User Manual

TOTOLINK F1 SOHO Fiber Router

TOTO LINK

www.totolink.net

TABLE OF CONTENT

Copyright Statement

All the photos and product specifications mentioned in this manual are for references only, as the upgrading of software and hardware. They are subject to change without notice. No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TOTOLINK. If you want to know more about our products information, please visit our website at http://www.totolink.net

1. ABOUT THIS GUIDE

Thank you very much for purchasing F1 150Mbps Wireless N Fiber AP/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 fiber router and its features.

Hardware Installation. Describes the hardware installation and settings on computer.

Connecting to Internet. Tells how you can connect your computer to Internet successfully using the fiber router.

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

2. PRODUCT OVERVIEW

2.1 Introduction

F1 is a wireless N Fiber Router with 1 high gain antenna. It allows users to access Internet by DHCP/PPPoE/Static IP and can deliver up to 150Mbps wireless data rate. With the fiber-optic WAN port, this device makes user access internet in an easy, enjoyable and secure way better than ever. Besides, F1 can be also used as a repeater. So it is a high performance and cost-effective solution for users connecting Internet by fiber-optic.

2.2 Features

- Complies with IEEE 802.11n/g/b standards for 2.4GHz Wireless LAN.
- Up to 150Mbps high speed wireless data rate.
- Fiber WAN port allows you connect fiber optical network quickly.
- Supports PPPoE, Dynamic IP and Static IP broadband functions.
- Connects to secure network easily and fast using WPS (one-button).
- Provides 64/128-bit WEP, WPA/WPA2 and WPA-Mixed security.
- Multiple APs function allows user to add more SSIDs for different needs.
- Supports VLAN function, more secure and efficient network management.
- IP/MAC Address/URL filtering makes access and time control more flexibly.
- Repeater function expands the wireless coverage and allows more terminals to access

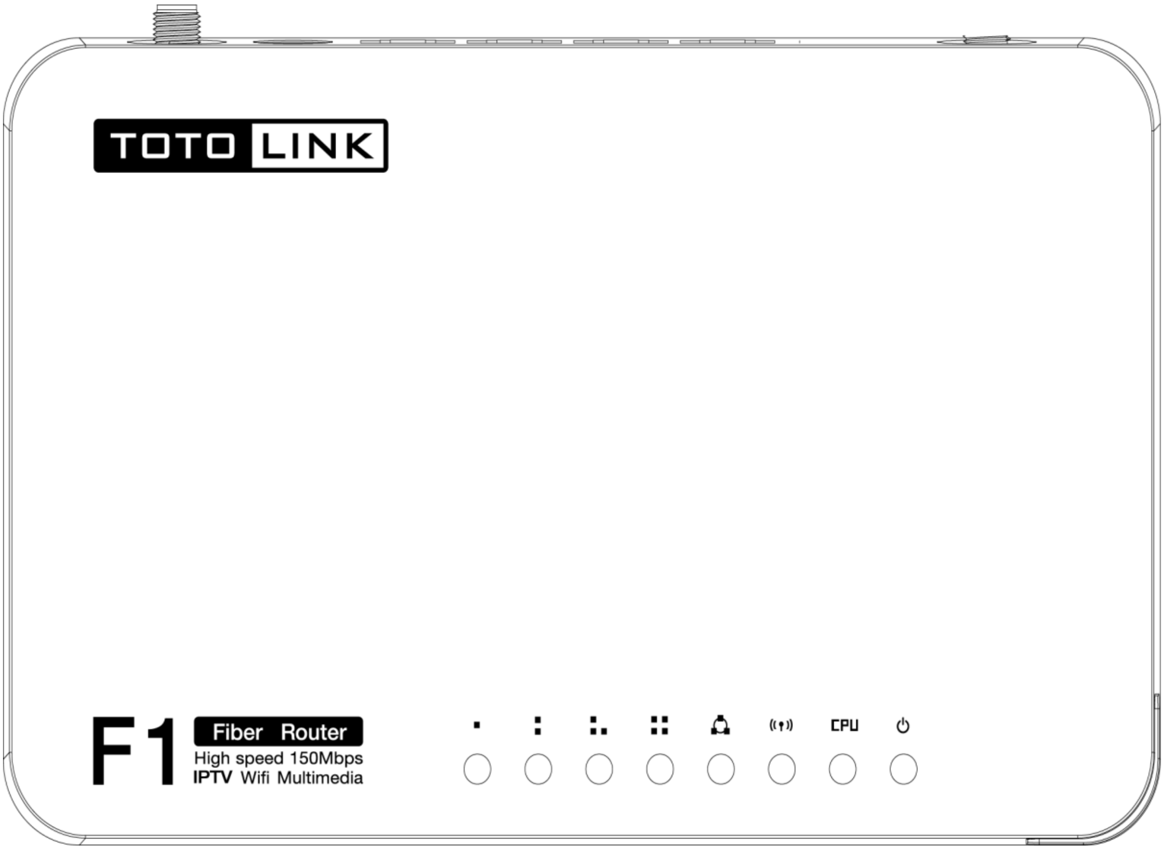
Internet.

- Supports WMM for improved audio and video signals.
- QoS makes the bandwidth control more easily.

2.3 Panel Layout

2.3.1 Front Panel

The front panel of F1 router consists of 8 LEDs, which is designed to indicate connection status.

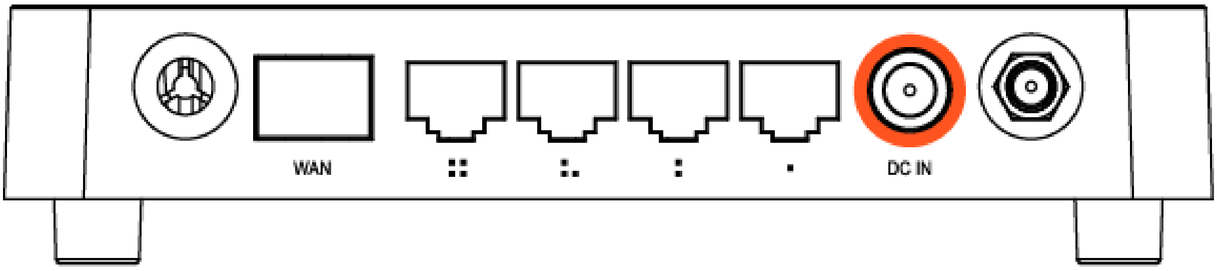


POWER	This indicator lights blue when the router is powered on, otherwise it is off.	
CPU	When the router is powered on, this indicator keeps lighting blue.	
WLAN	The indicator blinks blue while the WiFi of the Router is on.	
WAN	On	When the WAN port is connected successfully the indicator lights blue.
	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 indicator lights blue.
	Blink	During transmitting or receiving data through the LAN port the 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 F1 Router.



DC IN	The Power socket is where you will connect the power adapter.
Fiber WAN	This port is where you will connect with the SFP Module
1/2/3/4 LAN	This port connects the router to local PC.

Note: *There is a RST/WPS button on the bottom of the Router. If you press and hold this button for about 5 seconds, it will be WPS working. Press and hold the button for about 10 seconds, the router will reboot to default factory settings.*

3. HARDWARE INSTALLATION

3.1 Hardware Installation

For those computers you wish to connect with Internet by this Fiber Router, each of the computers must be properly connected with the router through provided UTP LAN Cables.

1. Connect the provided UTP LAN cable to one of the router's LAN port.
2. Connect the other end of the UTP LAN cable to your computer's LAN port.
3. Connect your Small Form Pluggable Module to router's Fiber WAN 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**, the WPS is lighting.

3.2 Check the Installation

The control LEDs of the Fiber Router are clearly visible and the status of the network link can be seen instantly:
1. With the power source on, the Power, WPS, LAN, WLAN and WAN port LEDs of the Fiber Router will light up indicating a normal status.

2. When the Fiber 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.

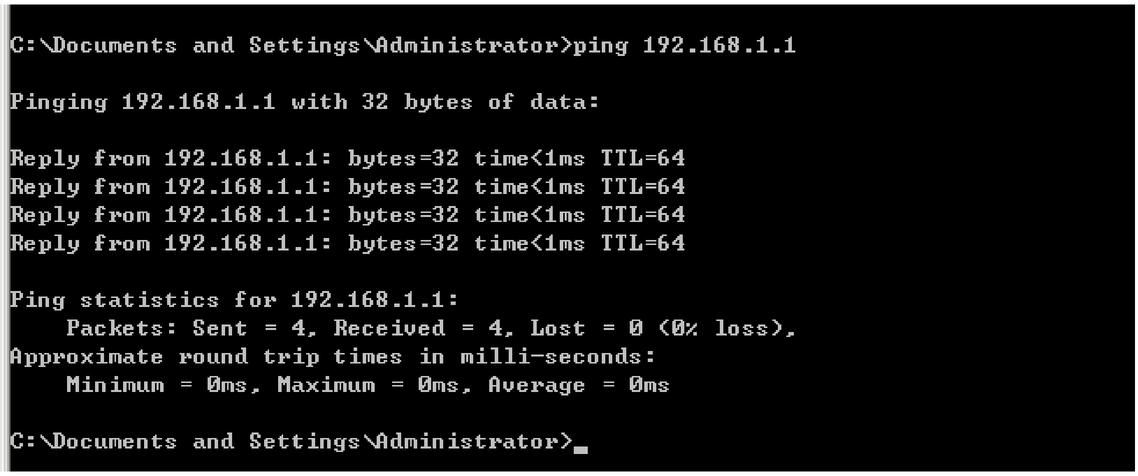
- **Configure the IP address manually**

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**

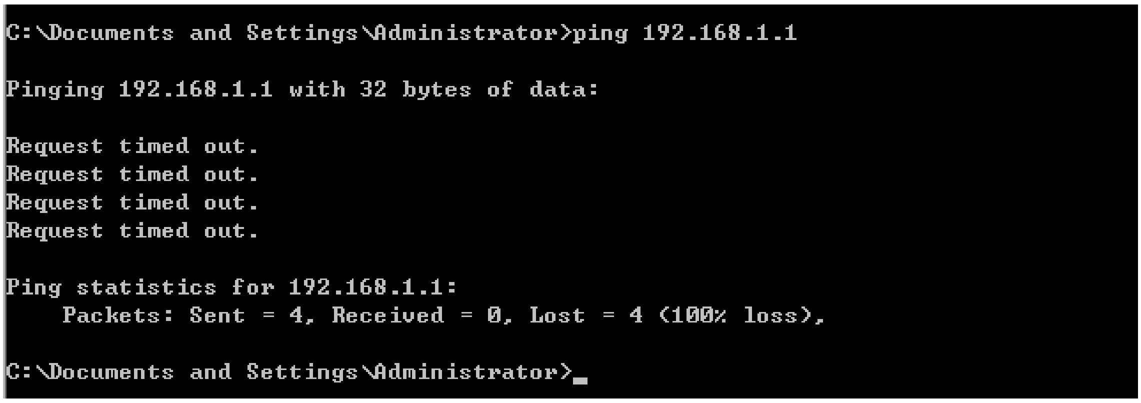
Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.

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.**



```
C:\Documents and Settings\Administrator>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 = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

If the result displayed is similar to that shown in above figure, it means that the connection between your PC and the Router has been established.



