Wireless Broadband Router

User Manual

V2.0

2009-6-5

Package Contents

The following items should be found in your package

- One Wireless Broadband Router
- One DC 9v power adapter
- One QIG
- One CD

Please make sure that the package contains the above items, if any of the listed items are damaged or missing, please contact with your distributor.

Contents

1. Introduction

1.1. Product Overview

This Wireless Broadband Router is a cost-effective IP Sharing Router that enables multiple users to share the Internet through an ADSL or cable modem. Simply configure your Internet connection settings in the Wireless Broadband Router and plug your PC to the LAN port and you're ready to share files and access the Internet. As your network grows, you can connect another hub or switch to the router’s LAN ports, allowing you to easily expand your network. The Wireless Broadband Router is embedded with a IEEE 802.11g/b access point that allows you to build up a wireless LAN. With the support of new emerged 802.11g standard, the access point provides data transfer of up to 54Mbps, up to 5 times faster than 802.11b, it is backwards compatible with existing 802.11b infrastructure while migrating to the new screaming fast 802.11g.The Wireless Broadband Router provides a total solution for the Small and Medium-sized Business (SMB) and the Small Office/Home Office (SOHO) markets, giving you an instant network today, and the flexibility to handle tomorrow's expansion and speed.

1.2. Main Features

- Complies with IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u standards
- Supports Auto MDI/MDIX
- Supports 54/48/36/24/18/12/9/6/11/5.5/2/1Mbps wireless LAN data transfer rates
- Supports Virtual Server, and DMZ host
- Built-in firewall supporting IP address filtering, Port filtering, URL filtering, MAC address filtering and so on
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT
- Supports Dynamic DNS, Static Routing, VPN pass-through
- Supports Flow Statistics
- Supports firmware upgrade
- Supports Web management
- Shares data and Internet access for users, supporting PPPoE, Dynamic IP, Static IP and PPTP Internet access
- Provides 64/128-bit WEP encryption security
- Provides wireless LAN ACL (Access Control List) filtering
- Built-in NAT and DHCP server supporting static IP address distributing
- Provides WPA/WPA2 authentication and TKIP/AES encryption security

1.3. Supporting Standard and Protocol

- IEEE 802.11b/g/n
- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX

1.4. Working Environment

Temperature

- 0° to 50° 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

- Broadband Internet Access Service(DSL/Cable/Ethernet)
- 10/100Base-T Ethernet card and TCP/IP protocol installed for each PC
- Internet Explorer 5.0 or higher for Web configuration
- 802.11g or 802.11b compliant wireless adapters (for wireless connection)

2.2. Panel

Front panel

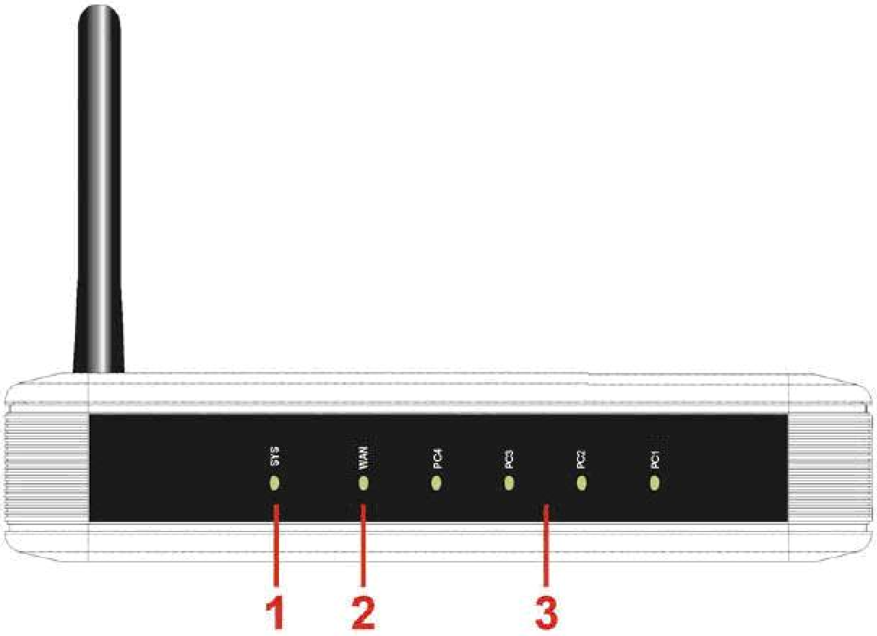


Figure 2-1

LED	Function	
PWR	Flashing	Power on CPU on WLAN ACT
	Off	Power 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

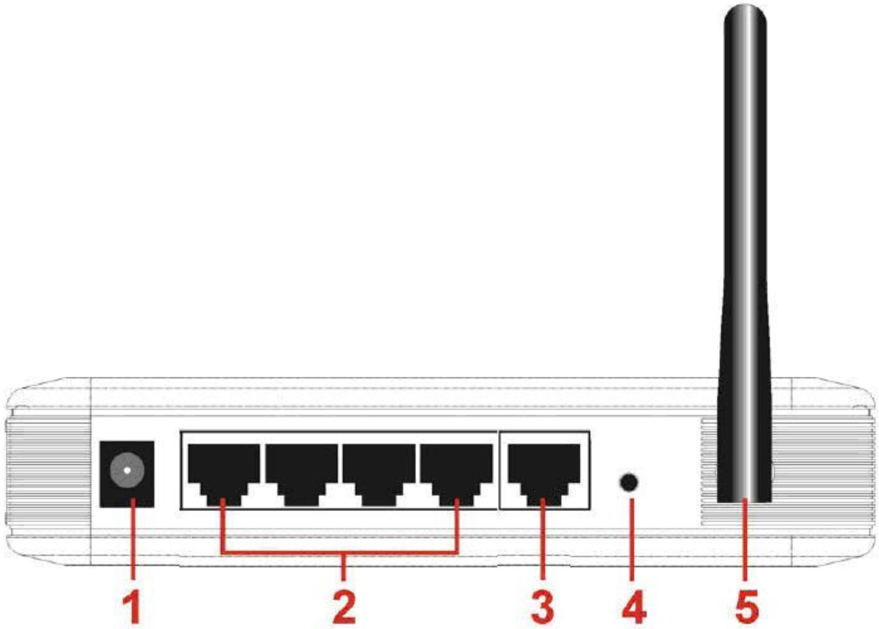


Figure 2-2

Number	Description	Function
1	PWR port	Connect to Power adapter, please don't use the unknown power adapter, otherwise your device may be damaged.
2	LAN port	Connect with computer NIC or Ethernet device
3	WAN port	Internet access
4	Default	Restore settings, please press the button for about 10 seconds, it will restore settings to the factory configuration
5	Antenna	

2.3. Hardware Installation Procedures

The procedures to install the wireless broadband router please refer to Figure 2-3.

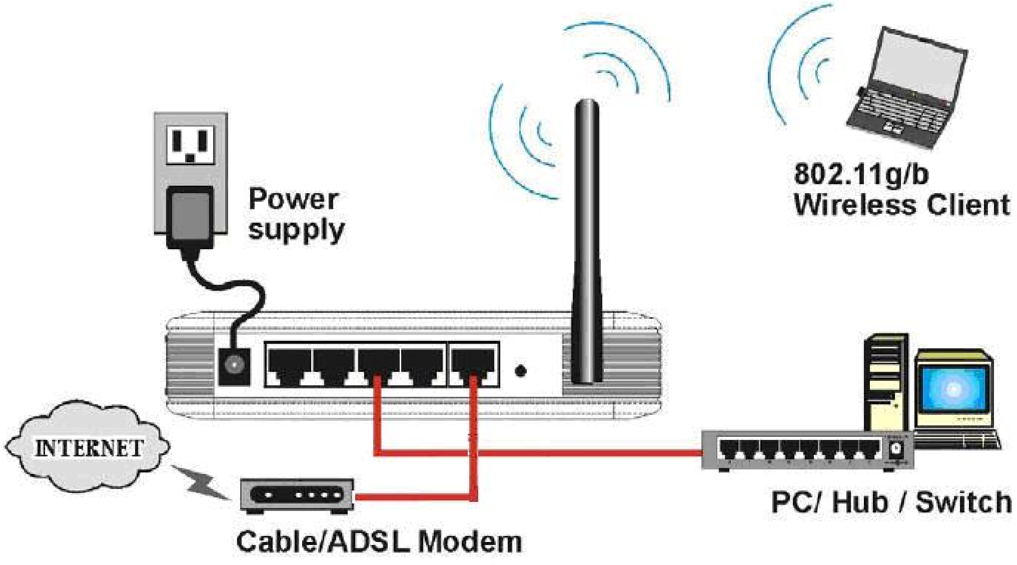


Figure 2-3

- Step 1 connecting your computer to the LAN port.

Attach one end of the Ethernet cable with RJ-45 connector to your hub, switch or a computer's Ethernet port, and the other end to one of the LAN ports of your Wireless Broadband Router.

- Step 2 Connecting Cable/ADSL Modem to the WAN port.

Connect the Ethernet cable attaching to your Cable/ADSL modem to the WAN port of your Wireless Broadband Router.

- Step 3 connecting the power adapter.

Connect the single DC output connector of the power adapter to the power jack on the side of the Wireless Broadband Router. Then plug the Power Adapter into an AC outlet.

- Step 4 Power on the following devices in this order:

Cable/ADSL modem, Router, and PCs

2.3.1. Additional Settings for Wireless Client

If you choose to access the router via a wireless client, also verify the following:
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.
2. Set the wireless adapter to use appropriate TCP/IP settings as described in previous section.

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.

