User Manual

Wireless-N ADSL2+ Modem Router

TOTOLINK

www.totolink.net

Table of Contents

1. ABOUT THIS GUIDE

Thank you very much for purchasing the wireless N router. This guide will introduce the features of this router and tell you how to connect, use and configure the router to access Internet. Please follow the instructions in this guide to avoid affecting the router's performance by improper operation.

1.1 Navigation of the User's Guide

Product Overview: Describes the router's function and its features.

Hardware Installation: Describes the hardware installation and settings on user's computer.

Connecting to Internet: Tells you how to connect your computer to Internet successfully by the router.

Advanced Settings: Lists all technical functions including Wireless, TCP/IP Settings, Firewall and System of the router.

2. PRODUCT OVERVIEW

2.1 Introduction

This is a wireless router which integrates with internet-sharing router, 4-port switch and firewall all-in-one. Multiple encryptions including wireless LAN 64/128-bit WEP, WPA/WPA2 and WPA-mixed security are supported by the router. The VLAN function also makes amazing interactive entertainment experience of IPTV be achieved easily. The IP, Port, URL and MAC address filtering function also makes it easy for user management. In view of the above, it will allow you to connect your network wirelessly in an easy and secure way better than ever. It is really a high performance and cost-effective solution for home and small offices.

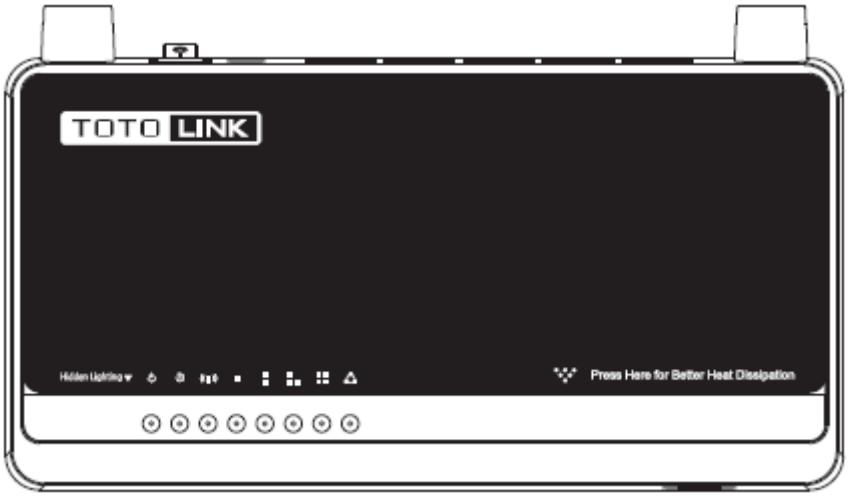
2.2 Features

- Complies with IEEE 802.11n/g/b standards for 2.4GHz Wireless LAN.
- Supports DHCP, Static IP, PPPoE broadband functions.
- Provides three operation modes: Gateway, Repeater Bridge and Repeater WISP.
- Connects to secure network easily and fast using WPS (one-button).
- Provides 64/128-bit WEP, WPA/WPA2 and WPA-Mixed security.
- Supports VLAN function.
- Supports IP, Port, MAC, URL filtering and Port Forwarding.
- QoS function allocates network bandwidth reasonably.

2.3 Panel Layout

2.3.1 Front Panel

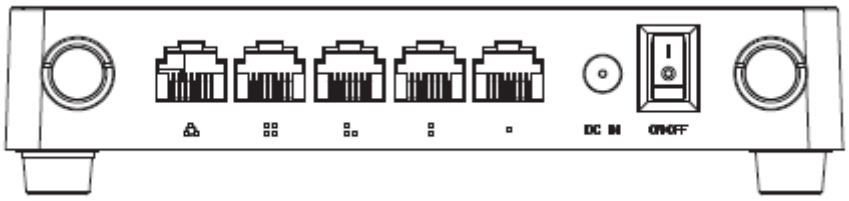
The front panel of this router consists of 8 LEDs, which is designed to indicate connection status.



POWER	This indicator lights blue when the router powered on, otherwise it is off.	
CPU	This indicator blinks blue when router powered on.	
WLAN	This indicator blinks blue when there are wireless devices connected and transmitting data to the router.	
WAN	On	When the WAN port is connected successfully the indicator lights blue.
	Blink	During transmitting or receiving data through the WAN port the indicator blinks blue.
	Off	There is no device linked to the WAN port.
1/2/3/4 LAN	On	When the LAN port has a successful connection, the corresponding indicator lights blue.
	Blink	During transmitting or receiving data through the LAN port the corresponding indicator blinks blue.
	Off	There is no device linked to the LAN port.

2.3.2 Rear Panel

The figure below shows the rear panel of this router.



DC IN	The Power socket is where you will connect the power adapter.
WAN	This port is where you will connect with the cable to access Internet.
1/2/3/4 LAN	This port connects the router to local PC.
RST-WPS Button	Press for about 2~3 seconds, the system LED indicator keep solid light, it means WPS working, while press for about 10 seconds, all LEDs blinks quickly, the device will restore to factory default settings.

3. HARDWARE INSTALLATION

3.1 Hardware Installation

For those computers you wish to connect with Internet by this router, each of the computers must be properly connected with the router through provided Ethernet cables.

1. Connect the Modem to ADSL Filter using RJ11 network cable, LINE port to LINE port.
2. Connect the ADSL's LAN port to Router's WAN port using RJ45 network cable.
3. Connect your PC to any one of router's LAN port.
4. Plug the Power Adapter into the router and then into an outlet.
5. Turn on your computer.
6. Check and confirm that the Power & LAN LED on the router are **ON**.

3.2 Check the Installation

The control LEDs of the router are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected to the broadband modem, the Power, WPS, LAN, WLAN and WAN port LEDs of the WLAN Router will light up indicating a normal status.

2. When the WAN Port is connected to Internet successfully, the WAN LED will light up.

3. When the LAN Port is connected to the computer system, the LAN LED will light up.

3.3 Set up the Computer

The default IP address of the router is 192.168.1.1, the default Subnet Mask is 255.255.255.0. Both of these parameters can be changed as you want. In this guide, we will use the default values for description.

Connect the local PC to the LAN port on the router. There are then two ways to configure the IP address for your PC.

- **Configure the IP address manually**

Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.1.1 (router's default IP address).

- **Obtain an IP address automatically**

Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. Open a command prompt, and type in **ping 192**.168.1.1, then press Enter.

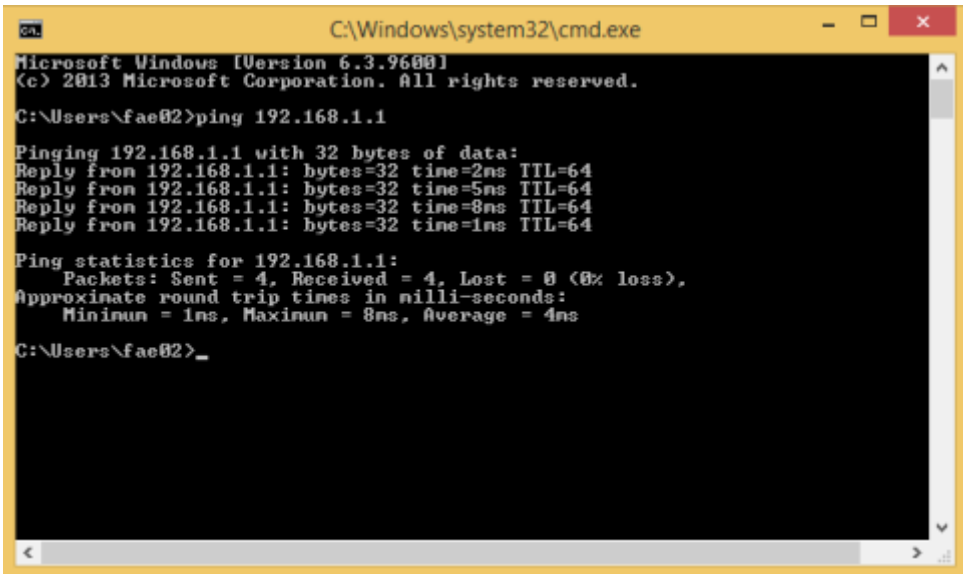


Figure 3-1 Successful Ping command

If the result displayed is similar to the figure 3-1, it means that the connection between your PC and the router has been established.

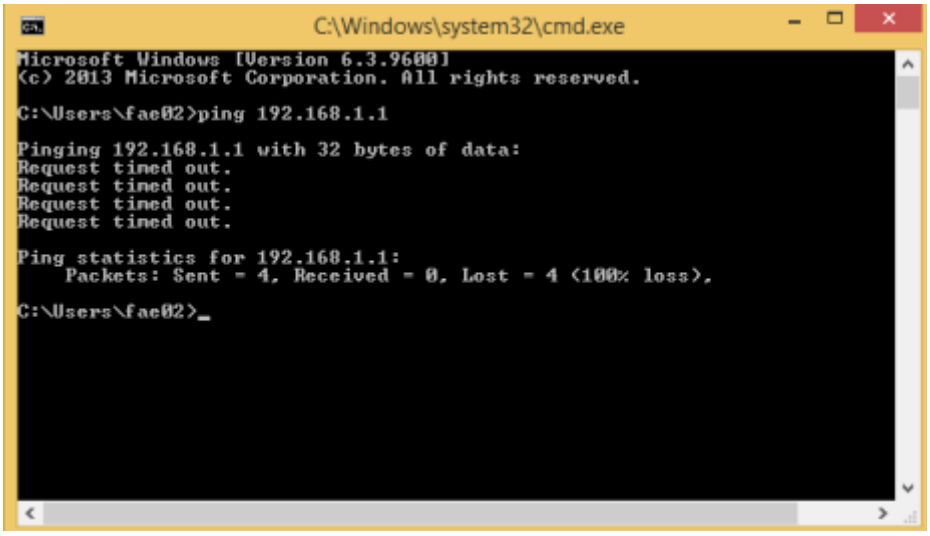


Figure 3-2 Failure Ping command

If the result displayed is similar to the figure 3-2, it means that your PC has not connected to the router successfully. Please check it following below steps:

1. Is the connection between your PC and the router correct?

If correct, the LAN port on the router and LED on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Since the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

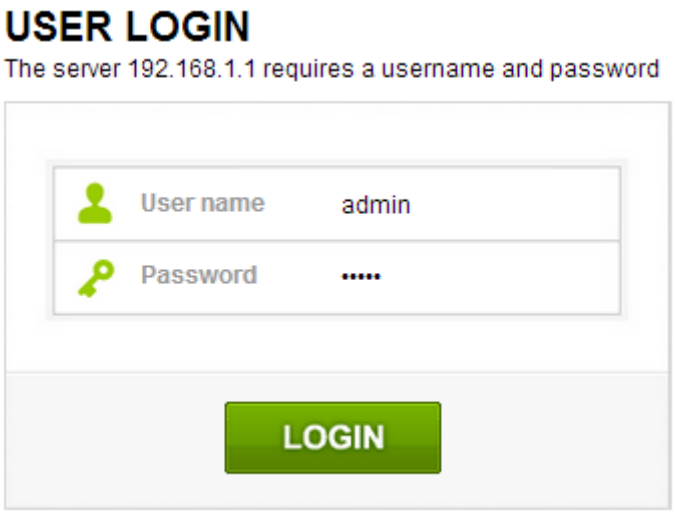
4. CONNECTING TO INTERNET

This chapter introduces how to configure the basic functions of your router so that you can surf the Internet.

4.1 Accessing Web page

Connect to the router by typing 192.168.1.1 in the address field of web browser. Then press **Enter** key.

Then below window will pop up that requires you to enter valid User Name and Password.

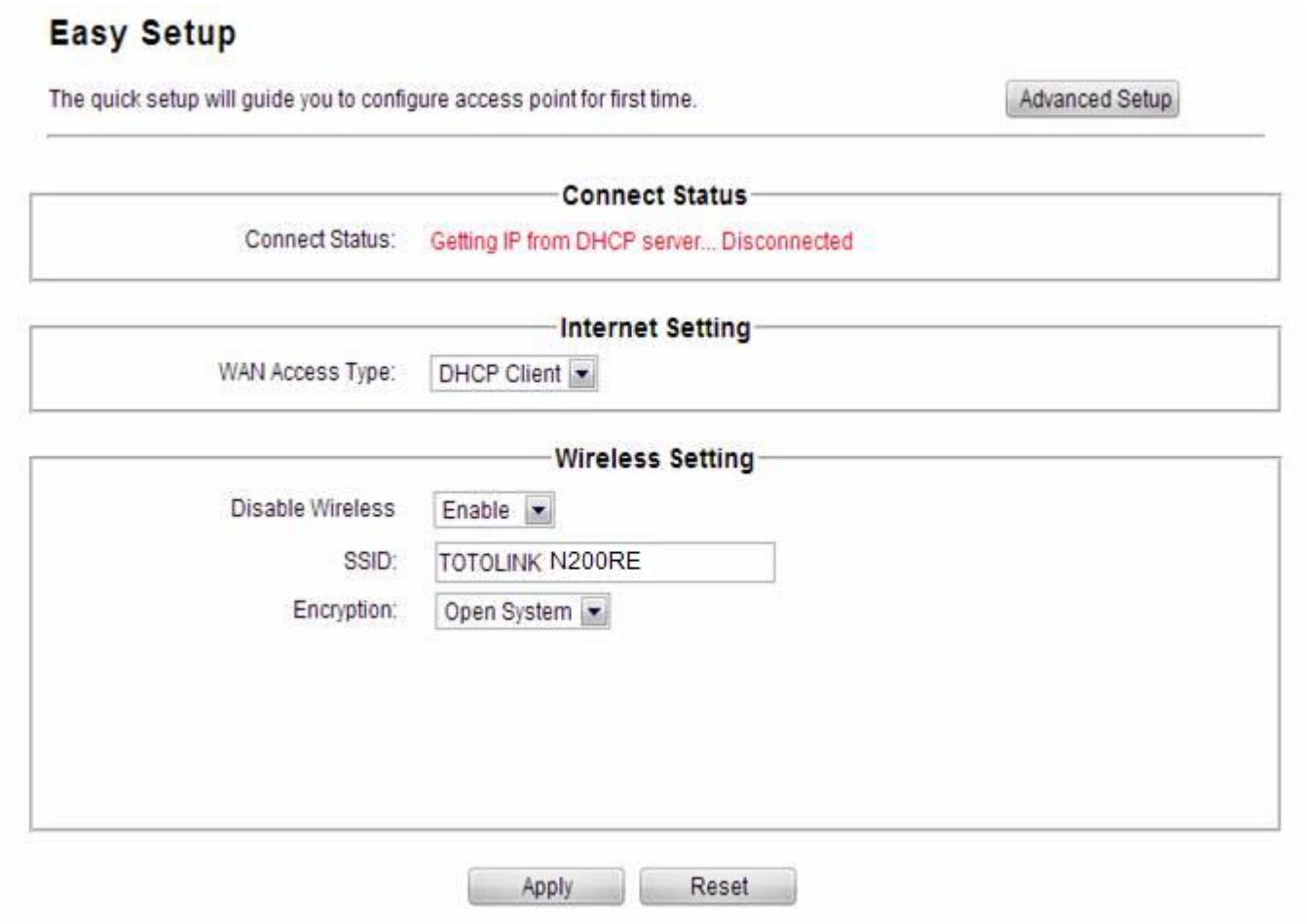


Enter **admin** for User Name and Password, both in lower case letters. Then click **OK** button or press **Enter** key.

Now you will get into the web interface of the device. The Main screen will appear.

> ***Note:*** *If the above screen does not prompt, it means that your web-browser has been set to using a proxy. Go to* ***Tools menu>Internet Options>Connections>LAN Settings****, in the screen that appears, cancel the* ***Using Proxy checkbox****, and click* ***OK*** *to finish it.*

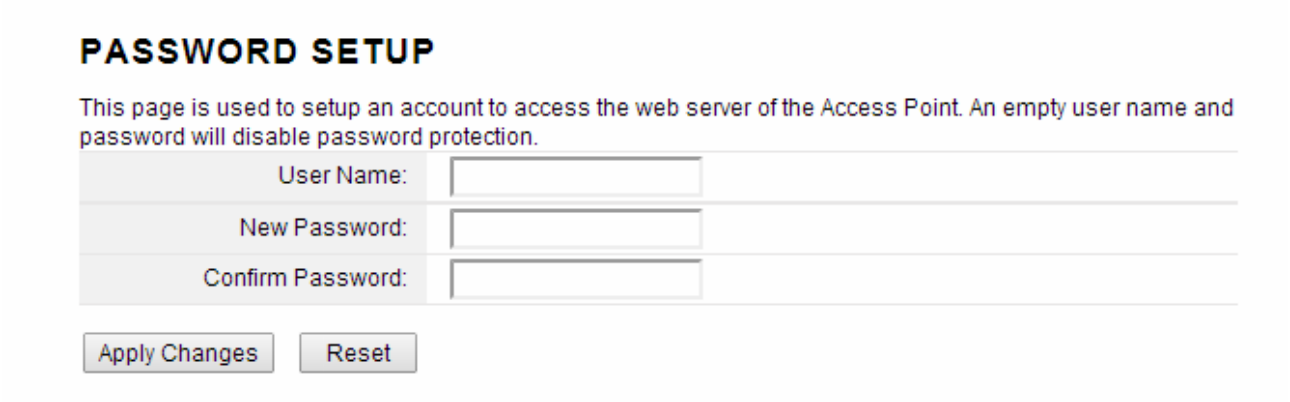
Now you have logged into the web interface of the router. First, you will see the Easy Setup page.



.

4.2 Changing Password

Now, we recommend that you change the password to protect the security of your router. Please go to **Management**—**Password** to change the password required to log in your router.

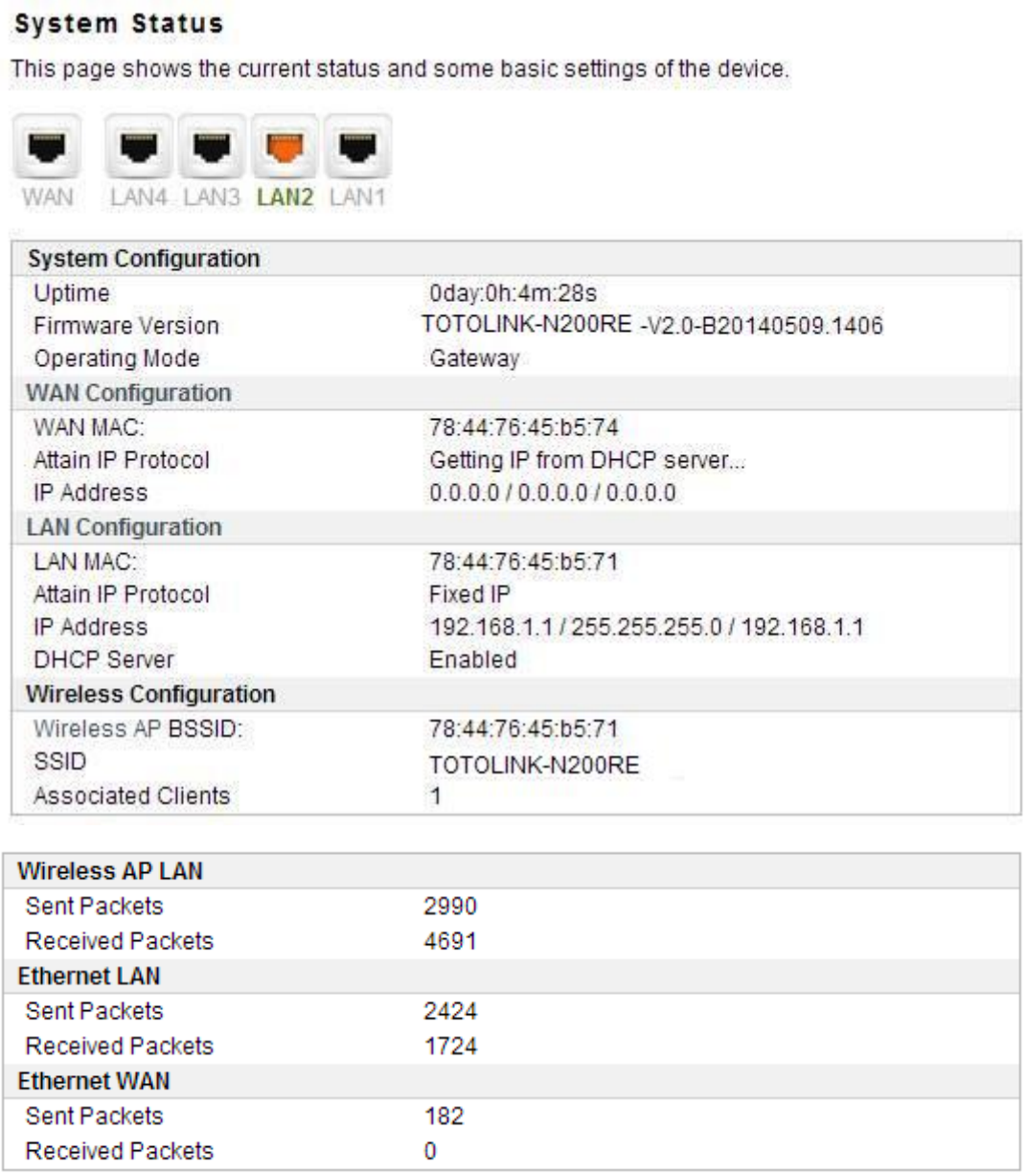


User Name: type in the name that you use to login the web interface of the router.
New Password: new password is used for administrator authentication.
Confirm Password: new password should be re-entered to verify its accuracy.

Note: *password length is 8 characters maximum, characters after the 8th position will be truncated.*

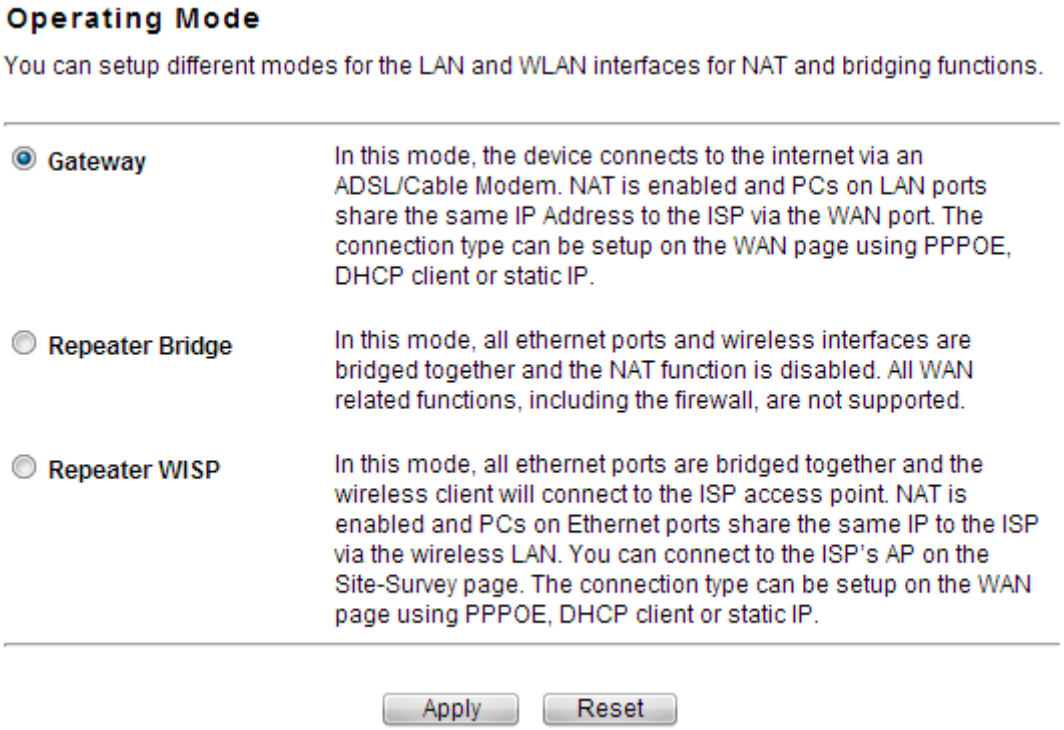
4.3 Status

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



4.4 Operation Mode

This parameter specifies the operating network modes for the Router. This router provides three modes: **Gateway**, **Repeater Bridge** and **Repeater WISP**. You could refer to the following description to choose the right one.



1. Gateway

In this mode, the device connects to the internet via an ADSL/Cable Modem. NAT is enabled and PCs on LAN ports share the same IP Address to the ISP via the WAN port. The connection type can be setup on the WAN page using PPPOE, DHCP client or static IP.

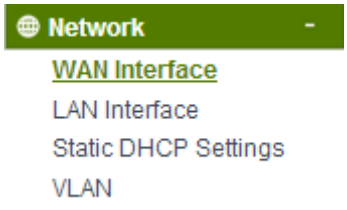
2. Repeater Bridge

In this mode, all ethernet ports and wireless interfaces are bridged together and the NAT function is disabled. All WAN related functions, including the firewall, are not supported.