```
C:\Documents and Settings\Administrator>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),

C:\Documents and Settings\Administrator>_
```

If the result displayed is similar to that shown in the above figure, 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?

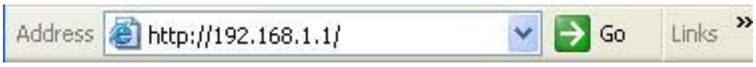
Since the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

4. CONNECTING TO INTERNET

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

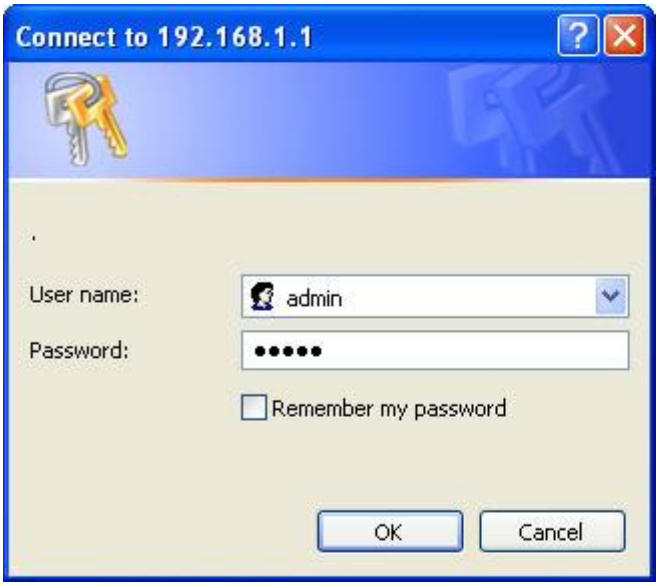
4.1 Accessing Web page

Connect to the Router by typing 192.168.1.1 in the address field of Web Browser. Then press **Enter** key.



Address http://192.168.1.1/

It will show up the following page:



Connect to 192.168.1.1

User name: admin

Password: •••••

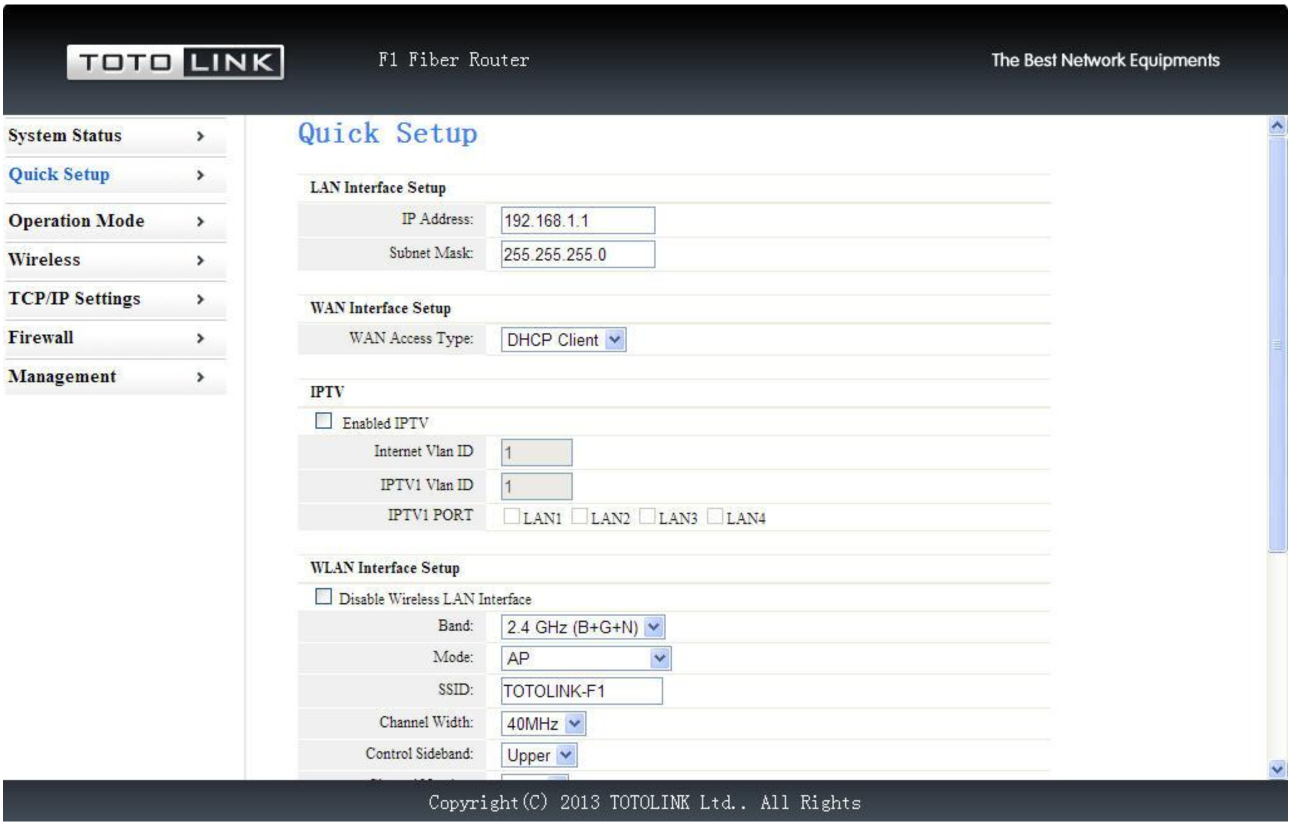
□ Remember my password

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.*
> *If the User Name and Password are correct, you can configure the router using the web browser.*

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



Quick Setup

LAN Interface Setup

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

WAN Interface Setup

WAN Access Type:	DHCP Client

IPTV

□ Enabled IPTV

Internet Vlan ID	1
IPTV1 Vlan ID	1
IPTV1 PORT	□LAN1 □LAN2 □LAN3 □LAN4

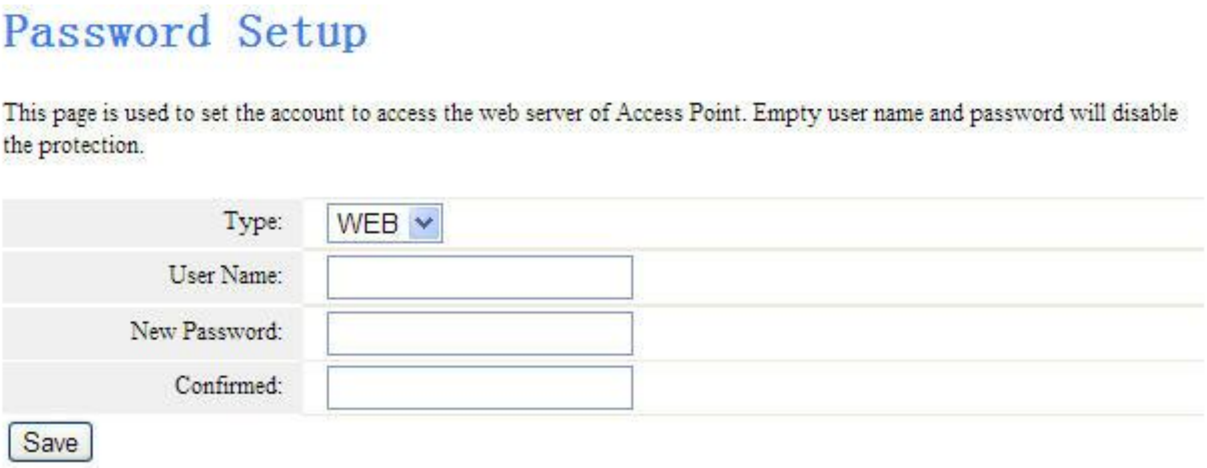
WLAN Interface Setup

□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP
SSID:	TOTOLINK-F1
Channel Width:	40MHz
Control Sideband:	Upper

4.2 Changing Password

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



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.

Type:	WEB
User Name:	
New Password:	
Confirmed:	

Type: here you can choose WEB and SSH. If you choose SSH, you don’t need to enter the User Name.

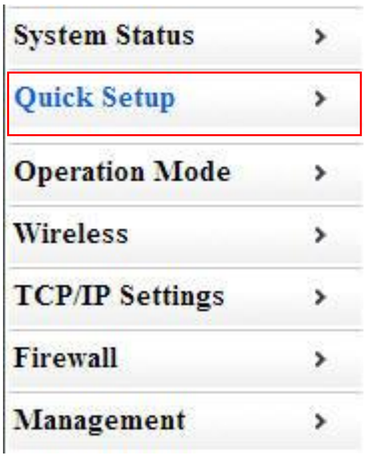
User Name: type in the name that you use to login the web interface of the router.

New Password: new password is used for administrator authentication.

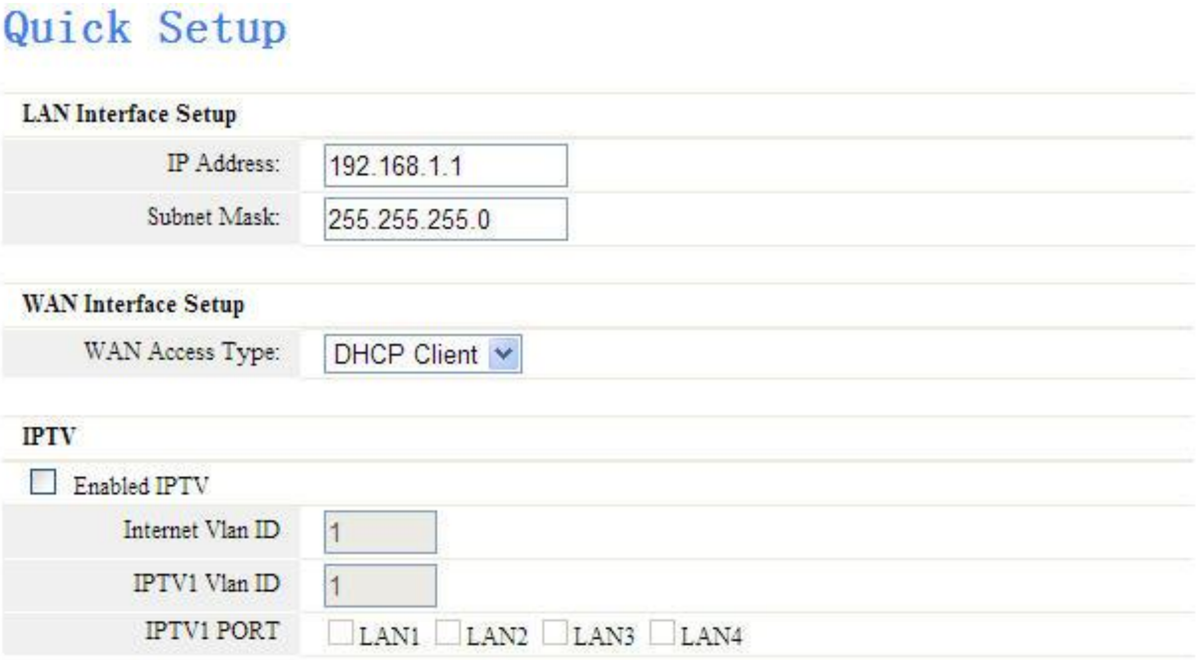
Confirmed: new password should be re-entered to verify its accuracy.

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

4.3 Quick Setup



Quick Setup is provided as part of the web configuration utility. Users can simply finish the settings all in one page to access Internet. In this section, you can setup LAN, WAN, WLAN, IPTV and Time Zone Settings.



Quick Setup

LAN Interface Setup

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

WAN Interface Setup

WAN Access Type: DHCP Client

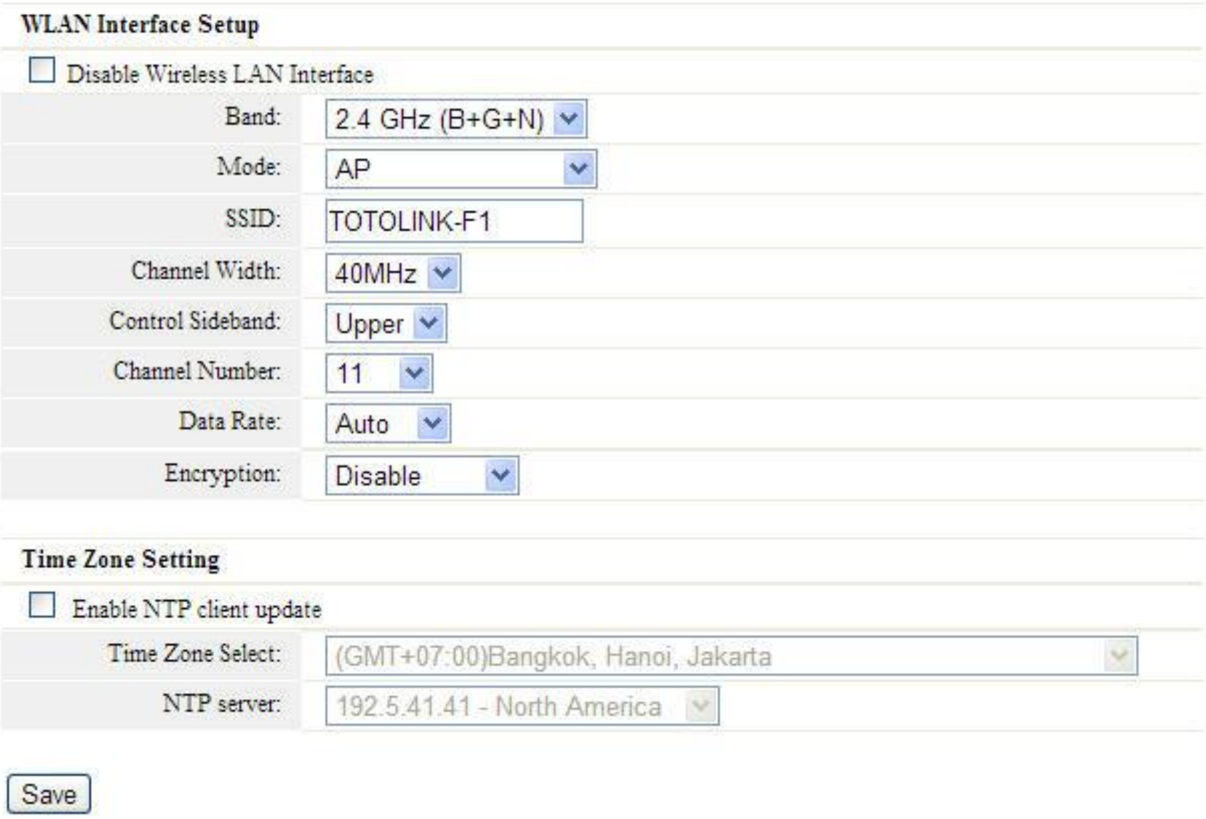
IPTV

□ Enabled IPTV

Internet Vlan ID: 1

IPTV1 Vlan ID: 1

IPTV1 PORT: □ LAN1 □ LAN2 □ LAN3 □ LAN4



WLAN Interface Setup

□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP
SSID:	TOTOLINK-F1
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Data Rate:	Auto
Encryption:	Disable

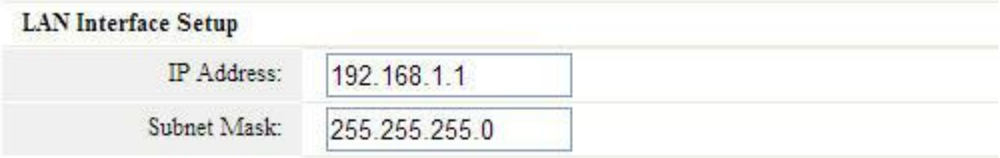
Time Zone Setting

□ Enable NTP client update

Time Zone Select:	(GMT+07:00)Bangkok, Hanoi, Jakarta
NTP server:	192.5.41.41 - North America

4.3.1 LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point.



LAN Interface Setup

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

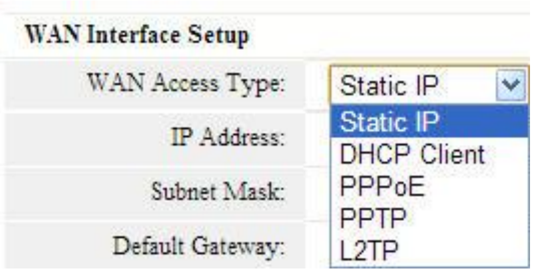
IP Address: this is the IP address to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

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.

> ***Note:*** *If this IP address changed, you can log into the WEB configuration interface only using the new IP address. AND if the new IP address and the original IP address are not in the same segment, the Virtual Server and DMZ Host service will not work. If you need to enable these functions, you will have to reset this IP address.*

4.3.2 WAN Interface Setup

This interface is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.



WAN Interface Setup

WAN Access Type: Static IP