2.3.2. 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:

```
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.

3. Login

You can manage the Wireless 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 Wireless Broadband 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. Before setting up the Router, make sure your PCs are configured to obtain an IP address automatically from the Router by the steps below.

3.1. Configure computer

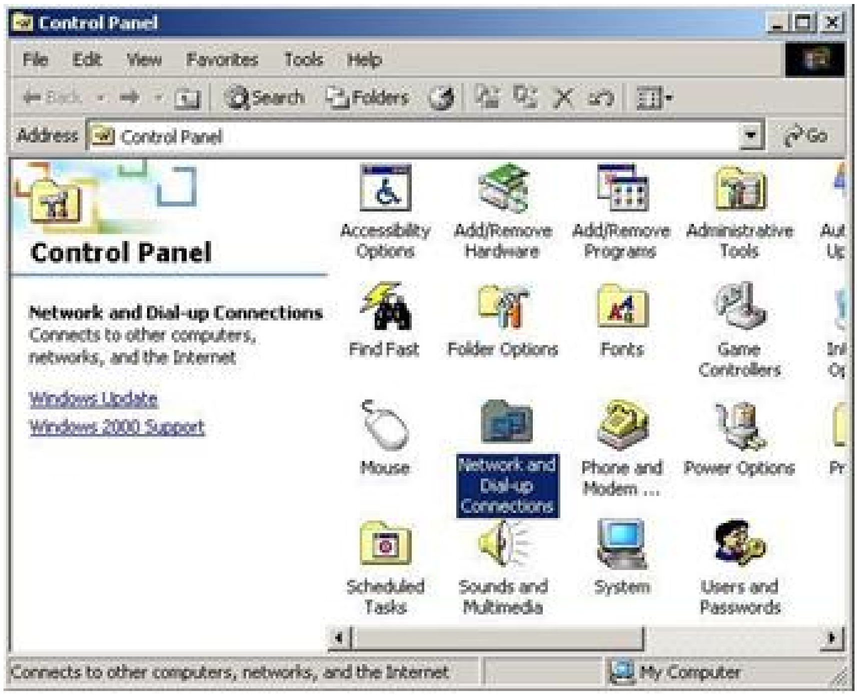
3.1.1. Windows 98/Me

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



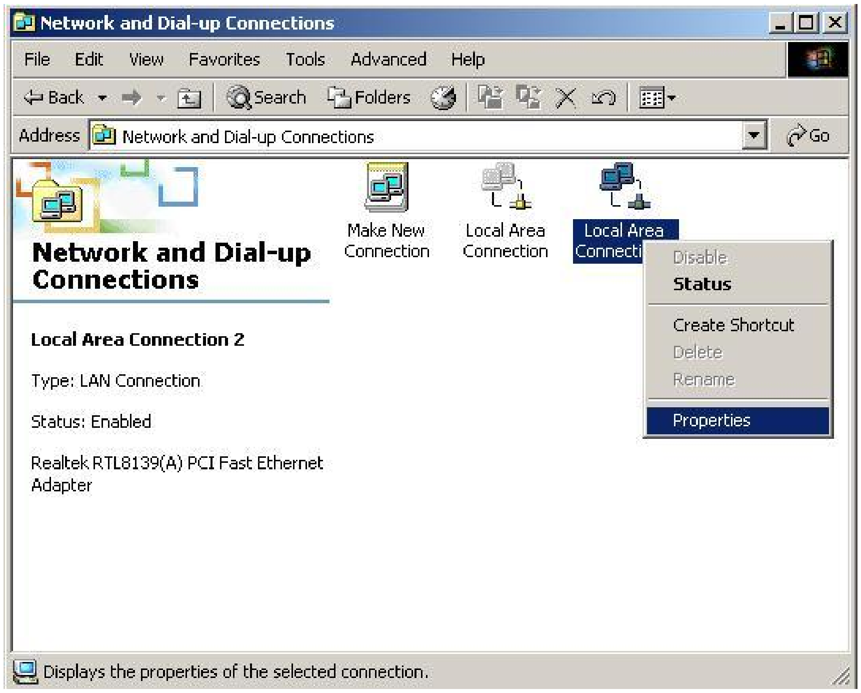
Network and Dial-up Connections
Connects to other computers, networks, and the Internet

Connects to other computers, networks, and the Internet

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


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Local Area Connection
Local Area Connecti
Disable
Status
Create Shortcut
Delete
Rename
Properties

Local Area Connection 2

Type: LAN Connection

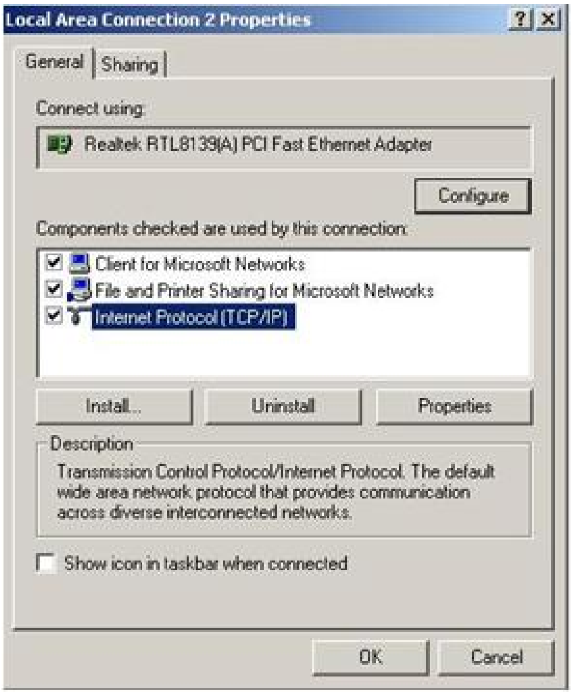
Status: Enabled

Realtek RTL8139(A) PCI Fast Ethernet Adapter

Displays the properties of the selected connection.

Figure 3-2

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



Local Area Connection 2 Properties

General | Sharing

Connect using:

Realtek RTL8139(A) PCI Fast Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

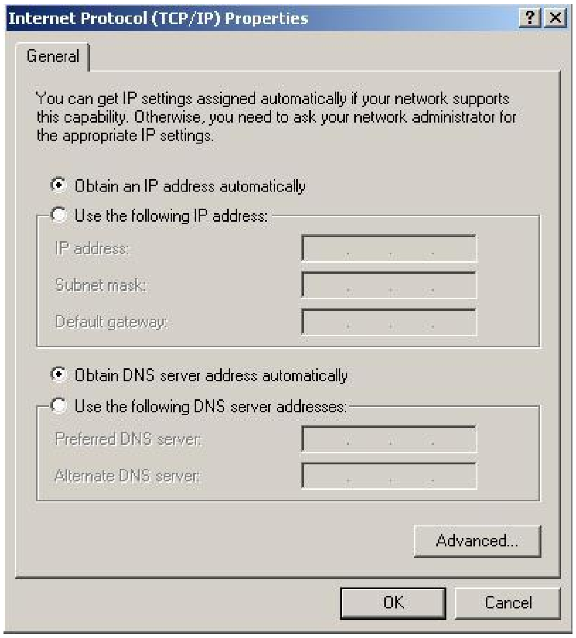
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

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



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

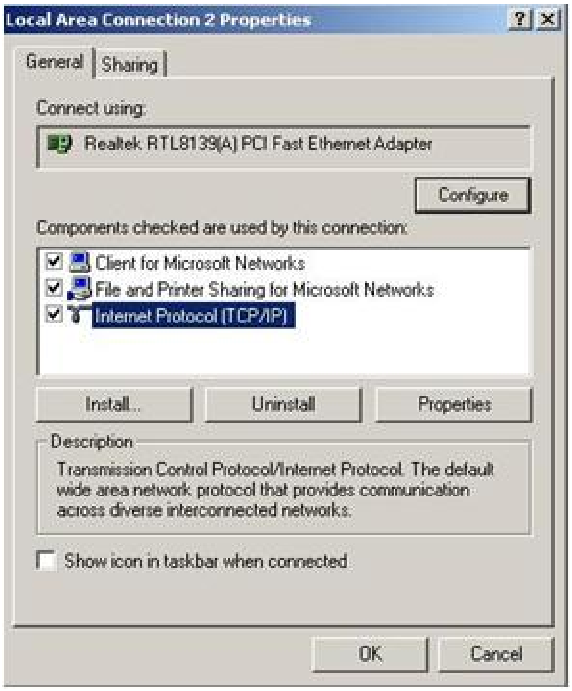
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Figure 3-4

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



Local Area Connection 2 Properties

Connect using:

Realtek RTL8139(A) PCI Fast Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

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

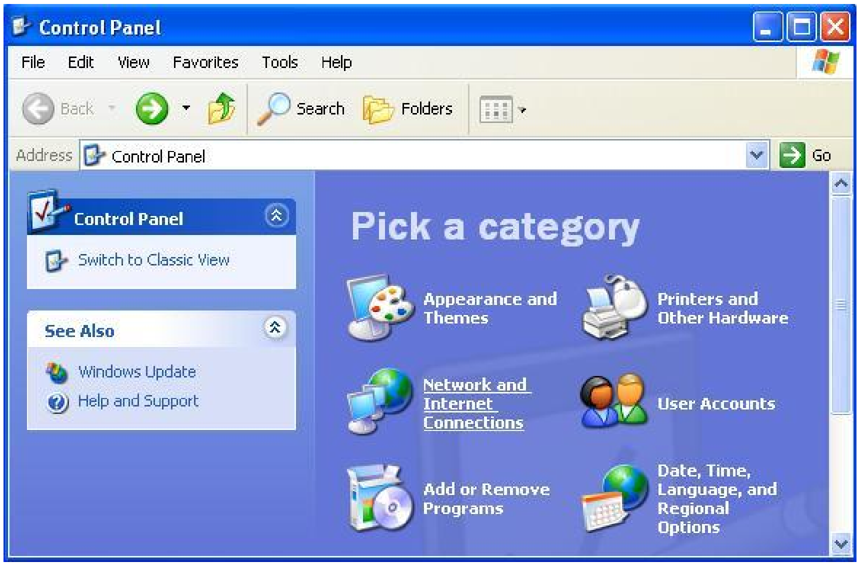


Figure 3-6

3. Click Network Connections

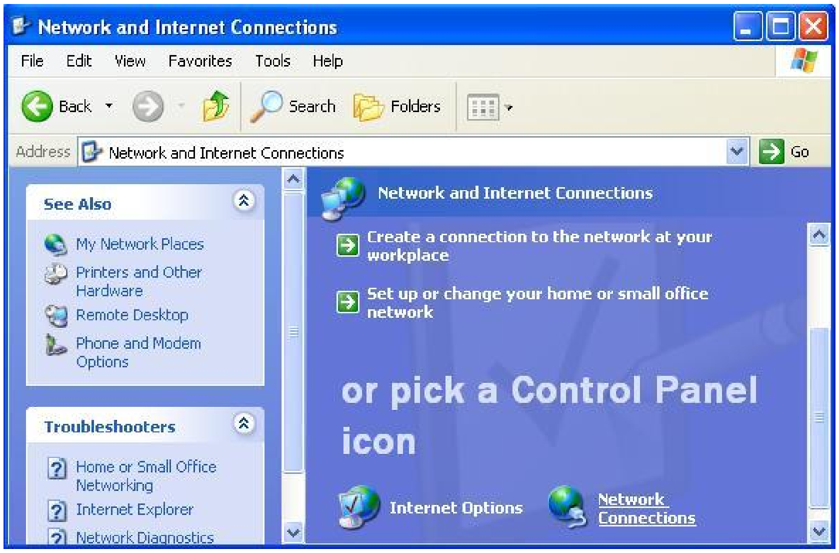

Network and Internet Connections
File Edit View Favorites Tools Help
Back
Search
Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Create a connection to the network at your workplace
Set up or change your home or small office network
or pick a Control Panel icon
Internet Options
Network Connections

Figure 3-7