3. Repeater WISP

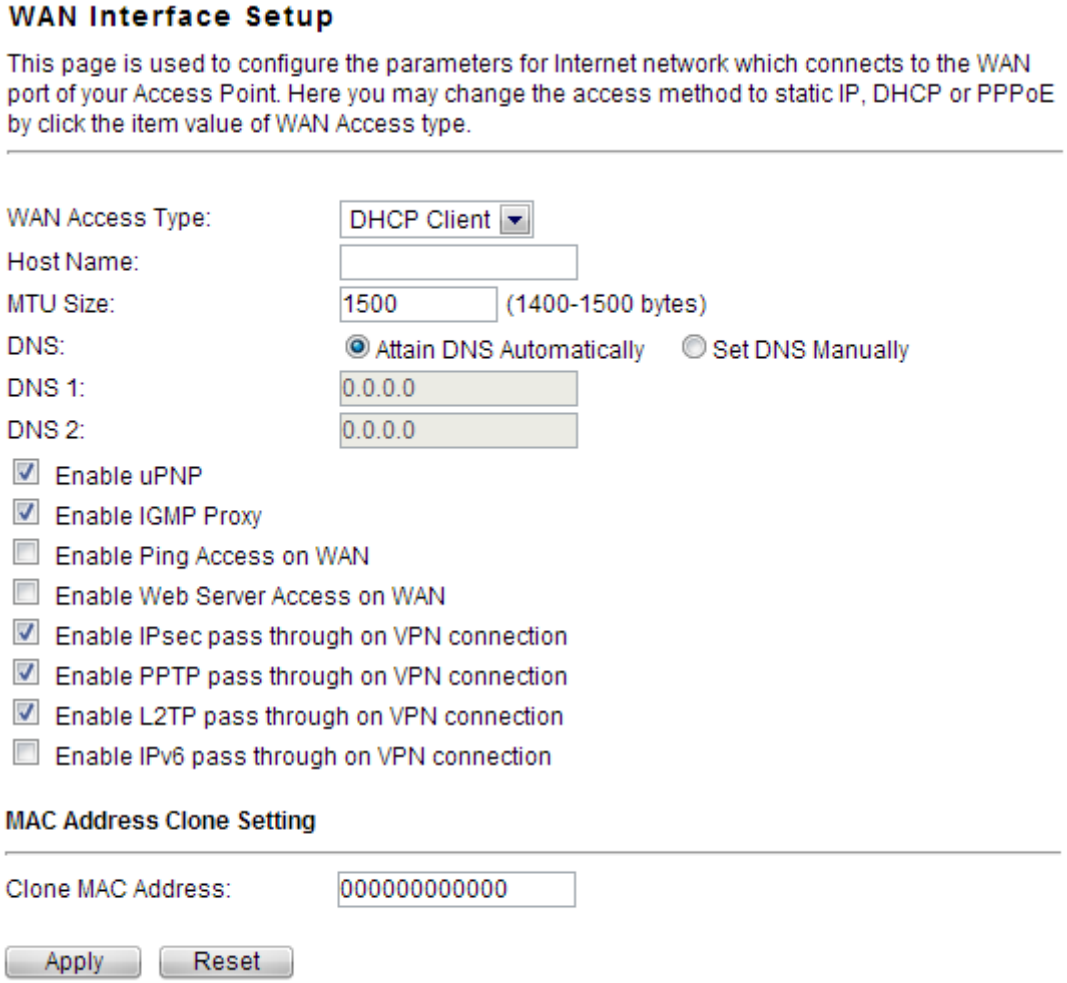
In this mode, all ethernet ports are bridged together and the wireless client will connect to the ISP access point. NAT is enabled and PCs on Ethernet ports share the same IP to the ISP via the wireless LAN. You can connect to the ISP's AP on the Site-Survey page. The connection type can be setup on the WAN page using PPPOE, DHCP client or static IP.

4.5 Network



4.5.1 WAN Interface

This part allows you to configure the WAN port parameters so that your computer can access Internet.



Enable UPnP: the UPnP (Universal Plug and play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows “Plug and Play” system. You can enable this function so that the router doesn’t need to work out which port need to be opened.

Enable IGMP Proxy: IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. If you select this checkbox, the application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.

Enable Ping Access on WAN: enable users use Ping command to access WAN.

Enable Web Server Access on WAN: enable users to access Web Server on WAN.

Enable IPsec pass through on VPN connection: IPsec pass through is a technique for allowing IPsec packets to pass through a NAT router.

Enable PPTP pass through on VPN connection: PPTP pass through is a technique for allowing PPTP packets to pass through a NAT router.

Enable L2TP pass through on VPN connection: L2TP pass through is a technique for allowing L2TP packets to pass through a NAT router.

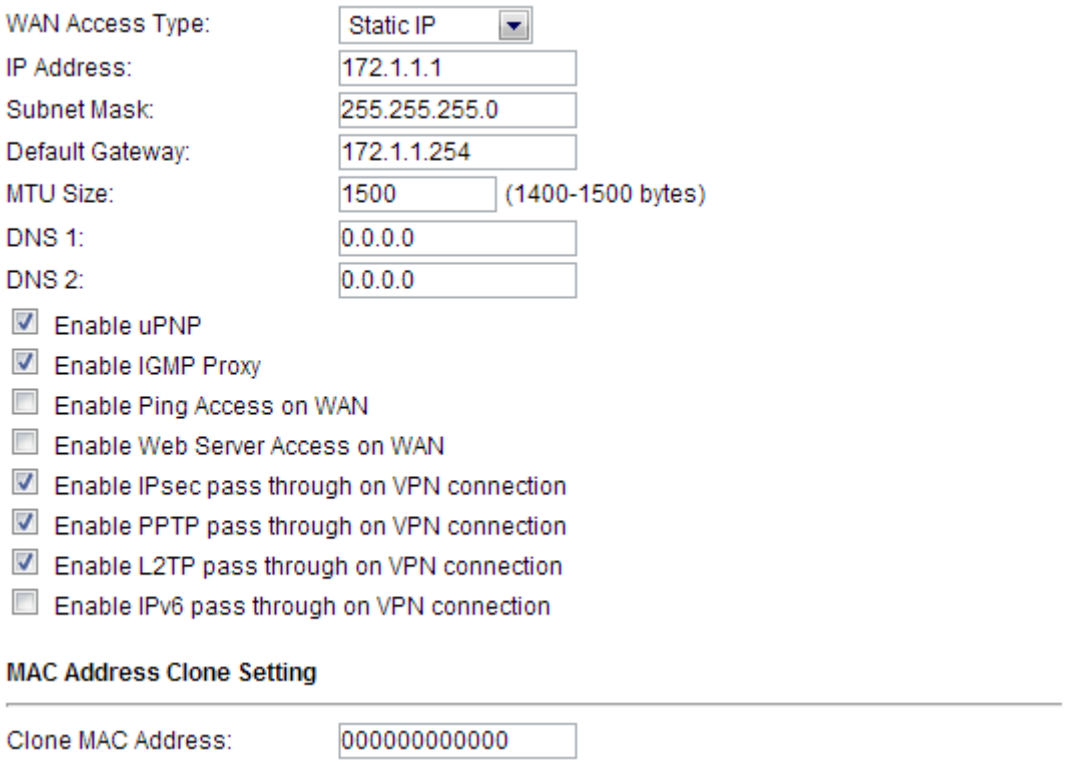
Enable IPv6 pass through on VPN connection: IPv6 pass through is a technique for allowing

IPv6 packets to pass through a NAT router.

Clone MAC Address: MAC address is the physical address of your computer's network card. Generally, every network card has one unique Mac address. Since many ISPs only allow one computer in LAN to access Internet, users can enable this function to make more computers surf Internet.

4.5.1.1 Static IP

If your ISP has provided the fixed IP that allows you to access Internet, please choose this option.



IP Address: the IP address provided by your ISP.

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.

Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.

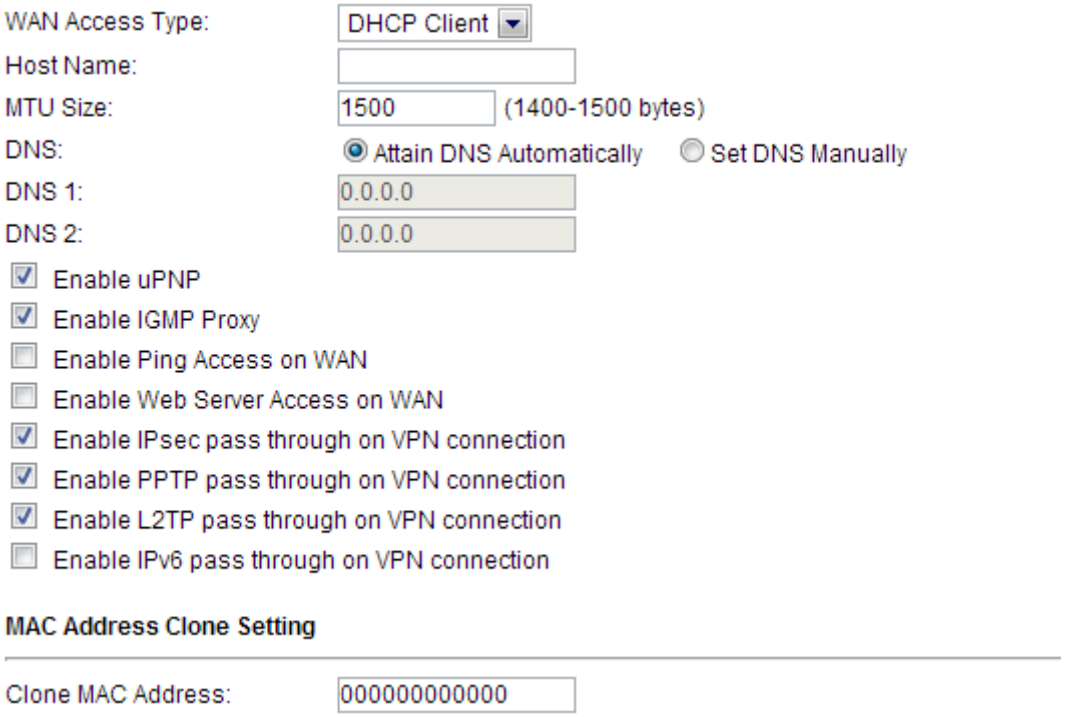
MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

DNS: The Domain Name System (DNS) is an Internet "phone book", which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requested are forwarded by this router.

4.5.1.2 DHCP Client

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you

choose this mode, you will get a dynamic IP address from your ISP automatically.



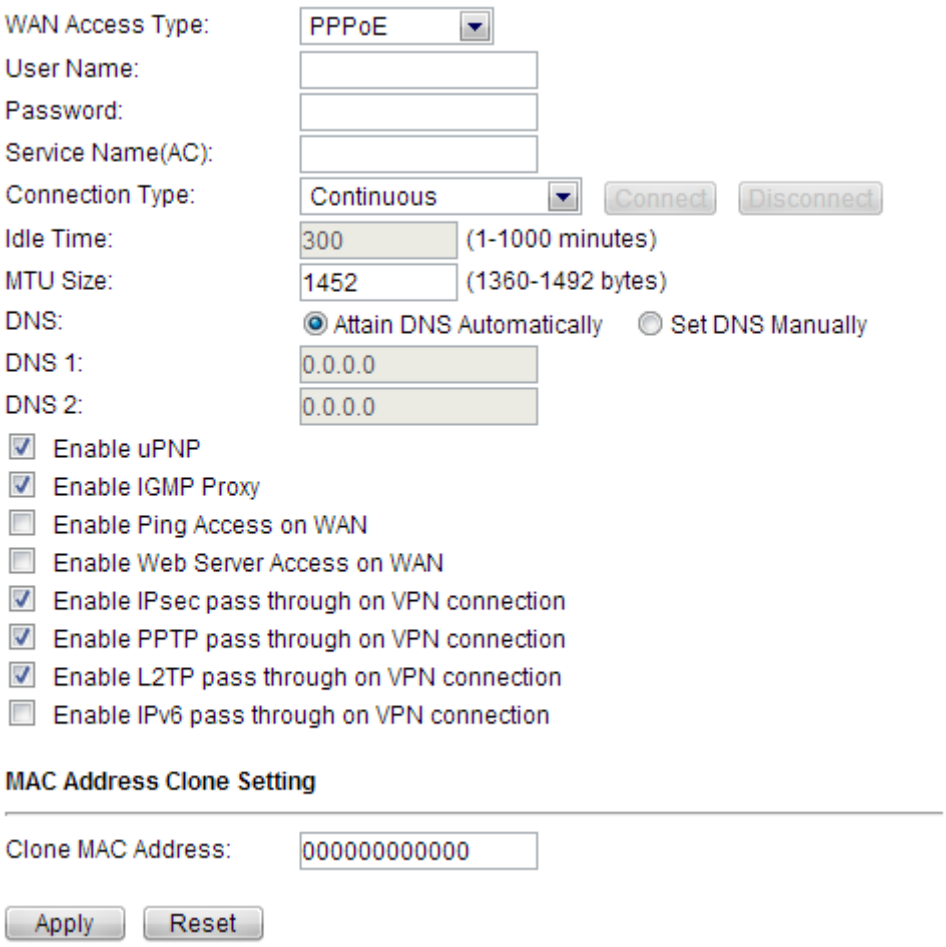
Host Name: the name of your computer, online neighbors will identify the computer according to the name.

MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

DNS: Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

4.5.1.3 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. Select PPPoE option if ISP provides a PPPoE connection. You should enter the following parameters.



User Name/Password: enter the User Name and Password provided by your ISP.
Service Name (AC): this is optional. It describes the service name your ISP provided to you. Generally, leaving these fields blank will work.
DNS: Domain Name System. If you select Set DNS Manually, you will have to type in the DNS address by yourself. It is chosen to Attain DNS by default.

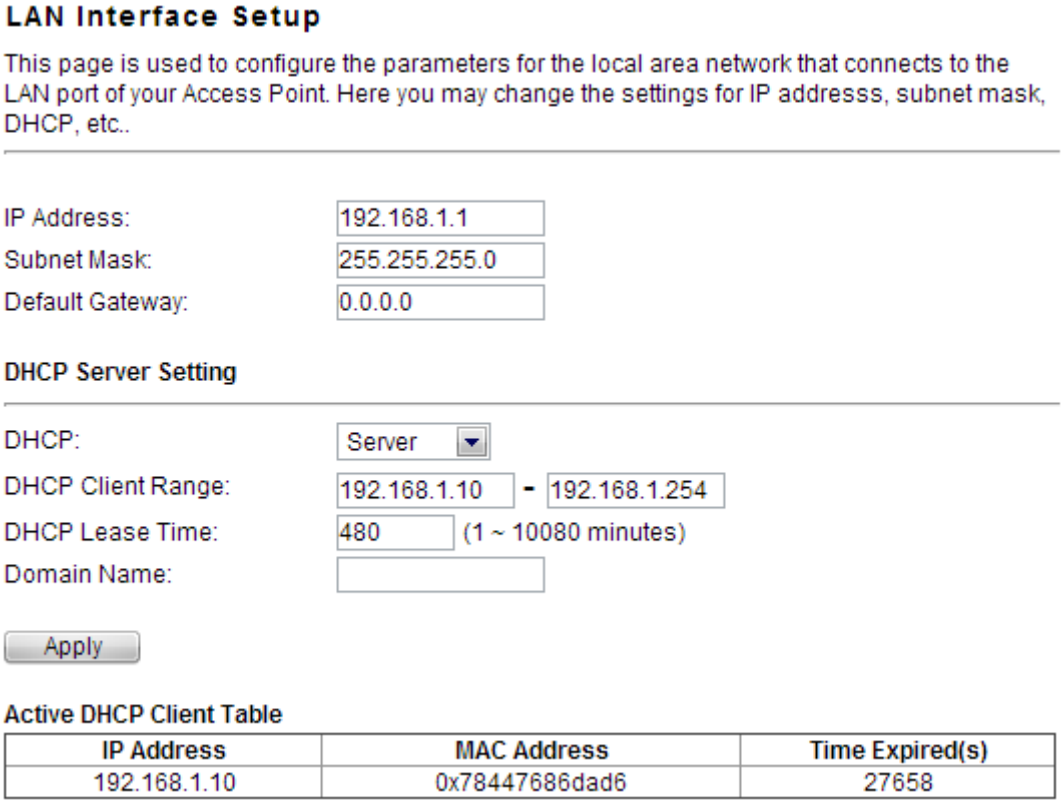
Connection Type: provides three modes to connect to the Internet.

- **Continuous**: the connection can be re-established automatically.
- **Connection on demand**: the Internet connection can be terminated automatically after a specified inactivity period (idle time).
- **Manual:** you can click **Connect** or **Disconnect** button to connect/disconnect immediately.

Idle Time: it is a term which generally refers to a lack of motion or energy.
MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

4.5.2 LAN Interface

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP. This part allows you to configure the parameters for LAN which connects to the LAN port of your Access Point.



IP Address: This is the IP addresses to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.

DHCP: You can disable or enable DHCP Server here.

DHCP Client Range: the range of IP addresses that will be assigned to each computer connected with the router.

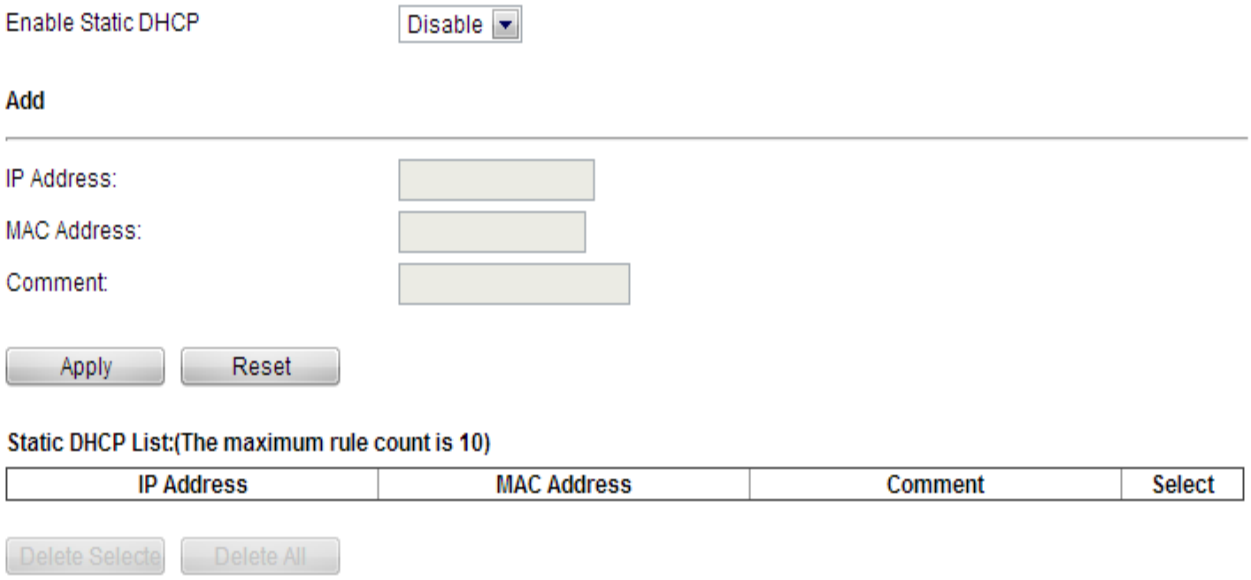
DHCP Lease Time: the IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

Domain name: this represents the name of your IP address.

Active DHCP Client Table: the table will list the detailed information of your users.

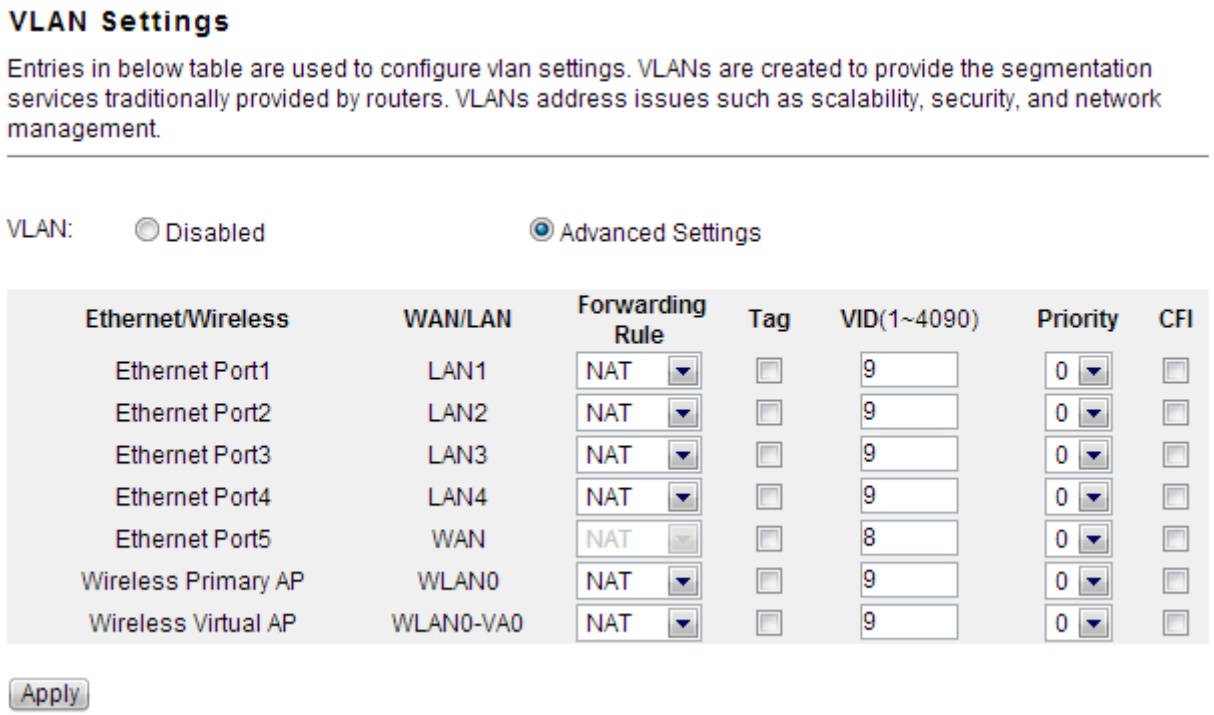
4.5.3 Static DHCP Settings

It allows you to reserve IP addresses and assign the same IP address to the network device with the specified MAC address any time it requests an IP address.



4.5.4 VLAN Settings

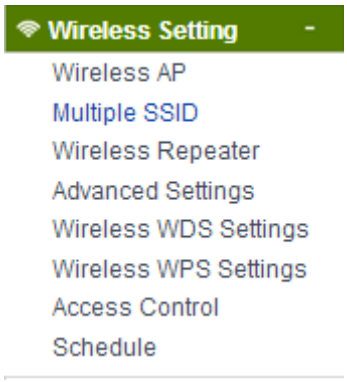
VLAN (Virtual Local Area Network) provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. VLANs are created to provide the segmentation services traditionally provided by routers.



Advanced Settings: this option enables VLAN function.

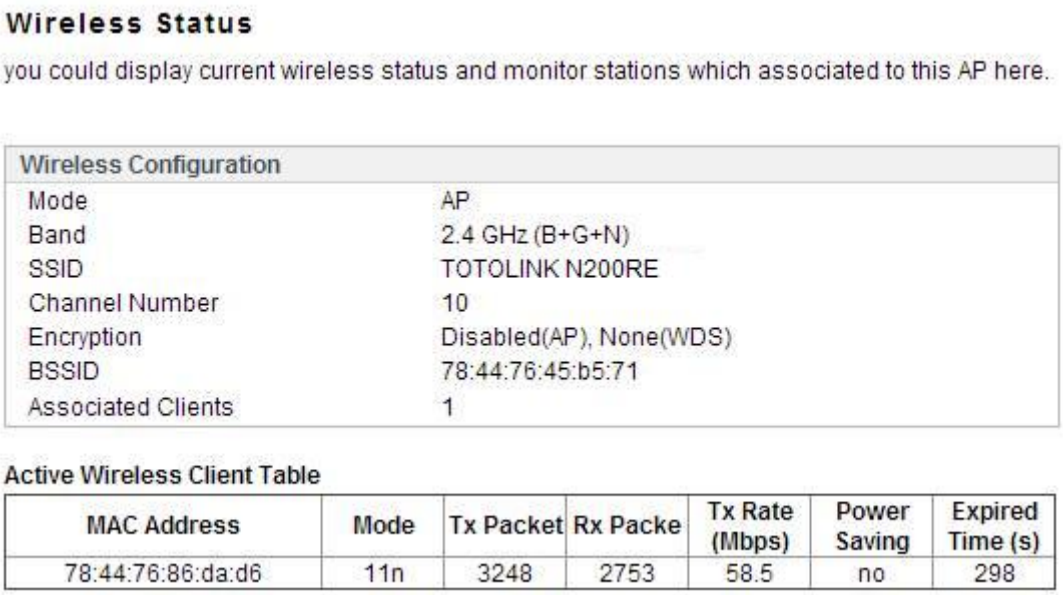
Ethernet/Wireless: specifies the WAN port and wireless AP.
WAN/LAN: defines the WAN port or LAN port.
Forwarding Rule: VLAN feature also support forwarding rule as bridge and NAT between LAN port and WAN port.
Tag: The router will add specific VLAN number to all packets on the LAN while sending them out. If enable the function of VLAN with tag, please type the tag value and specify the priority for the packets sending by LAN.
VID: type the value as Port-base VLAN ID.
Priority: Type the packet priority number for such VLAN. The range is from 0 to 7.
CFI: enable the CFI function which indicates whether MAC is encapsulated by standard format.
After the VLAN settings, please click **Apply** to finish **Network** Settings.

4.6 Wireless Setting



4.6.1 Wireless Status

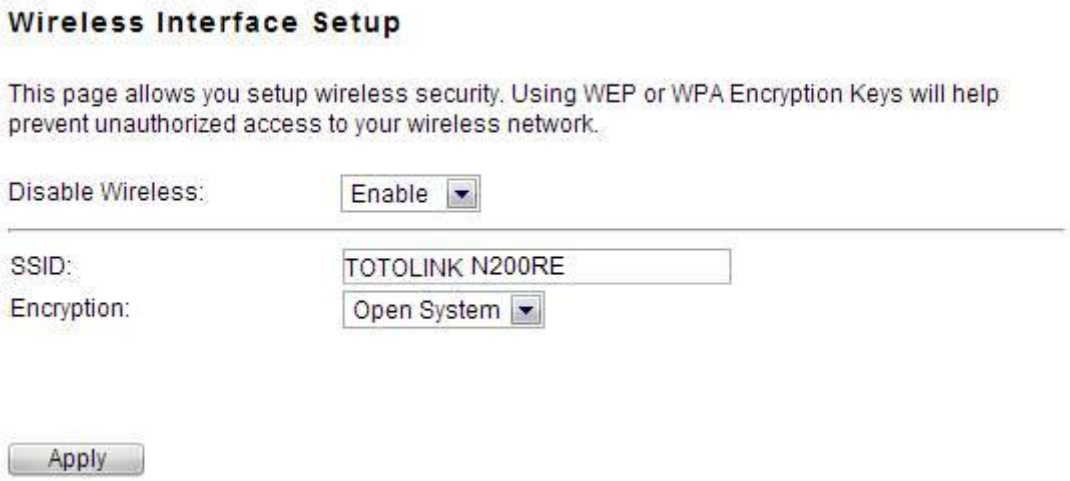
This page displays the current wireless status of the router.



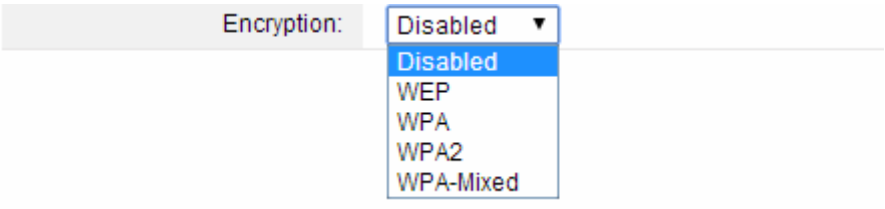
4.6.2 Wireless AP

This page allows you to setup wireless encryption to protect your wireless network from

unauthorized access.