IP Address:

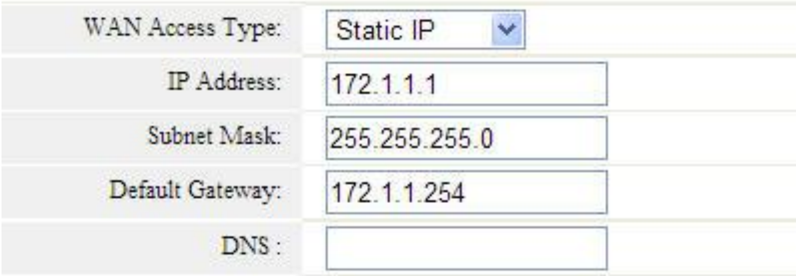
Subnet Mask:

Default Gateway:

WAN Access Type: there are three methods provided to allow you to access Internet. Please choose the appropriate one according to the information from your ISP (Internet Service Provider).

4.3.2.1 Static IP

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



WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS :

IP Address: the IP address provided by your ISP.

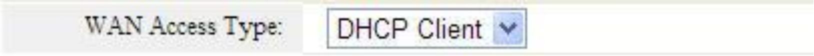
Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.

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.

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.

4.3.2.2 DHCP

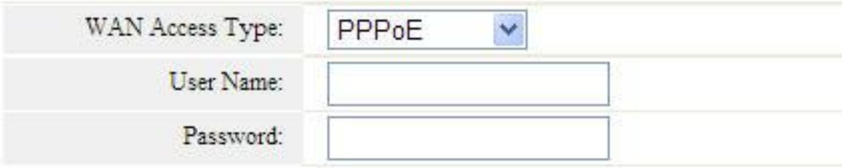
Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you choose this mode, you will get a dynamic IP address from your ISP automatically.



WAN Access Type: DHCP Client

4.3.2.3 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It replies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as wireless device or cable modem. All the users over the Ethernet can share a common connection. If you use ADSL virtual dial-up to connect Internet, please choose this option.

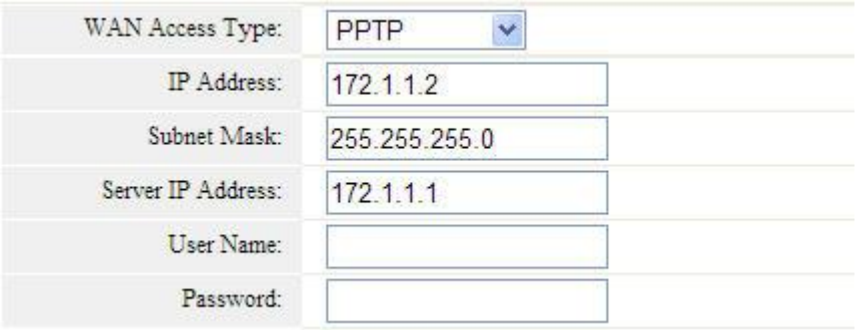


WAN Access Type:	PPPoE
User Name:	
Password:	

User Name: a specific valid ADSL user name provided by your ISP.
Password: the corresponding valid password provided by your ISP.

4.3.2.4 PPTP

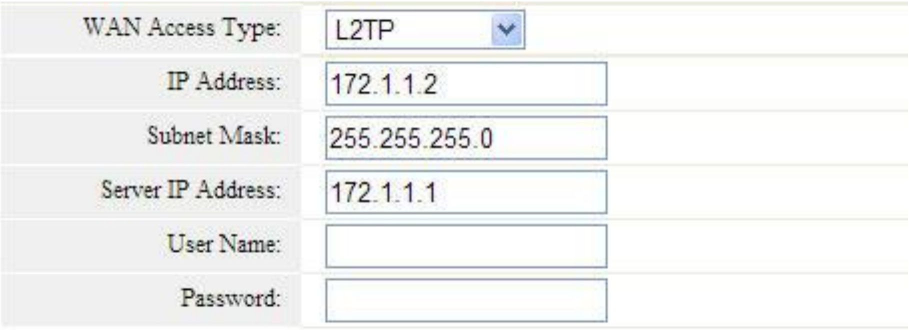
PPTP means Point to Point Tunneling Protocol. You should select PPTP option if ISP provides a PPTP connection and enter the following parameters. Please refer to PPPoE and Static IP configuration if there are the same parameters.



WAN Access Type:	PPTP
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	

4.3.2.5 L2TP

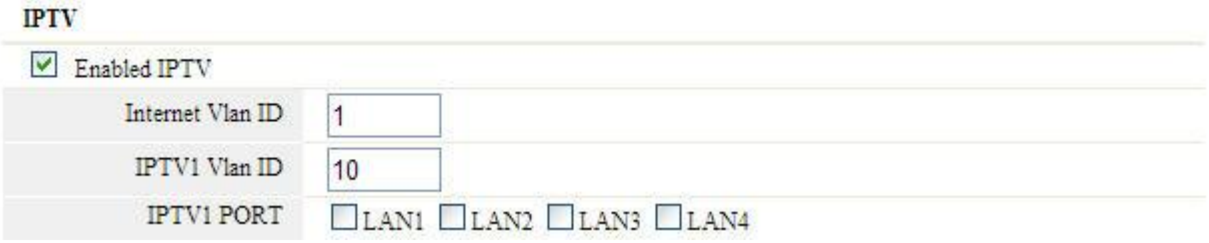
L2TP means Layer 2 Tunneling Protocol is a VPN connection that only applies in Europe, Middle East and Africa (MEA) regions. You should select L2TP option if ISP provides a L2TP connection and enter the following parameters.



WAN Access Type:	L2TP
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	

4.3.3 IPTV

Choose the Enable IPTV option to enable IPTV function, and please enter the Internet and IPTV VIDs provided by corresponding service providers and choose the port for IPTV.



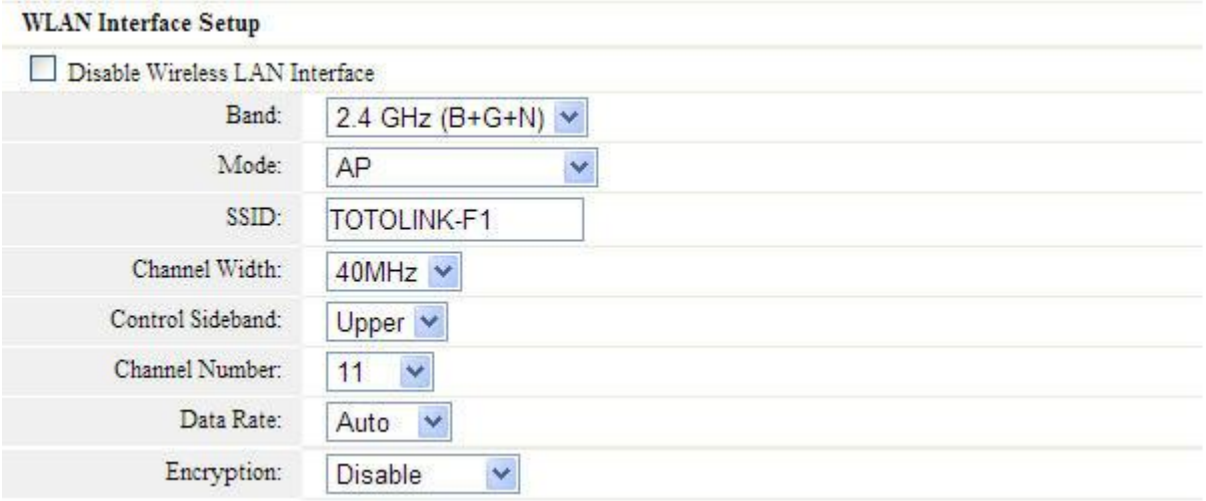
IPTV

☑ Enabled IPTV

Internet Vlan ID	1
IPTV1 Vlan ID	10
IPTV1 PORT	□LAN1 □LAN2 □LAN3 □LAN4

4.3.4 WLAN Interface Setup

The general wireless settings, such as 802.11 modes, SSID and data rates can be configured in this section.



WLAN Interface Setup

□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP
SSID:	TOTOLINK-F1
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Data Rate:	Auto
Encryption:	Disable

Band-- In fact, 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 (2.4GHz and/or 5GHz, in this case, only supports 2.4GHz) is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. Here, you can choose the last one 2.4GHz (B+G+N), this mode offers better compatibility. If you choose 2.4 GHz (B)/(G)/(B+G), you cannot setup Channel Width and Control Sideband parameters.

Mode--Wireless mode specifies the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported in this software.

AP: This mode allows users with laptop to surf Internet by wireless connection. It's designed to add wireless function for existed wired Router which is just suitable for home and small offices.

Client (+ Reapter): If you choose this mode, the Channel Number and Channel Width can't be edited.

WDS: Wireless Distribution System means connecting multiple wireless networks to one. It will use two or more wireless bandwidth Router/AP connecting with each other to expand wireless signal to longer distance. This mode is suitable for medium-size networks like school and enterprise network.