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

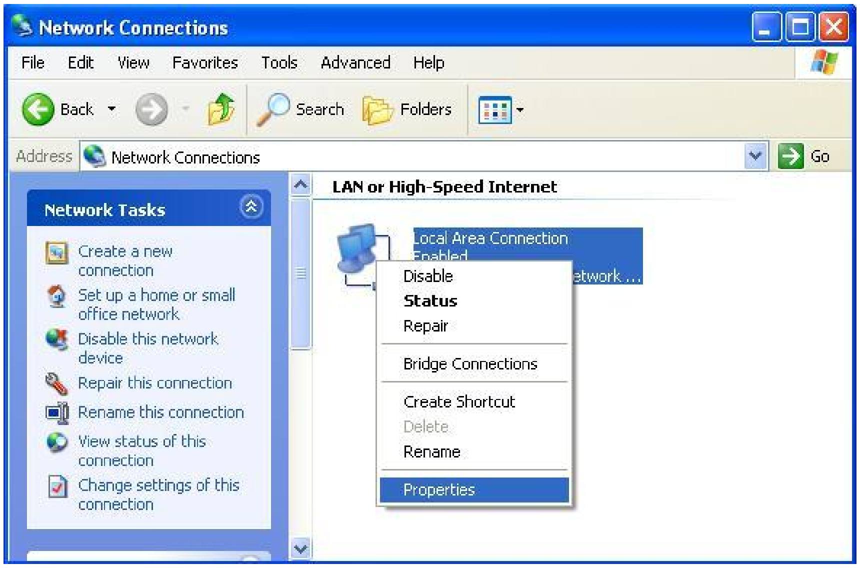
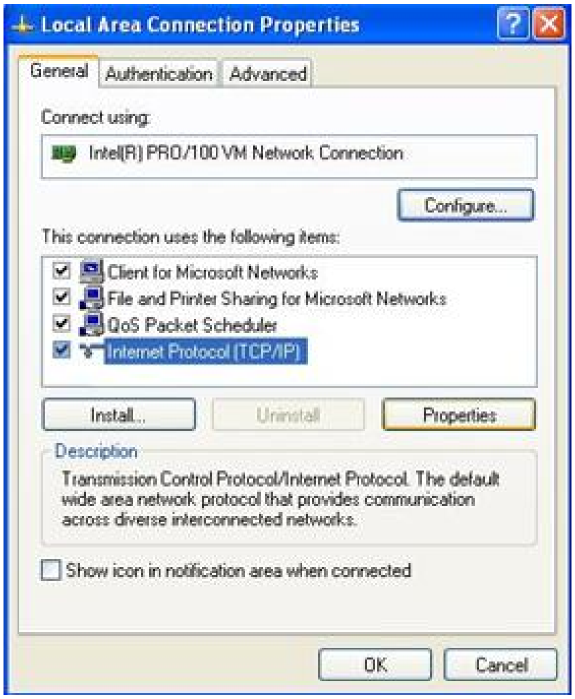


Figure 3-8

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



Connect using:

Intel(R) PRO/100 VM Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

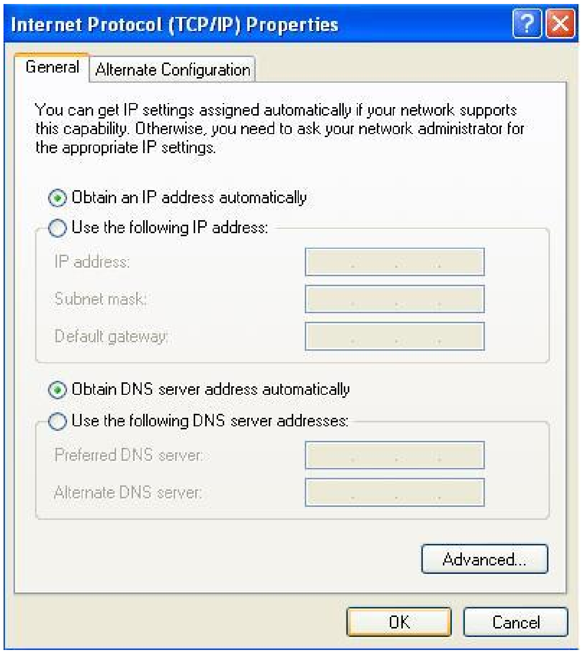
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

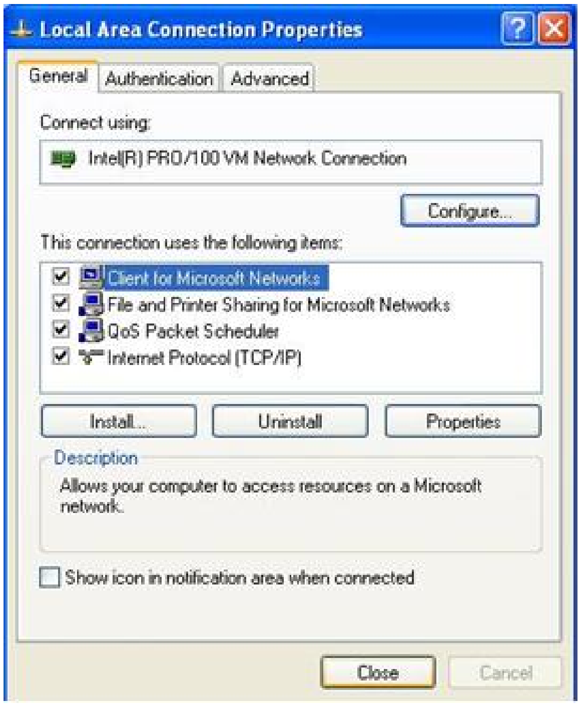
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 3-10

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



Connect using:

Intel(R) PRO/100 VM Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

□ Show icon in notification area when connected

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

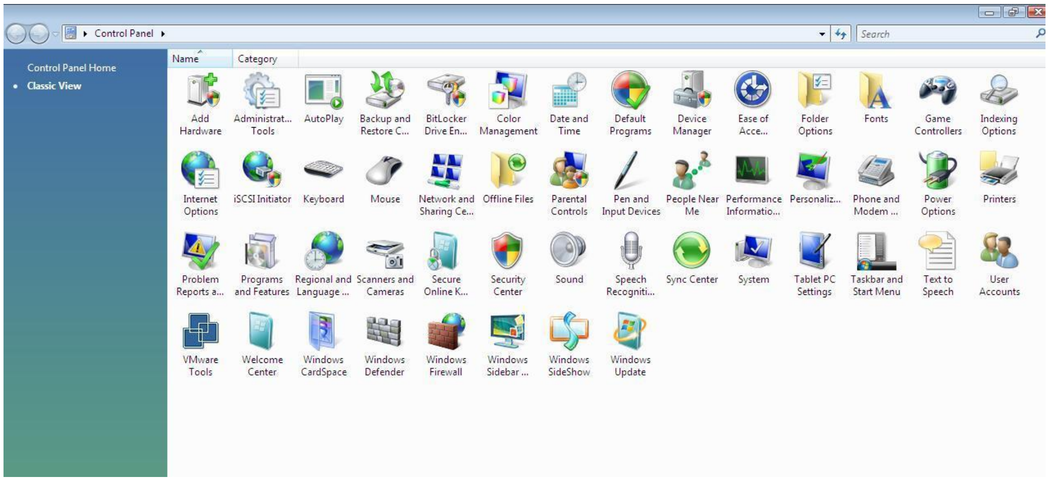
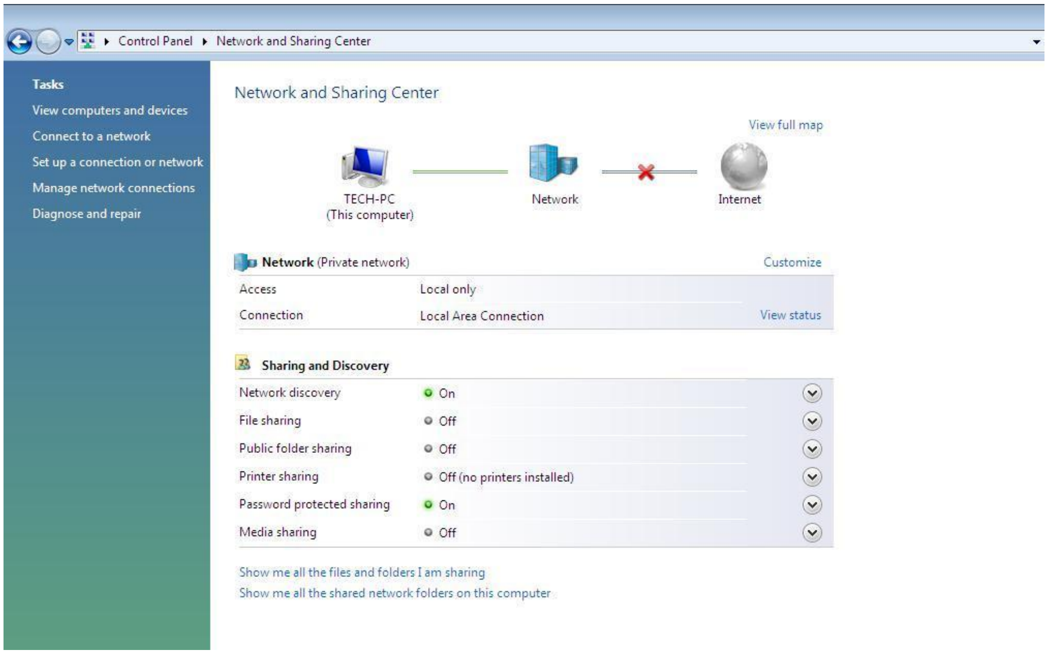


Figure 3-12

3. Click Manage Network Connections


Control Panel ▸ Network and Sharing Center
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
View full map
TECH-PC
(This computer)
Network
Internet
Customize
View status
Show me all the files and folders I am sharing
Show me all the shared network folders on this computer

Network and Sharing Center

Network (Private network)

Access	Local only
Connection	Local Area Connection

Sharing and Discovery

Network discovery	● On
File sharing	● Off
Public folder sharing	● Off
Printer sharing	● Off (no printers installed)
Password protected sharing	● On
Media sharing	● Off

Figure 3-13

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

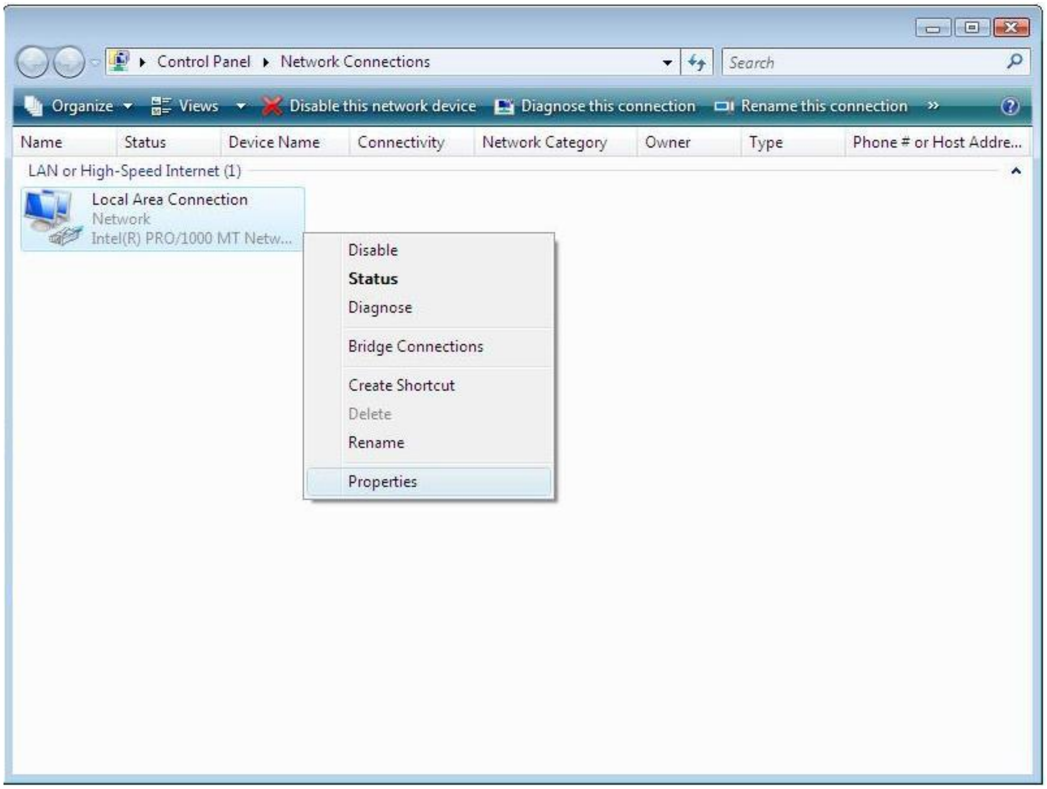
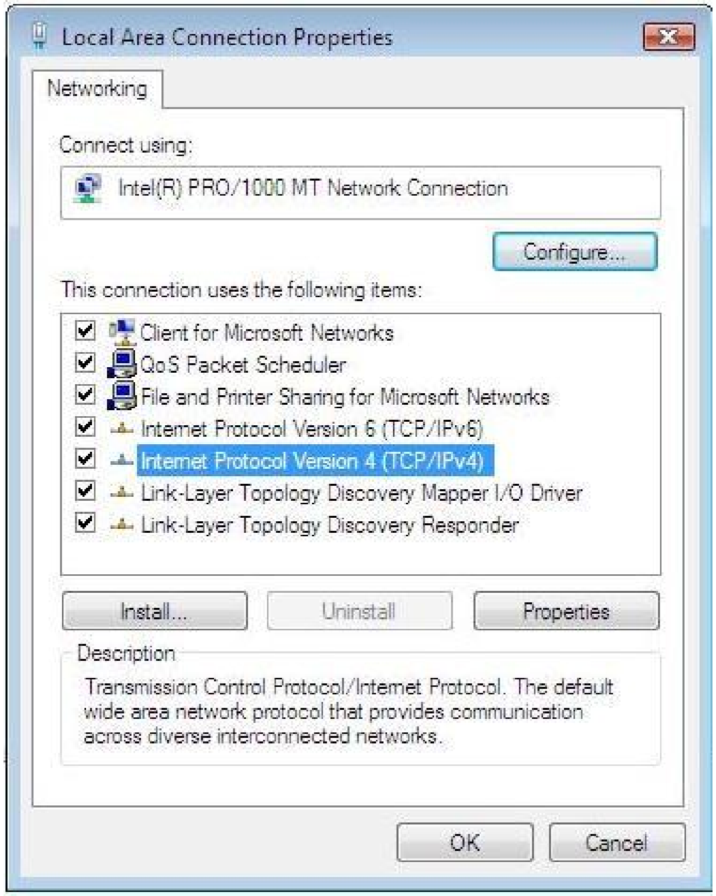


Figure 3-14

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



Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

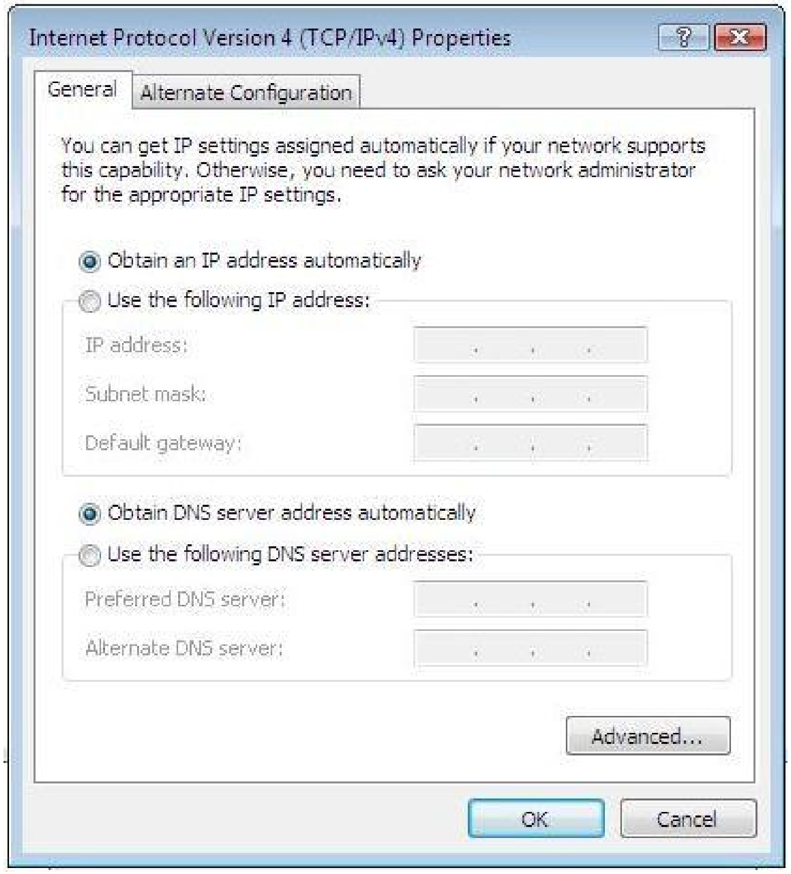
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

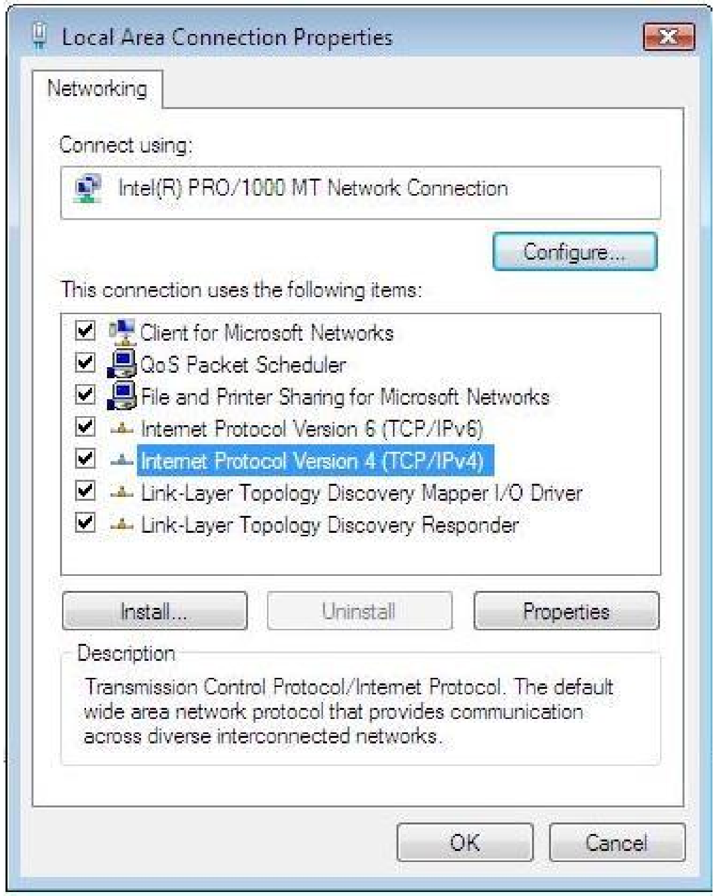
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 3-16

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



Local Area Connection Properties

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 3-17

3.2. Additional Settings for Wireless Client

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

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

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

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

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:

```
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:

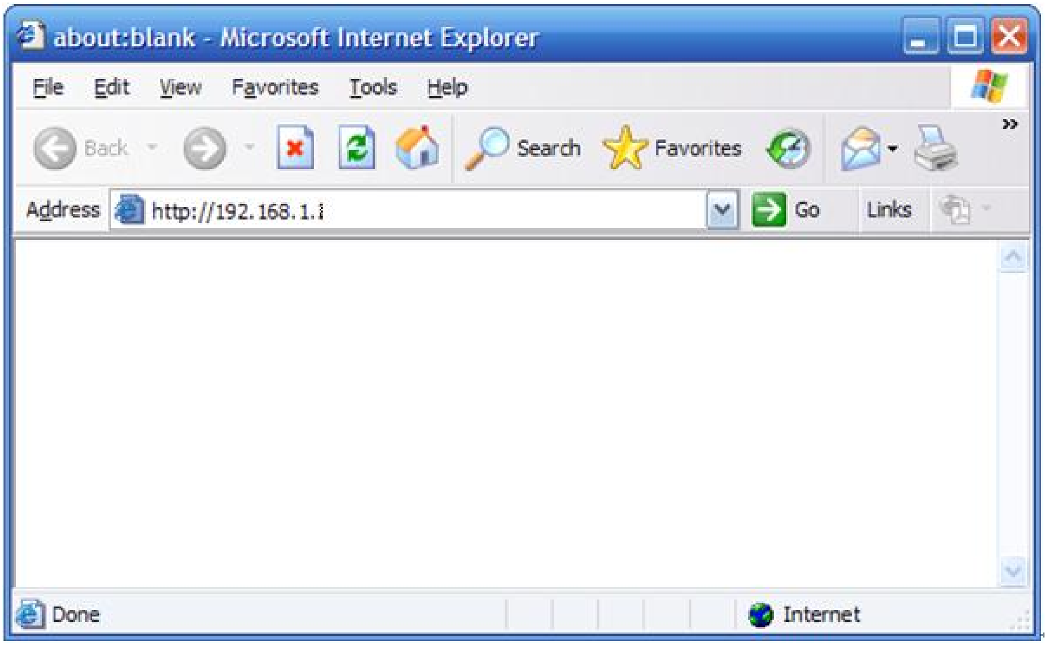
```
C:\Documents and Settings\admin>ping 192.168.1.1

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 Wireless Router through your computer has a WEB browser installed. Please follow up the steps listed below.

3.4. Login

1.Startup Internet Explorer，and enter http://192.168.1.1, then press Enter

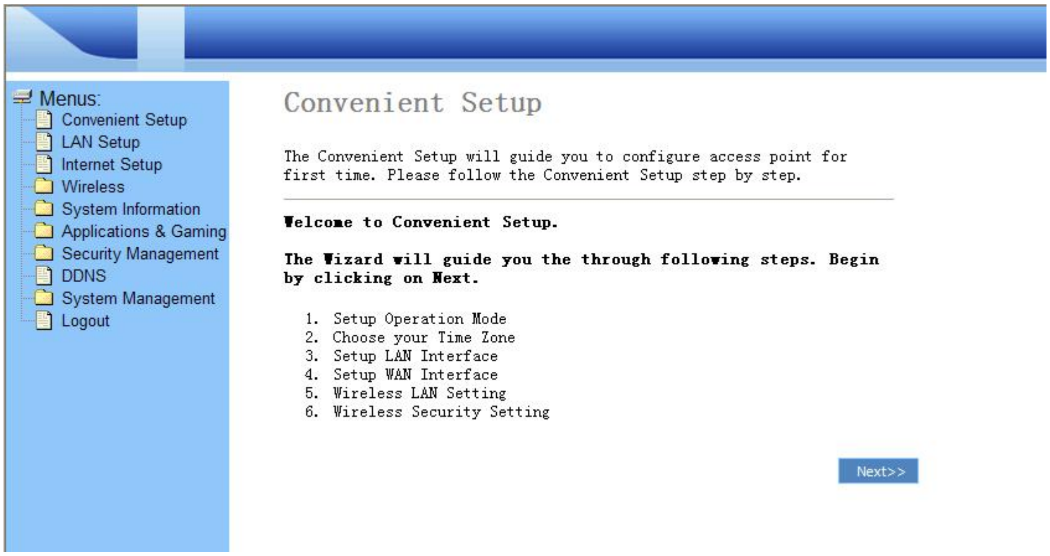


http://192.168.1.1

Figure 3-18

2. After successful login, you will be able to see the Wireless Broadband Router's web-based configuration utility refer to Figure 3-19. From now on the Wireless Broadband Router acts as a Web server sending HTML pages/forms at your request. You can click the menu options at the left to start the configuration task.

In the home 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.



Convenient Setup

The Convenient Setup will guide you to configure access point for first time. Please follow the Convenient Setup step by step.

Welcome to Convenient Setup.

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

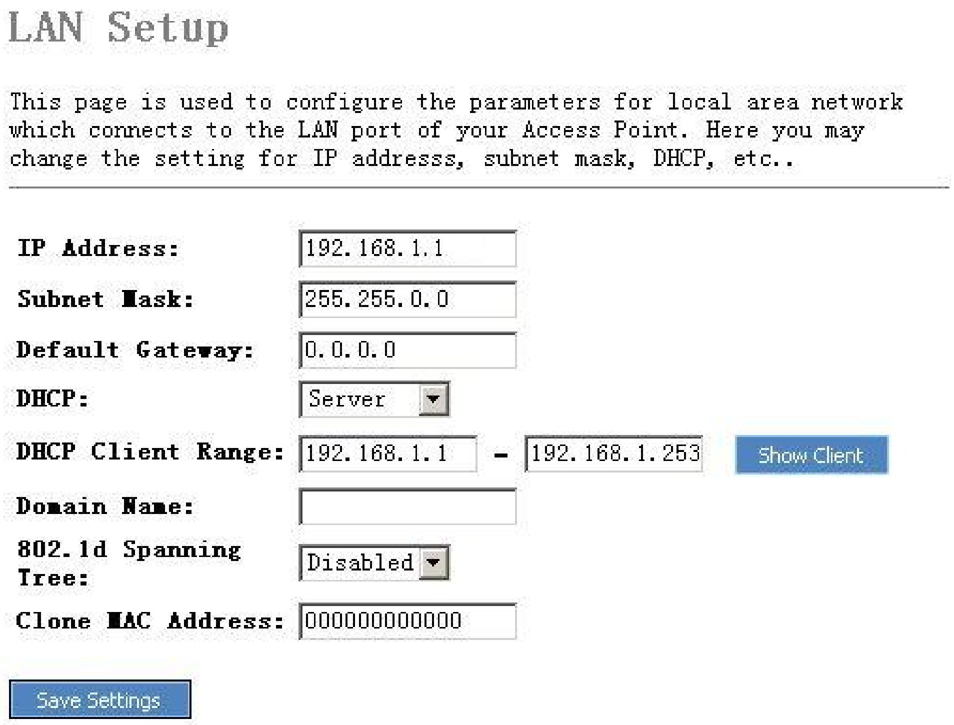
1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Figure 3-19

4. System configuration

4.1. LAN Setup

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.



LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.1
Subnet Mask:	255.255.0.0
Default Gateway:	0.0.0.0
DHCP:	Server ▼
DHCP Client Range:	192.168.1.1 - 192.168.1.253 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled ▼
Clone MAC Address:	000000000000

Figure 4-1

- **IP Address**
  This is the router's LAN port IP address (Your LAN clients default gateway IP address), the default is **192.168.1.1**
- **Subnet Mask**
  Specify a Subnet Mask for your LAN segment
- **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 blank.
- **DHCP Server**
  You can enable or disable the DHCP server. By enabling the DHCP server the router will automatically give your LAN clients an IP address. If the DHCP is selected client, the router will get an IP address from the other DHCP Server
- **DHCP Client Range**

You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.

- **Domain name**

  put into a name to mark your DHCP SERVER

- **802.1d Spanning tree**

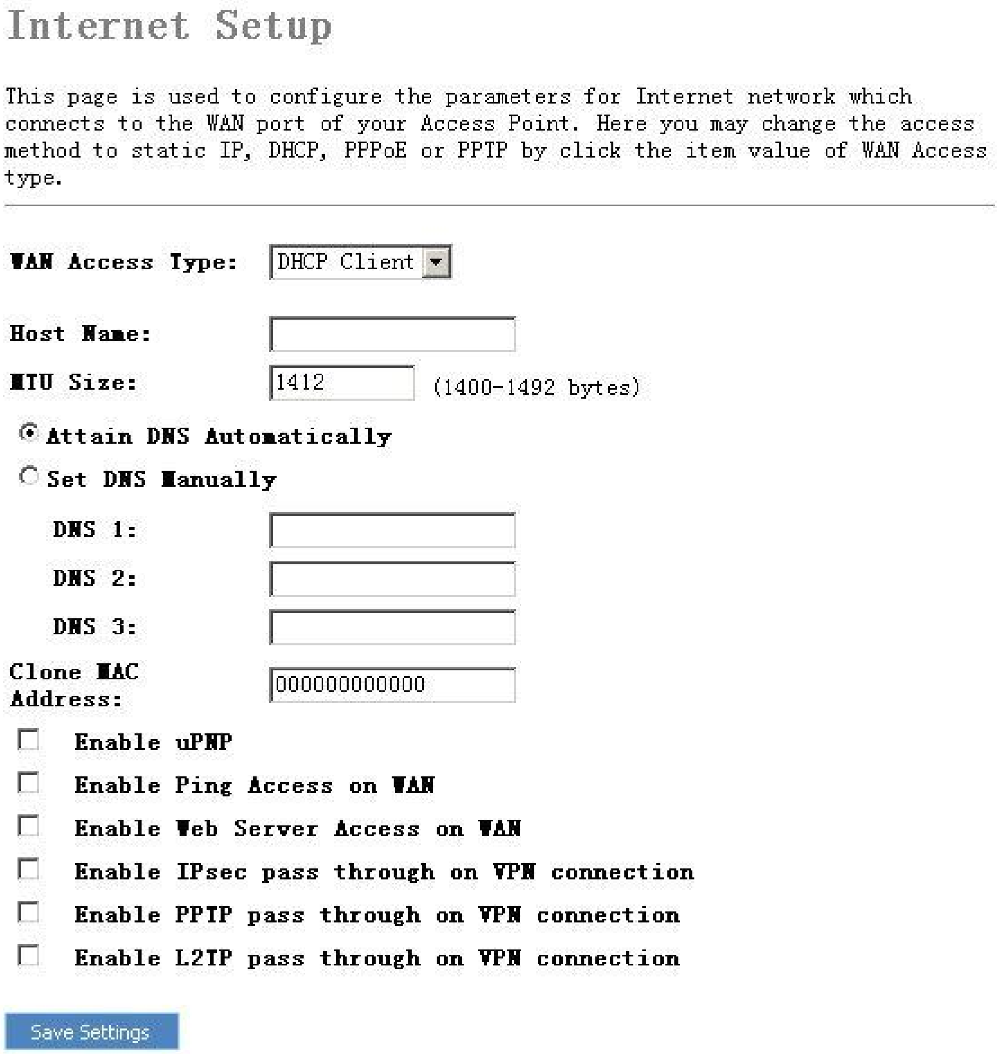
  You can enable or disable the Spanning tree for your router

- **Clone MAC address**

  Replace the LAN MAC address with the MAC address of that PC

4.2. Internet Setup

Configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.



Internet Setup

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

WAN Access Type:	DHCP Client ▾
Host Name:	
MTU Size:	1412 (1400-1492 bytes)

● **Attain DNS Automatically**

○ **Set DNS Manually**

DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

□ **Enable uPNP**

□ **Enable Ping Access on WAN**

□ **Enable Web Server Access on WAN**

□ **Enable IPsec pass through on VPN connection**

□ **Enable PPTP pass through on VPN connection**

□ **Enable L2TP pass through on VPN connection**

Figure 4-2

- **Static IP address**

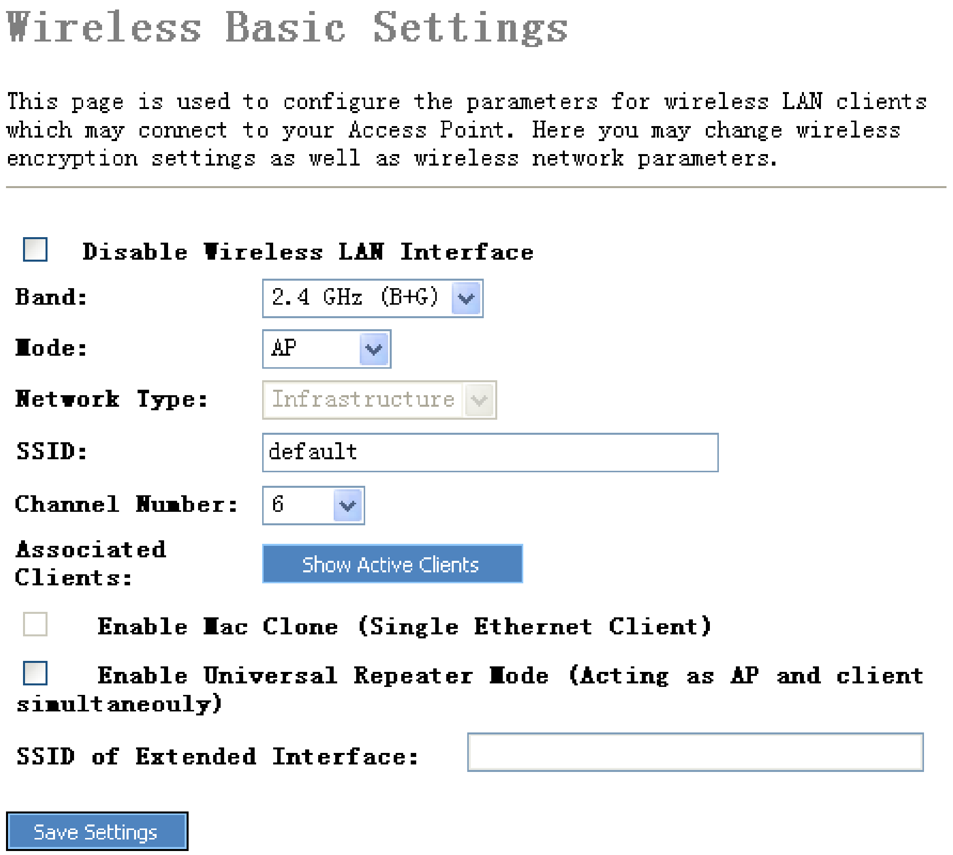
Your ISP has given you an IP address already

- **DHCP Client**
  Your ISP will automatically give you an IP address.
- **PPPoE**
  Your ISP requires PPPoE connection
- **PPTP**
  Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
- **DNS**
  You can specify a DNS server that you wish to use
- **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.
- **Clone MAC Address**
  Replace the WAN MAC address with the MAC address of that PC

4.3. Wireless

4.3.1. Basic Setting

The wireless router supplies the function of act as two AP simultaneously, but because the difference of privilege, besides normal function of AP, the primary AP also has extra function for some advanced settings and right management. So here you can manage and configure your primary AP.



Wireless Basic Settings

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

☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G)
Mode:	AP
Network Type:	Infrastructure
SSID:	default
Channel Number:	6
Associated Clients:	Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Figure 4-3

- **Mode**

  It allows you to set the Wireless AP to AP, Client, WDS or AP+WDS mode. The default is AP mode.
- **Band**

  It allows you to set the AP fix at 802.11b or 802.11g mode. You also can select B+G mode to allow the AP select 802.11b and 802.11g connection automatically.
