigger”.

4.8.1. Virtual Server

Virtual Service | DMZ Setting | UPnP | Port Trigger

FTP Private Port

Status: ☐ Enable ☒ Disable

Port Number:

Save

Virtual Setting

Description:

Internal Host IP Address:

Protocol:

External Port: -

Internal Port:

Save

Items show in every single page Apply

ID	Description	Internal Host IP Address	Protocol	External Port	Internal Port	Del
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="First"/> <input type="button" value="Last"/> <input type="text" value="0"/> Total 0 Pages						

Figure 4-36

Some games, servers, and applications (such as BT, QQ video, Edunkey, Web server) are no longer effect when behind the NAT router, so this item provides function of port mapping from LAN to WAN.

- Description: Describe current virtual server item
- Internal Host IP Address: The “Internal Host IP Address” indicates IP address of the internal host using virtual server
- Protocol: The protocol item supplies several protocols. For example, if you have web server within LAN, you can select the HTTP template then the router will input port number 80 automatically
- External Port: Input an extranet port number (the users in Internet can see these ports)
- Internal Port: Input an intranet port number

4.8.2. DMZ

The screenshot shows the router's configuration page with four tabs: 'Virtual Service', 'DMZ Setting', 'UPnP', and 'Port Trigger'. The 'DMZ Setting' tab is selected. Below the tabs is a section titled 'DMZ Setup'. It contains two rows: the first row is 'DMZ Status' with radio buttons for 'Enable' and 'Disable', where 'Disable' is selected; the second row is 'DMZ Host IP Address' with a text input field containing '0.0.0.0'. A 'Save' button is located at the bottom right of the 'DMZ Setup' section.

Figure 4-37

DMZ opens all the ports of one computer, exposing the computer to the Internet. So it should only be used for some special-purpose, especial for Internet online games. Using this function you can select "DMZ" item and input IP address of DMZ host, then click "Save". For the purpose of security, we suggested that using "Virtual servicer" instead of "DMZ"

4.8.3. UPnP

The screenshot shows the router's configuration page with four tabs: 'Virtual Service', 'DMZ Setting', 'UPnP', and 'Port Trigger'. The 'UPnP' tab is selected. Below the tabs is a section titled 'UPnP'. It contains one row: 'UPnP Status' with radio buttons for 'Enable' and 'Disable', where 'Disable' is selected. A 'Save' button is located at the bottom right of the 'UPnP' section.

Figure 4-38

The UPnP function supports load Application's port forward record automatically. Select "Enable" to enable this function

4.8.4. Port Trigger

Figure 4-39

Port trigger module dynamically registers virtual server rules when any IP host generates the packet from the specified trigger protocol and port. Port trigger module use forward protocol type and port number and use the IP address of host that generates the trigger packet when it registers a rule.

- Predefined Trigger Rules: select one of the Predefined Rules
- Rule Name: describe one Predefined Trigger that you will configure
- Trigger Protocol: you can select TCP/UDP
- Trigger Port: you can select a part of ports
- Forward Protocol: you can select TCP/UDP
- Forward Port: you can select a part of ports

4.9. Application gateway

VPN is commonly used for encapsulate and encrypt data across the public network. For VPN tunnel, the router supports IPSEC pass-through, PPTP pass-through and L2TP pass-through

Figure 4-40

- PPTP Pass-through: PPTP means the “Point to Point Tunneling Protocol”, you can select “enable” to allow PPTP pass-through the router
- L2TP Pass-through: L2TP means the “Layer 2 Tunneling Protocol”, you can select “enable” to allow L2TP pass-through the router
- IPSEC Pass-through: IPSEC (Internet Protocol Security) is a suite of protocols used to implement secure exchange; you can select “enable” to allow IPSEC pass-through the router

4.10. DDNS

The DDNS feature allows you using domain name (not IP address) to access Internet. Before you can use this feature, you need to register an account for DDNS service at DDNS service providers, such as “roay.cn”, ”TZO.com”, ”DynDNS”. For more information, you can visit <http://www.oray.net/Help>