AP+WDS: WDS allows you to bridge wireless traffic between devices that are operating in Access Point mode. Access Point is usually connected to a wired network

(Ethernet LAN) allowing wireless connection to the wired network. By connecting Access Points to one another in an Extend Service Set using the WDS, distant Ethernets can be bridged into a single LAN.

Note: *If you select WDS, you can't change SSID.*

SSID---Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in AP or AP+WDS mode. All the client devices within the range will receive broadcast messages from the access point advertising this SSID.

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 (selected by default).

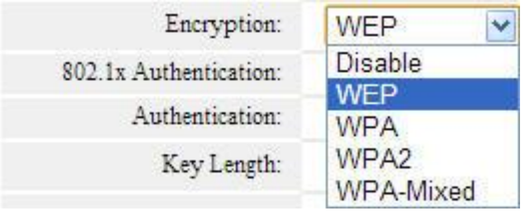
Control Sideband---This function is to control the sideband of the radio channel.

Upper: By default, it is Upper, and the Channel Number is 11.

Lower: If you choose Lower, the Channel Number will change to **Auto** automatically and you can't change the Control Sideband at the same time. The selectable Channel Number now will range from 1 to 9. Only when you choose other Channel Number you will activate the Control Sideband again. If you choose Upper, the Channel Number selectable will range from 5 to 13.

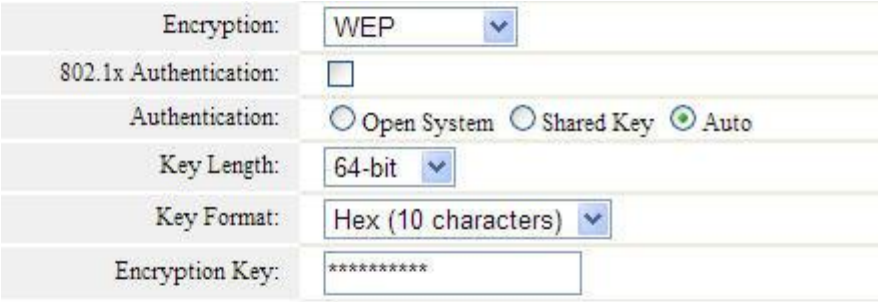
Channel Number---this option provides selectable channel numbers.

Encryption: This Router supports None, WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.


Encryption: WEP
802.1x Authentication:
Authentication:
Key Length:

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.


Encryption: WEP
802.1x Authentication: □
Authentication: ○ Open System ○ Shared Key ● Auto
Key Length: 64-bit
Key Format: Hex (10 characters)
Encryption Key: **********

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.)

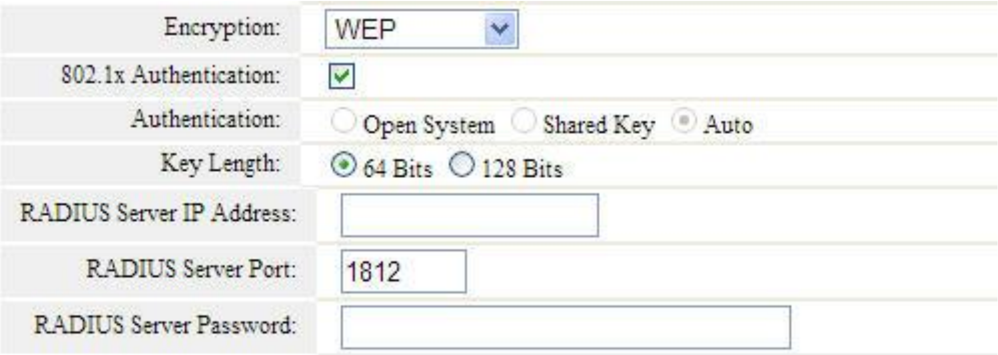
128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

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) 802.1x Authentication

WPA (Wi-Fi Protected Access) is separated into two categories: WPA/PSK and WPA/802.1x. If you choose this option, you will have to provide the RADIUS Server IP Address, Port and Password so that the encryption key will be obtained dynamically from RADIUS server.:



Encryption:	WEP
802.1x Authentication:	☑
Authentication:	○ Open System ○ Shared Key ● Auto
Key Length:	● 64 Bits ○ 128 Bits
RADIUS Server IP Address:	
RADIUS Server Port:	1812
RADIUS Server Password:	

RADIUS Server IP Address: Enter the IP address of RADIUS server.

RADIUS Server Port: the UDP port number that the RADIUS server that is used to authenticate the messages sent between them.

RADIUS Server Password: enter the password.

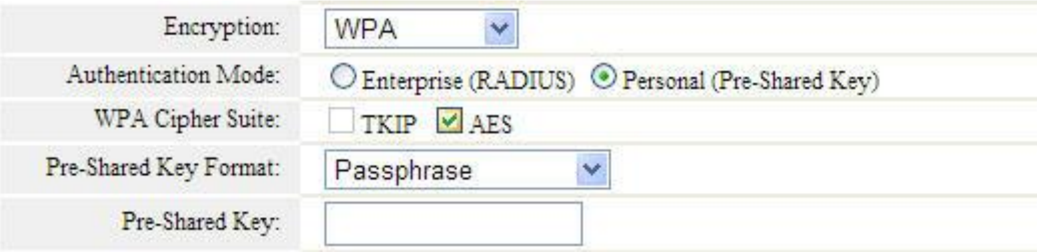
RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet Service Provider. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

3) WPA/WPA2

Wi-Fi Protected Access (WPA) is the most dominating security mechanism in industry. It is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x. WPA2 means Wi-Fi Protected Access 2, 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.

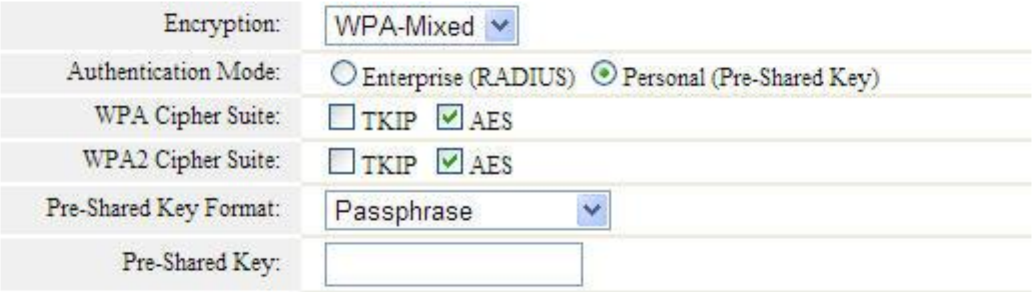


Encryption:	WPA
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	□ TKIP ☑ AES
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

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…”).

4) WPA Mixed

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

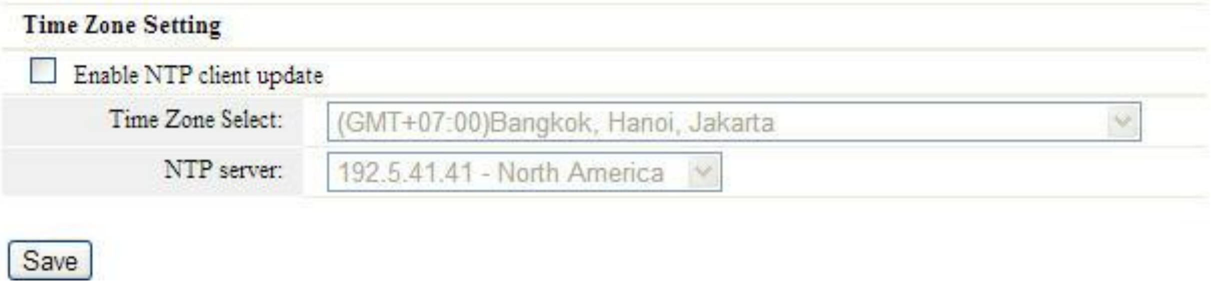


Encryption:	WPA-Mixed
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	□ TKIP ☑ AES
WPA2 Cipher Suite:	□ TKIP ☑ AES
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

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.*

4.3.5 Time Zone Setting