- **Network Type**

  There are two type, infrastructure and hoc, the default is infrastructure
- **SSID**

  This is the name of the wireless LAN. All the devices in the same wireless LAN should have the same SSID, the default SSID is default.
- **Channel Number**

  The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
- **Associated Clients**

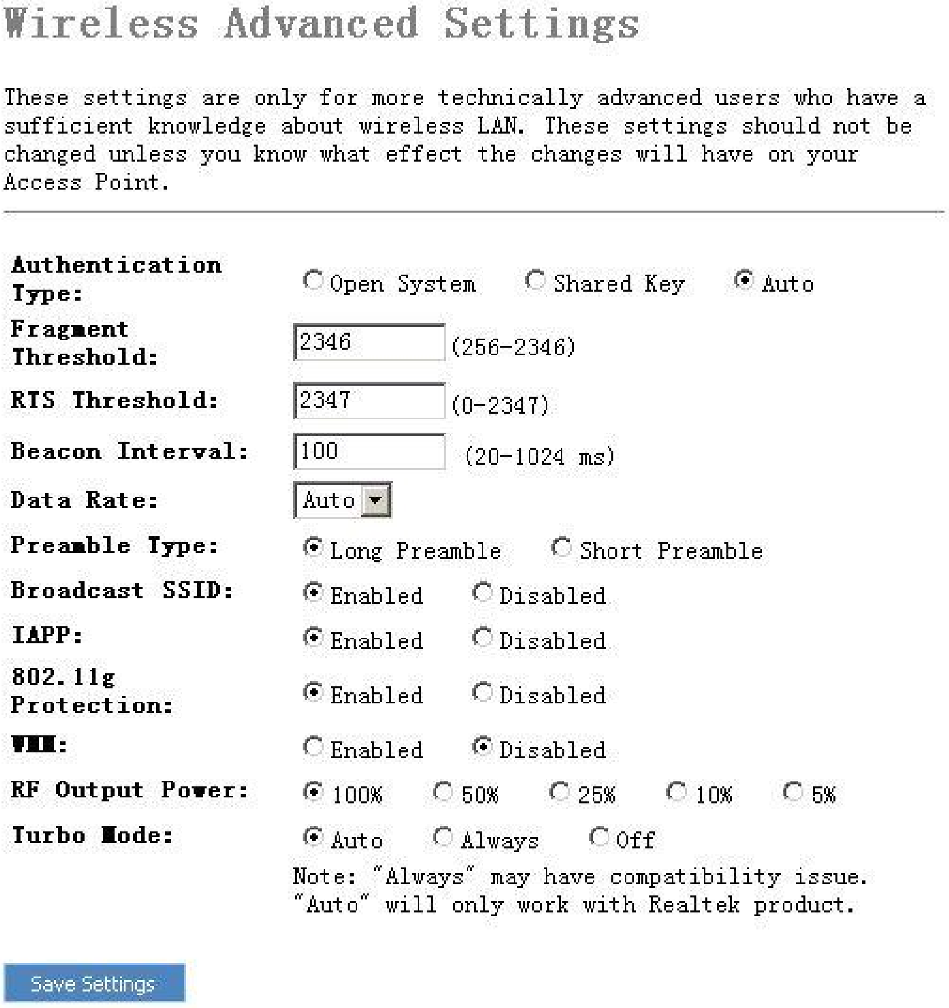
  Click “Show Active Clients” button, then an “Active Wireless Client Table” will pop up. You can see the status of all active wireless stations that are connecting to the access point.
- **Enable Mac Clone**

  Click the “Enable MAC Clone” button will copy the MAC address of your PC, that you are using to configure the AP, to the WLAN MAC.

- **Enable Universal Repeater Mode**
  To Enable Universal Repeater Mode, Acting as AP and client simultaneously

4.3.2. Advanced Setting

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Preamble Type …… You should not change these parameters unless you know what effect the changes will have on this router.



Wireless Advanced Settings

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

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
IAPP:	● Enabled ○ Disabled
802.11g Protection:	● Enabled ○ Disabled
WMM:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	● Auto ○ Always ○ Off Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

Figure 4-4

- **Authentication Type**
  There are two authentication types: "Open System" and "Shared Key". When you select "Open System", wireless stations can associate with this wireless router without WEP encryption. When you select "Shared Key", you should also setup WEP key in the "Encryption" page and wireless stations should use WEP encryption in the authentication phase to associate with this wireless router. If you select "Auto", the

wireless client can associate with this wireless router by using any one of these two authentication types.

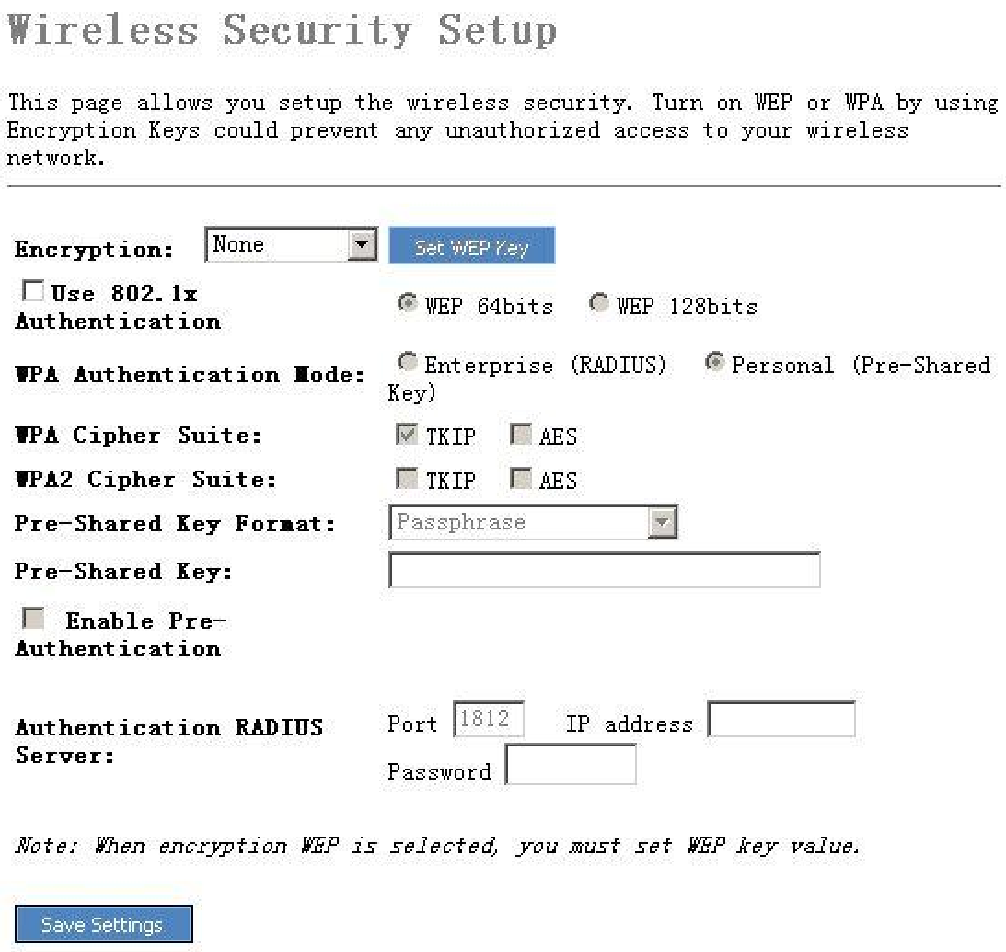
- **Fragment Threshold**
  "Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted.
- **RTS Threshold**
  When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
- **Beacon Interval**
  The interval that this wireless router broadcast a beacon, Beacon is used to synchronize the wireless network.
- **Data Rate**
  The “Data Rate” is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
- **Preamble Type**
  The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance
- **Broadcast SSID**
  If you enable “Broadcast SSID”, every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast SSID” can provide better security.
- **IAPP**
  If you enable “IAPP”, it will allow wireless station roaming between IAPP enabled access points within the same wireless LAN.
- **802.11g Protection**
  This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.

Click “Save Setting” at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

4.3.3. Security

This Access Point provides complete wireless LAN security functions, include WEP, WPA (TKIP), WPA2 (AES), WPA2 Mixed. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

4.3.3.1. None



Wireless Security Setup

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

Encryption: None ▾

☐ **Use 802.1x Authentication** ● WEP 64bits ○ WEP 128bits

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

WPA Cipher Suite: ☑ TKIP ☐ AES

WPA2 Cipher Suite: ☐ TKIP ☐ AES

Pre-Shared Key Format: Passphrase ▾

Pre-Shared Key:

☐ **Enable Pre-Authentication**

Authentication RADIUS Server: Port 1812 IP address

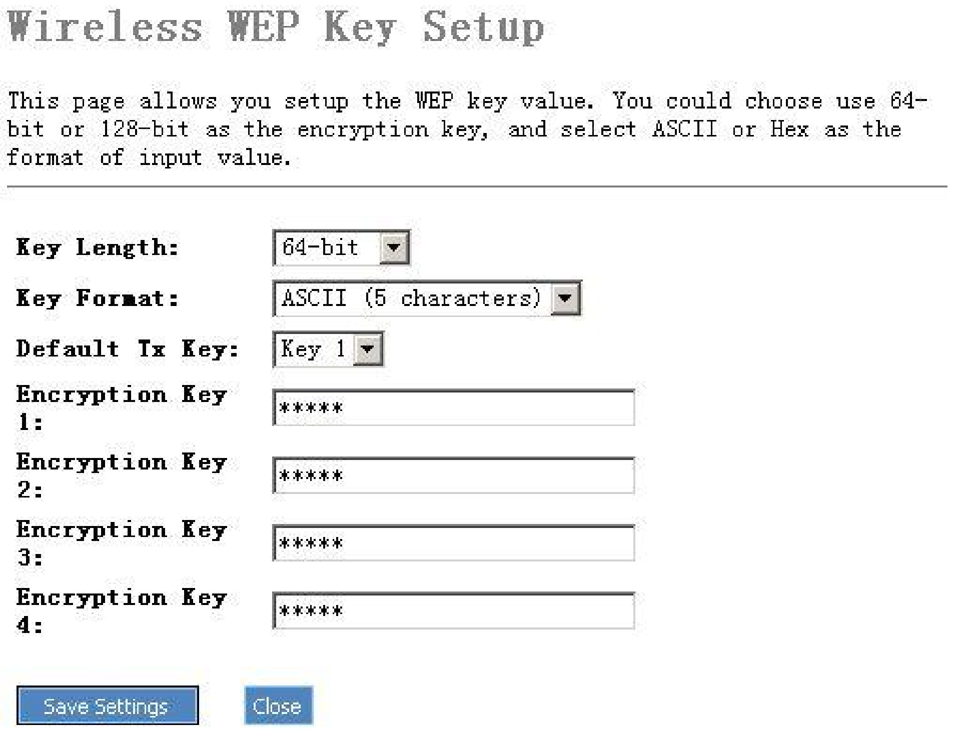
Password

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

Figure 4-5

4.3.3.2. WEP only

When you select 64-bit or128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys



Wireless WEP Key Setup

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

Key Length:	64-bit
Key Format:	ASCII (5 characters)
Default Tx Key:	Key 1
Encryption Key 1:	*****
Encryption Key 2:	*****
Encryption Key 3:	*****
Encryption Key 4:	*****

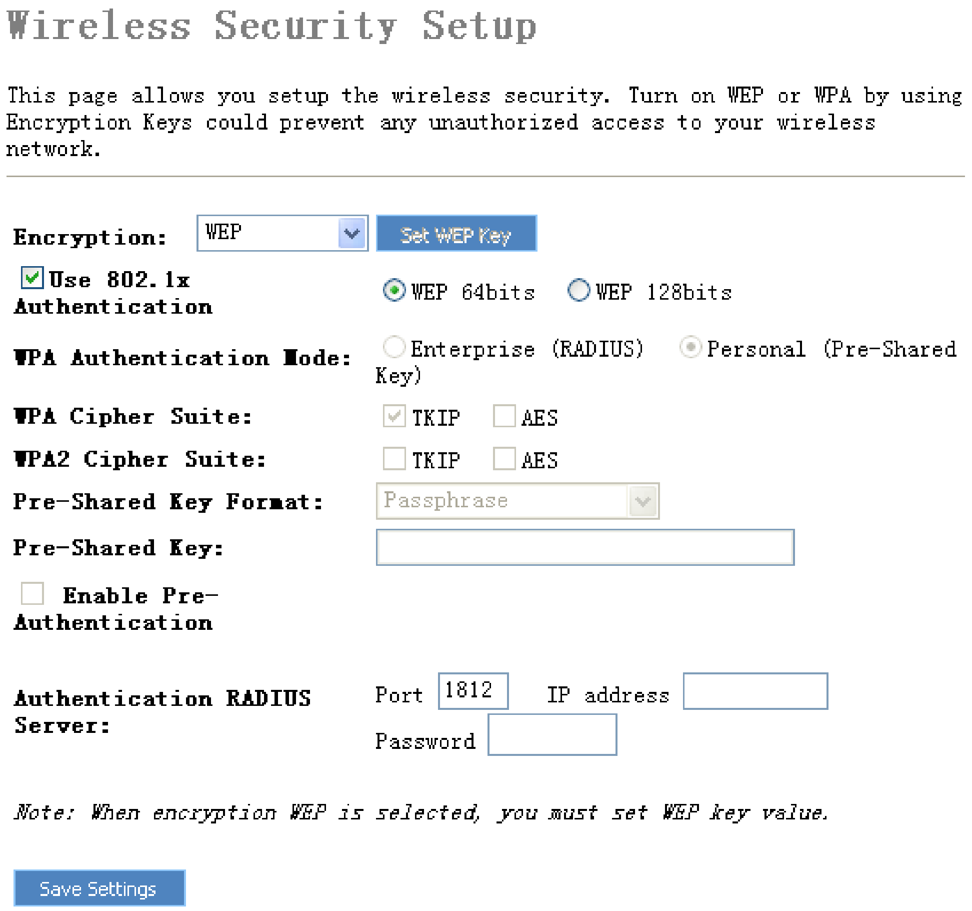
Figure 4-6

- **Key Length**
  You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower.
- **Key Format**
  You may to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. **< For example:** ASCII Characters: guest; Hexadecimal Digits: 12345abcde **>**
- **Default Key**
  Select one of the four keys to encrypt your data. Only the key you select it in the "Default key" will take effect.
- Key 1 - Key 4