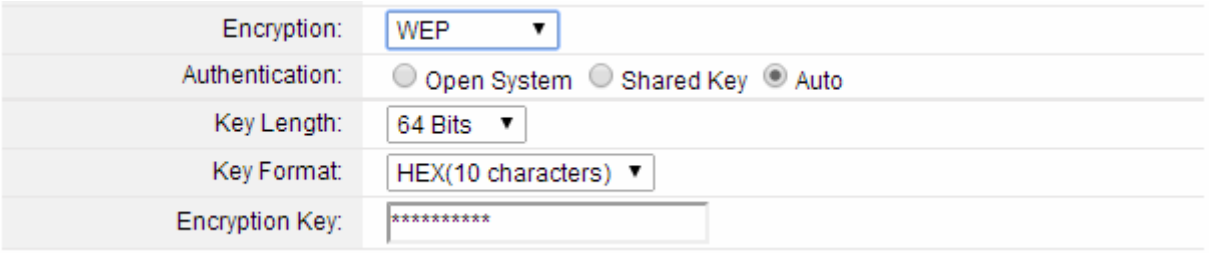


Encryption: This router supports WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.



1) WEP

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encryption data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes.



Key Length: 64-bit/128-bit, by default it is 64-bit.

64-bit—For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x414234445.)

128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).

Key Format: If you choose 64 bit, there will be two Key Formats selectable: ASCII (5 characters) and Hex (10 characters). If 128-bit, the Key Formats should comply with ASCII (13 characters) or Hex (26 characters)

Encryption Key: Please refer to Key Length to set this parameter.

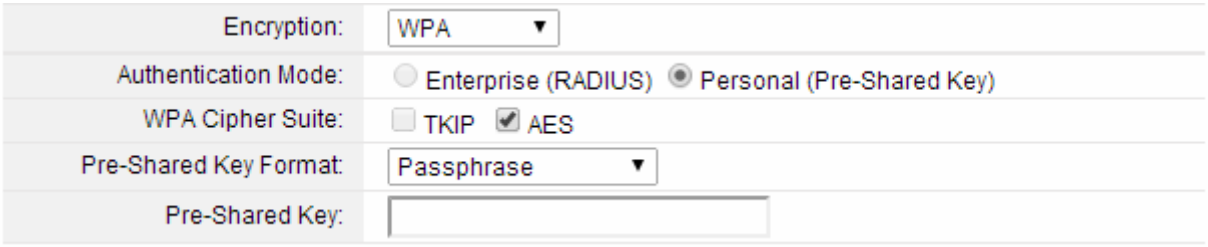
2) WPA/WPA2

Wi-Fi Protected Access (WPA) is the most dominating security mechanism in industry.

It is separated into two categories: WPA-personal and WPA-Enterprise, it is the current most secure method of wireless security and required for 802.11n performance.

TKIP--Temporal Key Integrity Protocol is one cipher for data encryption supported by WPA.

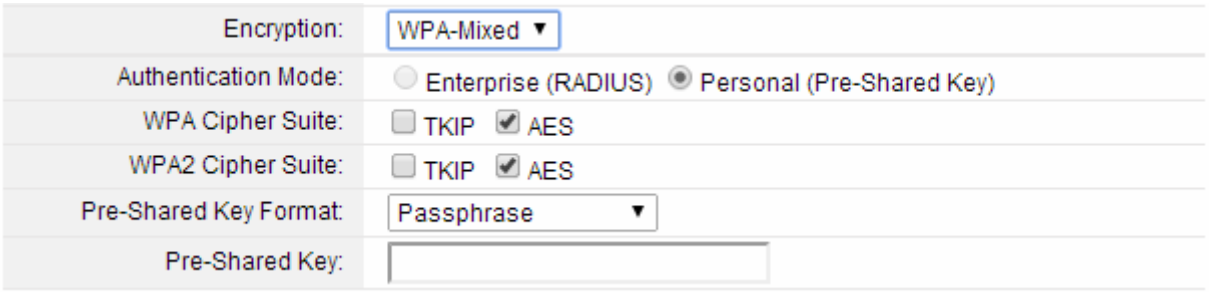
AES--Advanced Encryption Standard is another cipher for data encryption supported by WPA.



Pre-Shared Key Format/Pre-Shared Key: This is a pre-defined key used for encryption during data transmission. It has two formats: Passphrase and Hex (64 characters). Then you need to enter the Pre-Shared Key, either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as “0x321253abcde…”).

3) WPA Mixed

This option mixes WPA/WPA2 together. It will provide the best security for your router.

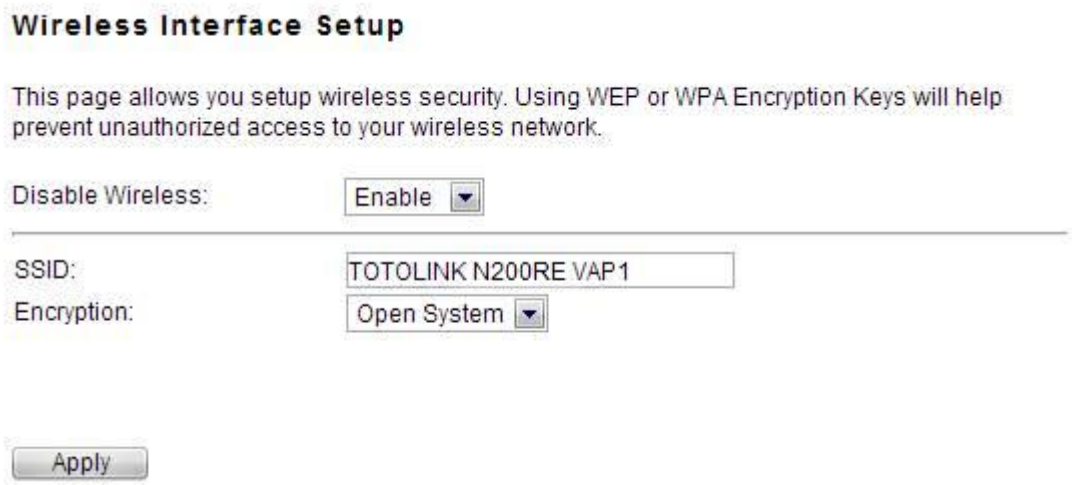


Note: *Since WEP has been proved vulnerable, you may consider using WPA2 for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and/or privacy on your wireless network.*

4.6.3 Multiple SSID

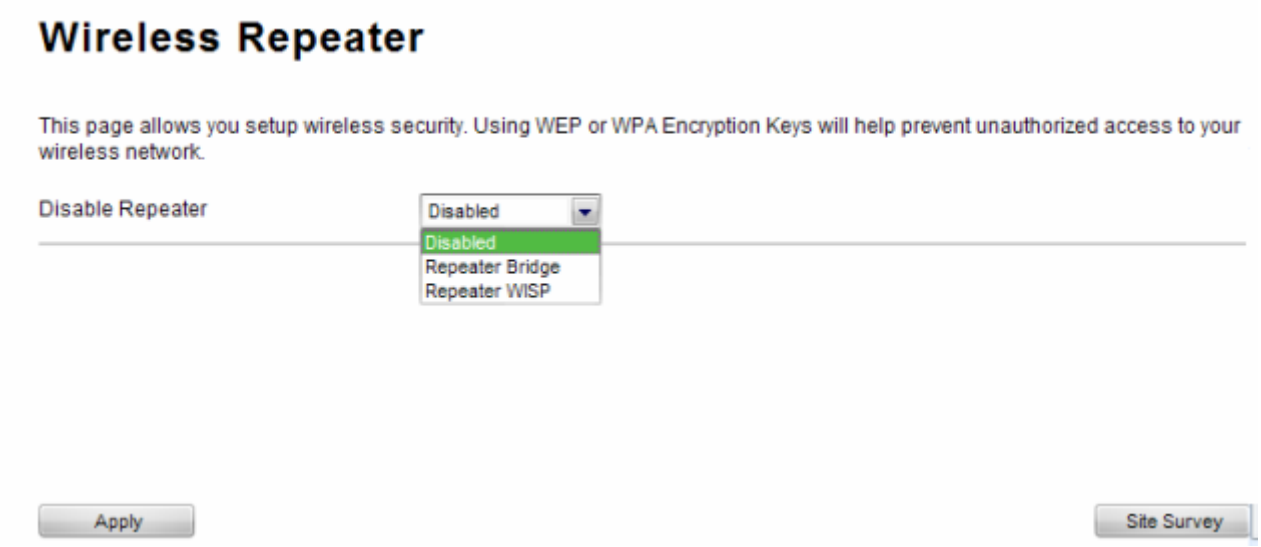
You can set another SSID for different needs. What’s more, you can setup different encryption in Security Settings section.

By default, it is disabled. You should select Enable and the configuration parameters will appear. The encryption please refer to **4.6.2 Wireless AP**



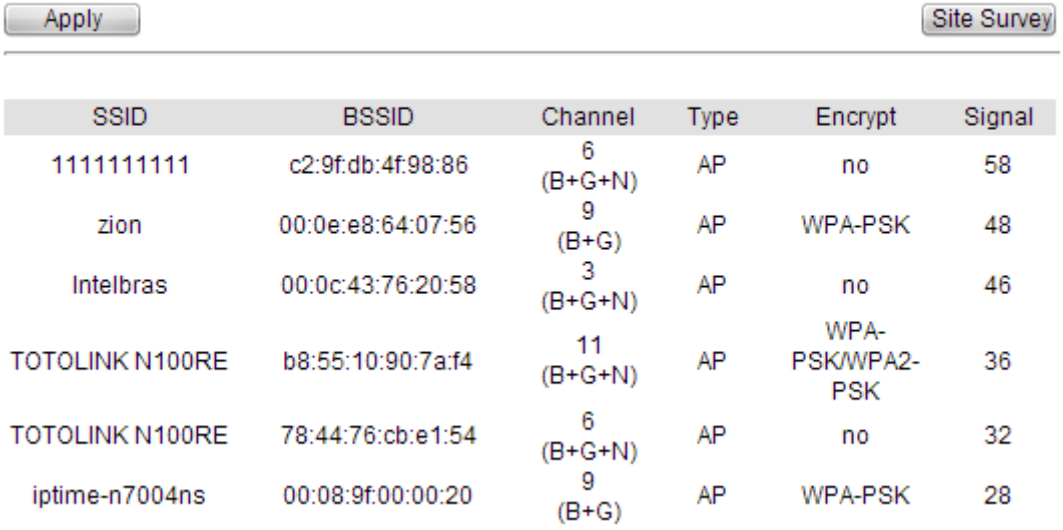
4.6.4 Wireless Repeater

You can setup wireless security in this page. It is very practical for protecting your private information.



It is disabled by default; please select a mode to enable this function.

Please click **Site Survey** button to search for any Access Point. Then they will be showed in the form.

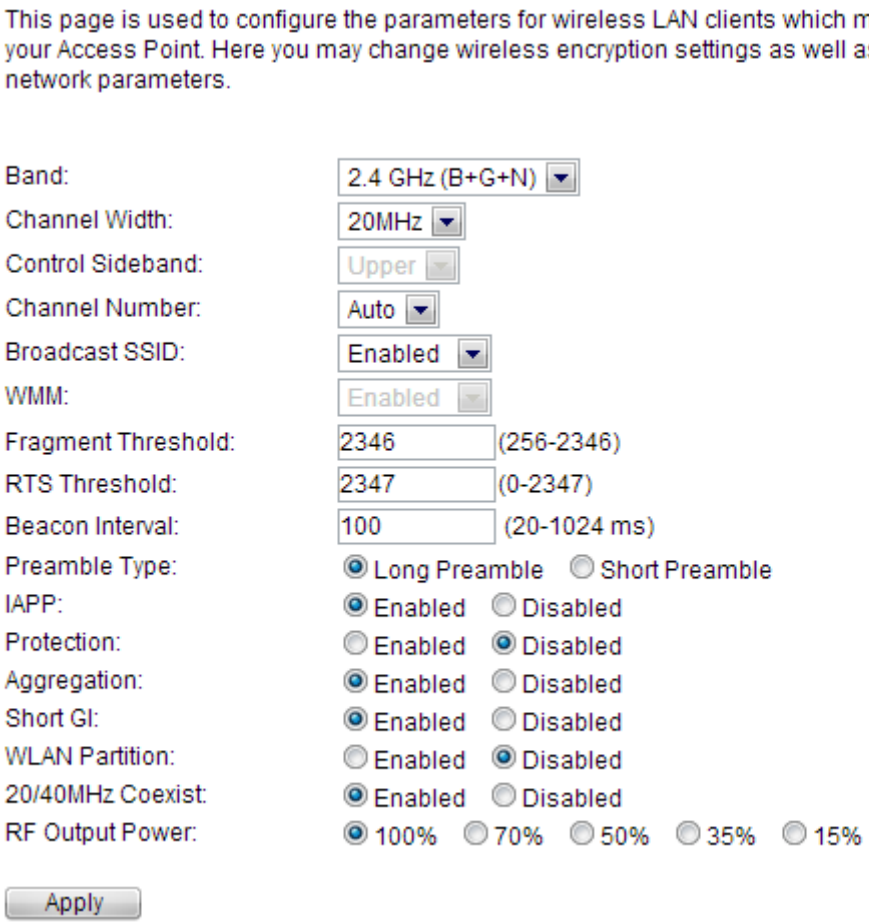


SSID	BSSID	Channel	Type	Encrypt	Signal
1111111111	c2:9f:db:4f:98:86	6 (B+G+N)	AP	no	58
zion	00:0e:e8:64:07:56	9 (B+G)	AP	WPA-PSK	48
Intelbras	00:0c:43:76:20:58	3 (B+G+N)	AP	no	46
TOTOLINK N100RE	b8:55:10:90:7a:f4	11 (B+G+N)	AP	WPA-PSK/WPA2-PSK	36
TOTOLINK N100RE	78:44:76:cb:e1:54	6 (B+G+N)	AP	no	32
iptime-n7004ns	00:08:9f:00:00:20	9 (B+G)	AP	WPA-PSK	28

Utility will search for wireless networks in range on all the supported channels while device is operating in Access Point mode. If any Access Point is found, you could choose to connect it manually when client mode is enabled.

4.6.5 Advanced Settings

On this page, you could configure the parameters for Wireless LAN client that may connect to your Access Point. Some settings should not be changed unless you know what effect the changes will have on your Access Point.



Band: This option allows you to choose the radio standard for operation of your Router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation.
Channel Width: This is the spectral width of the radio channel. Supported wireless channel spectrum widths:

20MHz is the standard channel spectrum width.
40MHz is the channel spectrum with the width of 40MHz.

Channel Number: This option provides selectable channel numbers.

Broadcast SSID: you can choose to enable or disable to broadcast your SSID.

WMM: it maintains the priority of audio, video and voice.

Fragment Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes. Setting the Fragment Threshold too low may result in poor network performance. The use of fragment can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the Fragment Threshold will result in lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes. The default value is 2347, which means that RTS is disabled.
Beacon Interval: By default, it is set to 100ms. Higher Beacon interval will improve the

device’s wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

Preamble Type: this option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses shot preamble with 56 bit sync filed instead of long preamble with 128 bit sync filed. However, some original 11b wireless network devices only support long preamble. By default, Long Preamble is selected.

IAPP： Inter-Access Point Protocol is designed for the enforcement of unique association throughout an ESS (Extended Service Set) and for secure exchange of station’s security context between current access point (AP) and new AP during handoff period. It is enabled by default.

Protection: it is disabled by default.

Aggregation: A part of the 802.11n standard. It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header. It is enabled by default.

Short GI: short Guide Interval. It is to assure the safety of propagation delays and reflections for the sensitive digital data.

WLAN Partition: divides the WLAN to several parts.

20/40MHz Coexist: enable this function will make the device select the channel with better performance automatically. It is disabled by default.

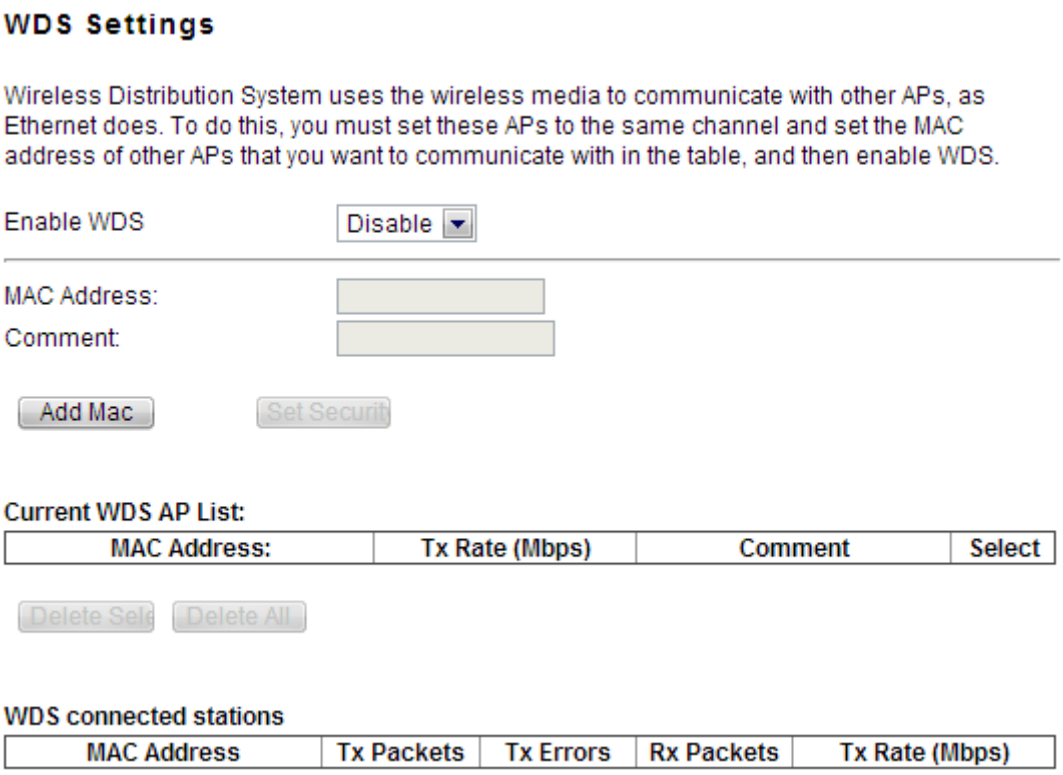
RF Output Power: you can select the output power of the wireless device. The default value is 100%. It will deliver the best performance of the device.

4.6.6 Wireless WDS Settings

WDS means Wireless Distribution System. It is a protocol for connecting two access points wirelessly. Usually, it can be used for the following application:

1. Provide bridge traffic between two LANs though the air.
2. Extend the coverage range of a WLAN.

To meet the above requirement, 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: by default, you can't select the checkbox to enable WDS.
MAC Address: the other AP's MAC Address that you want to communicate with.
Comment: describes the reason why you want to communicate with others.
The WDS Security Setup allows you to set encryption for your WDS connection. You can refer to the Wireless Security Setup.

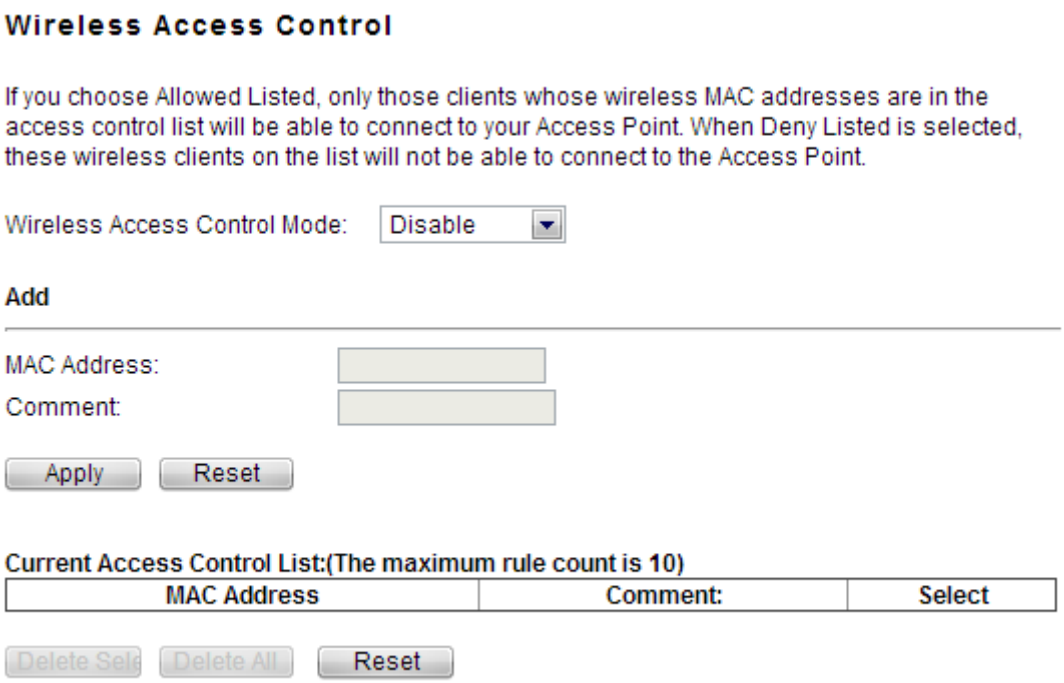
4.6.7 Wireless WPS Settings

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2.

Self-PIN Number: it will show the PIN Number of your device.
Push Button Configuration: click Start PBC button to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes.)
STOP WSC: Click the button to stop WSC function.

Client PIN Number: please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

4.6.8 Access Control



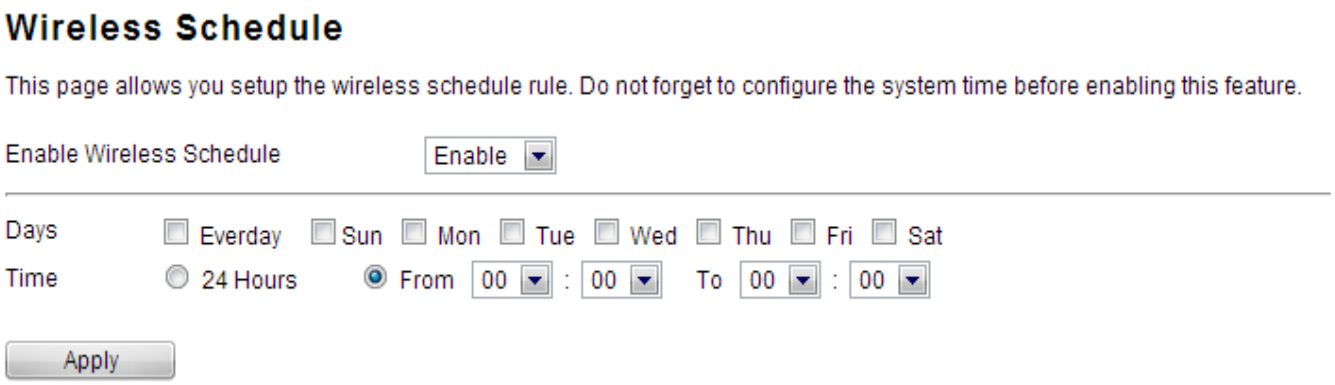
By default, Wireless Access Control Mode is disabled.
There are two ways to set the Access Control List:

1. If you select **Allow List** and enter the MAC Address of wireless client, the listed address will have granted access to the Access Point while the other access will be denied.
2. If you select **Deny List** and enter the MAC Address of wireless client, the listed address will have denied access to the Access Point while the other access will be granted.

MAC Address: the wireless MAC address that you allow to access or not.
Comment: describe the reason why you allow or deny the access of the MAC Address.
You need to click **Apply Changes** to make your setting work.
Current Access Control List: this list will show all the current access control that you have set. And you're able to delete some or all of them using the **Delete Selected** or **Delete All** button.

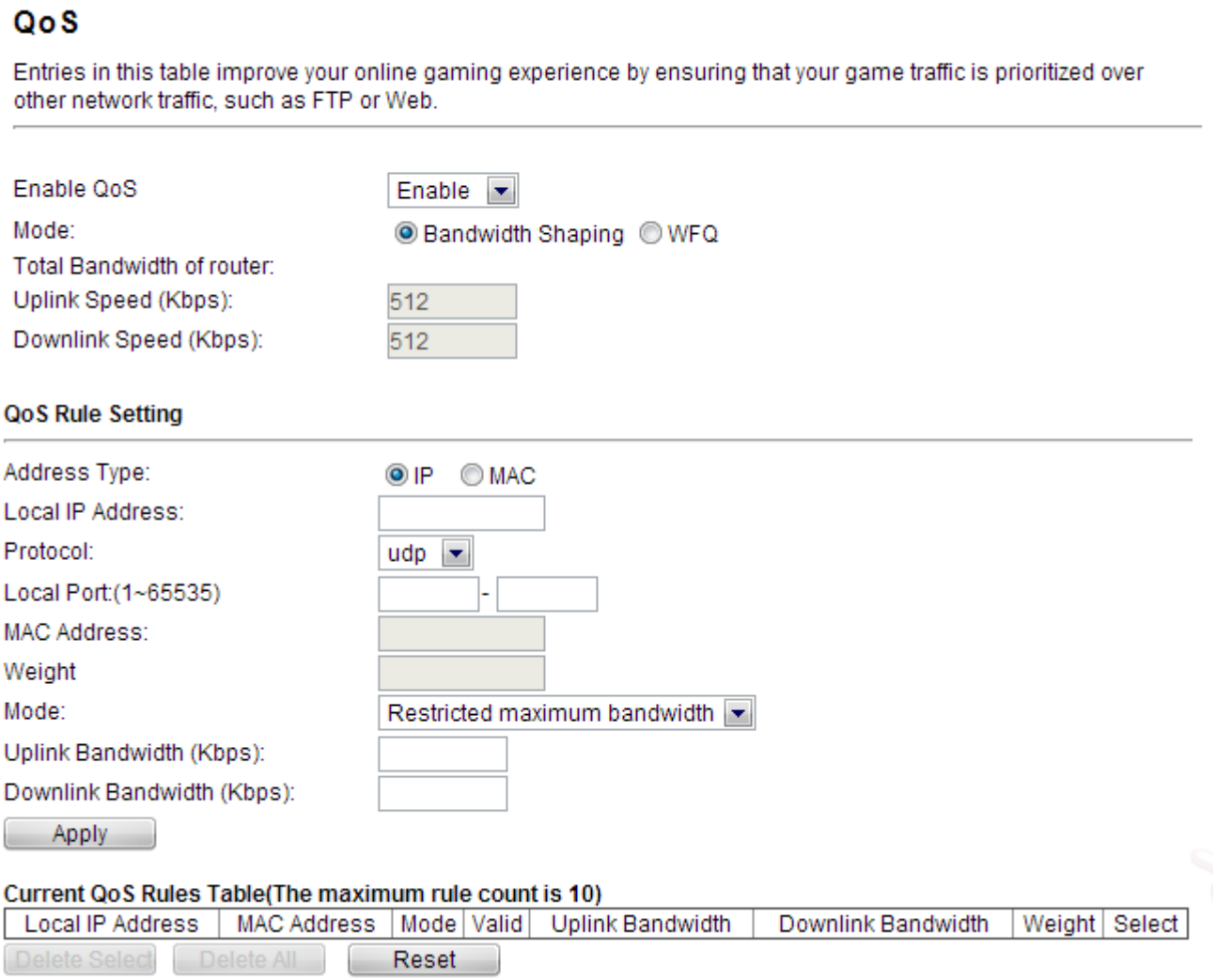
4.6.9 Schedule

The wireless schedule allows you to setup the time when WiFi is on. It is very convenient for users who often access the Internet very regularly. You have to enable **NTP in Time Zone Setting** part before setting schedule.