Here, you can specify the device’s time zone according to GMT (Greenwich Mean Time).



Time Zone Setting

□ Enable NTP client update

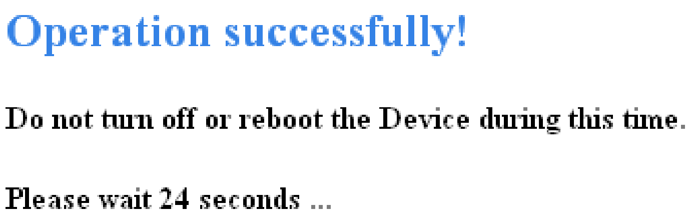
Time Zone Select:	(GMT+07:00)Bangkok, Hanoi, Jakarta
NTP server:	192.5.41.41 - North America

Enable NTP client update: NTP means Network Time Protocol which is used to make the computer 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.

Time Zone Select: Select the Time Zone where the router is located.

NTP server: Please choose the corresponding NTP server to get right time.

After all the above settings, please click **Save** button, then page with below messages will pop up:



Operation successfully!

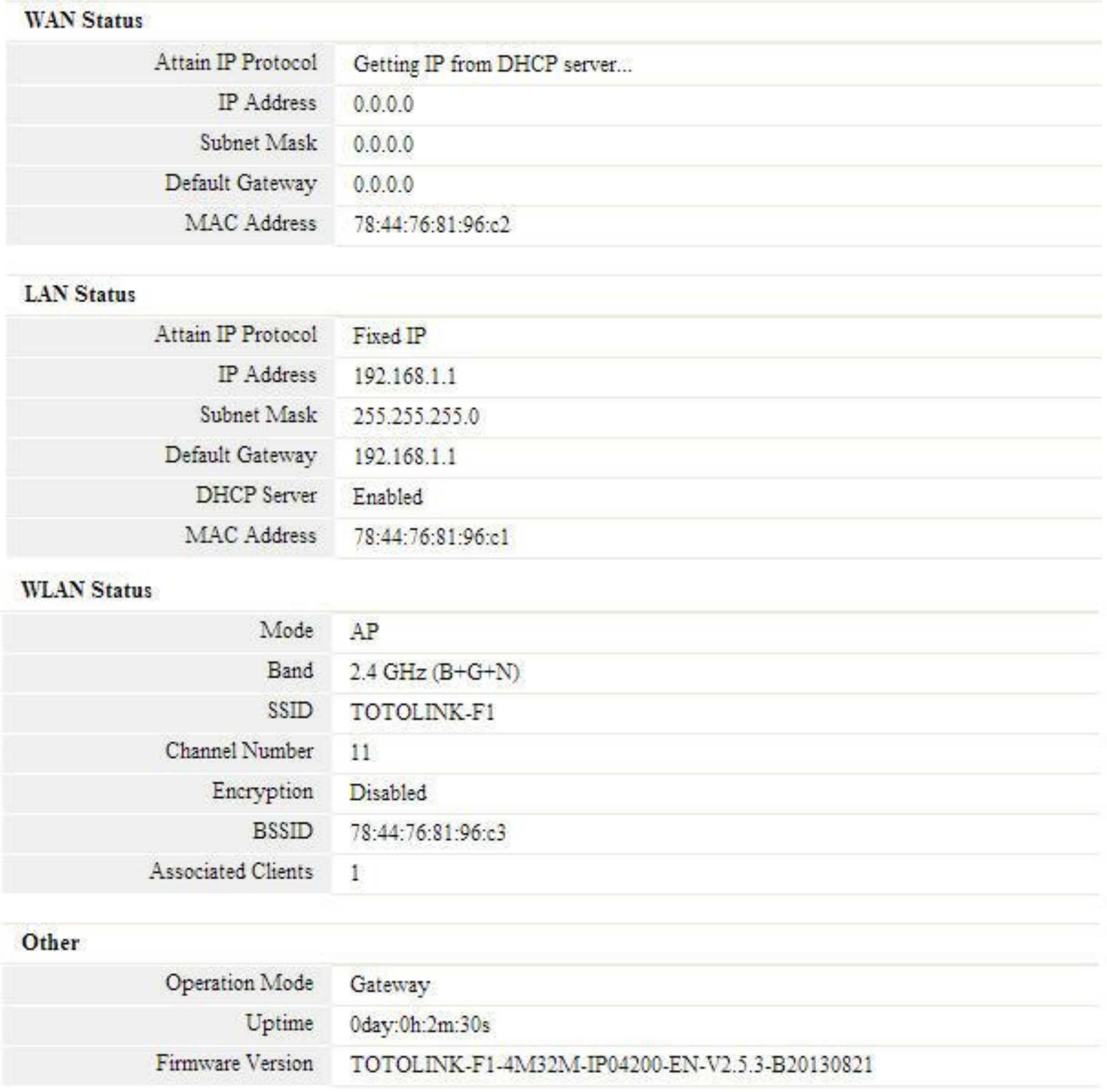
Do not turn off or reboot the Device during this time.

Please wait 24 seconds ...

Now you can surf Internet and enjoy the best wireless experience brought by this Fiber Router.

4.4 System Status

After quick start successfully completed, you can go to the Status page, which shows you the WAN Status, LAN Status, WLAN Status and other status.



WAN Status

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	78:44:76:81:96:c2

LAN Status

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	78:44:76:81:96:c1

WLAN Status

Mode	AP
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK-F1
Channel Number	11
Encryption	Disabled
BSSID	78:44:76:81:96:c3
Associated Clients	1

Other

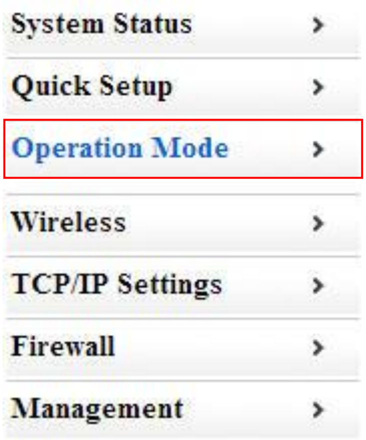
Operation Mode	Gateway
Uptime	0day:0h:2m:30s
Firmware Version	TOTOLINK-F1-4M32M-IP04200-EN-V2.5.3-B20130821

5. ADVANCED SETTINGS

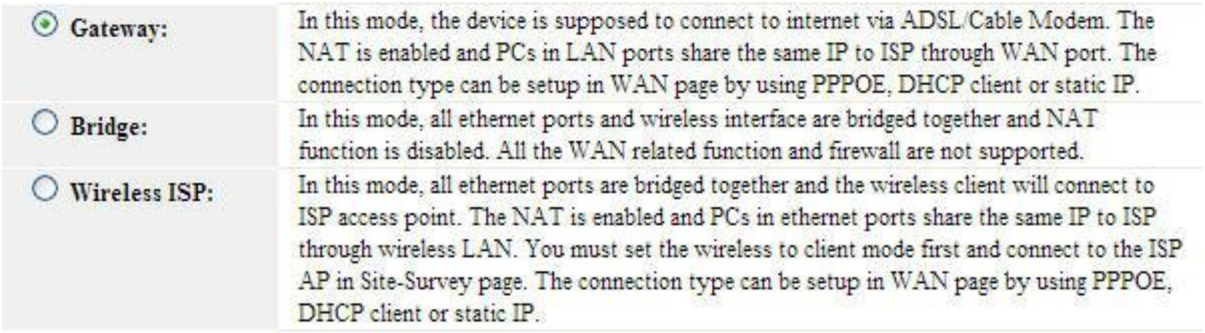
This chapter allows users to configure advanced settings includes Wireless, TCP/IP settings, Firewall and System Management. These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Also they should not be changed unless you know what effect the changes will have on your wireless Router.

5.1 Operation Mode

Click Operation Mode Option on the sidebar.



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



● Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.
○ Bridge:	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
○ Wireless ISP:	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

5.1.1 Gateway

Generally, this operating mode is selected by default as more and more users choose to access Internet by ADSL/Cable Modem. In this mode, the device works as a Software Router of the LAN, all clients will connect to Internet through this “agent”. If you choose this mode, PCs in four LAN ports share the same IP to ISP through WAN port. You can setup the connection type in WAN page by using PPPoE, DHCP client, PPTP client, L2TP client or Static IP.

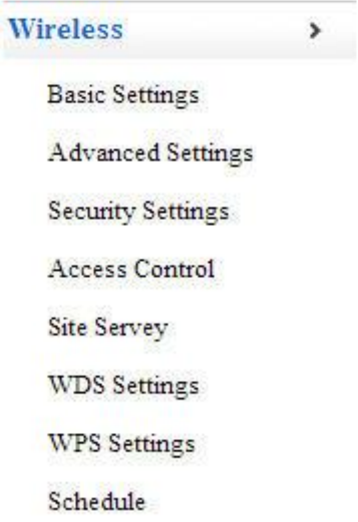
5.1.2 Bridge

In Bridge mode the router forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides an efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belongs to the same network segment that has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports.

5.1.2 Wireless ISP

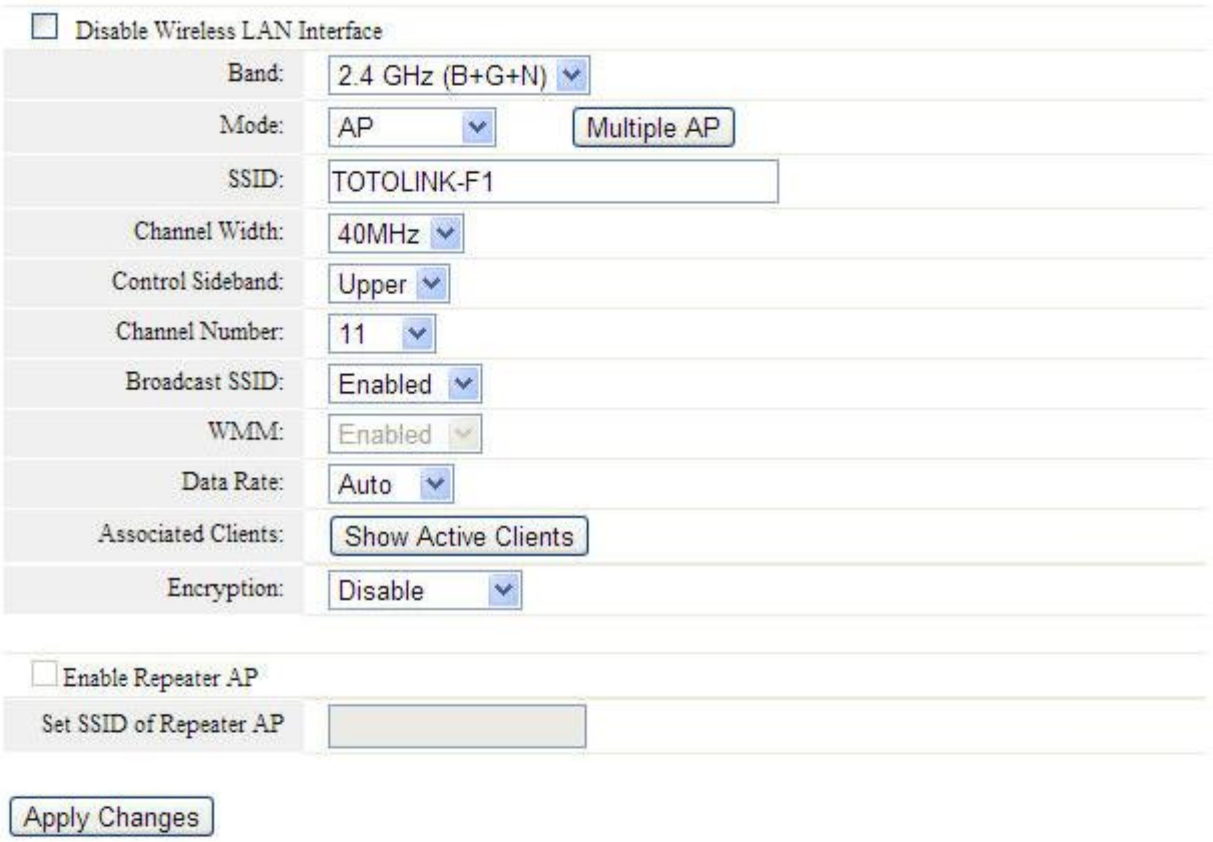
It means Wireless Internet Service Provider. If you need to access Internet through Wi-Fi, you can choose this mode. For example, when you are in a hotel, airport or other public commercial place, you can select wireless ISP to connect to Internet. In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point.

5.2 Wireless



5.2.1 Basic Settings

On this page, you could configure the parameters for Wireless LAN clients which may connect to your Access Point. Since we have discussed wireless settings on **Quick Setup**, here we will focus on the WMM function and Data Rate.



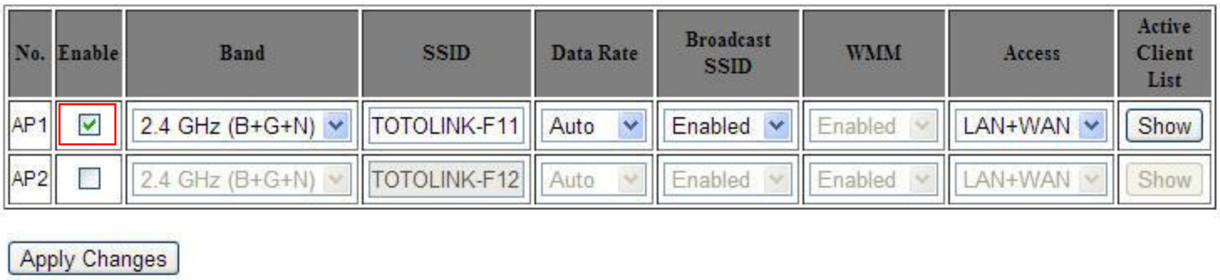
□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP Multiple AP
SSID:	TOTOLINK-F1
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients
Encryption:	Disable

□ Enable Repeater AP

Set SSID of Repeater AP	

While you choose the AP or AP+WDS mode, you can enable Multiple APs function by click Multiple APs button. The multiple APs setting interface will appear. See below:
You can check the box under Enable to enable this SSID and configure other parameters in this page.



No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1	☑	2.4 GHz (B+G+N)	TOTOLINK-F11	Auto	Enabled	Enabled	LAN+WAN	Show
AP2	□	2.4 GHz (B+G+N)	TOTOLINK-F12	Auto	Enabled	Enabled	LAN+WAN	Show

Broadcast SSID: you can select Enable or Disable to make your wireless visible or invisible to any wireless clients within coverage.

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data.

***Note**: This option will keep Enabled and can’t be changed by default.*

Data Rate

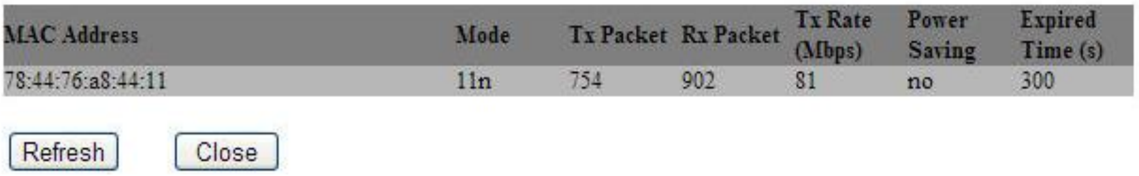
This defines the data rate (in Mbps) at which the device should transmit wireless packets. You can fix a specific data rate between MCS 0 and MCS 7 also. It is recommended to use Auto option, especially if you are having trouble getting connected or losing data at a higher rate.

MCS means Modulation Coding Scheme**.** Before 802.11n standard emerges, most Access Points complies with 802.11a/b/g standards and the data rate ranges from

1Mbps to 54Mbps, including only 12 possible physical speed. But when it comes to 802.11n technology, the physical speed can be affected by many factors, such as modulation type, coding rate, space flow quantity, whether 40MHz banding and so on. Combining these factors together will create a lot of selectable physical speed. Thus, 802.11n proposes the term MCS. You can consider this term to be a whole combination of these factors and every digit represents a combination.

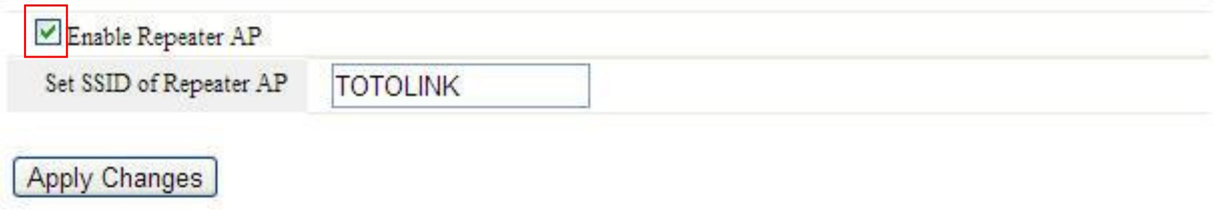
Note: *If you select 20MHz Channel Spectrum width the maximum data rate is MCS7 (65Mbps). If you select 40MHz Channel Spectrum width the maximum data rate is MCS7(150Mbps).*

Click **Show Active Clients** button, the active wireless client table interface will come out.



MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
78:44:76:a8:44:11	11n	754	902	81	no	300

When you choose the Client mode, the Repeater AP column is available. You can enable this function and set SSID of the Repeater AP in this section. Enter the SSID of Repeater AP and

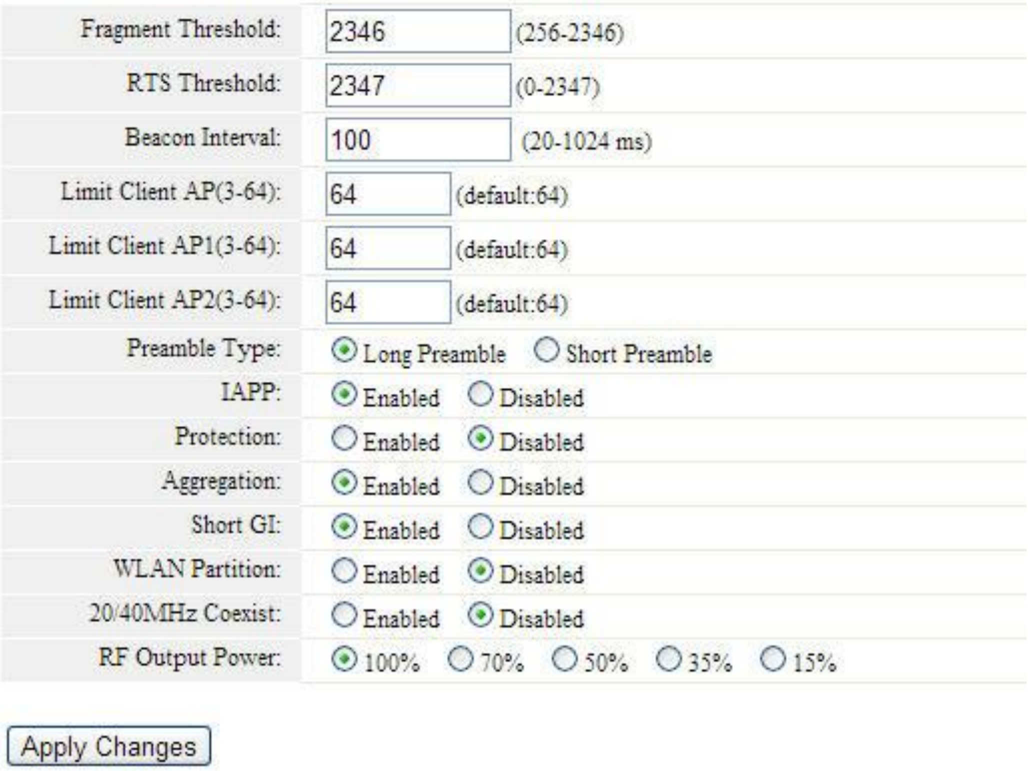


☑ Enable Repeater AP

Set SSID of Repeater AP: TOTOLINK

5.2.2 Advanced Settings

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



Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Limit Client AP(3-64):	64 (default:64)
Limit Client AP1(3-64):	64 (default:64)
Limit Client AP2(3-64):	64 (default:64)
Preamble Type:	● Long Preamble ○ Short Preamble
IAPP:	● Enabled ○ Disabled
Protection:	○ Enabled ● Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WLAN Partition:	○ Enabled ● Disabled
20/40MHz Coexist:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 70% ○ 50% ○ 35% ○ 15%

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.

> **RTS/CTS** (**Request to Send/Clear to Send**) are the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.
>
> System uses **Request to Send/Clear to Send** frames for the handshake that provide collision reduction for an access point with hidden stations. The stations are sending a RTS frame first while data is sent only after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provide clear media for the requesting station to send the data. CTS collision control management has a time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

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.

Frames—determines the number of frames combined on the new larger frame.

Bytes—determines the size (in **Bytes**) of the larger frame.