  The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules: 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click “Save Setting” at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

4.3.3.3. 802.1x&WEP

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.



Wireless Security Setup

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

Encryption: WEP

☑ **Use 802.1x Authentication** ● WEP 64bits ○ WEP 128bits

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

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP □ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

□ **Enable Pre-Authentication**

Authentication RADIUS Server: Port 1812 IP address

Password

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

Figure 4-7

- **Authentication RADIUS Server port**

  The service port of the external RADIUS server.

- **Authentication RADIUS Server IP address**

  The IP address of external RADIUS server.

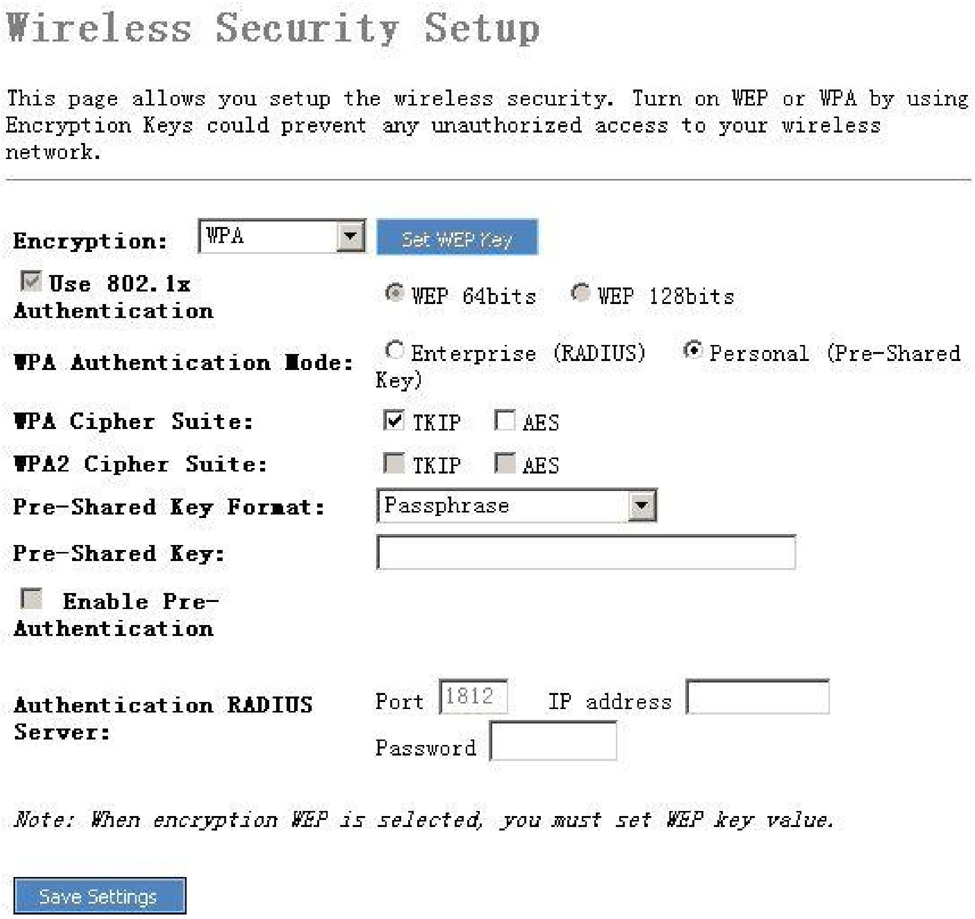
- **Authentication RADIUS Server IP Password**

  The password used by external RADIUS server.

For the WEP settings, please refer to section 5.3.2 “WEP only”.

4.3.3.4. WPA

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 or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.



Wireless Security Setup

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

Encryption: WPA ▾ [Set WEP Key]

☑ **Use 802.1x Authentication** ● WEP 64bits ○ WEP 128bits

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

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP □ AES

Pre-Shared Key Format: Passphrase ▾

Pre-Shared Key:

□ **Enable Pre-Authentication**

Authentication RADIUS Server: Port 1812 IP address Password

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

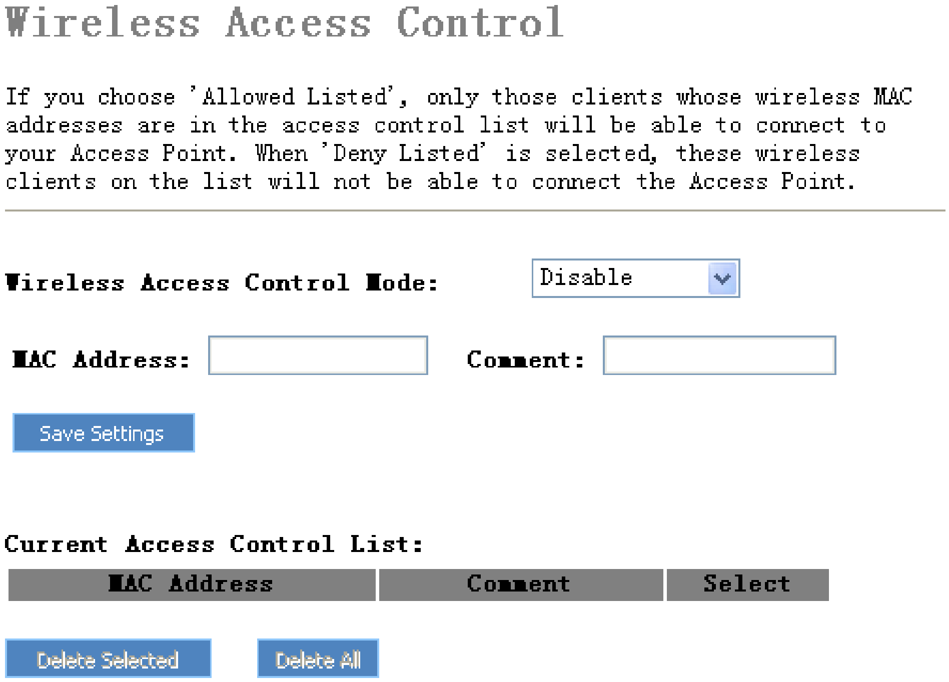
[Save Settings]

Figure 4-8

- **WPA(TKIP)**
  TKIP can change the encryption key frequently to enhance the wireless LAN security.
- **WPA(AES)**
  This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
- **Personal (Pre-Shared Key)**
  You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. **<For example:** Passphrase: iamguest Hexadecimal Digits: 12345abcde**>**
- **Enterprise (Radius)**
  You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP(AES) to change the encryption key frequently. This can improve security very much.
- **RADIUS Server port**
  The service port of the external RADIUS server.
- **RADIUS Server IP Address**
  The IP address of external RADIUS server.
- **RADIUS Server Password**
  The password used by external RADIUS server.

4.3.4. Access control

This wireless router provides MAC Address Control, which prevents the unauthorized MAC Addresses from accessing your wireless network.



Wireless Access Control

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

Wireless Access Control Mode: Disable

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select

Figure 4-9

- **Wireless Access Control Mode**

  Disable: wireless access control

  Allowed Listed: only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

  Deny Listed: these wireless clients on the list will not be able to connect the Access Point

- **Add MAC address**

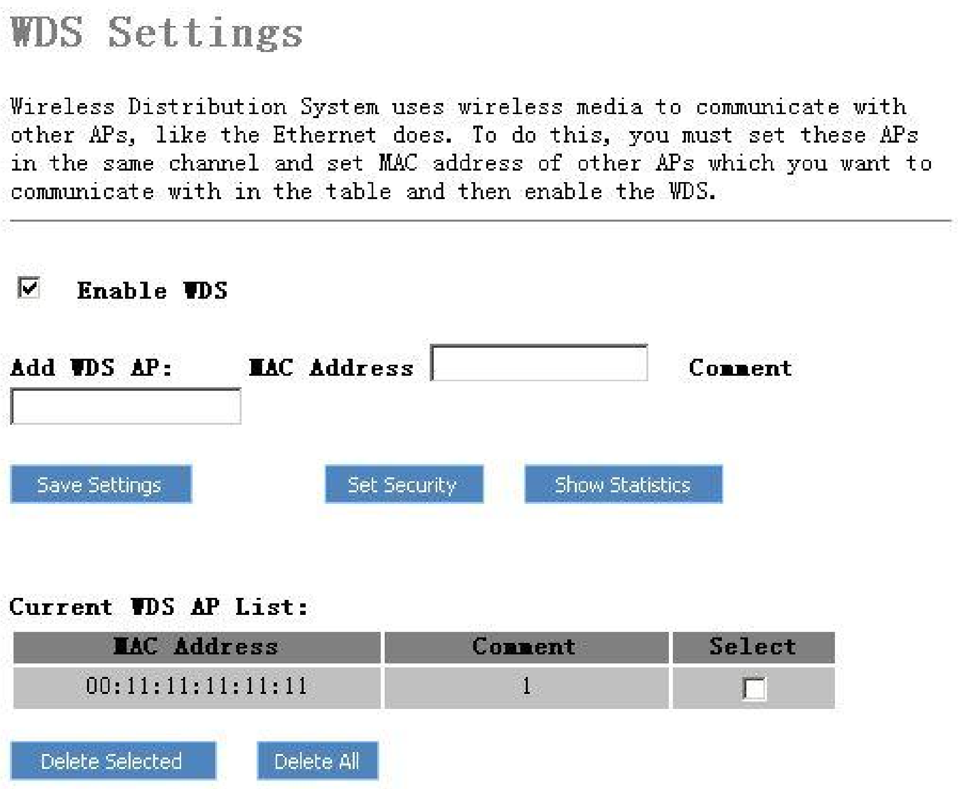
  Fill in the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". Then this wireless station will be added into the "Current Access Control List" below.

- **Current Access Control List**

  If you find any issues before adding it and want to retype again. Just click "delete" and both "MAC Address" and "Comment" fields will be cleared.

4.3.5. WDS Setting

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



WDS Settings

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

☑ Enable WDS

Add WDS AP: MAC Address ▭ Comment ▭

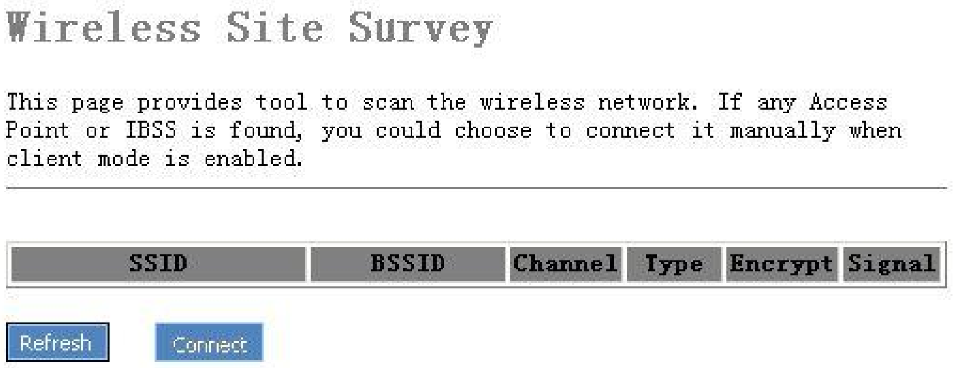
Current WDS AP List:

MAC Address	Comment	Select
00:11:11:11:11:11	1	□

Figure 4-10

4.4. Site survey

This function provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

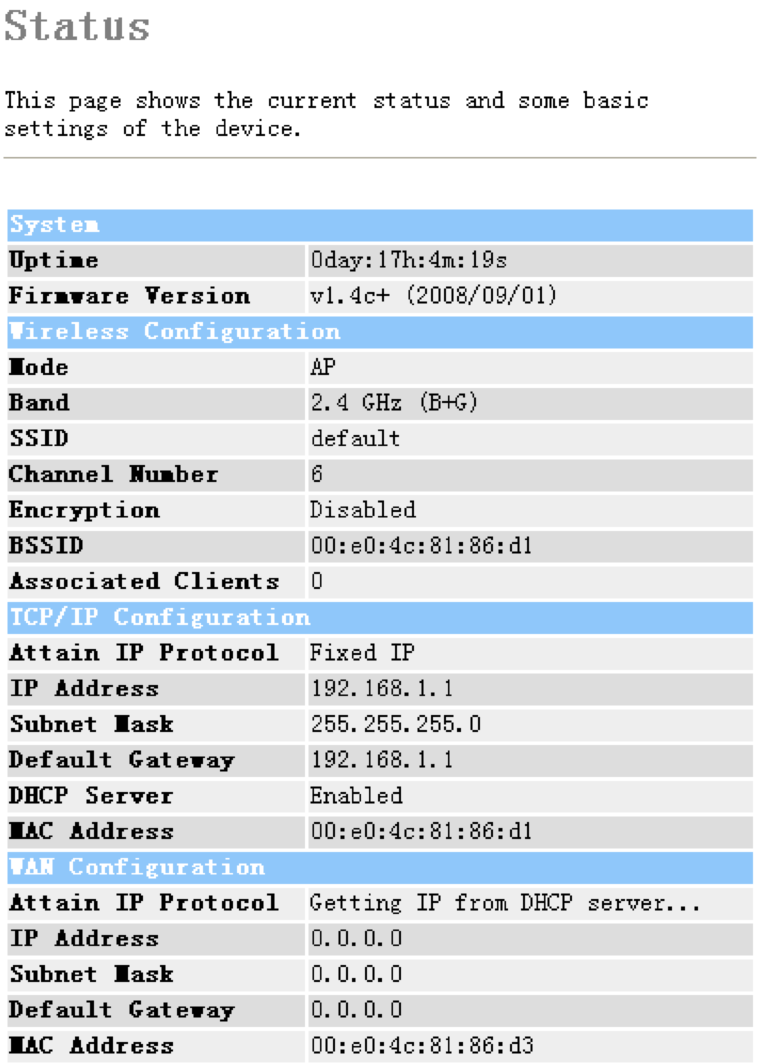
SSID	BSSID	Channel	Type	Encrypt	Signal

Figure 4-11

4.5. System Information

4.5.1. Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the connection status of the Broadband router's WAN/LAN interfaces, the current firmware and so on.



Status

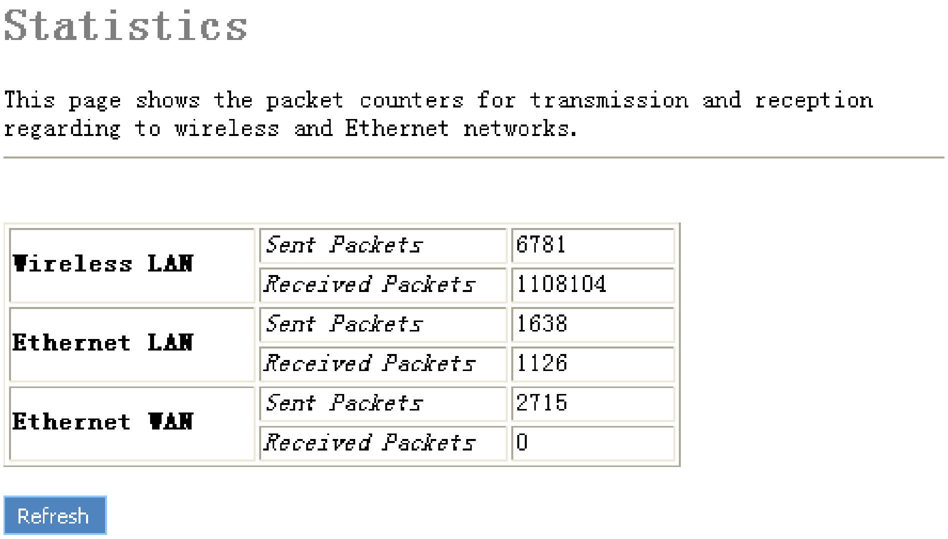
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:17h:4m:19s
Firmware Version	v1.4c+ (2008/09/01)
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	default