DDNS Setup	
DDNS Status :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DDNS Server Provider :	DynDNS <input type="button" value="v"/> www.dyndns.org
Username :	<input type="text"/>
Password :	<input type="text"/>
Dynamic Domain Name :	<input type="text"/>
Status :	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Refresh"/>	

Figure 4-41

- DDNS Status: Current status of DDNS server
- DDNS Server Provider: For example, if you want to use service of “roay.cn”, you have to first register and accounts for it. Other DDNS service providers as the same
- Username, Password, Dynamic Domain Name: After register an DDNS account from DDNS service providers, you will get “User Name”, “Password”, ”Dynamic Domain Name”, Input information in appropriate field

4.11. Routing

Most of broadband router and wireless router are using NAT mode, so this feature is designed for most common network environment

Routing

Routing Table Configuration

Type: NET

Destination Network or IP address:

Subnet Mask:

Next-Hop IP address:

Save

Items show in every single page 3 Apply Total 0 Pages

ID	Type	Dst IP address	Mask	Next-hop address	Del
----	------	----------------	------	------------------	-----

Figure 4-42

- Destination Network or IP Address: Specify a certain destination Network or IP address which static route forward to
- Subnet Mask: Subnet mask is used for distinguish Network portion and Host portion for an IP address
- Next-hop IP Address: This is an IP address of the next-hop device (and also is the gateway address for local host) that allows forwarding data between router and remote network or host
- Routing Table: You can check out all current route items, click “delete” button to delete an route item existed in routing table

4.12. System management

System management includes password setup, web Setup, upgrade, reboot, restore, WOL and System time

4.12.1. Password setup

Password Setup Web Setup Upgrade Reboot Restore WOL System Time

User name is: guest

New Password: ('Password' only include letter and number)

Confirm Password:

Save

Figure 4-43

The default username/password is guest/guest. To ensure the Router’s security, it is suggested that you change the default password to one of your choice, here enter a new password and then Re-enter it again to confirm your new password. Click “Save” button to save settings

4.12.2. Web setup

WEB Management	
WEB Management status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Management Port	<input type="text" value="8080"/>
Save	

Figure 4-44

WEB Management Status: the default is disable. Router can be accessed on the remote site using “Web setup”. Check the “Management Port” and enter the port number and then press “save” button to enable web management

4.12.3. Upgrade

Upgrade File	<input type="text"/> 浏览...
Upgrade	

Figure 4-45

Click "Browse..." button and select a File to upgrade, after you have selected the appropriate file, click "Upgrade" button to execute upgrade procedure. Do not cut off the power supply during the process of upgrading

4.12.4. Reboot

Restart

Figure 4-46

Click “Restart” button to restart the router

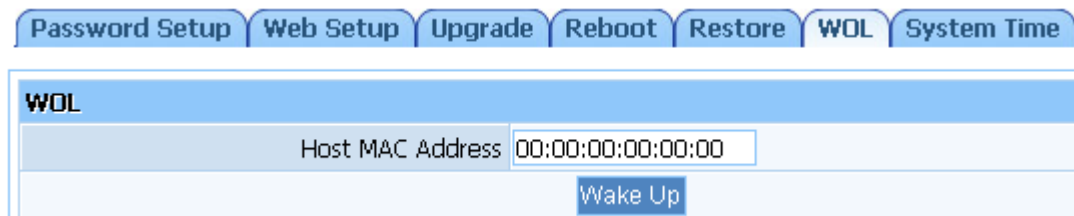
4.12.5. Restore

Restore

Figure 4-47

Click "Restore" button, the Router will erase all of your settings and replace them with the factory defaults, make sure you have backup current settings before click this button