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

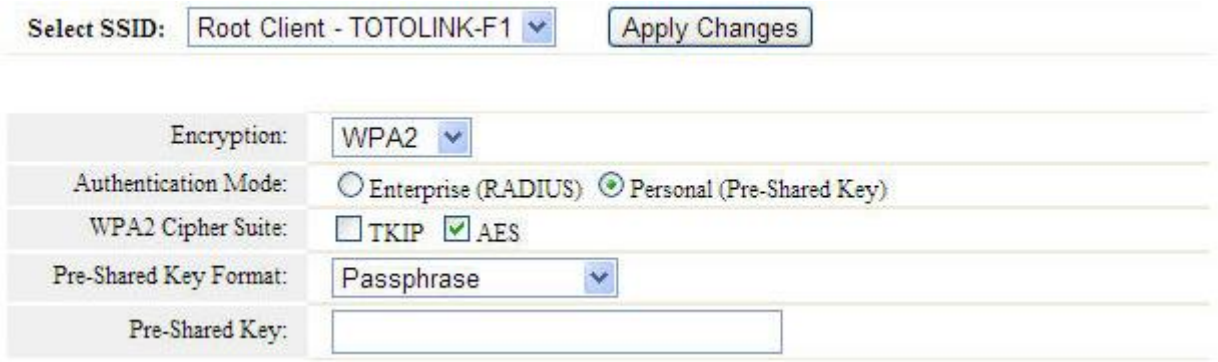
WLAN Partition: divides the WLAN to several part.

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.

5.2.3 Security Settings

You can setup wireless security in this page. Setup different encryptions for different SSIDs so that makes your wireless network more secure. It is very practical for protecting your private information.



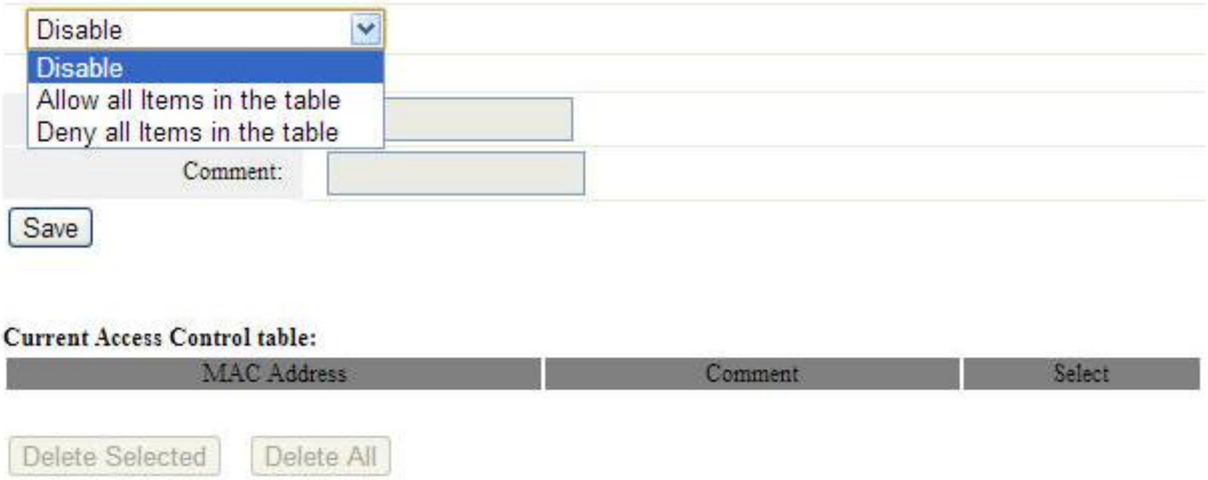
Select SSID: Root Client - TOTOLINK-F1

Encryption:	WPA2
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA2 Cipher Suite:	□ TKIP ☑ AES
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

5.2.4 Access Control

If you choose '**Allow all items in the table**', only those clients whose wireless MAC addresses are in the Current Access Control List will be able to your Access Point. When

‘**Deny all items in the table**’ is selected, these wireless clients on the list will not be able to connect the Access Point.



Current Access Control table:

MAC Address	Comment	Select

By default, Wireless Access Control Mode is disabled.

There are two ways to set the Access Control List:

1. If you select **Allow all items in the table** 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 all items in the table** 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.

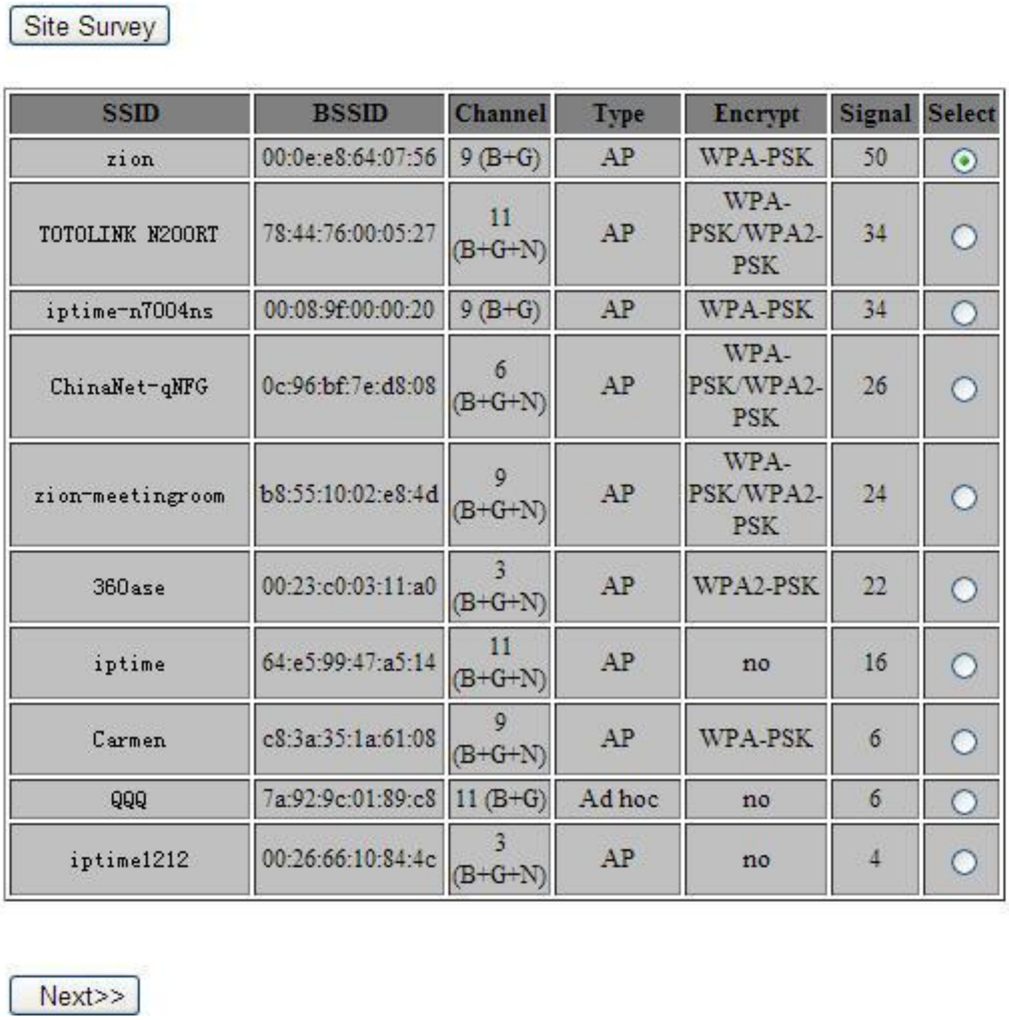
You need to click **Save** to make your setting work.

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.

5.2.5 Site Survey

Utility will search for wireless networks in range on all the supported channels while device is operating in Access Point mode. This page provides a 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.

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



Site Survey

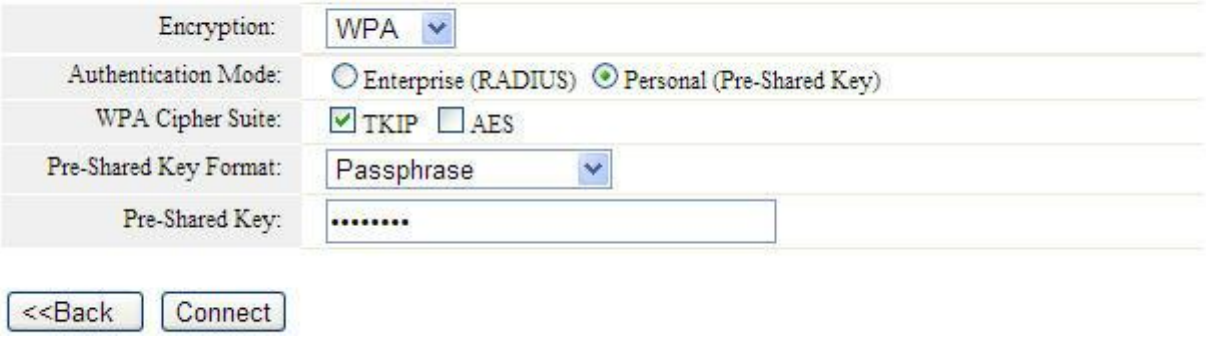
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
zion	00:0e:e8:64:07:56	9 (B+G)	AP	WPA-PSK	50	●
TOTOLINK N200RT	78:44:76:00:05:27	11 (B+G+N)	AP	WPA-PSK/WPA2-PSK	34	○
iptime-n7004ns	00:08:9f:00:00:20	9 (B+G)	AP	WPA-PSK	34	○
ChinaNet-qNFG	0c:96:bf:7e:d8:08	6 (B+G+N)	AP	WPA-PSK/WPA2-PSK	26	○
zion-meetingroom	b8:55:10:02:e8:4d	9 (B+G+N)	AP	WPA-PSK/WPA2-PSK	24	○
360ase	00:23:c0:03:11:a0	3 (B+G+N)	AP	WPA2-PSK	22	○
iptime	64:e5:99:47:a5:14	11 (B+G+N)	AP	no	16	○
Carmen	c8:3a:35:1a:61:08	9 (B+G+N)	AP	WPA-PSK	6	○
QQQ	7a:92:9c:01:89:c8	11 (B+G)	Ad hoc	no	6	○
iptime1212	00:26:66:10:84:4c	3 (B+G+N)	AP	no	4	○

Next>>

Site Survey reports MAC Address, SSID, wireless mode, Encryption type (if any), Signal Strength/Noise (dBm) and wireless channel of all the surrounding Access Points which can be found by this device.

Setup Repeater

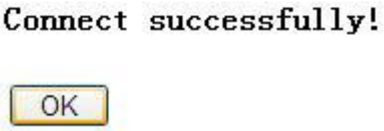
Select the one you want to connect to and then it will come to the encryption interface. Enter the Pre-Shared Key of the Network and click Connect button.



Encryption:	WPA
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	☑ TKIP □ AES
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	••••••••

<<Back Connect

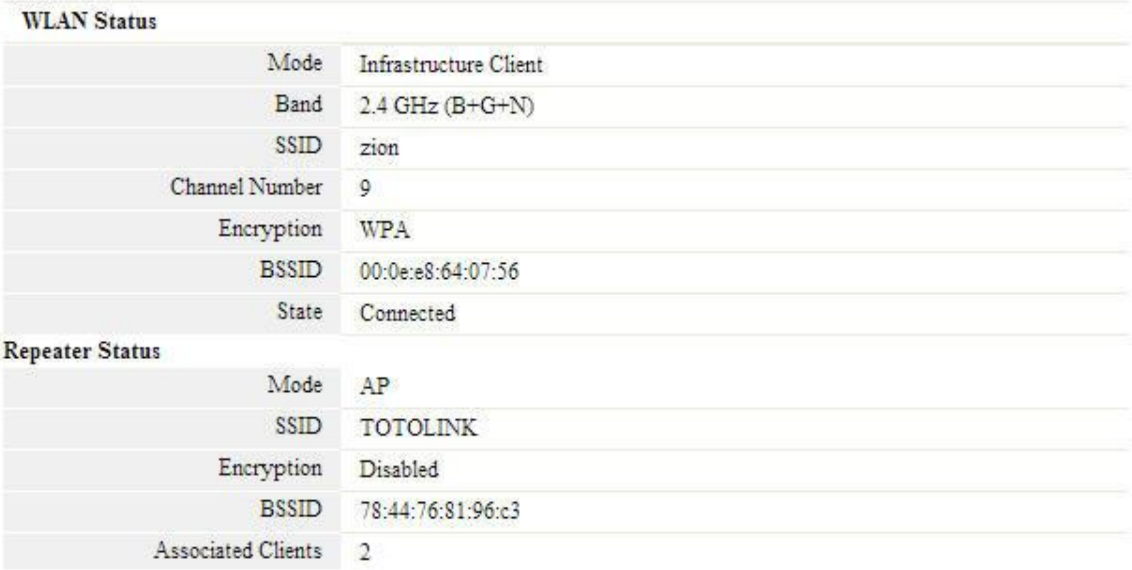
Click OK if it comes out this page.



Connect successfully!

OK

After setup repeater successfully, you can see the repeater status in the status page. If you have set SSID of Repeater AP in wireless basic settings section (e.g. TOTOLINK), other devices within coverage can scan TOTOLINK and connect to it to access Internet now if the upper AP can connect to the Internet.



WLAN Status

Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	zion
Channel Number	9
Encryption	WPA
BSSID	00:0e:e8:64:07:56
State	Connected

Repeater Status

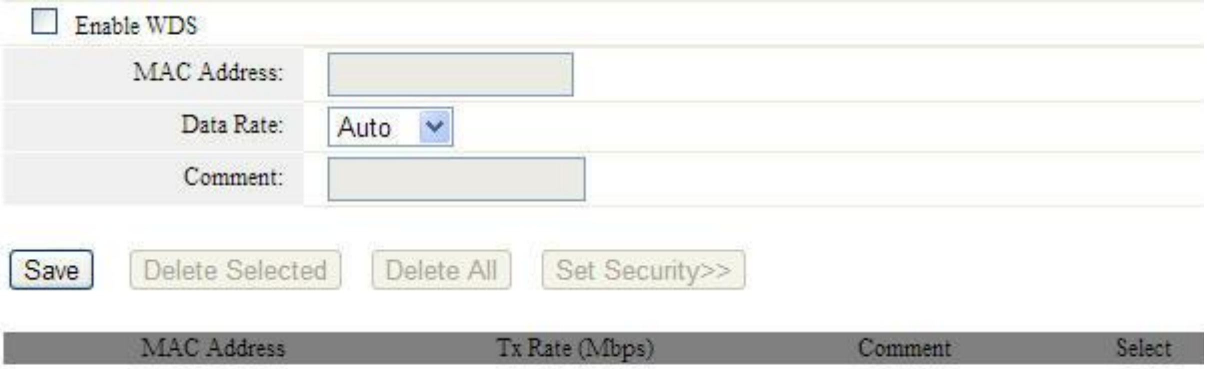
Mode	AP
SSID	TOTOLINK
Encryption	Disabled
BSSID	78:44:76:81:96:c3
Associated Clients	2

5.2.6 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.