Channel Number	6
Encryption	Disabled
BSSID	00:e0:4c:81:86:d1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:86:d1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:86:d3

Figure 4-12

4.5.2. Statistics

View the statistics of packets sent and received on WAN, LAN and Wireless LAN.



Statistics

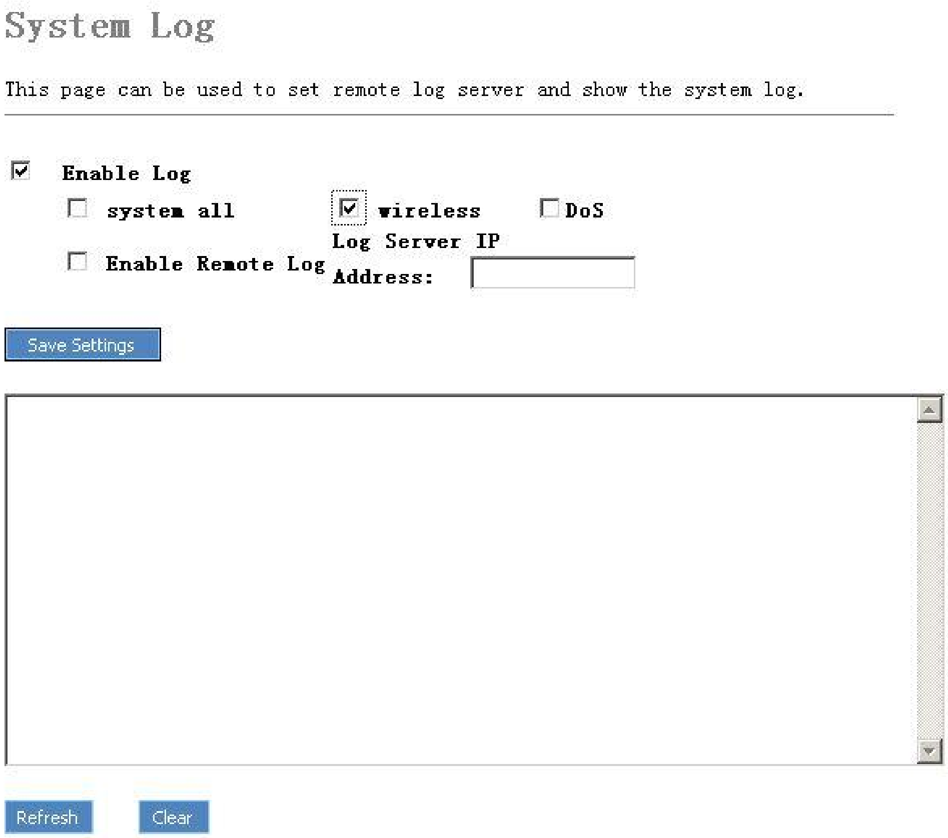
This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	6781
	Received Packets	1108104
Ethernet LAN	*Sent Packets*	1638
	Received Packets	1126
Ethernet WAN	*Sent Packets*	2715
	Received Packets	0

Figure 4-13

4.5.3. System Log

This page shows the current system log of the Broadband router. It displays any event occurred after system start up, including view all information of system, wireless information, Dos attack information and so on.



System Log

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

☑ Enable Log

□ system all ☑ wireless □ DoS

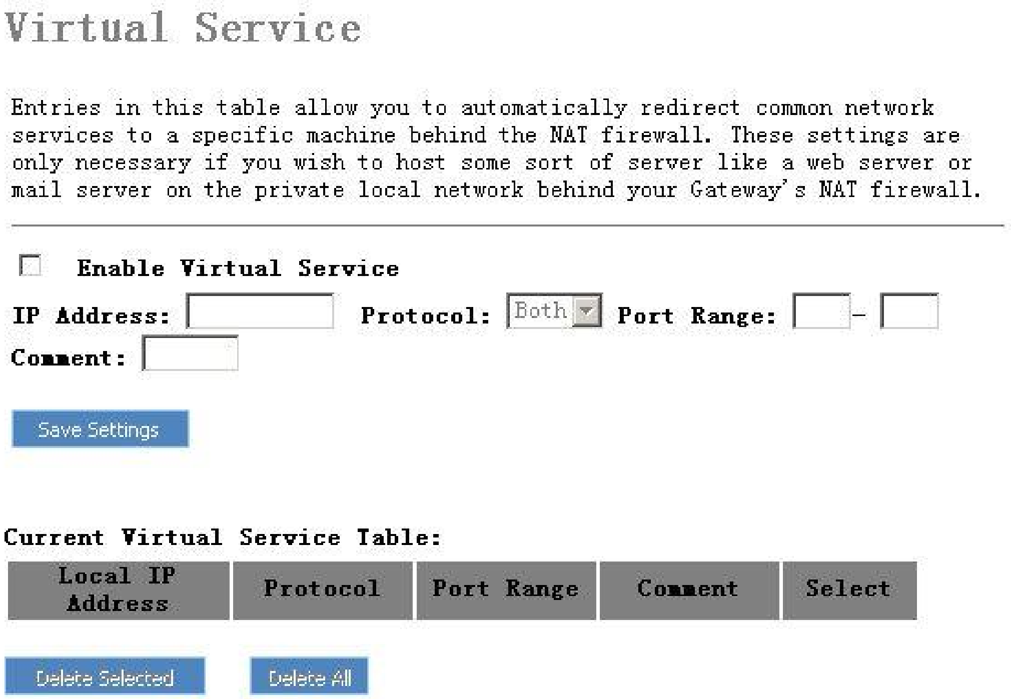
□ Enable Remote Log Log Server IP Address:

Figure 4-14

4.6. Applications & Gaming

4.6.1. Virtual Service

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.) from the Internet. Computers use numbers called 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 particular LAN private IP address and its service port number. (See Glossary for an explanation on Port number)



Virtual Service

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

□ Enable Virtual Service

IP Address: Protocol: Both Port Range: -

Comment:

Current Virtual Service Table:

Local IP Address	Protocol	Port Range	Comment	Select

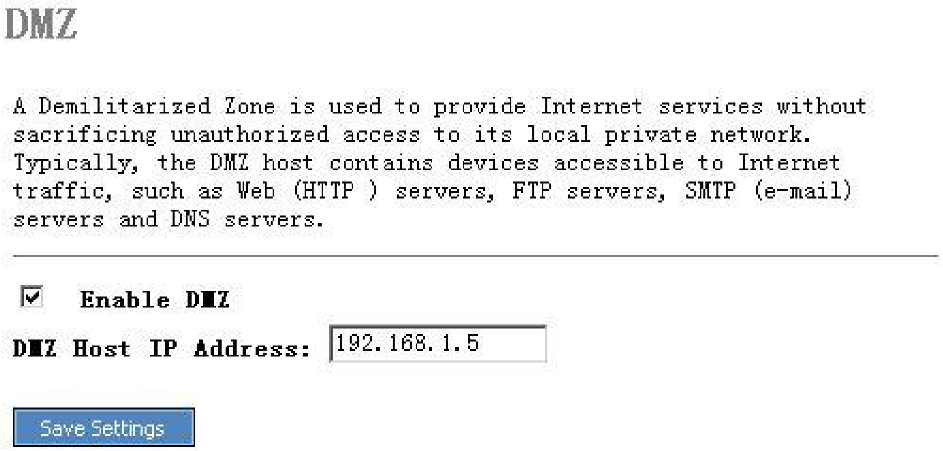
Figure 4-15

- **Enable Virtual Service**
  Enable Virtual Service
- **IP Address**
  This is the LAN client/host IP address that the Public Port number packet will be sent to. **Note:** You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
- **Protocol**
  Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocols.
- **Port Range**
  This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP)
- **Comment**
  The description of this setting

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

4.6.2. DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up 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 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

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

☑ Enable DMZ

DMZ Host IP Address: 192.168.1.5

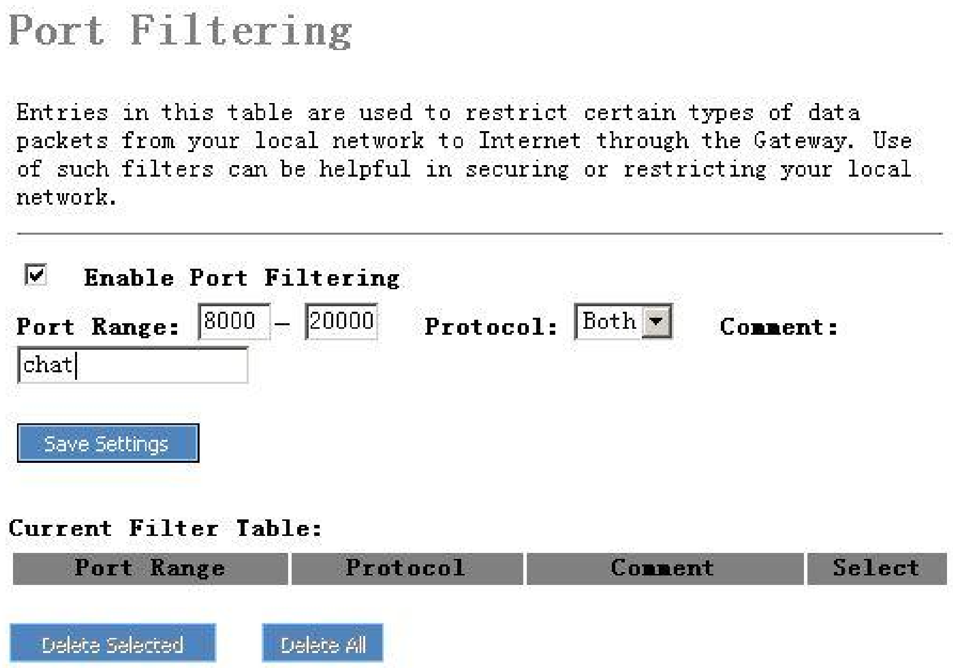
Figure 4-16

4.7. Security Management

The Broadband router provides extensive security 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. Port Filtering

You can filter wired users by enabling this function; thus unauthorized users can not access the network.



Port Filtering

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

☑ Enable Port Filtering

Port Range: 8000 – 20000 Protocol: Both Comment: chat

Current Filter Table:

Port Range	Protocol	Comment	Select

Figure 4-17

- **Enable Port Filtering**

  Enable port filtering
- **Port Range**

  Add ports you want to control
- **Protocol**

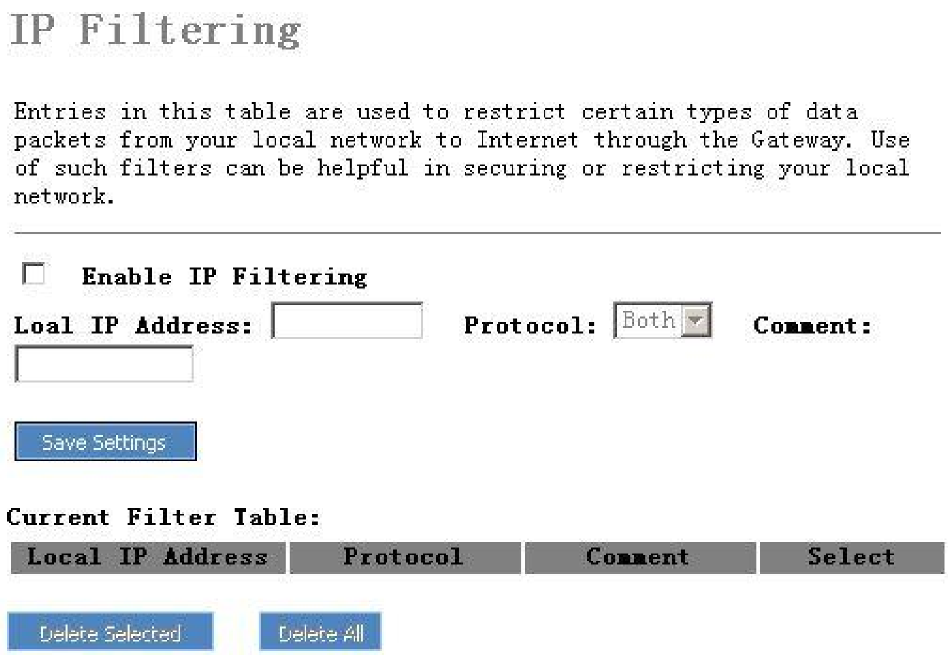
  Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocol
- **Comment**

  The description of this setting

Click “Save settings” at the bottom of the screen to save the above configurations

4.7.2. IP Filtering

You can filter wired users by enabling this function; thus unauthorized users can not access the network.



IP Filtering

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

□ Enable IP Filtering

Loal IP Address: Protocol: Both Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Figure 4-18

- **Enable IP Filtering**

  Enable IP filtering

- **Local IP Address**

  Add LAN IP address you want to control

- **Protocol**

  Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocol

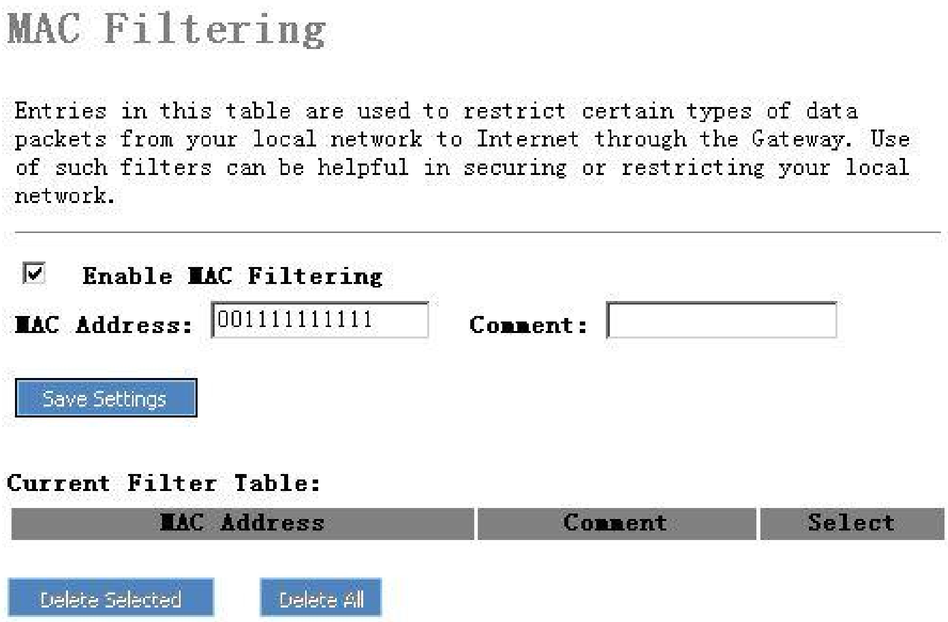
- **Comment**

  The description of this setting

Click “Save settings” at the bottom of the screen to save the above configurations

4.7.3. MAC Filtering

You can filter wired users by enabling this function; thus unauthorized users can not access the network.



MAC Filtering

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

☑ Enable MAC Filtering

MAC Address: 001111111111 Comment:

Current Filter Table:

MAC Address	Comment	Select

Figure 4-19

- **Enable MAC Filtering**

  Enable MAC filtering
- **MAC Address**

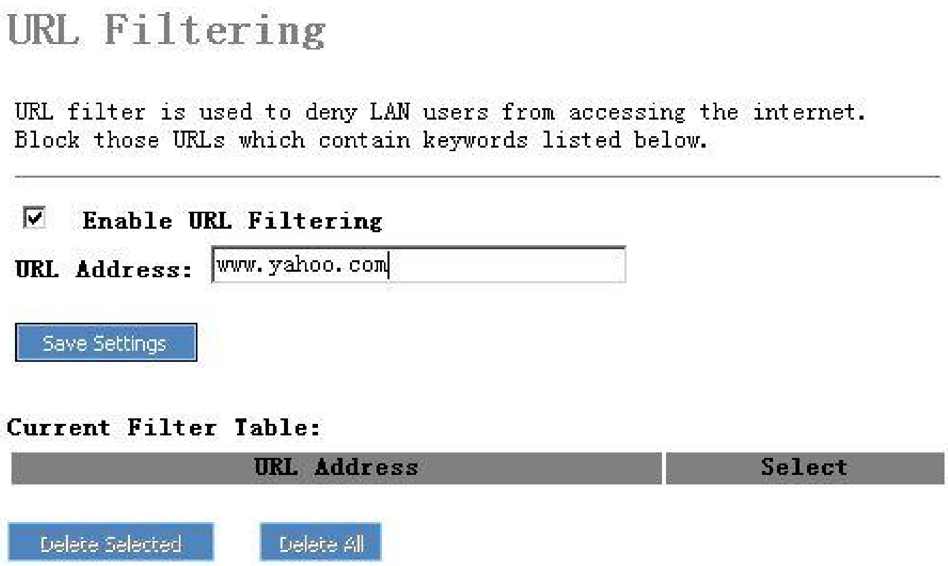
  Add MAC address you want to control
- **Comment**