4.7 QoS

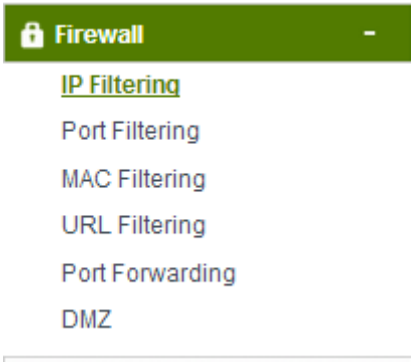
QoS means Quality of Service. Deploying QoS management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.



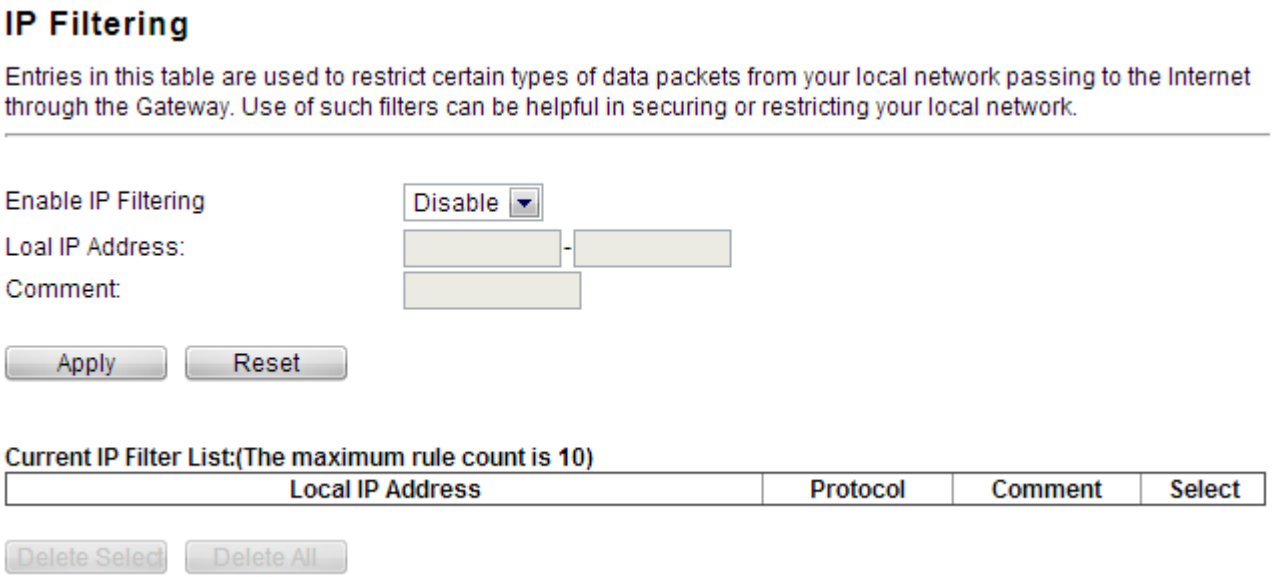
4.8 Firewall

The firewall of this router helps to protect you local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the

Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

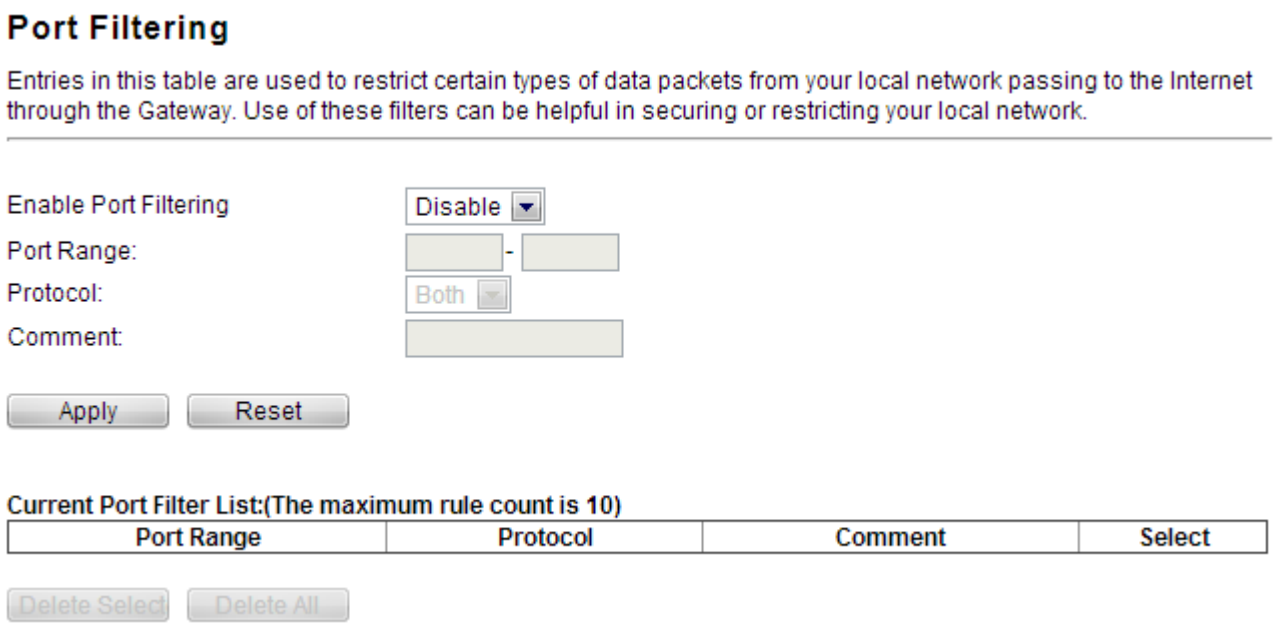


4.8.1 IP Filtering



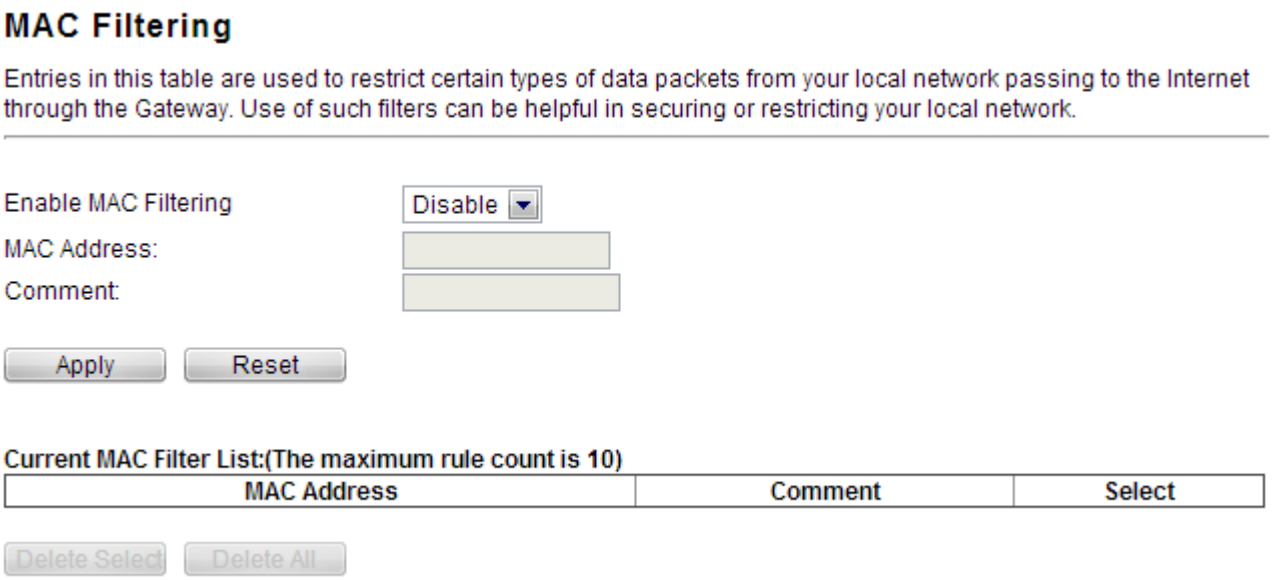
Enable IP filtering: you can select this checkbox to enable IP Filtering function.
Local IP Address: the IP address that you want to filter.
Comment: describe the reason why you want to filter the IP address. Just few words are saved there usually.
Current IP Filter List: this table will list the detailed information about the IP addresses that will be filtered.

4.8.2 Port Filtering



Enable Port Filtering: you can select this checkbox to enable Port Filtering function.
Port Range: the port range that you want to filter.
Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP/Both.
Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.
Current Port Filter List: this table will list the detailed information about the Port that will be filtered.

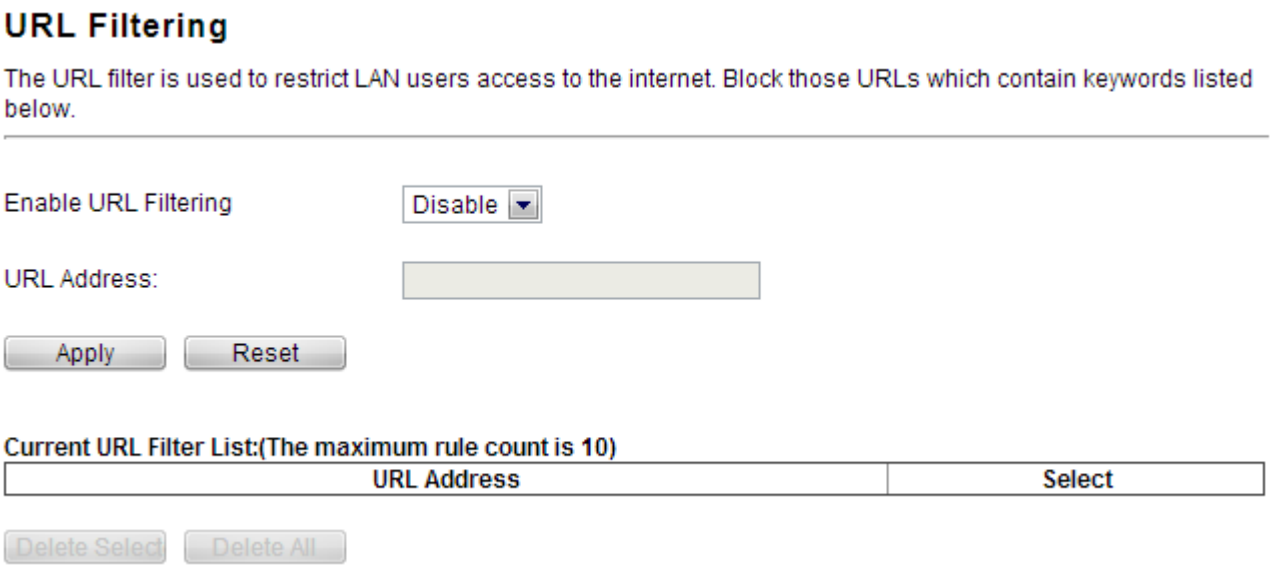
4.8.3 MAC Filtering



Enable MAC Filtering: you can check the box to enable MAC Filtering function.
MAC Address: the MAC address that you want to filter.

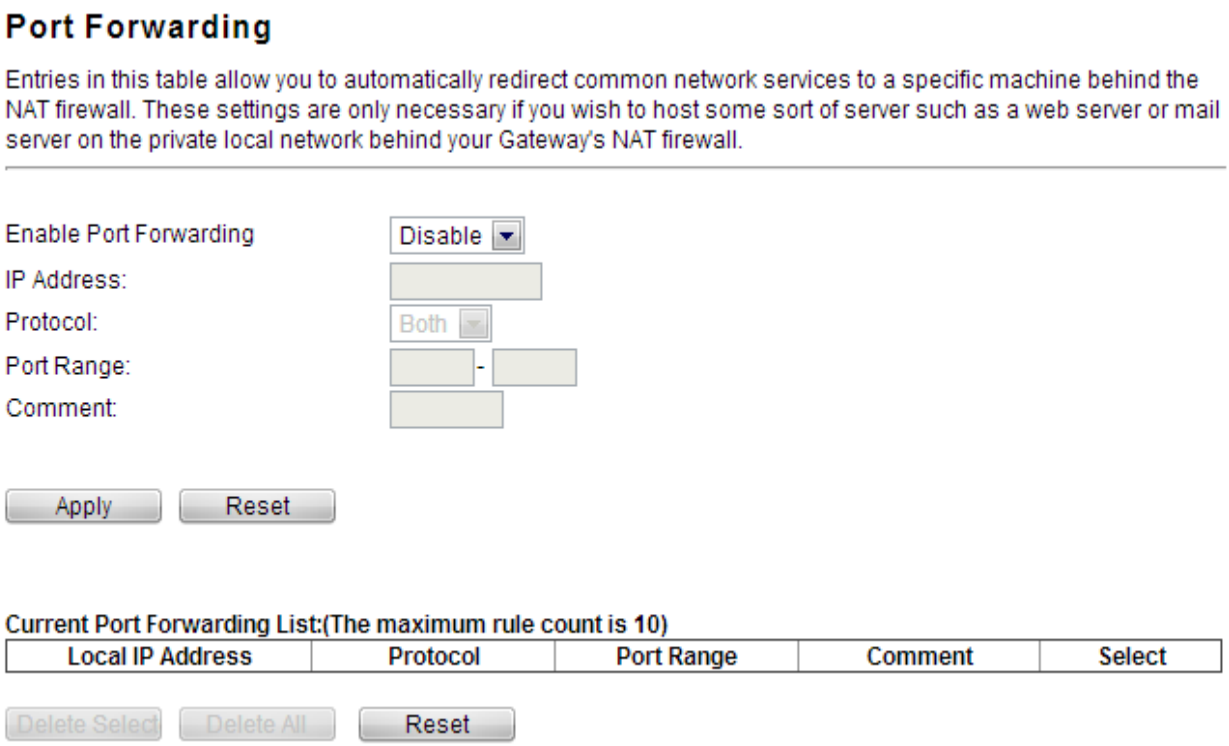
Comment: describe the reason why you want to filter the MAC address. Just few words are saved there usually.
Current MAC Filter List: this table will list the detailed information about the MAC address that will be filtered.

4.8.4 URL Filtering



Enable URL Filtering: you can select this checkbox to enable URL filtering function.
URL Addresses: type in the keywords contained in URLs that you don't allow LAN users to access.
Current URL Filter List: this table will list the detailed information about the URL that will be filtered.

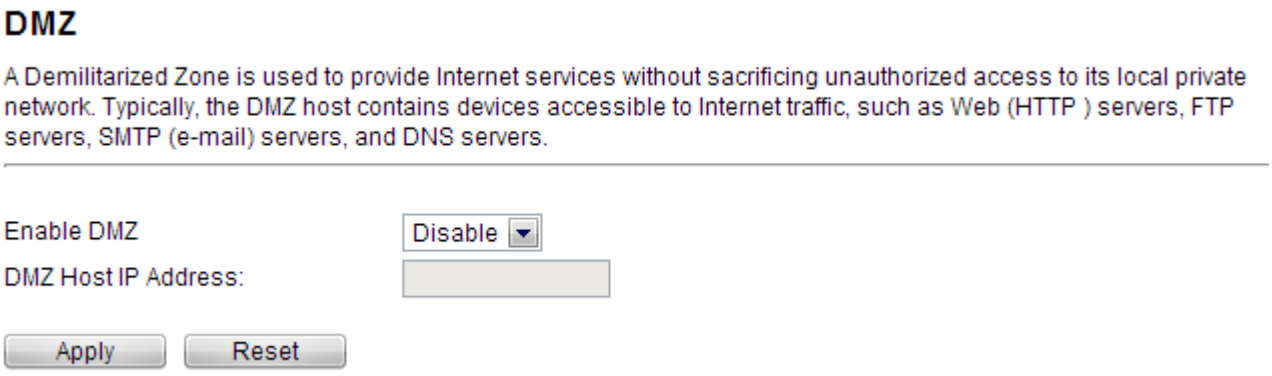
4.8.5 Port Forwarding



Enable Port Forwarding: you can select this checkbox to enable Port Forwarding function.
I**P Address:** enter the Port's IP address.
Protocol: choose which particular protocol type should be forwarding. Here you can choose Both/UDP/TCP.
Port Range: set the range that the port forward to.
Comment: describe the reason why you want to use port forward function. Just few words are saved there usually.

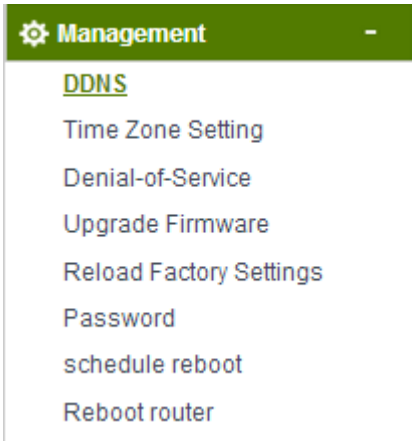
4.8.6 DMZ

DMZ means Demilitarized Zone. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.



Enable DMZ: you can select this checkbox to Enable DMZ function.
DMZ Host IP Address: type in the IP address of the DMZ host.

4.9 Management

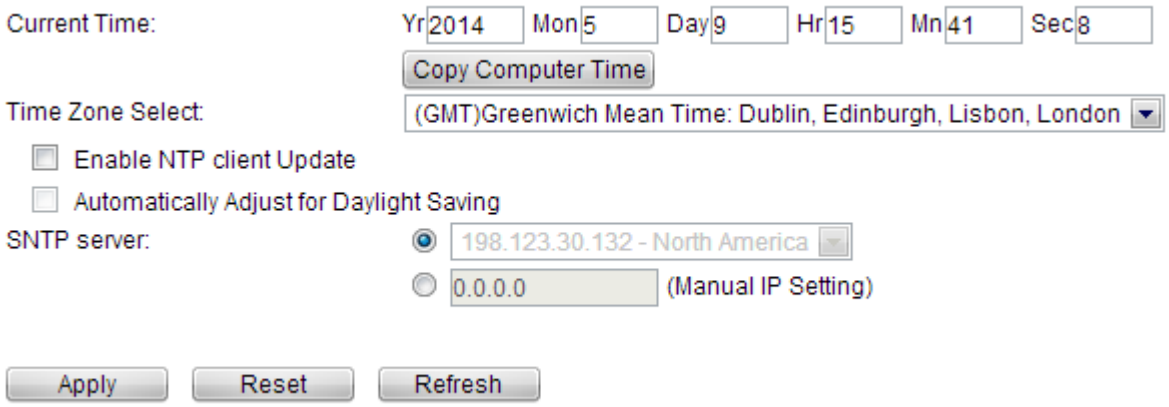


4.9.1 DDNS

DDNS means Dynamic Domain Name System. The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet.
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers.

4.9.2 Time Zone Setting

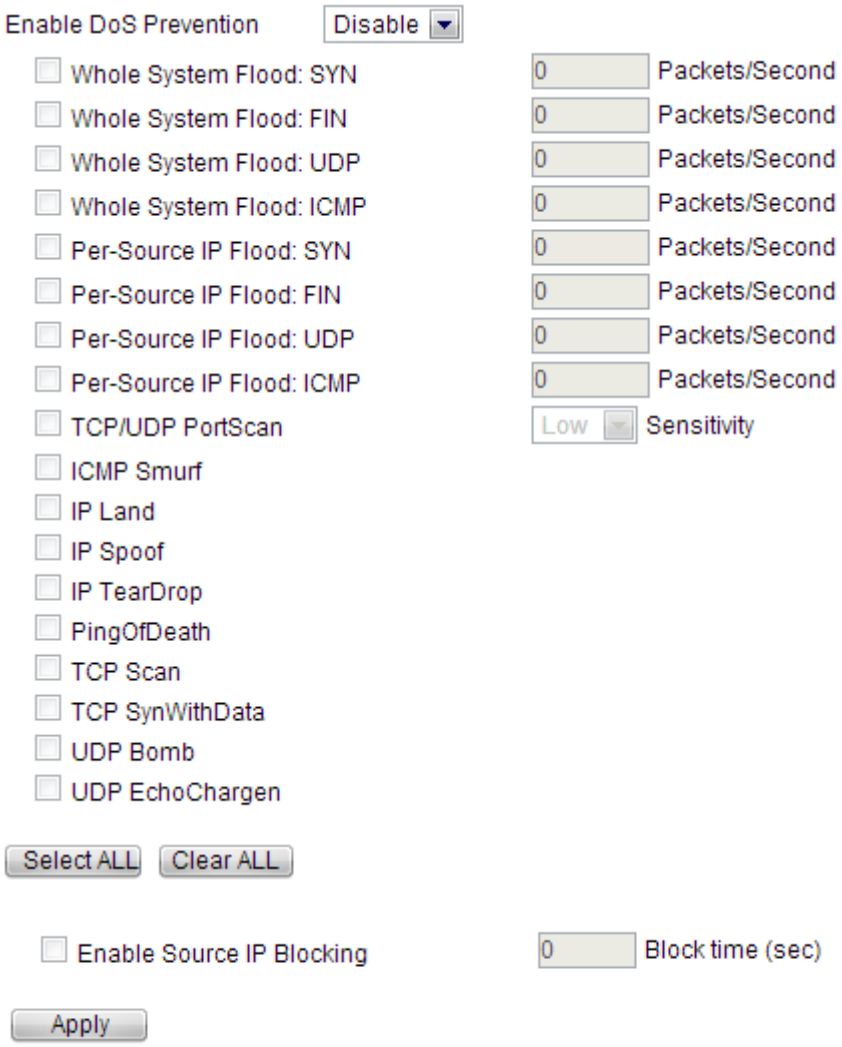
This page allows you to maintain the system time by synchronizing with a public time server over the Internet.



You can specify the device's time zone according to GMT (Greenwich Mean Time) or copy computer time as the current time only by clicking the **Copy Computer Time** button.
Time Zone Select: Select the Time Zone where the router is located.
Enable NTP client update: NTP means Network Time Protocol which is used to make the computer's time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption. You need to check this box to activate this page.
Automatically Adjust for Daylight Saving: the system will adjust for daylight saving automatically for you.
SNTP server: Please choose the corresponding SNTP server to get right time.

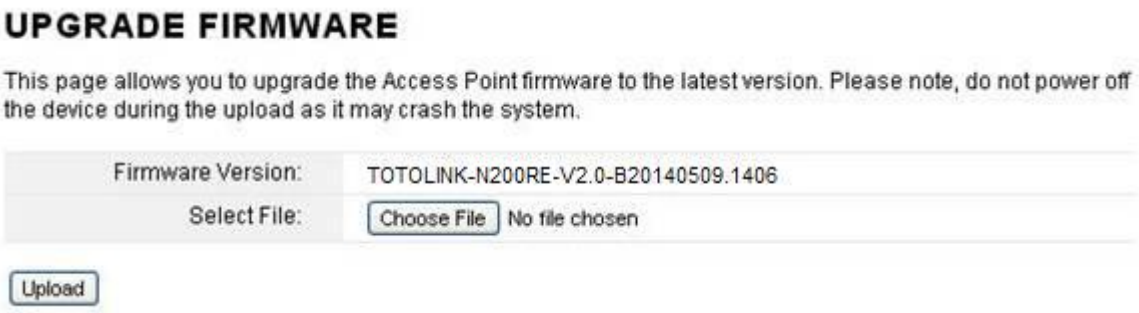
4.9.3 Denial-of-Service

The DoS Prevention functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.



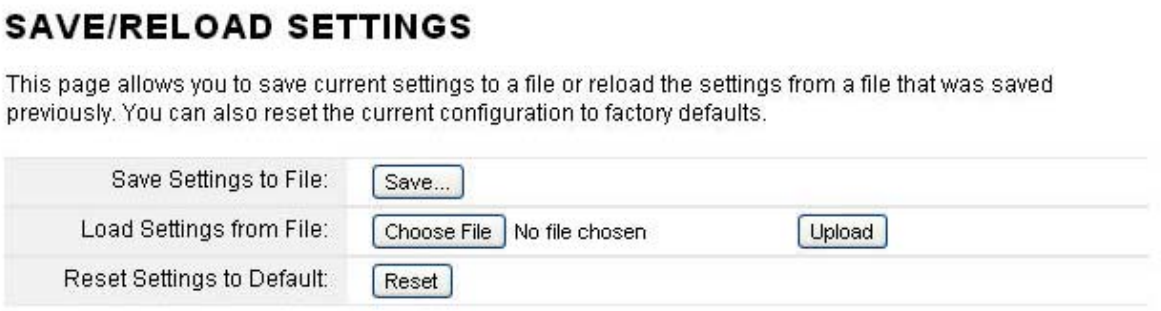
4.9.4 Upgrade Firmware

This page allows you to 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.



4.9.5 Reload Factory Settings

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



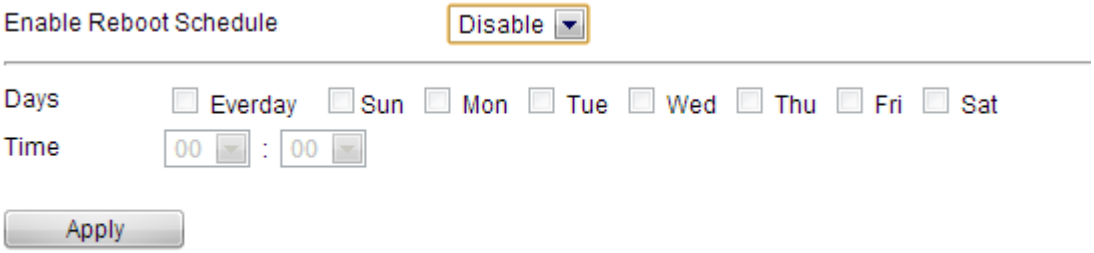
4.9.6 Password

User Name: type in the name that you use to login the web interface of the router.
New Password: new password is used for administrator authentication.
Confirm Password: new password should be re-entered to verify its accuracy.