4.12.6. WOL

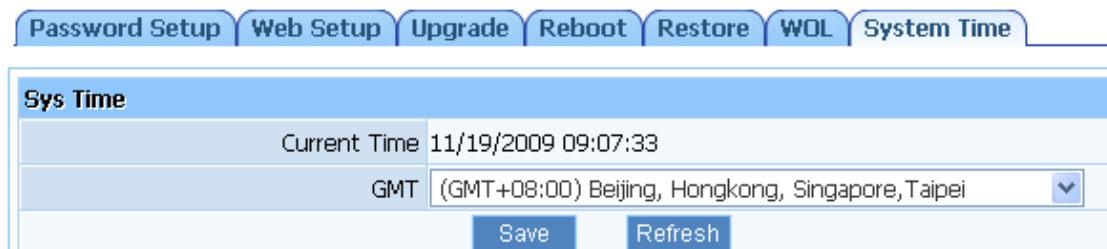


WOL	
Host MAC Address	00:00:00:00:00:00
<input type="button" value="Wake Up"/>	

Figure 4-48

Input host MAC address, and then click button of "Wake up" to wake up the target host which in the LAN

4.12.7. System time



Sys Time	
Current Time	11/19/2009 09:07:33
GMT	(GMT+08:00) Beijing, Hongkong, Singapore, Taipei
<input type="button" value="Save"/> <input type="button" value="Refresh"/>	

Figure 4-49

You can choose the time server and the time zone for the system time

5. FAQ

1. I cannot access the Web-based Configuration Utility from the Ethernet computer used to configure the router.

- Check that the LAN LED is on. If the LED is not on, verify that the cable for the LAN connection is firmly connected.
- Check whether the computer resides on the same subnet with the router's LAN IP address.
- If the computer acts as a DHCP client, check whether the computer has been assigned an IP address from the DHCP server. If not, you will need to renew the IP address.
- Use the ping command to ping the router's LAN IP address to verify the connection.
- Make sure your browser is not configured to use a proxy server.
- Check that the IP address you entered is correct. If the router's LAN IP address has been changed, you should enter the reassigned IP address instead.

2. I forget Password (Reset the Router without Login)

- Use a pencil to press the button for about 1-2 seconds with a pencil when it is working, then leave your hands, it will restore settings to the factory configuration. The default password is **guest**.

3. I have some problems related to Connection with Cable Modem

Please follow the following steps to check the problems:

- Check whether the DSL modem works well or the signal is stable. Normally there will be some indicator lights on the modem, users can check whether the signal is ok or the modem works well from those lights. If not, please contact the ISP.
- Check the front panel of the Router, there are also some indicator lights there. When the physical connection is correct, the Power light and the CPU light should be solid; the WAN light should be blinking. If you use your computer, the corresponding LAN port light should be blinking too. If not, please check whether the cables work or not.
- Repeat the steps in **WAN Setup** Connect with Internet through DSL Modem.

4. I can browse the router's Web-based Configuration Utility but cannot access the Internet.

- Check if the WAN LED is ON. If not, verify that the physical connection between the router and the DSL/Cable modem is firmly connected. Also ensure the DSL/Cable modem is working properly.
- If WAN LED is ON, open the System Overview page of the Web configuration utility and

check the status group to see if the router's WAN port has successfully obtained an IP address.

- Make sure you are using the correction method (Dynamic IP Address, PPPoE, or Static IP) as required by the ISP. Also ensure you have entered the correct settings provided by the ISP.
- For cable users, if your ISP requires a registered Ethernet card MAC address, make sure you have cloned the network adapter's MAC address to the WAN port of the router. (See the **MAC Address** field in **WAN Setup**.)

5. My wireless client cannot communicate with another Ethernet computer.

- Ensure the wireless adapter functions properly. You may open the Device Manager in Windows to see if the adapter is properly installed.
- Make sure the wireless client uses the same SSID and security settings (if enabled) as the 300Mbps wireless-N Broadband Router.
- Ensure that the wireless adapter's TCP/IP settings are correct as required by your network administrator.
- If you are using a 802.11b wireless adapter, and check that the **802.11G Mode** item in **Wireless Basic Setting** page, is not configured to use 802.11G Performance.
- Use the ping command to verify that the wireless client is able to communicate with the router's LAN port and with the remote computer. If the wireless client can successfully ping the router's LAN port but fails to ping the remote computer, then verify the TCP/IP settings of the remote computer.