  The description of this setting

Click “Save settings” at the bottom of the screen to save the above configurations

4.7.4. URL Filtering

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



URL Filtering

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

☑ Enable URL Filtering

URL Address: www.yahoo.com

Current Filter Table:

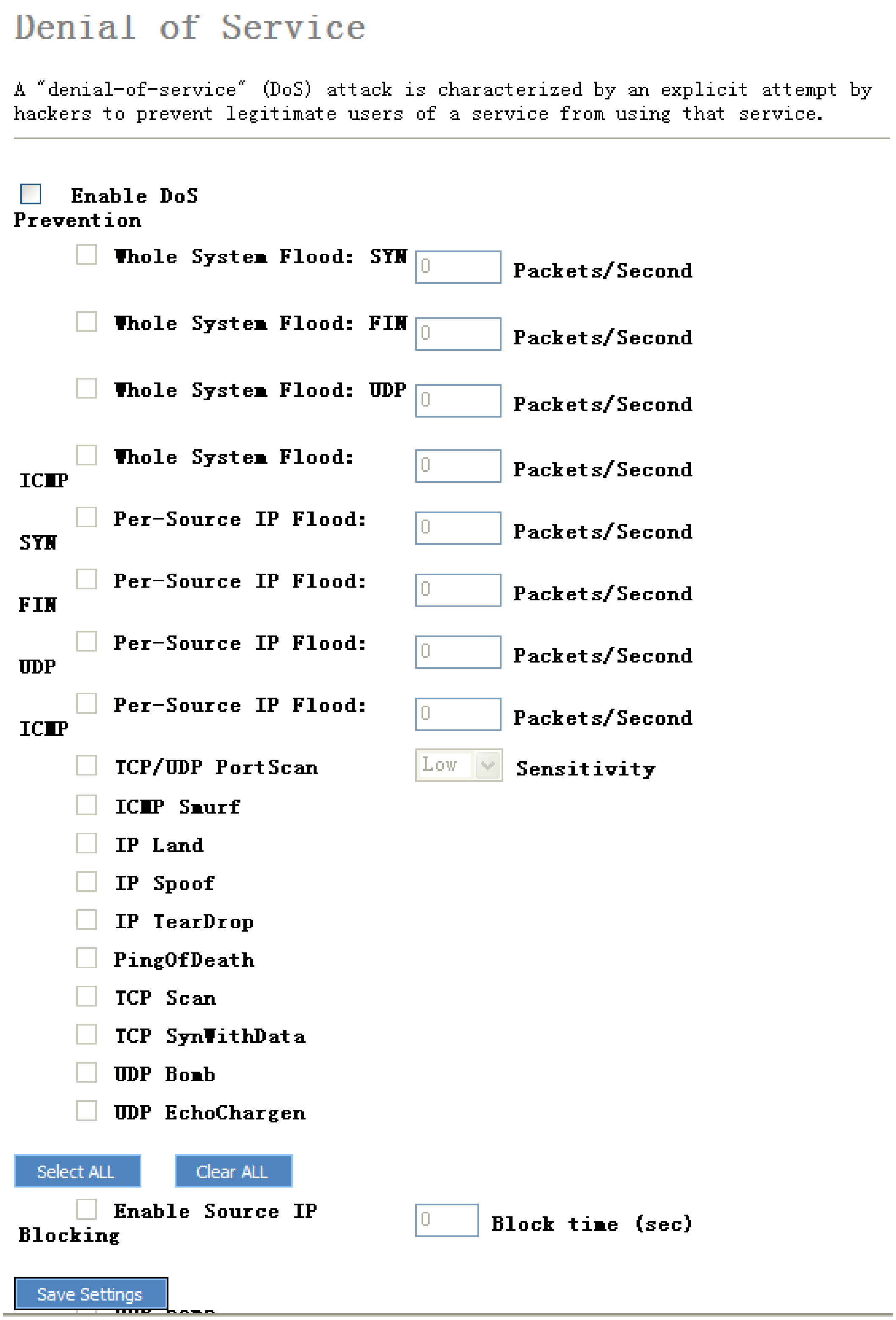
URL Address	Select

Figure 4-20

Fill in “**URL/Keyword**” and then click “Save Settings”. You can enter the full URL address or the keyword of the web site you want to block. If you find any typo before adding it and want to retype again, just click "Delete" and the field will be cleared.

4.7.5. Denial-of-Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.



Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☐ Enable DoS Prevention

☐ Whole System Flood: SYN	0	Packets/Second
☐ Whole System Flood: FIN	0	Packets/Second
☐ Whole System Flood: UDP	0	Packets/Second
☐ Whole System Flood: ICMP	0	Packets/Second
☐ Per-Source IP Flood: SYN	0	Packets/Second
☐ Per-Source IP Flood: FIN	0	Packets/Second
☐ Per-Source IP Flood: UDP	0	Packets/Second
☐ Per-Source IP Flood: ICMP	0	Packets/Second
☐ TCP/UDP PortScan	Low	Sensitivity

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

☐ UDP Bomb

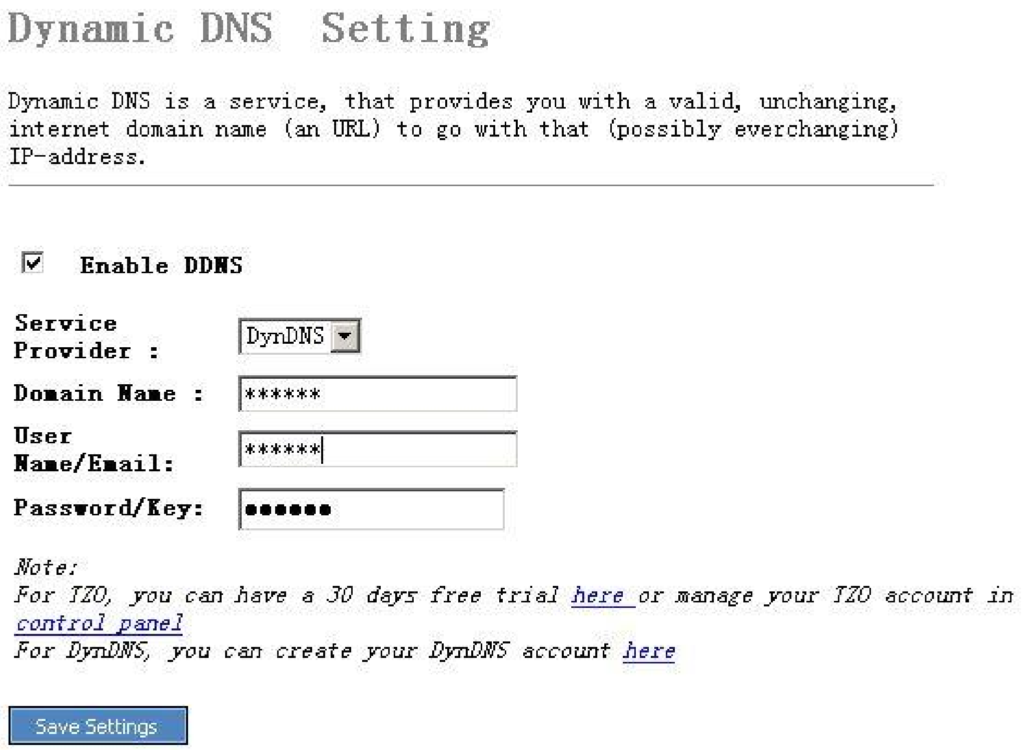
☐ UDP EchoChargen

☐ Enable Source IP Blocking 0 Block time (sec)

Figure 4-21

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. This router supports DynDNS, TZO and other common DDNS service providers.



Dynamic DNS Setting

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

☑ Enable DDNS

Service Provider :	DynDNS
Domain Name :	******
User Name/Email:	******
Password/Key:	●●●●●●

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

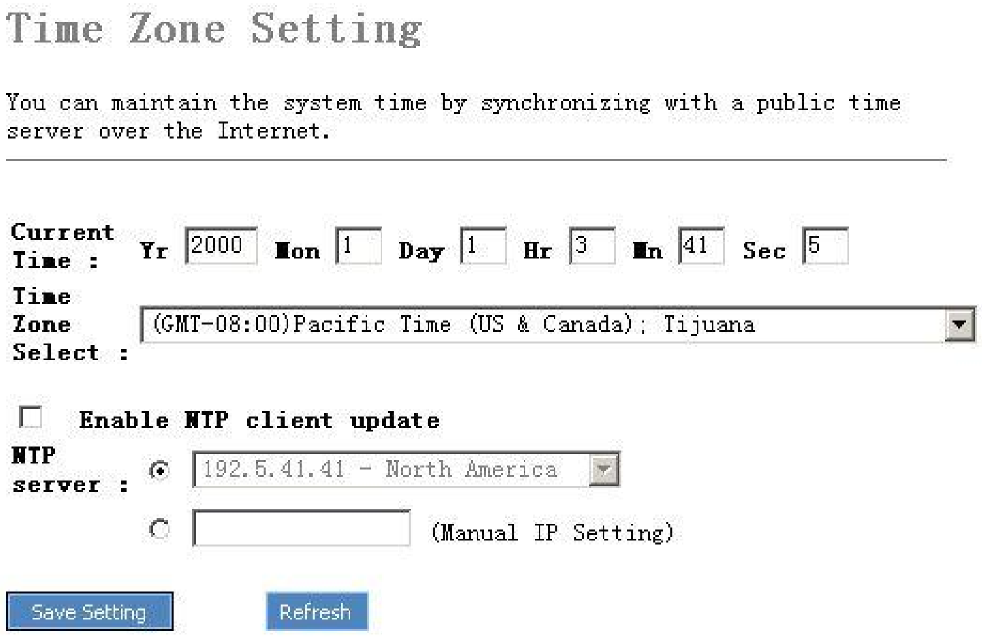
Figure 4-22

- **Enable DDNS**
  Enable/Disable the DDNS function of this router
- **Service Provider**
  Select a DDNS service provider
- **Domain Name**
  Your static domain name that use DDNS
- **User Name/Email**
  The account that your DDNS service provider assigned to you
- **Password/Key**
  The password you set for the DDNS service account above

4.9. System Management

4.9.1. Time Zone Setting

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



Time Zone Setting

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

Current Time :	Yr 2000 Mon 1 Day 1 Hr 3 Mn 41 Sec 5
Time Zone Select :	(GMT-08:00)Pacific Time (US & Canada); Tijuana

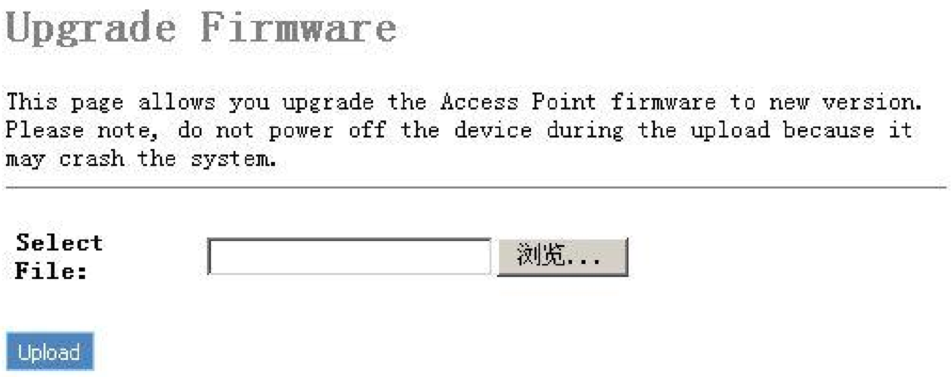
□ Enable NTP client update

NTP server : ● 192.5.41.41 - North America
○ (Manual IP Setting)

Figure 4-23

4.9.2. Upgrade Firmware

This page allows you to upgrade the router’s firmware



Upgrade Firmware

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

Select File:

Figure 4-24

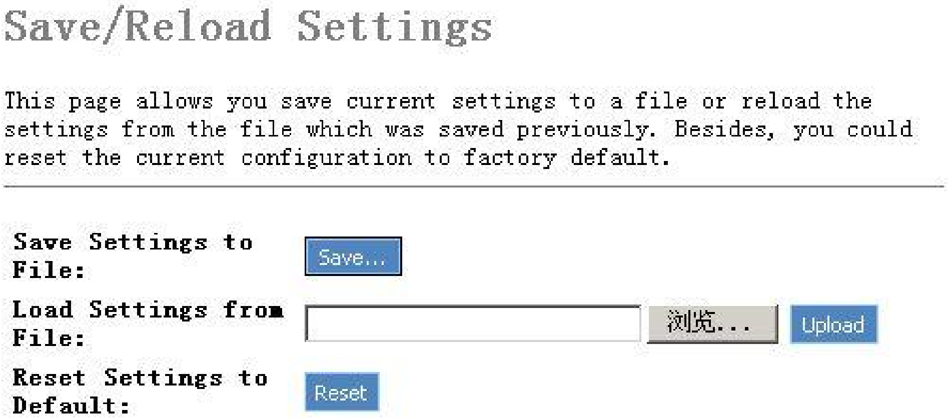
- **Select File**

  This tool allows you to upgrade the Broadband router’s system firmware. To upgrade the firmware of your Broadband router, you need to download 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.

Once you've selected the new firmware file, click "Upload" at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is complete you can start using the router.

4.9.3. Save/Reload Setting

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



Save/Reload Settings

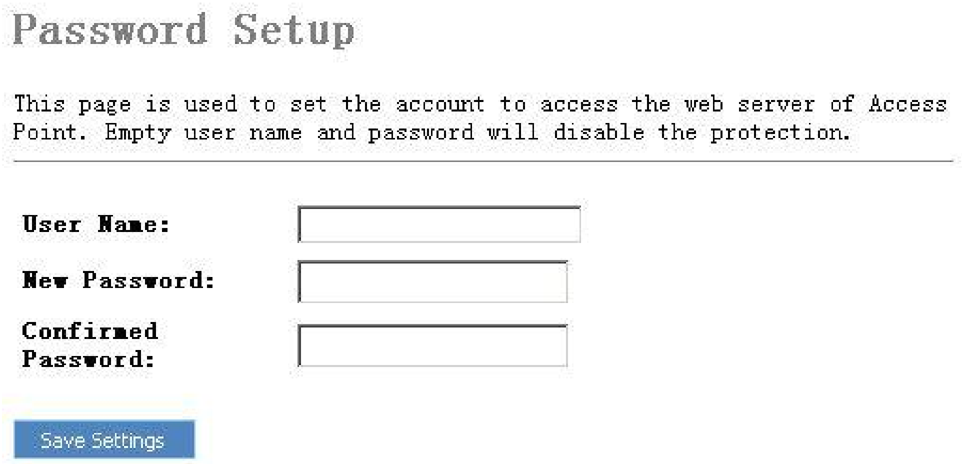
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:	Save...
Load Settings from File:	[ ] 浏览... Upload
Reset Settings to Default:	Reset

Figure 4-25

4.9.4. Password

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.



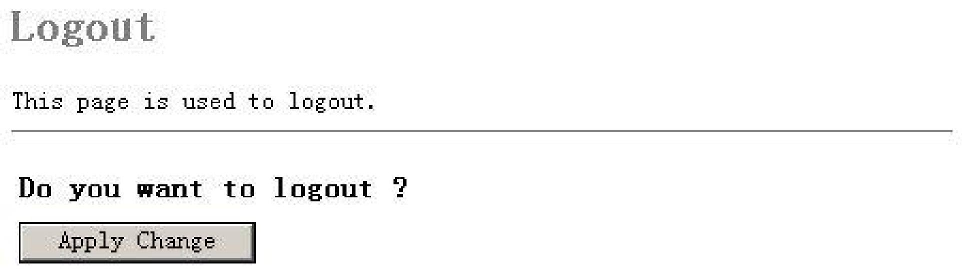
Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Figure 4-26

4.10. Logout

This function is used to logout



Logout

This page is used to logout.

Do you want to logout ?

Figure 4-27

Click “Apply Change” at the bottom of the screen to logout, pay attention.

5. Appendix □: Troubleshooting

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)

- Plug out the power of the Router.
- Use a pencil to press and hold the default button on the back panel of the Router. Then plug in the power of the Router.
- Press and hold the default button wait for a few seconds until the CPU LED indicator stays green.
- Reboot the AP.
- After the above those steps, the manufacture's parameters will be restored in the Router. 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 Wireless 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.