Note: *password length is 8 characters maximum, characters after the 8th position will be truncated.*

4.9.7 Schedule Reboot

The schedule function allows you to setup the time that the router will reboot automatically.



4.9.8 Reboot Router

Please click this **Reboot** button to reboot your router quickly.

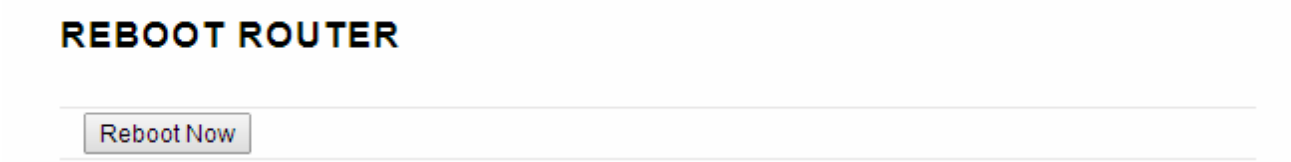


Table of Contents

1. ABOUT THIS GUIDE

Thank you very much for purchasing the wireless N router. This guide will introduce the features of this router and tell you how to connect, use and configure the router to access Internet. Please follow the instructions in this guide to avoid affecting the router's performance by improper operation.

1.1 Navigation of the User's Guide

Product Overview: Describes the router's function and its features.

Hardware Installation: Describes the hardware installation and settings on user's computer.

Connecting to Internet: Tells you how to connect your computer to Internet successfully by the router.

Advanced Settings: Lists all technical functions including Wireless, TCP/IP Settings, Firewall and System of the router.

2. PRODUCT OVERVIEW

2.1 Introduction

This is a wireless router which integrates with internet-sharing router, 4-port switch and firewall all-in-one. Multiple encryptions including wireless LAN 64/128-bit WEP, WPA/WPA2 and WPA-mixed security are supported by the router. The VLAN function also makes amazing interactive entertainment experience of IPTV be achieved easily. The IP, Port, URL and MAC address filtering function also makes it easy for user management. In view of the above, it will allow you to connect your network wirelessly in an easy and secure way better than ever. It is really a high performance and cost-effective solution for home and small offices.

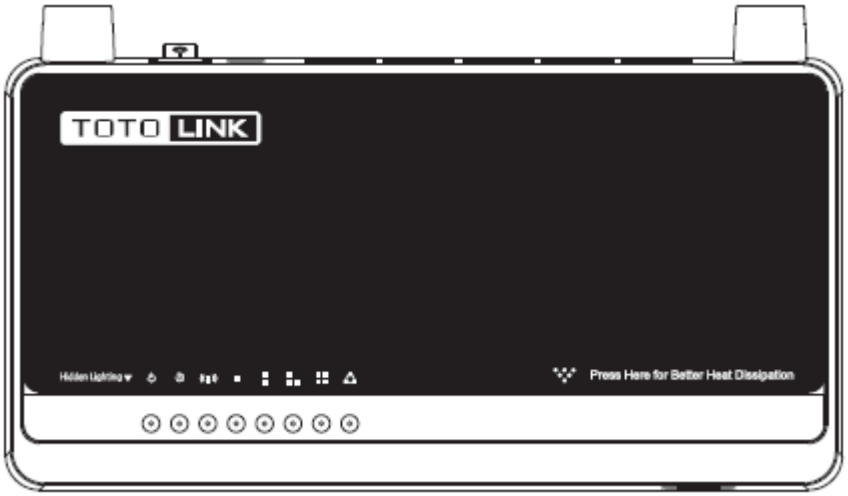
2.2 Features

- Complies with IEEE 802.11n/g/b standards for 2.4GHz Wireless LAN.
- Supports DHCP, Static IP, PPPoE broadband functions.
- Provides three operation modes: Gateway, Repeater Bridge and Repeater WISP.
- Connects to secure network easily and fast using WPS (one-button).
- Provides 64/128-bit WEP, WPA/WPA2 and WPA-Mixed security.
- Supports VLAN function.
- Supports IP, Port, MAC, URL filtering and Port Forwarding.
- QoS function allocates network bandwidth reasonably.

2.3 Panel Layout

2.3.1 Front Panel

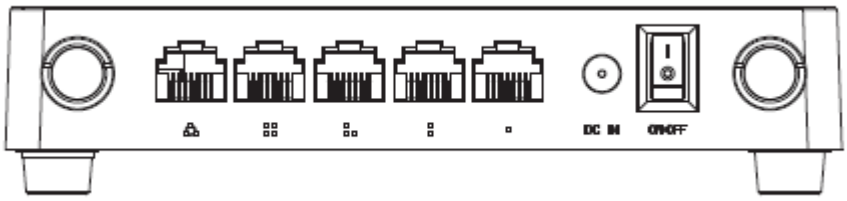
The front panel of this router consists of 8 LEDs, which is designed to indicate connection status.



POWER	This indicator lights blue when the router powered on, otherwise it is off.	
CPU	This indicator blinks blue when router powered on.	
WLAN	This indicator blinks blue when there are wireless devices connected and transmitting data to the router.	
WAN	On	When the WAN port is connected successfully the indicator lights blue.
	Blink	During transmitting or receiving data through the WAN port the indicator blinks blue.
	Off	There is no device linked to the WAN port.
1/2/3/4 LAN	On	When the LAN port has a successful connection, the corresponding indicator lights blue.
	Blink	During transmitting or receiving data through the LAN port the corresponding indicator blinks blue.
	Off	There is no device linked to the LAN port.

2.3.2 Rear Panel

The figure below shows the rear panel of this router.



DC IN	The Power socket is where you will connect the power adapter.
WAN	This port is where you will connect with the cable to access Internet.
1/2/3/4 LAN	This port connects the router to local PC.
RST-WPS Button	Press for about 2~3 seconds, the system LED indicator keep solid light, it means WPS working, while press for about 10 seconds, all LEDs blinks quickly, the device will restore to factory default settings.

3. HARDWARE INSTALLATION

3.1 Hardware Installation

For those computers you wish to connect with Internet by this router, each of the computers must be properly connected with the router through provided Ethernet cables.

1. Connect the Modem to ADSL Filter using RJ11 network cable, LINE port to LINE port.
2. Connect the ADSL's LAN port to Router's WAN port using RJ45 network cable.
3. Connect your PC to any one of router's LAN port.
4. Plug the Power Adapter into the router and then into an outlet.
5. Turn on your computer.
6. Check and confirm that the Power & LAN LED on the router are **ON**.

3.2 Check the Installation

The control LEDs of the router are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected to the broadband modem, the Power, WPS, LAN, WLAN and WAN port LEDs of the WLAN Router will light up indicating a normal status.

2. When the WAN Port is connected to Internet successfully, the WAN LED will light up.

3. When the LAN Port is connected to the computer system, the LAN LED will light up.

3.3 Set up the Computer

The default IP address of the router is 192.168.1.1, the default Subnet Mask is 255.255.255.0. Both of these parameters can be changed as you want. In this guide, we will use the default values for description.

Connect the local PC to the LAN port on the router. There are then two ways to configure the IP address for your PC.

- **Configure the IP address manually**

Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.1.1 (router's default IP address).

- **Obtain an IP address automatically**

Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. Open a command prompt, and type in **ping 192**.168.1.1, then press Enter.

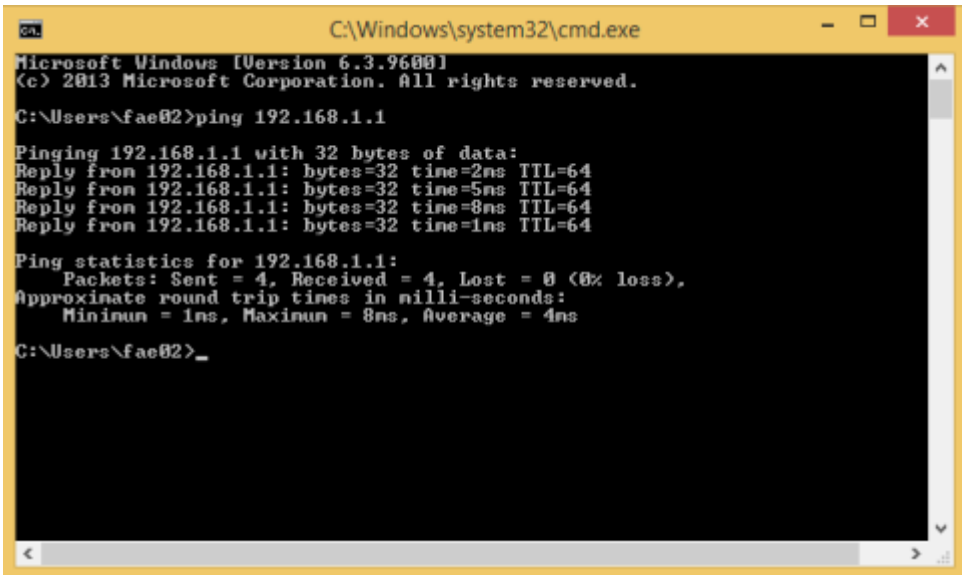


Figure 3-1 Successful Ping command

If the result displayed is similar to the figure 3-1, it means that the connection between your PC and the router has been established.

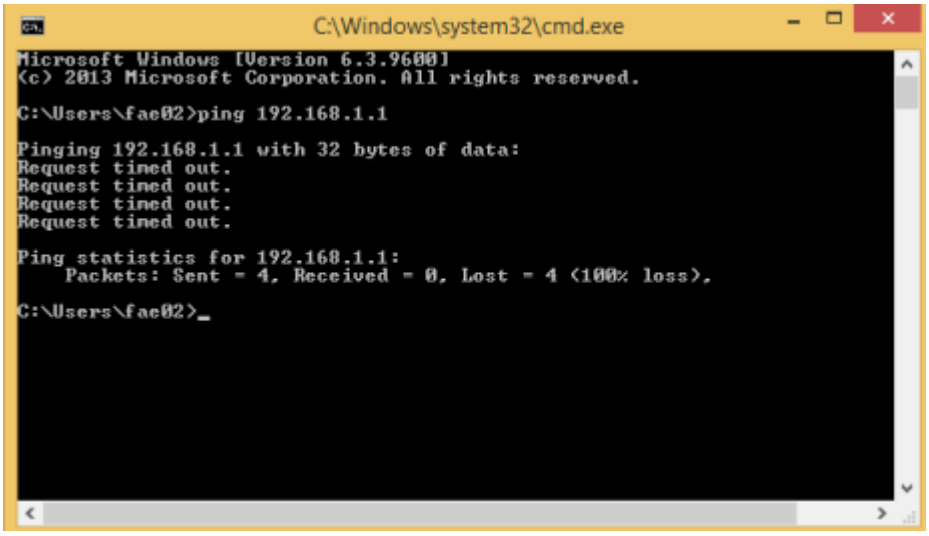


Figure 3-2 Failure Ping command

If the result displayed is similar to the figure 3-2, it means that your PC has not connected to the router successfully. Please check it following below steps:

1. Is the connection between your PC and the router correct?

If correct, the LAN port on the router and LED on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Since the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

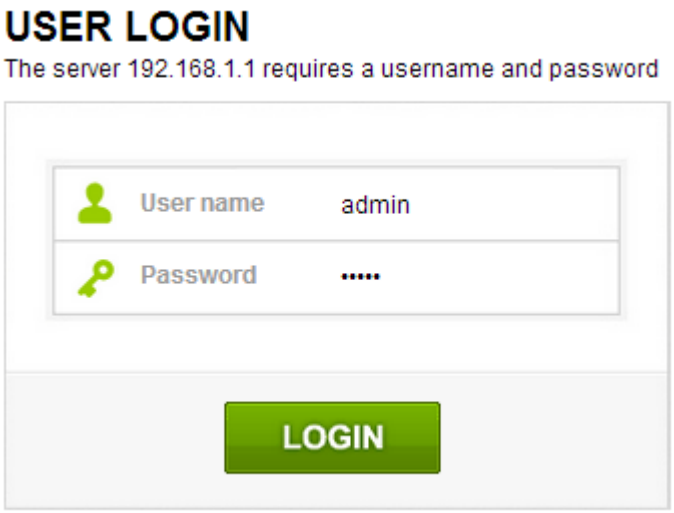
4. CONNECTING TO INTERNET

This chapter introduces how to configure the basic functions of your router so that you can surf the Internet.

4.1 Accessing Web page

Connect to the router by typing 192.168.1.1 in the address field of web browser. Then press **Enter** key.

Then below window will pop up that requires you to enter valid User Name and Password.

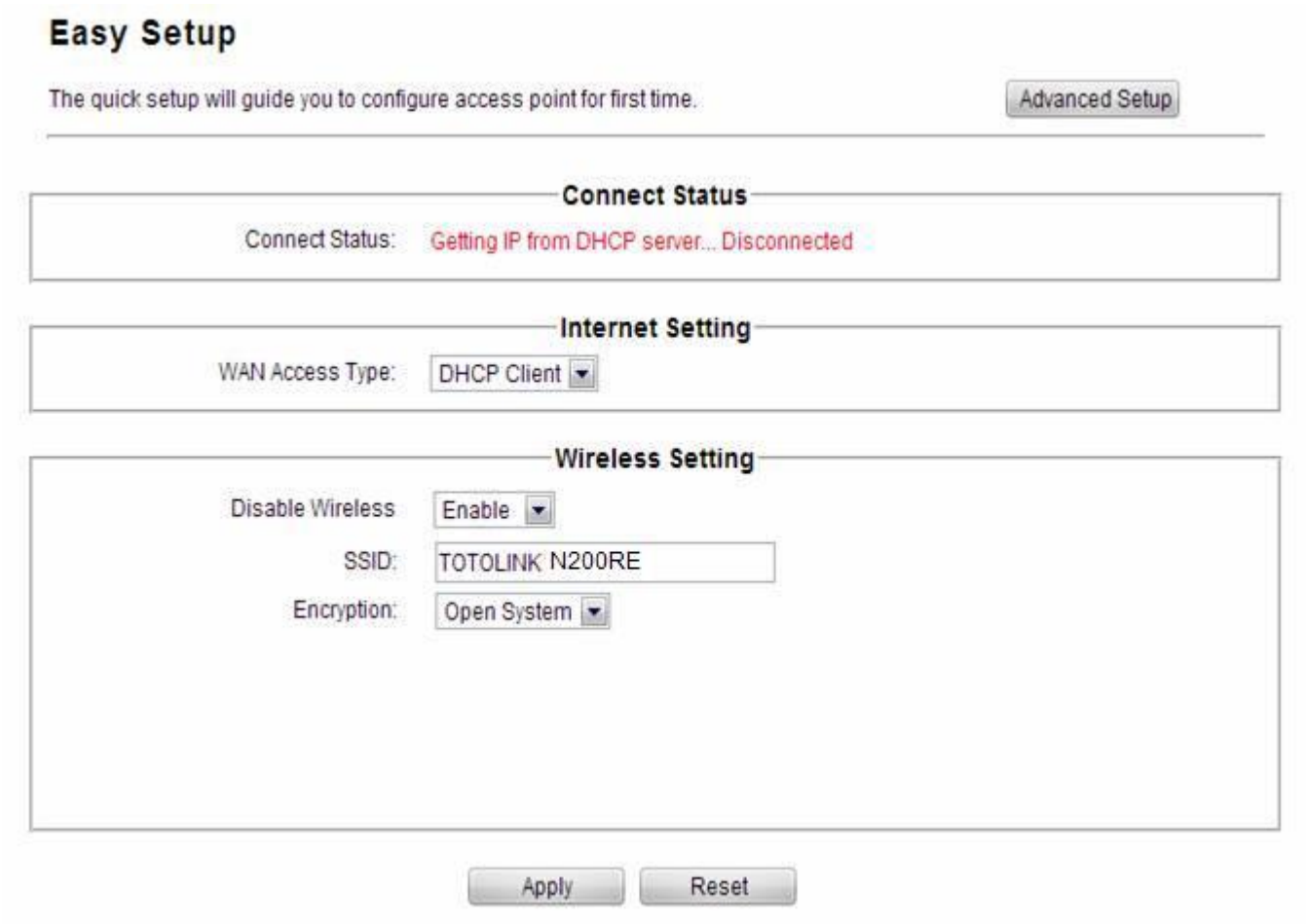


Enter **admin** for User Name and Password, both in lower case letters. Then click **OK** button or press **Enter** key.

Now you will get into the web interface of the device. The Main screen will appear.

> ***Note:*** *If the above screen does not prompt, it means that your web-browser has been set to using a proxy. Go to* ***Tools menu*****>*****Internet Options*****>*****Connections*****>*****LAN Settings****, in the screen that appears, cancel the* ***Using Proxy checkbox****, and click* ***OK*** *to finish it.*

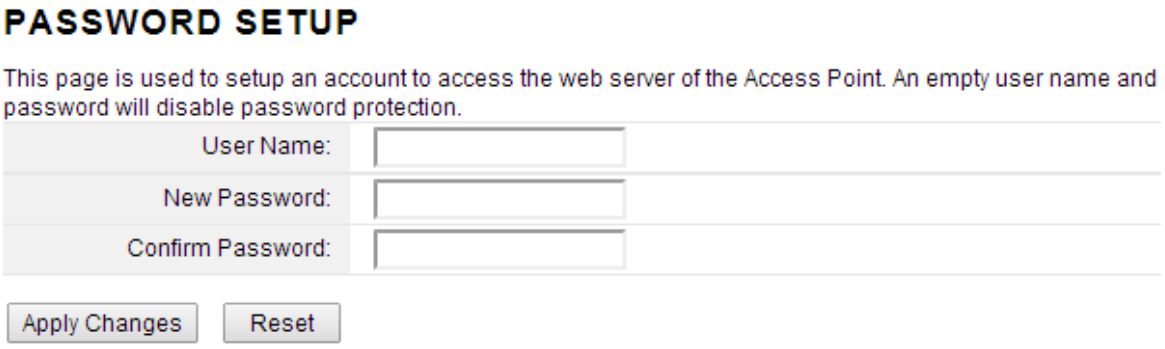
Now you have logged into the web interface of the router. First, you will see the Easy Setup page.



.

4.2 Changing Password

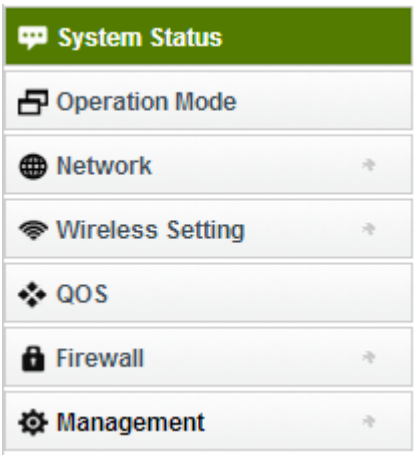
Now, we recommend that you change the password to protect the security of your router. Please go to **Management—Password** to change the password required to log in your router.



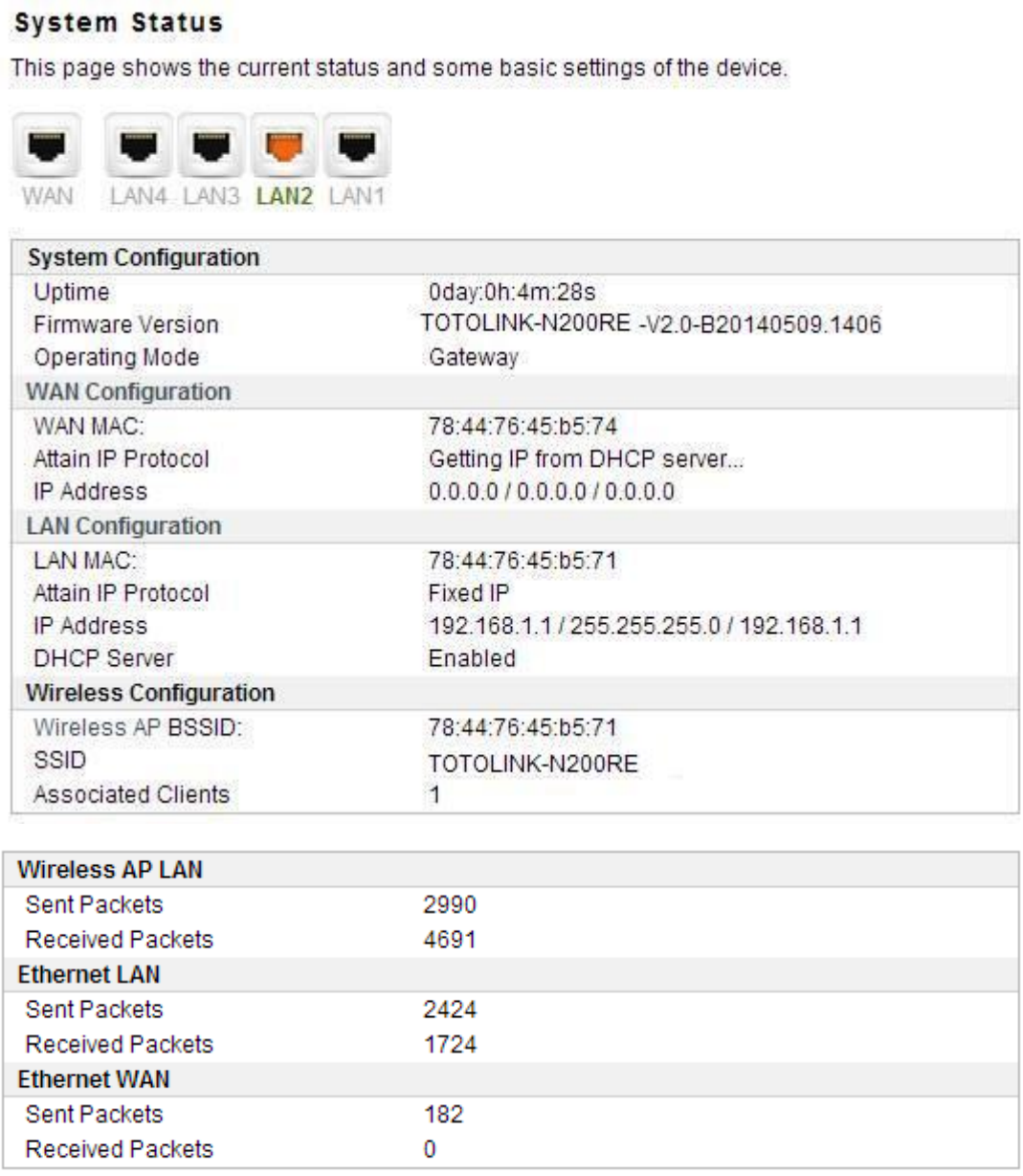
User Name: type in the name that you use to login the web interface of the router.
New Password: new password is used for administrator authentication.
Confirm Password: new password should be re-entered to verify its accuracy.

Note: *password length is 8 characters maximum, characters after the 8th position will be truncated.*

4.3 Status

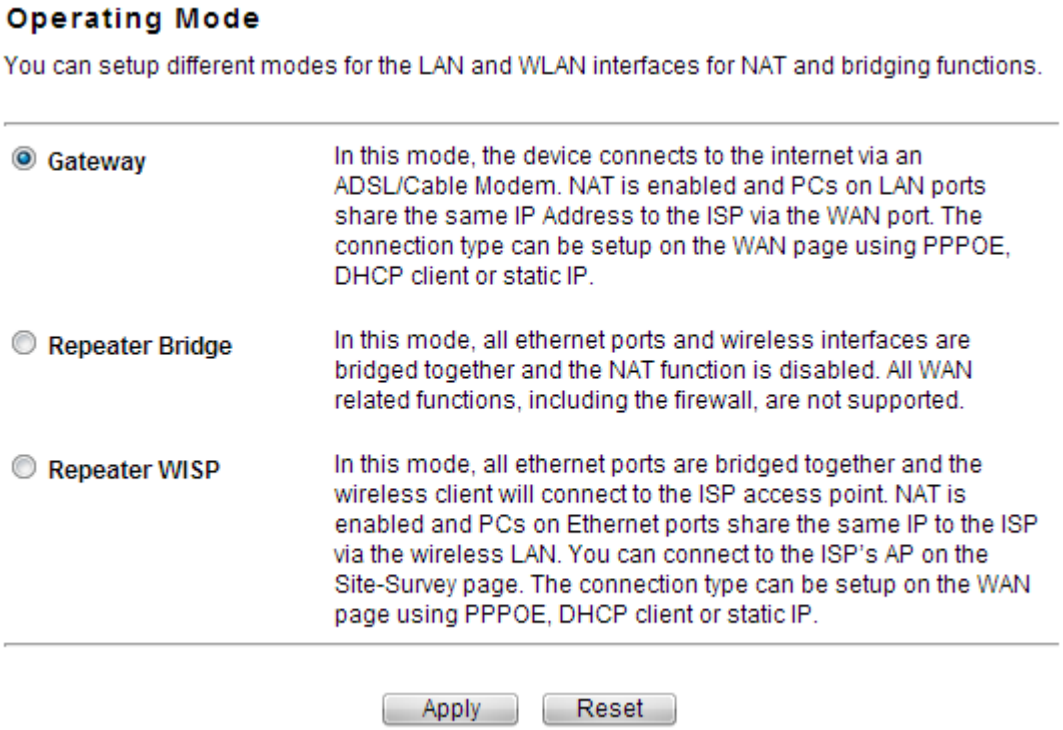


This page shows the current status and some basic parameters of the device.



4.4 Operation Mode

This parameter specifies the operating network modes for the Router. This router provides three modes: **Gateway**, **Repeater Bridge** and **Repeater WISP**. You could refer to the following description to choose the right one.



1. Gateway

In this mode, the device connects to the internet via an ADSL/Cable Modem. NAT is enabled and PCs on LAN ports share the same IP Address to the ISP via the WAN port. The connection type can be setup on the WAN page using PPPOE, DHCP client or static IP.

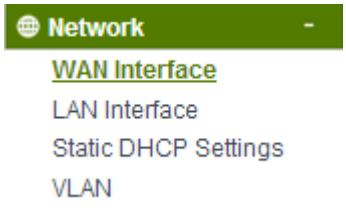
2. Repeater Bridge

In this mode, all ethernet ports and wireless interfaces are bridged together and the NAT function is disabled. All WAN related functions, including the firewall, are not supported.

3. Repeater WISP

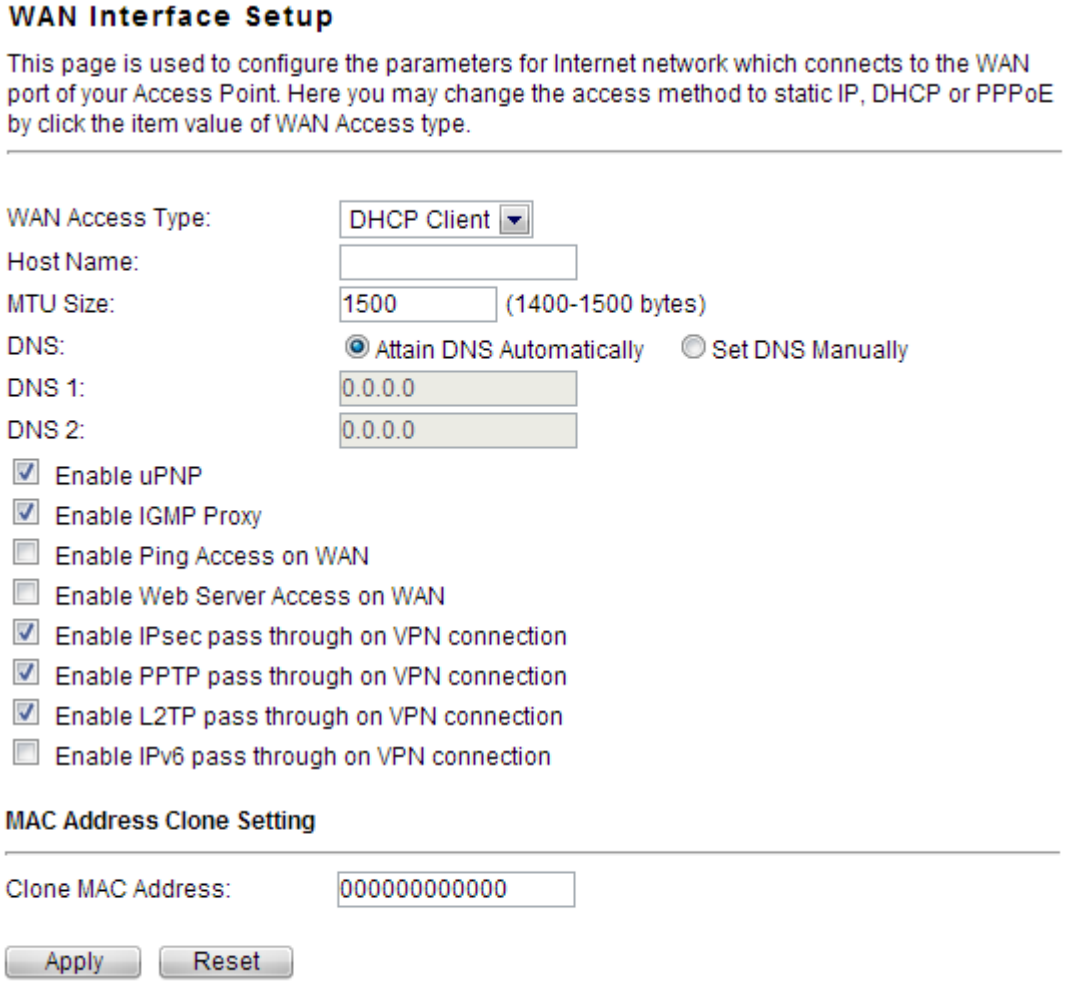
In this mode, all ethernet ports are bridged together and the wireless client will connect to the ISP access point. NAT is enabled and PCs on Ethernet ports share the same IP to the ISP via the wireless LAN. You can connect to the ISP's AP on the Site-Survey page. The connection type can be setup on the WAN page using PPPOE, DHCP client or static IP.

4.5 Network



4.5.1 WAN Interface

This part allows you to configure the WAN port parameters so that your computer can access Internet.



Enable UPnP: the UPnP (Universal Plug and play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows “Plug and Play” system. You can enable this function so that the router doesn’t need to work out which port need to be opened.

Enable IGMP Proxy: IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. If you select this checkbox, the application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.

Enable Ping Access on WAN: enable users use Ping command to access WAN.

Enable Web Server Access on WAN: enable users to access Web Server on WAN.

Enable IPsec pass through on VPN connection: IPsec pass through is a technique for allowing IPsec packets to pass through a NAT router.

Enable PPTP pass through on VPN connection: PPTP pass through is a technique for allowing PPTP packets to pass through a NAT router.

Enable L2TP pass through on VPN connection: L2TP pass through is a technique for allowing L2TP packets to pass through a NAT router.

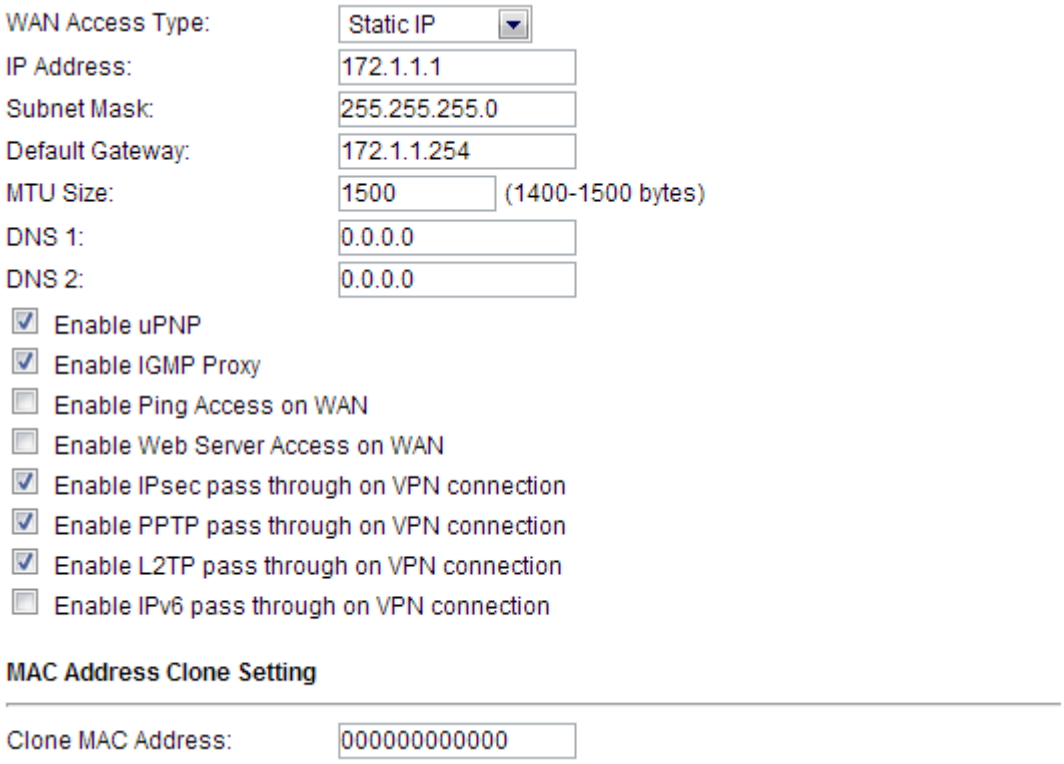
Enable IPv6 pass through on VPN connection: IPv6 pass through is a technique for allowing

IPv6 packets to pass through a NAT router.

Clone MAC Address: MAC address is the physical address of your computer's network card. Generally, every network card has one unique Mac address. Since many ISPs only allow one computer in LAN to access Internet, users can enable this function to make more computers surf Internet.

4.5.1.1 Static IP

If your ISP has provided the fixed IP that allows you to access Internet, please choose this option.



IP Address: the IP address provided by your ISP.

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.

Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.

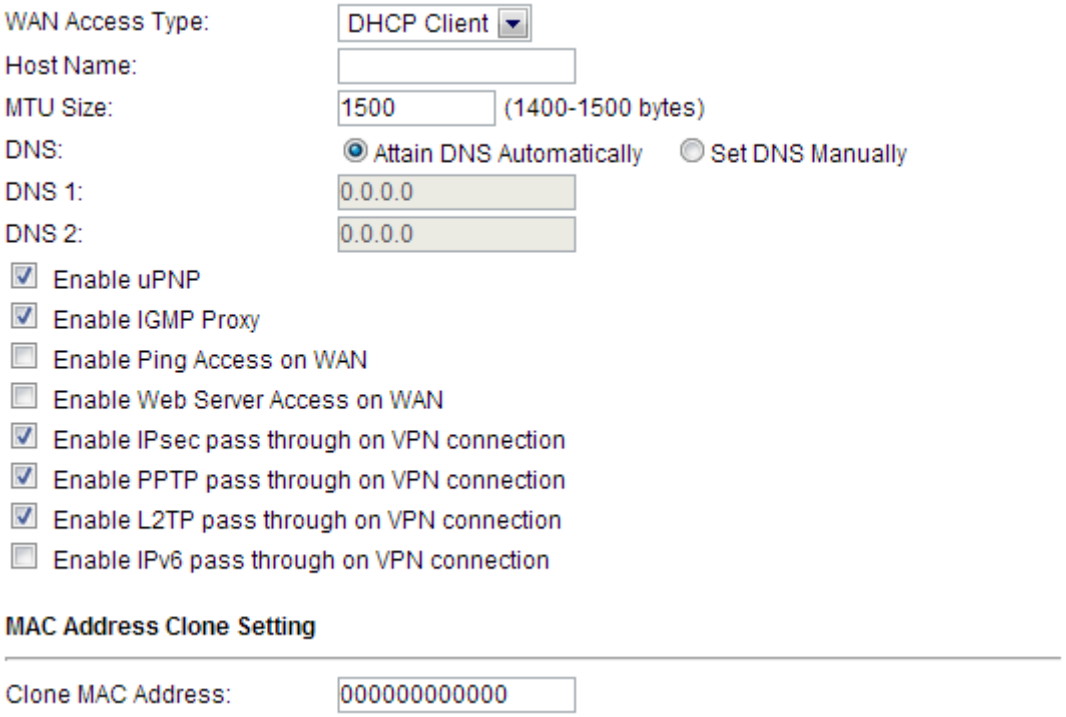
MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

DNS: The Domain Name System (DNS) is an Internet "phone book", which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requested are forwarded by this router.

4.5.1.2 DHCP Client

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you

choose this mode, you will get a dynamic IP address from your ISP automatically.



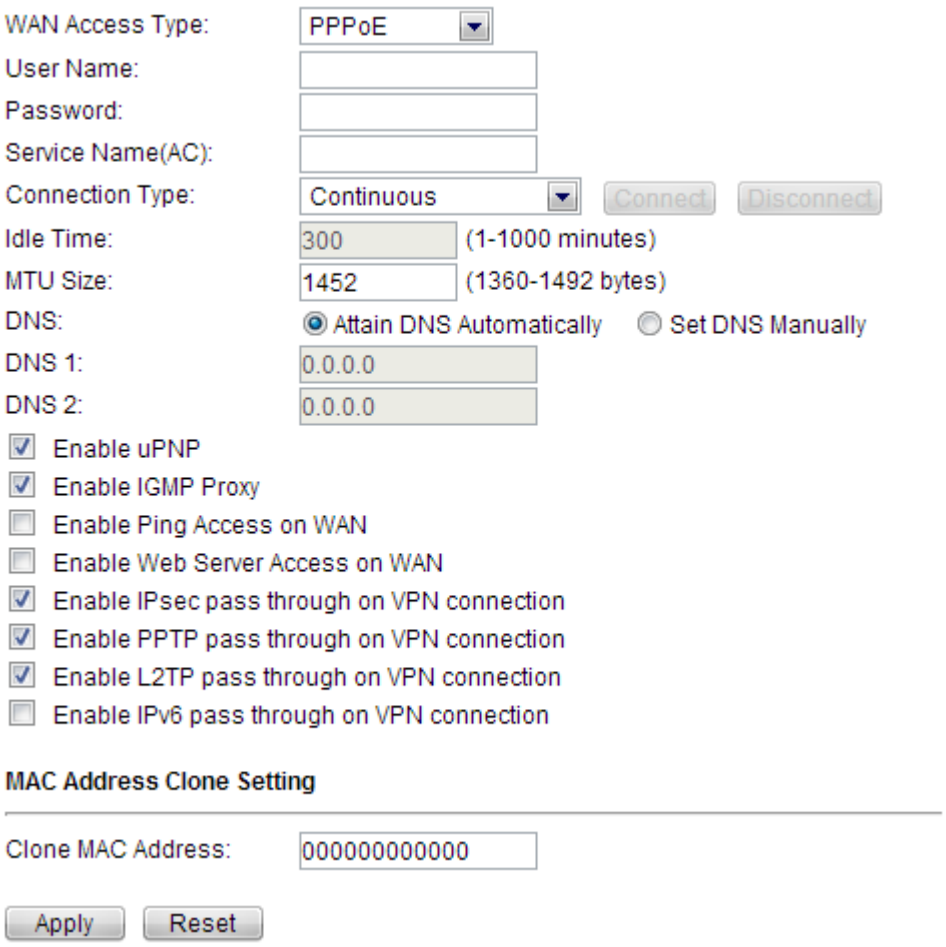
Host Name: the name of your computer, online neighbors will identify the computer according to the name.

MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

DNS: Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

4.5.1.3 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. Select PPPoE option if ISP provides a PPPoE connection. You should enter the following parameters.



User Name/Password: enter the User Name and Password provided by your ISP.
Service Name (AC): this is optional. It describes the service name your ISP provided to you. Generally, leaving these fields blank will work.
DNS: Domain Name System. If you select Set DNS Manually, you will have to type in the DNS address by yourself. It is chosen to Attain DNS by default.

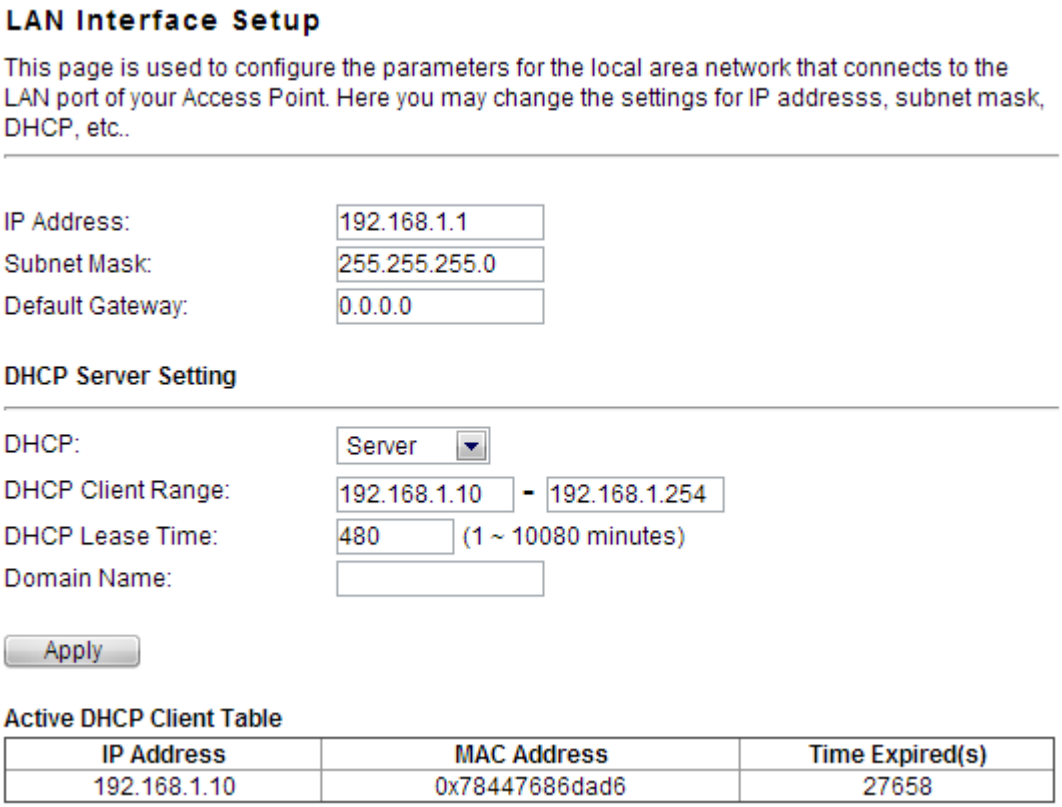
Connection Type: provides three modes to connect to the Internet.

- **Continuous**: the connection can be re-established automatically.
- **Connection on demand**: the Internet connection can be terminated automatically after a specified inactivity period (idle time).
- **Manual:** you can click **Connect** or **Disconnect** button to connect/disconnect immediately.

Idle Time: it is a term which generally refers to a lack of motion or energy.
MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

4.5.2 LAN Interface

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP. This part allows you to configure the parameters for LAN which connects to the LAN port of your Access Point.



IP Address: This is the IP addresses to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.

DHCP: You can disable or enable DHCP Server here.

DHCP Client Range: the range of IP addresses that will be assigned to each computer connected with the router.

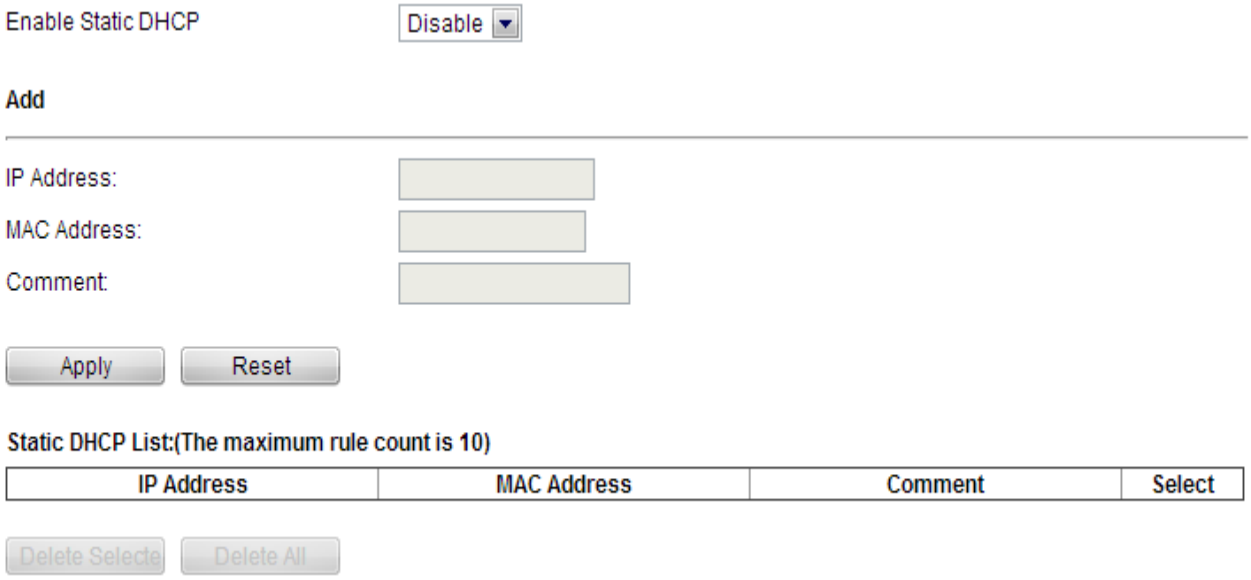
DHCP Lease Time: the IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

Domain name: this represents the name of your IP address.

Active DHCP Client Table: the table will list the detailed information of your users.

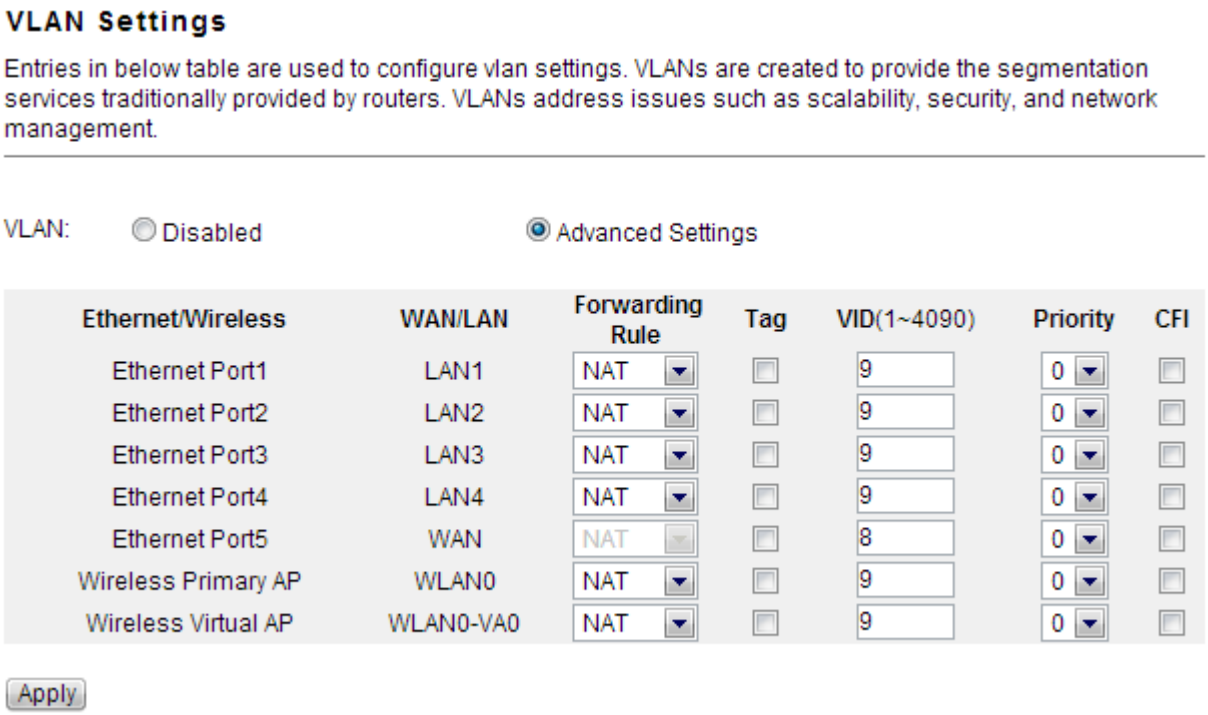
4.5.3 Static DHCP Settings

It allows you to reserve IP addresses and assign the same IP address to the network device with the specified MAC address any time it requests an IP address.



4.5.4 VLAN Settings

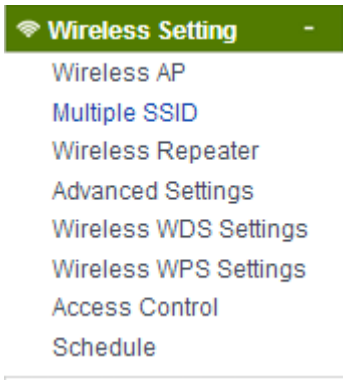
VLAN (Virtual Local Area Network) provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. VLANs are created to provide the segmentation services traditionally provided by routers.



Advanced Settings: this option enables VLAN function.

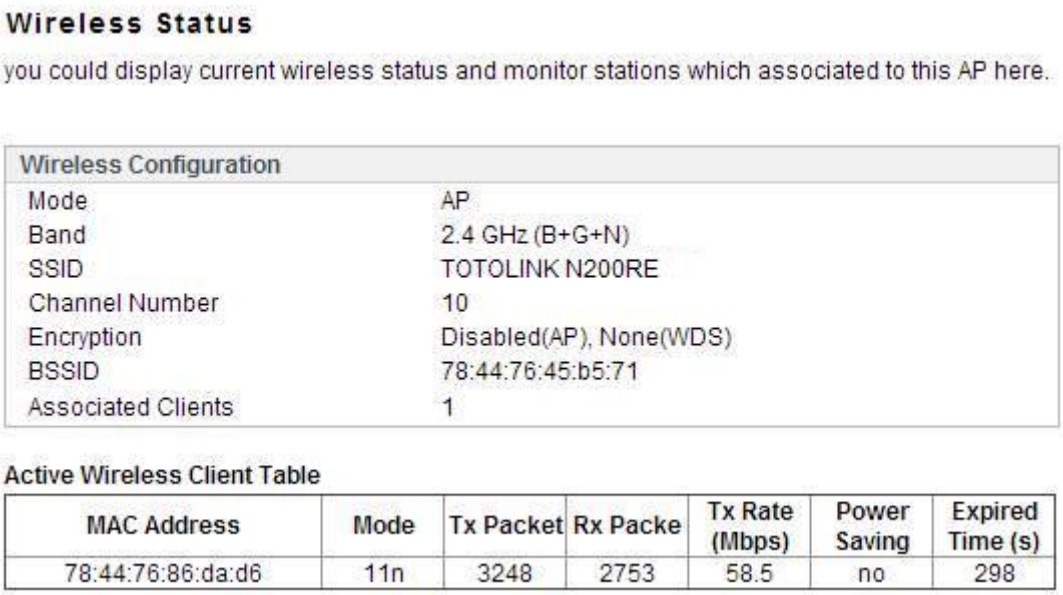
Ethernet/Wireless: specifies the WAN port and wireless AP.
WAN/LAN: defines the WAN port or LAN port.
Forwarding Rule: VLAN feature also support forwarding rule as bridge and NAT between LAN port and WAN port.
Tag: The router will add specific VLAN number to all packets on the LAN while sending them out. If enable the function of VLAN with tag, please type the tag value and specify the priority for the packets sending by LAN.
VID: type the value as Port-base VLAN ID.
Priority: Type the packet priority number for such VLAN. The range is from 0 to 7.
CFI: enable the CFI function which indicates whether MAC is encapsulated by standard format.
After the VLAN settings, please click **Apply** to finish **Network** Settings.

4.6 Wireless Setting



4.6.1 Wireless Status

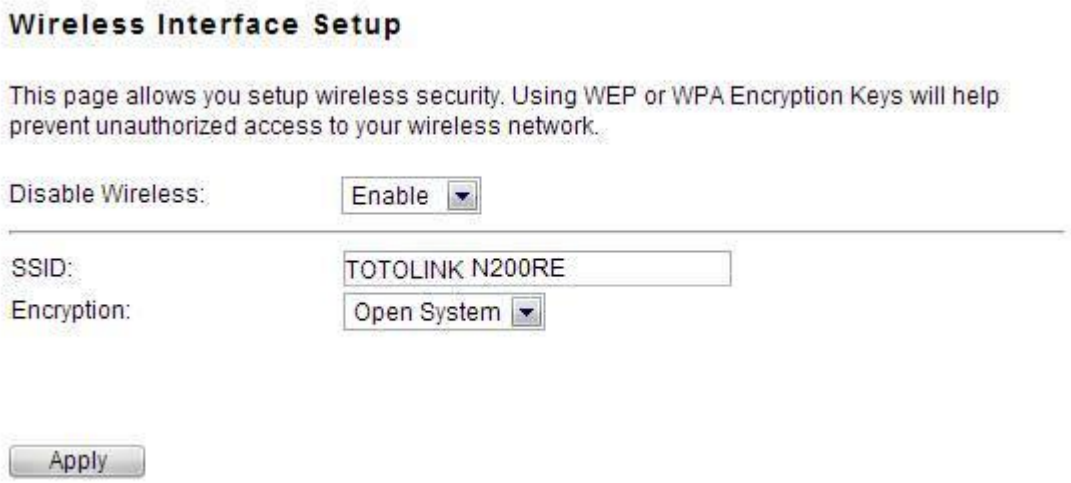
This page displays the current wireless status of the router.



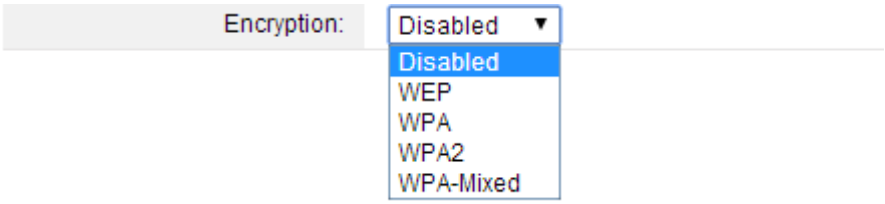
4.6.2 Wireless AP

This page allows you to setup wireless encryption to protect your wireless network from

unauthorized access.

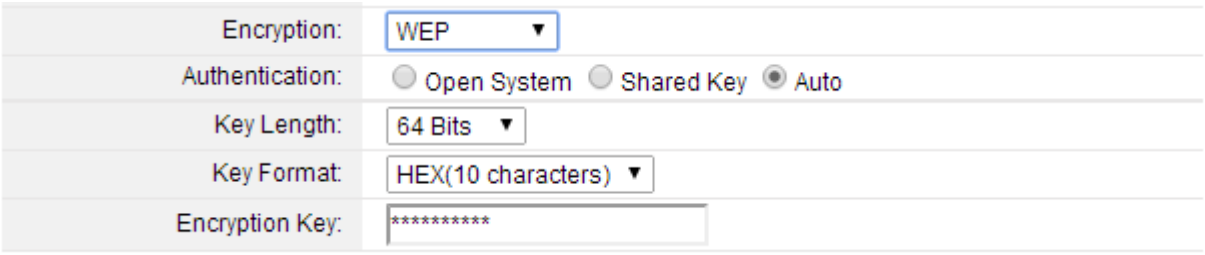


Encryption: This router supports WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.



1) WEP

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encryption data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes.



Key Length: 64-bit/128-bit, by default it is 64-bit.

64-bit—For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x414234445.)

128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).

Key Format: If you choose 64 bit, there will be two Key Formats selectable: ASCII (5 characters) and Hex (10 characters). If 128-bit, the Key Formats should comply with ASCII (13 characters) or Hex (26 characters)

Encryption Key: Please refer to Key Length to set this parameter.

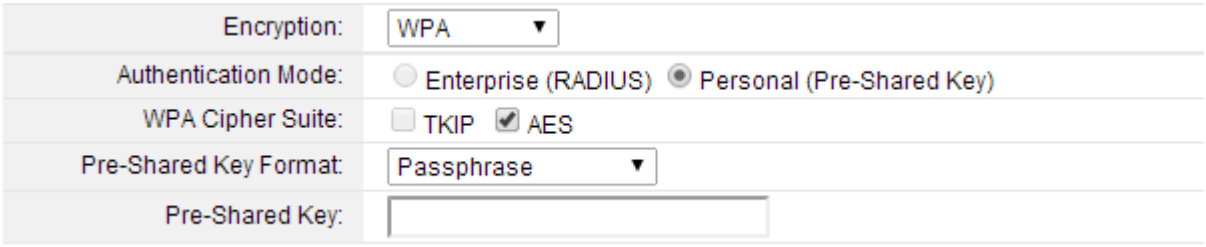
2) WPA/WPA2

Wi-Fi Protected Access (WPA) is the most dominating security mechanism in industry.

It is separated into two categories: WPA-personal and WPA-Enterprise, it is the current most secure method of wireless security and required for 802.11n performance.

TKIP--Temporal Key Integrity Protocol is one cipher for data encryption supported by WPA.

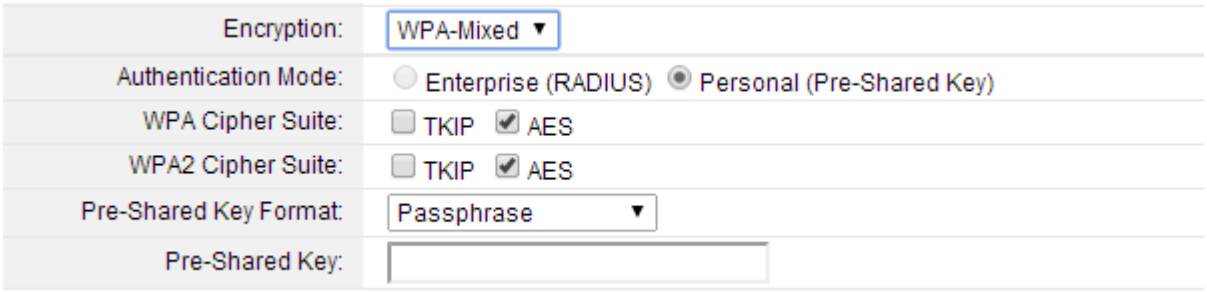
AES--Advanced Encryption Standard is another cipher for data encryption supported by WPA.



Pre-Shared Key Format/Pre-Shared Key: This is a pre-defined key used for encryption during data transmission. It has two formats: Passphrase and Hex (64 characters). Then you need to enter the Pre-Shared Key, either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as “0x321253abcde…”).

3) WPA Mixed

This option mixes WPA/WPA2 together. It will provide the best security for your router.

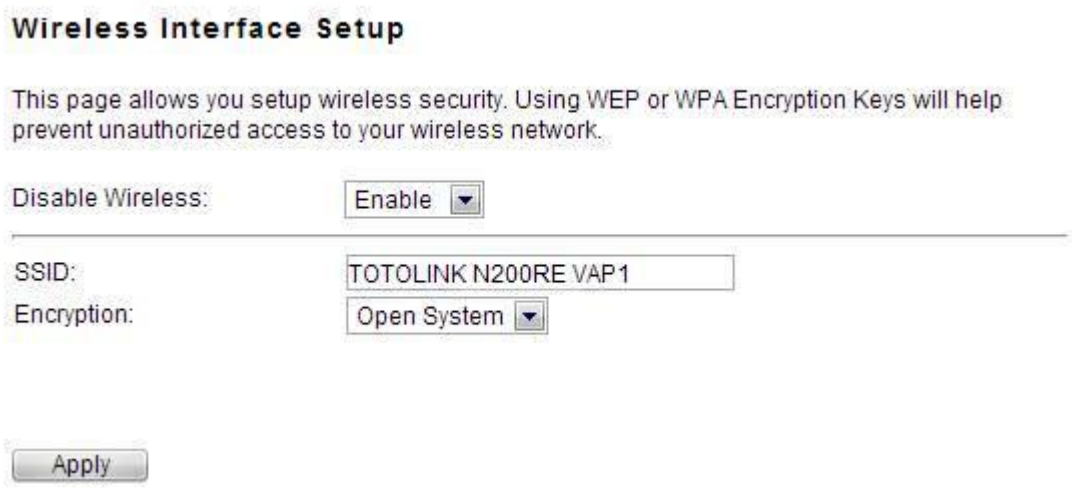


Note: *Since WEP has been proved vulnerable, you may consider using WPA2 for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and/or privacy on your wireless network.*

4.6.3 Multiple SSID

You can set another SSID for different needs. What’s more, you can setup different encryption in Security Settings section.

By default, it is disabled. You should select Enable and the configuration parameters will appear. The encryption please refer to **4.6.2 Wireless AP**

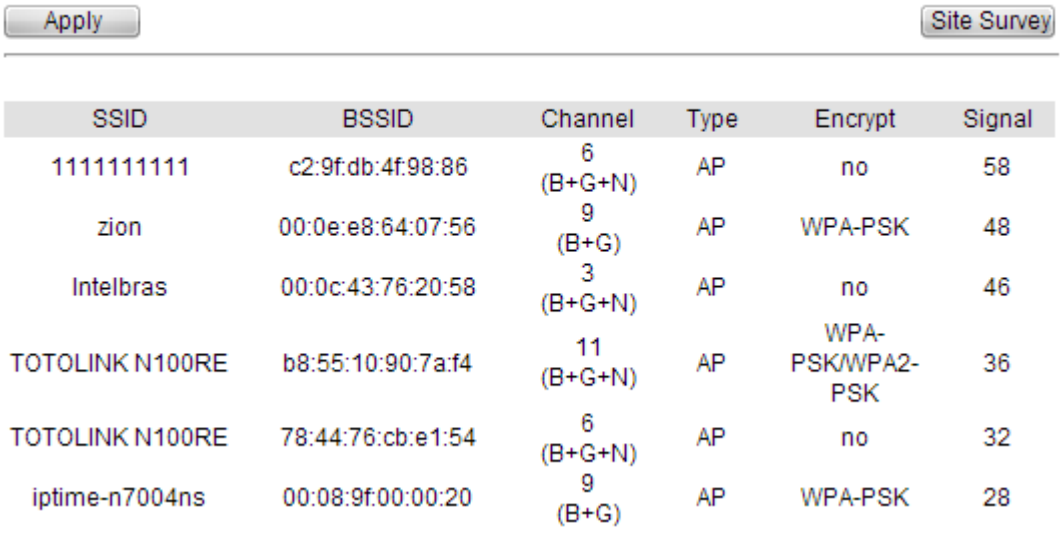


4.6.4 Wireless Repeater

You can setup wireless security in this page. It is very practical for protecting your private information.

It is disabled by default; please select a mode to enable this function.

Please click **Site Survey** button to search for any Access Point. Then they will be showed in the form.

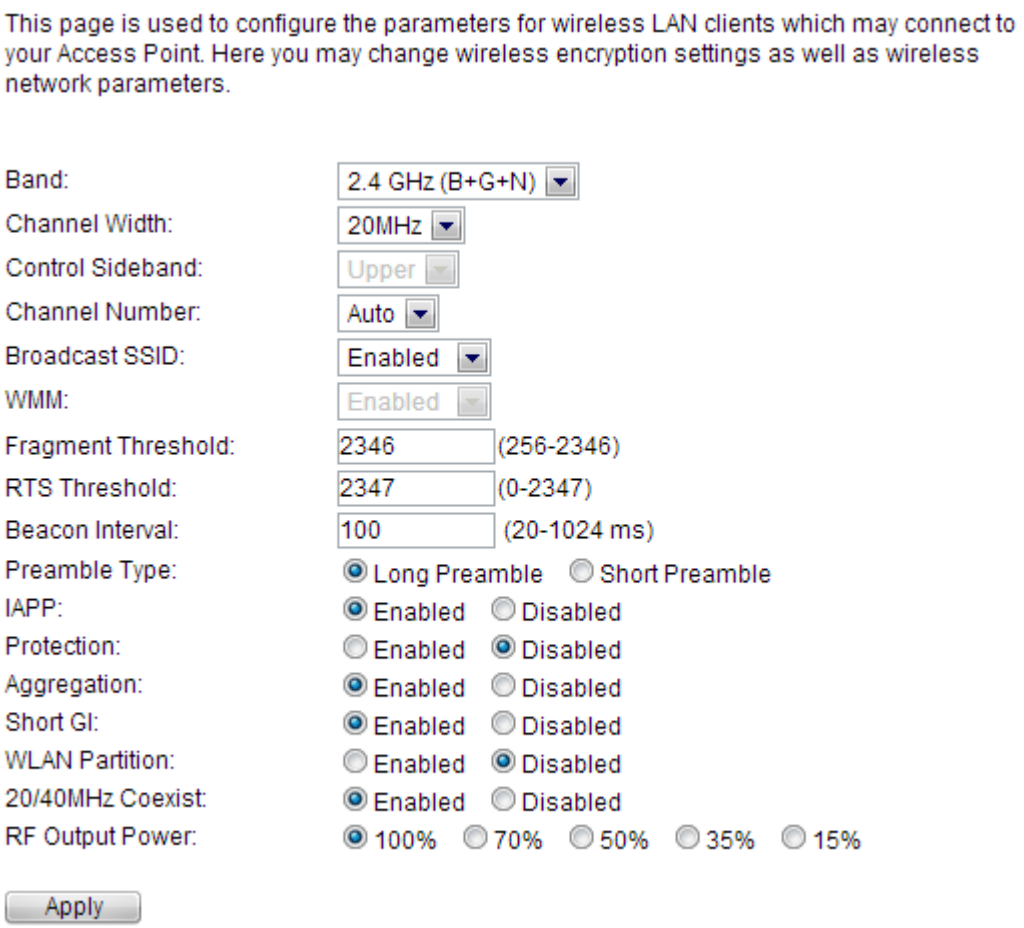


SSID	BSSID	Channel	Type	Encrypt	Signal
1111111111	c2:9f:db:4f:98:86	6 (B+G+N)	AP	no	58
zion	00:0e:e8:64:07:56	9 (B+G)	AP	WPA-PSK	48
Intelbras	00:0c:43:76:20:58	3 (B+G+N)	AP	no	46
TOTOLINK N100RE	b8:55:10:90:7a:f4	11 (B+G+N)	AP	WPA-PSK/WPA2-PSK	36
TOTOLINK N100RE	78:44:76:cb:e1:54	6 (B+G+N)	AP	no	32
iptime-n7004ns	00:08:9f:00:00:20	9 (B+G)	AP	WPA-PSK	28

Utility will search for wireless networks in range on all the supported channels while device is operating in Access Point mode. If any Access Point is found, you could choose to connect it manually when client mode is enabled.

4.6.5 Advanced Settings

On this page, you could configure the parameters for Wireless LAN client that may connect to your Access Point. Some settings should not be changed unless you know what effect the changes will have on your Access Point.



Band: This option allows you to choose the radio standard for operation of your Router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation.
Channel Width: This is the spectral width of the radio channel. Supported wireless channel spectrum widths:

20MHz is the standard channel spectrum width.
40MHz is the channel spectrum with the width of 40MHz.

Channel Number: This option provides selectable channel numbers.

Broadcast SSID: you can choose to enable or disable to broadcast your SSID.

WMM: it maintains the priority of audio, video and voice.

Fragment Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes. Setting the Fragment Threshold too low may result in poor network performance. The use of fragment can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the Fragment Threshold will result in lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes. The default value is 2347, which means that RTS is disabled.
Beacon Interval: By default, it is set to 100ms. Higher Beacon interval will improve the

device's wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

Preamble Type: this option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses shot preamble with 56 bit sync filed instead of long preamble with 128 bit sync filed. However, some original 11b wireless network devices only support long preamble. By default, Long Preamble is selected.

IAPP： Inter-Access Point Protocol is designed for the enforcement of unique association throughout an ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period. It is enabled by default.

Protection: it is disabled by default.

Aggregation: A part of the 802.11n standard. It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header. It is enabled by default.

Short GI: short Guide Interval. It is to assure the safety of propagation delays and reflections for the sensitive digital data.

WLAN Partition: divides the WLAN to several parts.

20/40MHz Coexist: enable this function will make the device select the channel with better performance automatically. It is disabled by default.

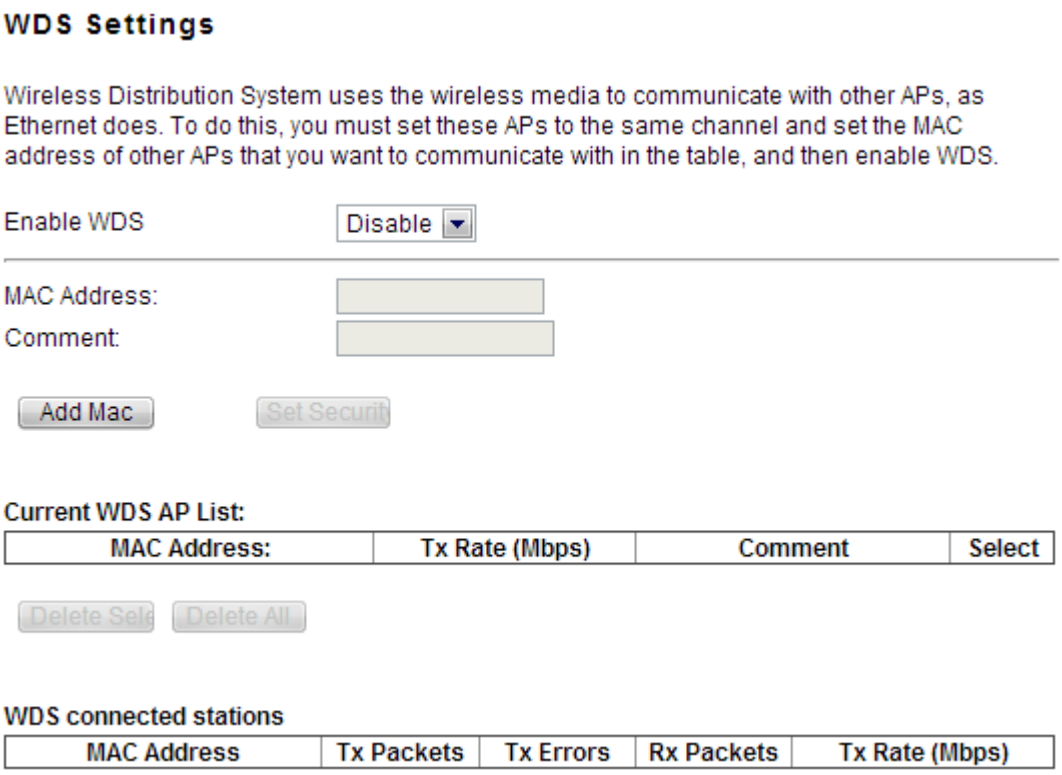
RF Output Power: you can select the output power of the wireless device. The default value is 100%. It will deliver the best performance of the device.

4.6.6 Wireless WDS Settings

WDS means Wireless Distribution System. It is a protocol for connecting two access points wirelessly. Usually, it can be used for the following application:

1. Provide bridge traffic between two LANs though the air.
2. Extend the coverage range of a WLAN.

To meet the above requirement, 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: by default, you can't select the checkbox to enable WDS.
MAC Address: the other AP's MAC Address that you want to communicate with.
Comment: describes the reason why you want to communicate with others.
The WDS Security Setup allows you to set encryption for your WDS connection. You can refer to the Wireless Security Setup.

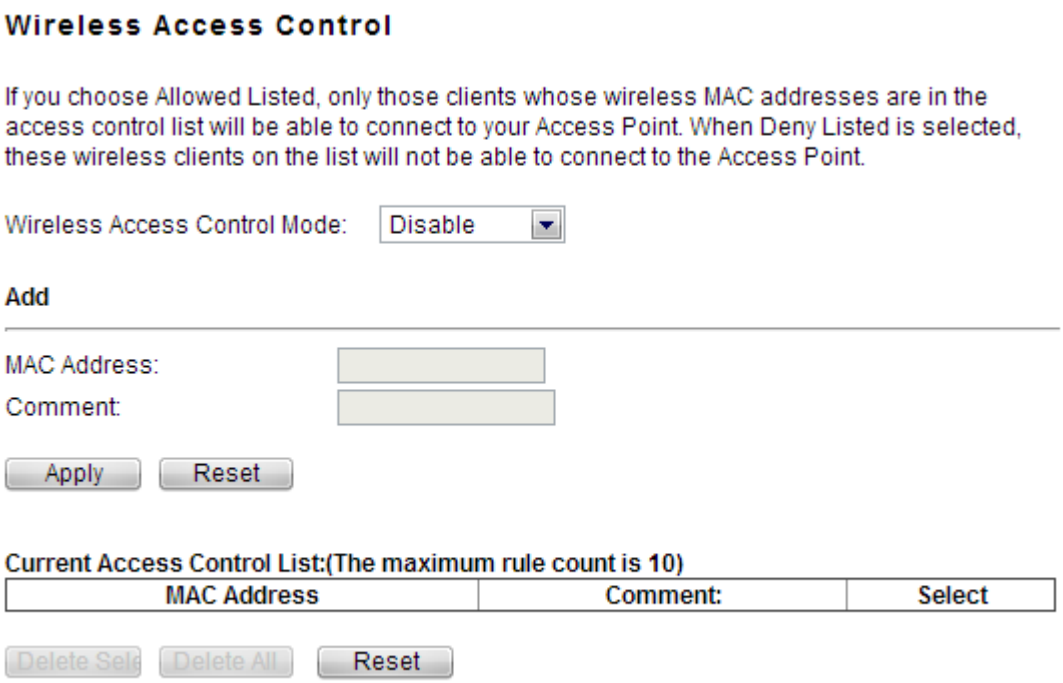
4.6.7 Wireless WPS Settings

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2.

Self-PIN Number: it will show the PIN Number of your device.
Push Button Configuration: click Start PBC button to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes.)
STOP WSC: Click the button to stop WSC function.

Client PIN Number: please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

4.6.8 Access Control



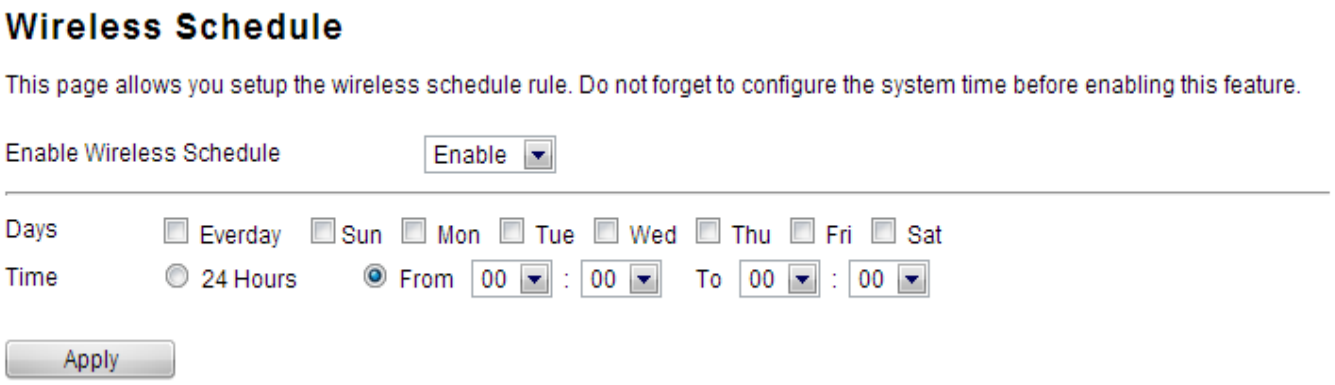
By default, Wireless Access Control Mode is disabled.
There are two ways to set the Access Control List:

1. If you select **Allow List** and enter the MAC Address of wireless client, the listed address will have granted access to the Access Point while the other access will be denied.
2. If you select **Deny List** and enter the MAC Address of wireless client, the listed address will have denied access to the Access Point while the other access will be granted.

MAC Address: the wireless MAC address that you allow to access or not.
Comment: describe the reason why you allow or deny the access of the MAC Address.
You need to click **Apply Changes** to make your setting work.
Current Access Control List: this list will show all the current access control that you have set. And you're able to delete some or all of them using the **Delete Selected** or **Delete All** button.

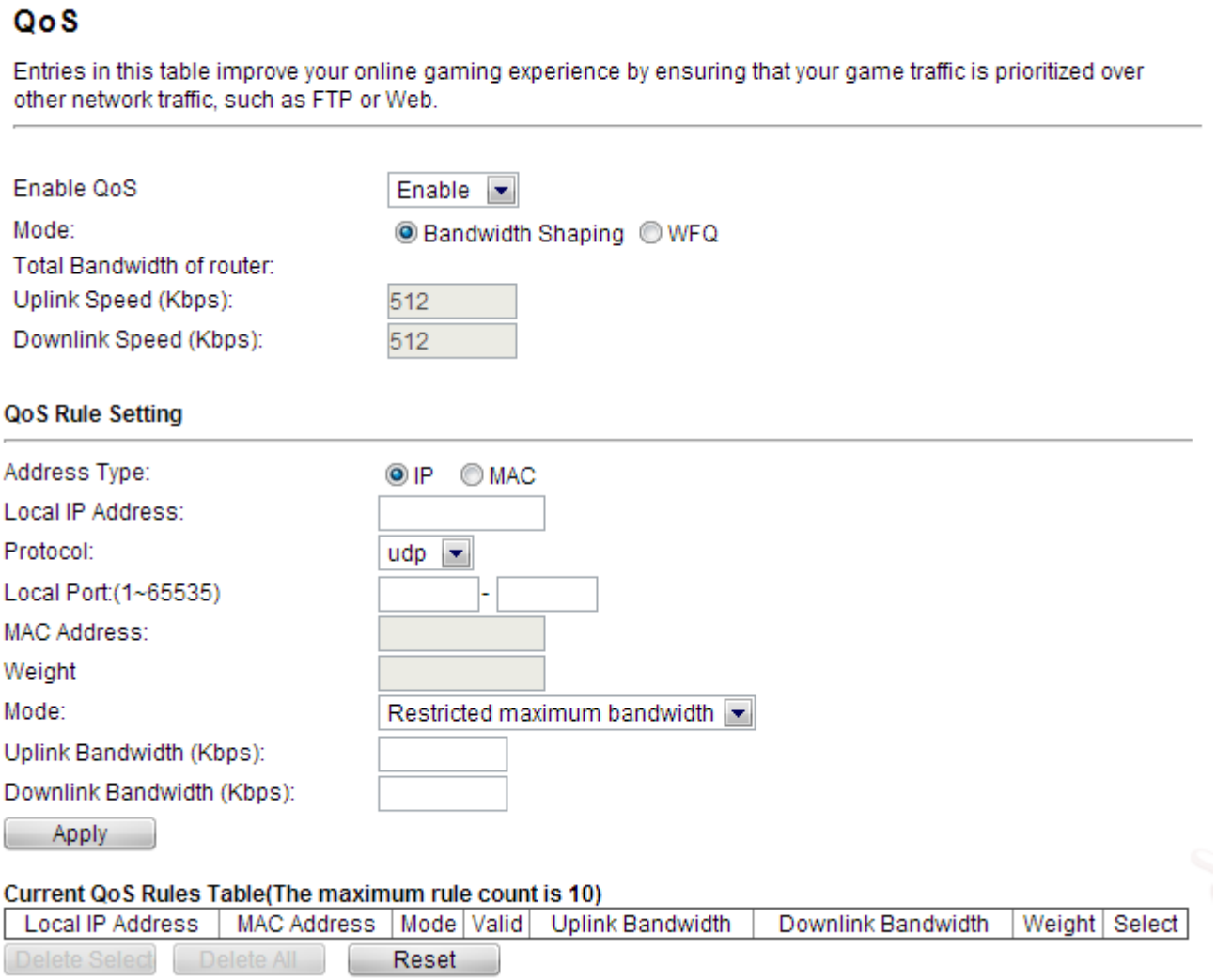
4.6.9 Schedule

The wireless schedule allows you to setup the time when WiFi is on. It is very convenient for users who often access the Internet very regularly. You have to enable **NTP in Time Zone Setting** part before setting schedule.



4.7 QoS

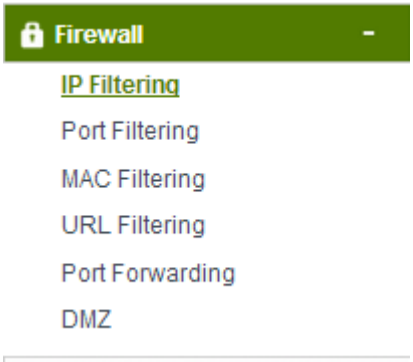
QoS means Quality of Service. Deploying QoS management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.



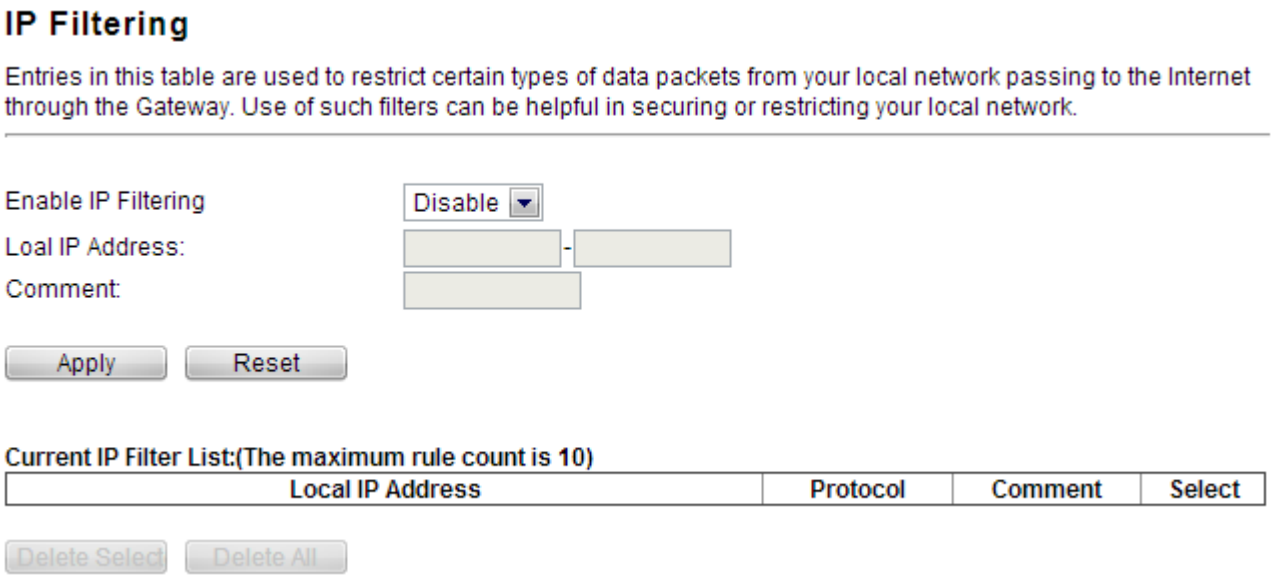
4.8 Firewall

The firewall of this router helps to protect you local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the

Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

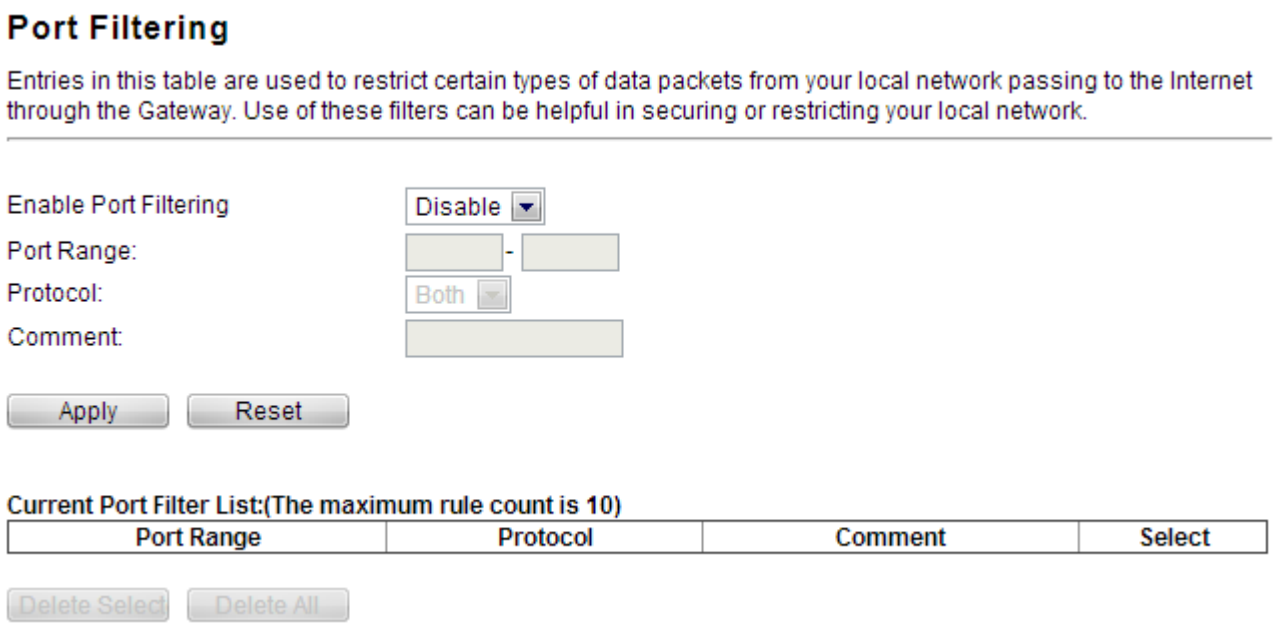


4.8.1 IP Filtering



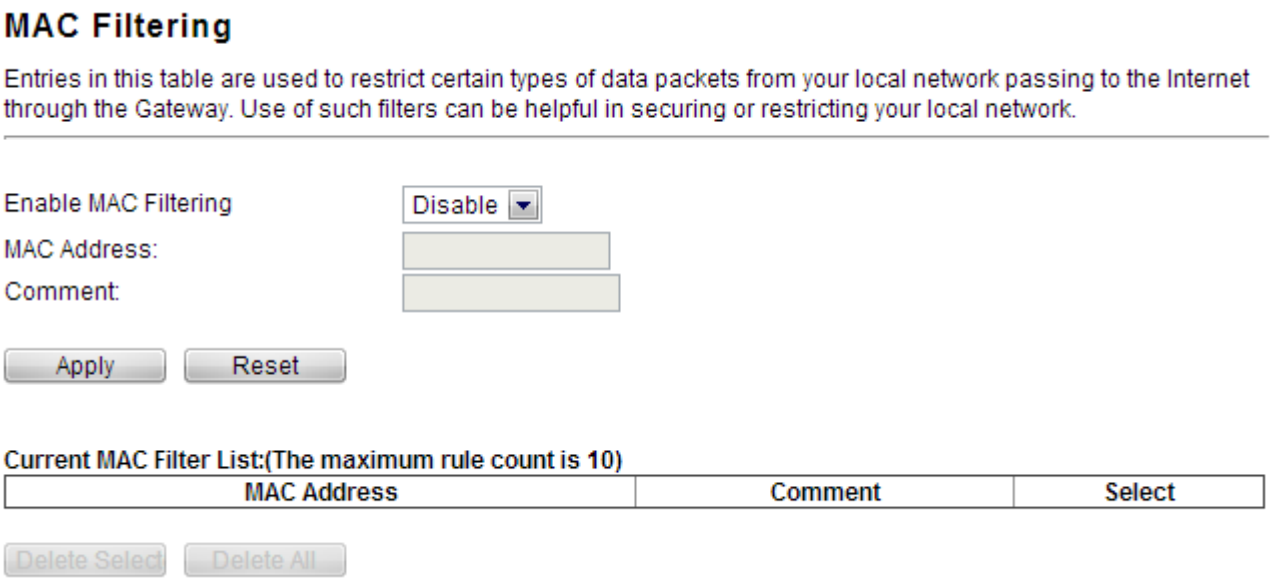
Enable IP filtering: you can select this checkbox to enable IP Filtering function.
Local IP Address: the IP address that you want to filter.
Comment: describe the reason why you want to filter the IP address. Just few words are saved there usually.
Current IP Filter List: this table will list the detailed information about the IP addresses that will be filtered.

4.8.2 Port Filtering



Enable Port Filtering: you can select this checkbox to enable Port Filtering function.
Port Range: the port range that you want to filter.
Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP/Both.
Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.
Current Port Filter List: this table will list the detailed information about the Port that will be filtered.

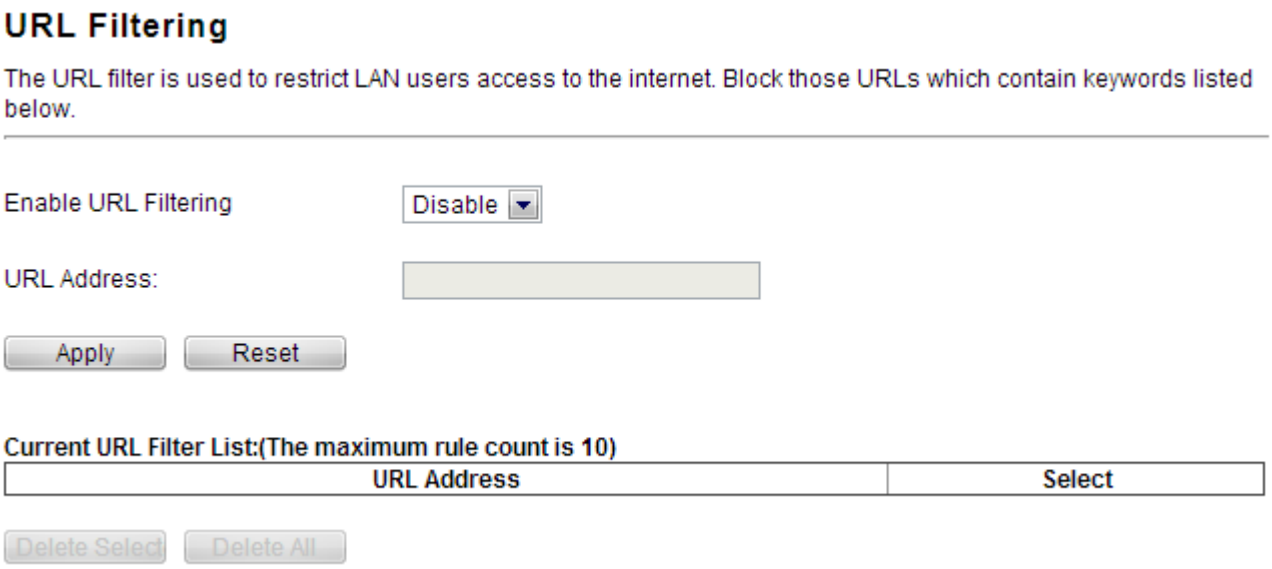
4.8.3 MAC Filtering



Enable MAC Filtering: you can check the box to enable MAC Filtering function.
MAC Address: the MAC address that you want to filter.

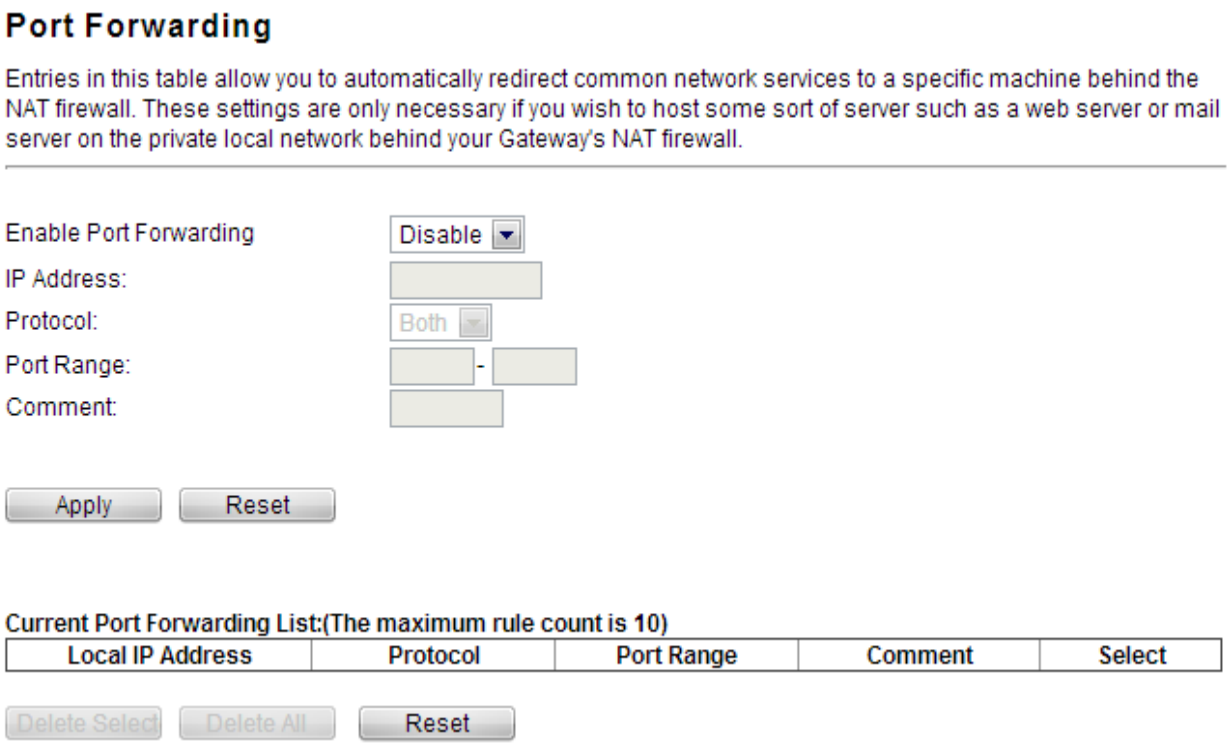
Comment: describe the reason why you want to filter the MAC address. Just few words are saved there usually.
Current MAC Filter List: this table will list the detailed information about the MAC address that will be filtered.

4.8.4 URL Filtering



Enable URL Filtering: you can select this checkbox to enable URL filtering function.
URL Addresses: type in the keywords contained in URLs that you don't allow LAN users to access.
Current URL Filter List: this table will list the detailed information about the URL that will be filtered.

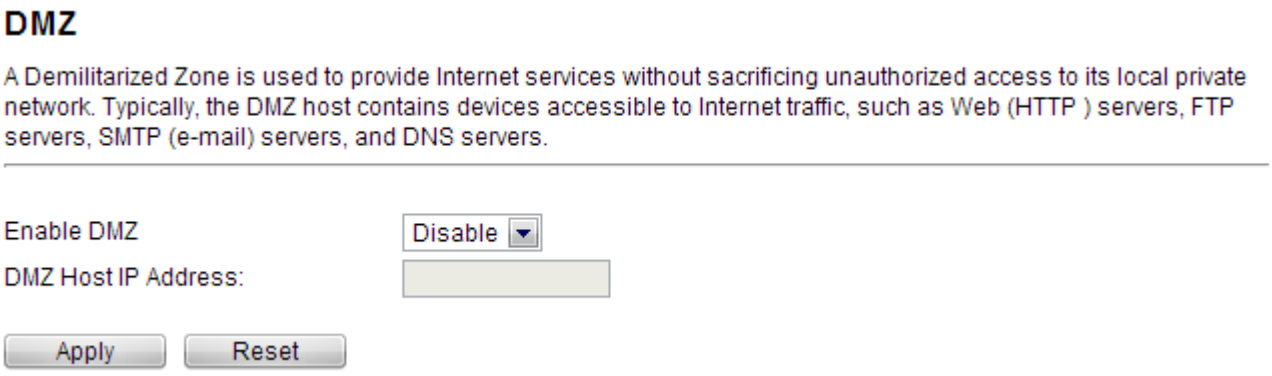
4.8.5 Port Forwarding



Enable Port Forwarding: you can select this checkbox to enable Port Forwarding function.
I**P Address:** enter the Port's IP address.
Protocol: choose which particular protocol type should be forwarding. Here you can choose Both/UDP/TCP.
Port Range: set the range that the port forward to.
Comment: describe the reason why you want to use port forward function. Just few words are saved there usually.

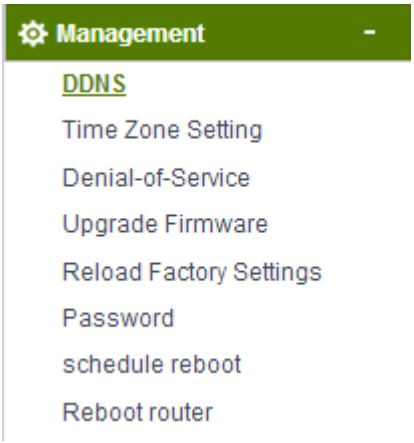
4.8.6 DMZ

DMZ means Demilitarized Zone. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.



Enable DMZ: you can select this checkbox to Enable DMZ function.
DMZ Host IP Address: type in the IP address of the DMZ host.

4.9 Management

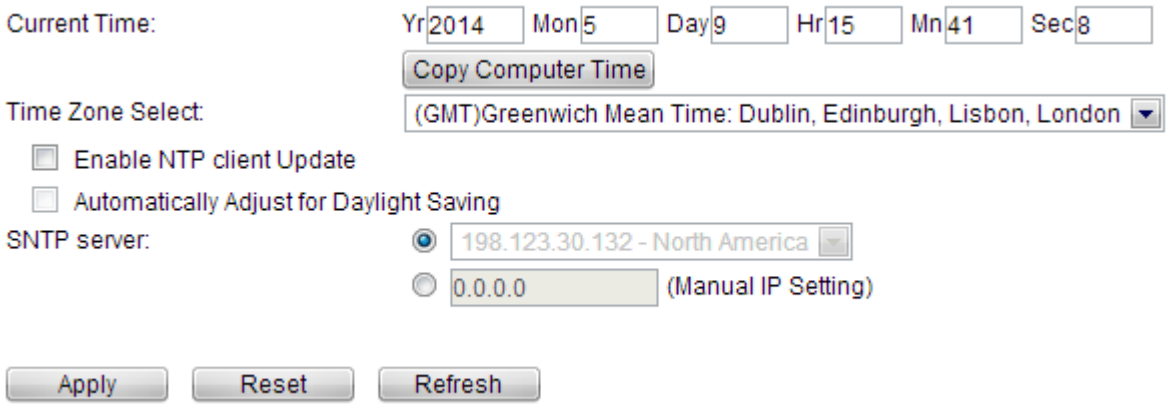


4.9.1 DDNS

DDNS means Dynamic Domain Name System. The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet.
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers.

4.9.2 Time Zone Setting

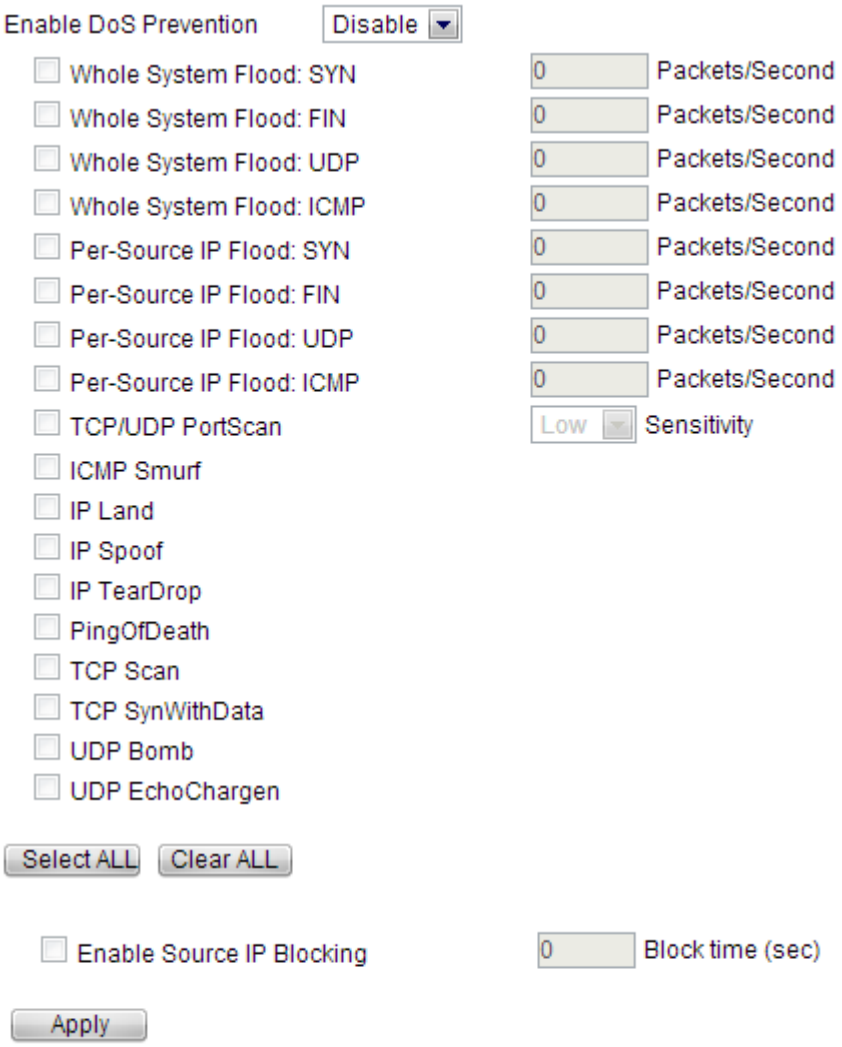
This page allows you to maintain the system time by synchronizing with a public time server over the Internet.



You can specify the device's time zone according to GMT (Greenwich Mean Time) or copy computer time as the current time only by clicking the **Copy Computer Time** button.
Time Zone Select: Select the Time Zone where the router is located.
Enable NTP client update: NTP means Network Time Protocol which is used to make the computer's time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption. You need to check this box to activate this page.
Automatically Adjust for Daylight Saving: the system will adjust for daylight saving automatically for you.
SNTP server: Please choose the corresponding SNTP server to get right time.

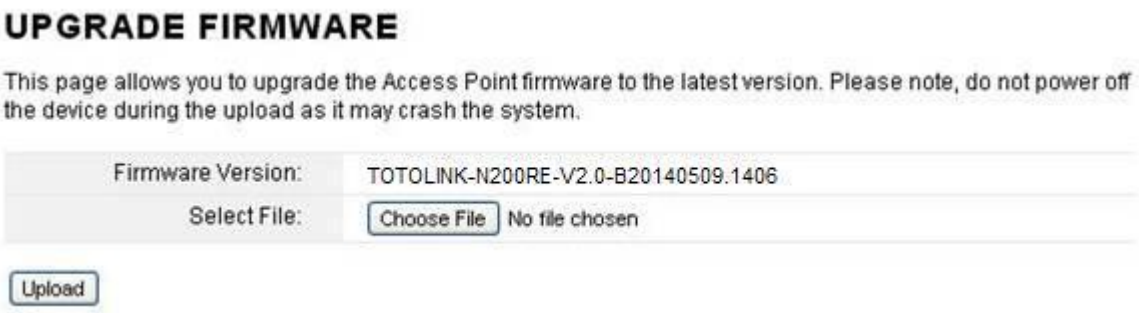
4.9.3 Denial-of-Service

The DoS Prevention functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.



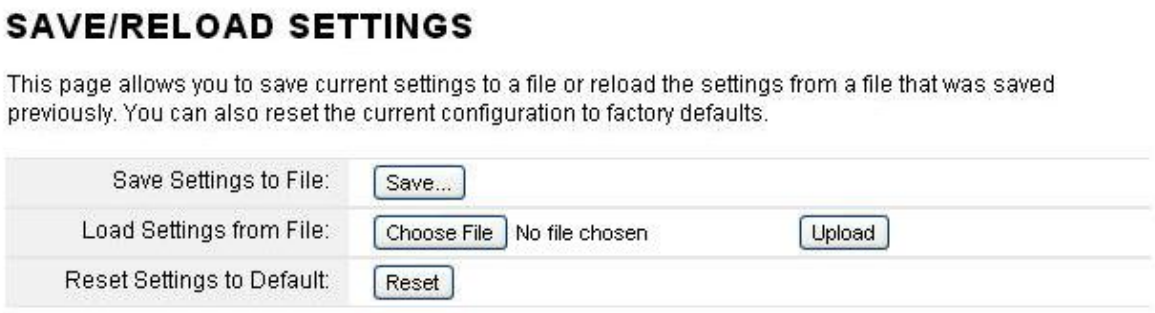
4.9.4 Upgrade Firmware

This page allows you to 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.



4.9.5 Reload Factory Settings

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



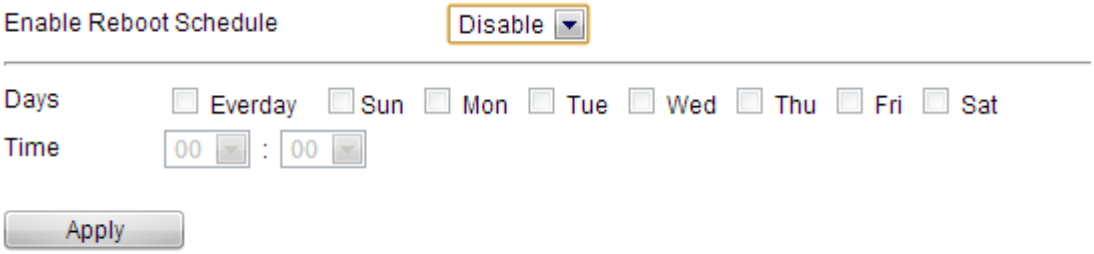
4.9.6 Password

User Name: type in the name that you use to login the web interface of the router.
New Password: new password is used for administrator authentication.
Confirm Password: new password should be re-entered to verify its accuracy.

Note: *password length is 8 characters maximum, characters after the 8th position will be truncated.*

4.9.7 Schedule Reboot

The schedule function allows you to setup the time that the router will reboot automatically.



4.9.8 Reboot Router

Please click this **Reboot** button to reboot your router quickly.