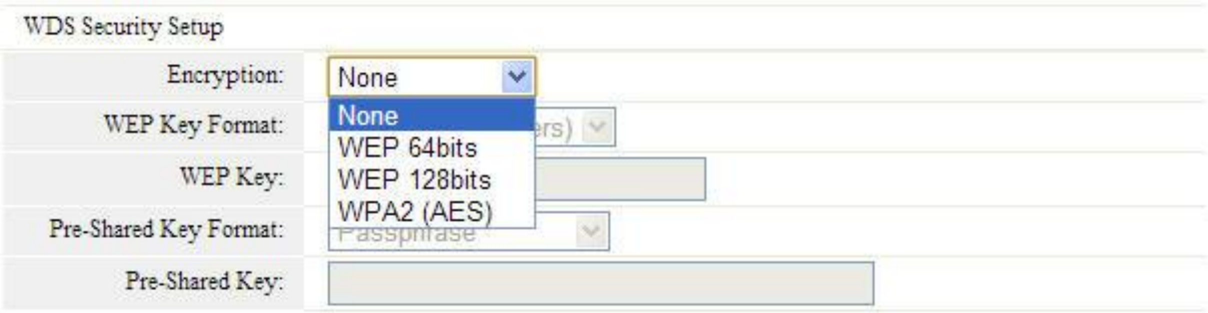


□ Enable WDS

MAC Address:	
Data Rate:	Auto
Comment:	

MAC Address	Tx Rate (Mbps)	Comment	Select

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.
Data Rate: please choose the transmission data rate.
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.



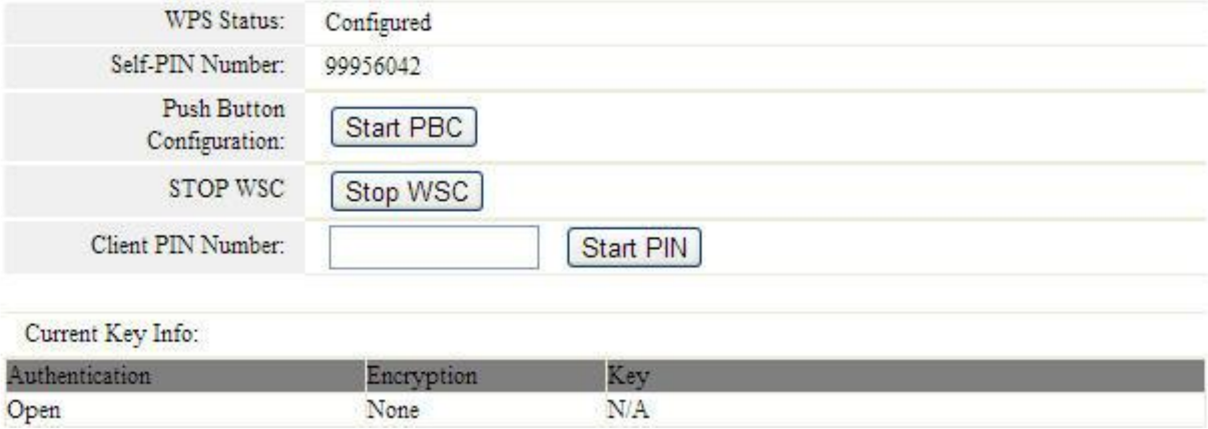
WDS Security Setup

Encryption:	None
WEP Key Format:	ers)
WEP Key:	
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

Please refer to **4.3.4 WLAN Interface Setup** in Quick Start to setup the encryption for WDS.

5.2.7 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.



WPS Status:	Configured
Self-PIN Number:	99956042
Push Button Configuration:	Start PBC
STOP WSC	Stop WSC
Client PIN Number:	Start PIN

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

WPS Status: display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see "**Configured**" chosen.

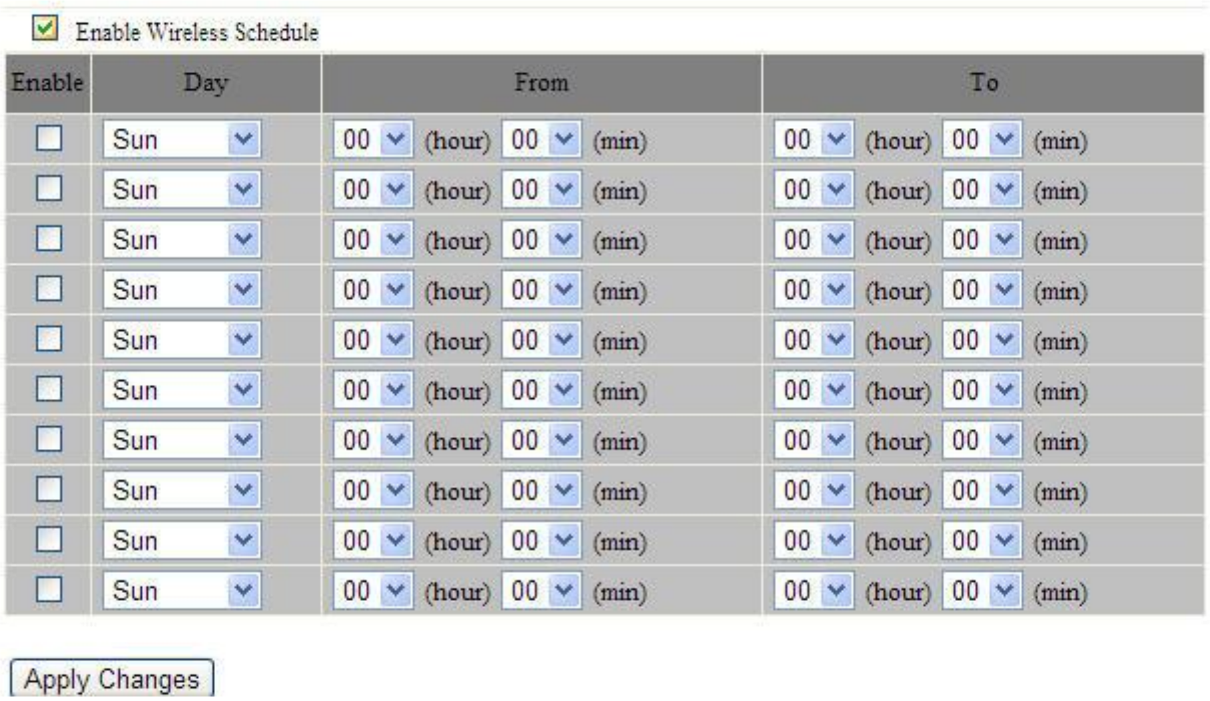
Self-PIN Number: it will show the PIN Number of your device.

Push Button Configuration: click Start PBC 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.)

Client PIN Number: please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button.

5.2.8 Schedule

This router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocol (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours. The schedule is also applicable to other functions. You have to set your time before setting schedule.

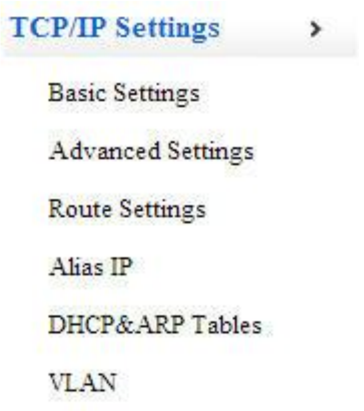


☑ Enable Wireless Schedule

Enable	Day	From				To			
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)
☐	Sun	00	(hour)	00	(min)	00	(hour)	00	(min)

After the settings, please click **Apply Changes** to make it work.

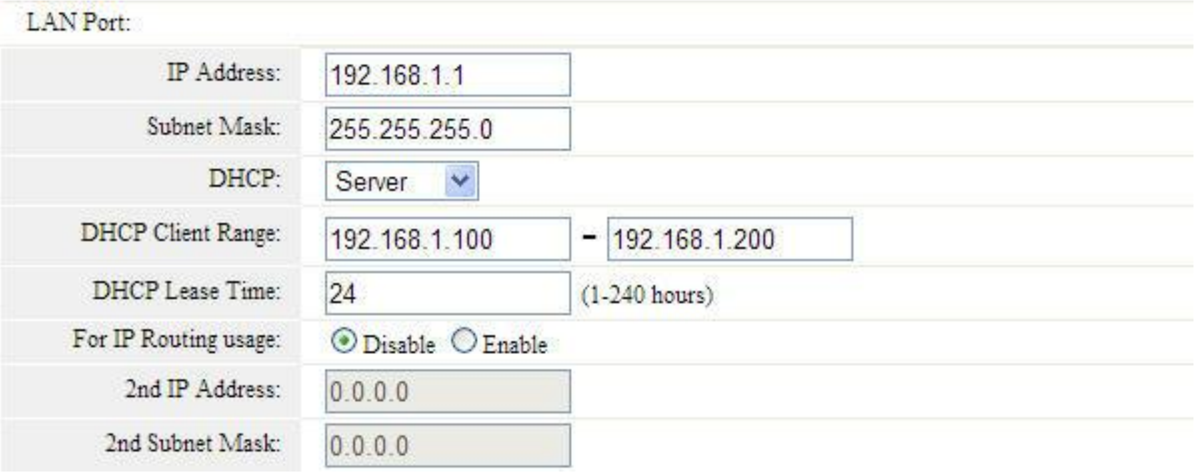
5.3 TCP/IP Settings



5.3.1 Basic Settings

5.3.1.1 LAN port

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.



LAN Port:

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 - 192.168.1.200
DHCP Lease Time:	24 (1-240 hours)
For IP Routing usage:	● Disable ○ Enable
2nd IP Address:	0.0.0.0
2nd Subnet Mask:	0.0.0.0

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).

Note: *If this IP address changed, you can log into the WEB configuration interface only using the new IP address. AND if the new IP address and the original IP address are not in the same segment, the Virtual Server and DMZ Host service will not work. If you need to enable these functions, you will have to reset this IP address.*

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.

DHCP: you can disable this function or choose DHCP server/client. If you select server, all the computers connected to this router will get the IP address dynamically. Client mode means that this device works as a client and you can’t change the default settings on this page.

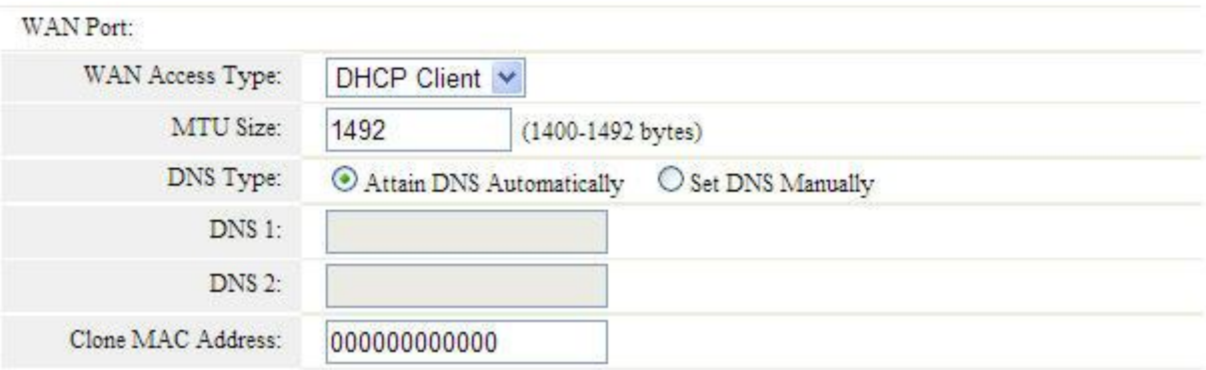
DHCP Client Range: the range of IP addresses that will be assigned to each computer connected with the router.

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.

For IP Routing usage: setting another address for IP routing usage, you can choose enable or disable according to need. By default, it is Disable.

5.3.1.2 WAN port

This part allows you to configure the WAN port parameters so that your computer can access Internet. Since we have discussed WAN Access Type on Quick Setup, we will explain the other settings here.



WAN Port:

WAN Access Type:	DHCP Client
MTU Size:	1492 (1400-1492 bytes)
DNS Type:	● Attain DNS Automatically ○ Set DNS Manually
DNS 1:	
DNS 2:	
Clone MAC Address:	000000000000

MTU Size: It means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency. The default setting is 1492.

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. 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.

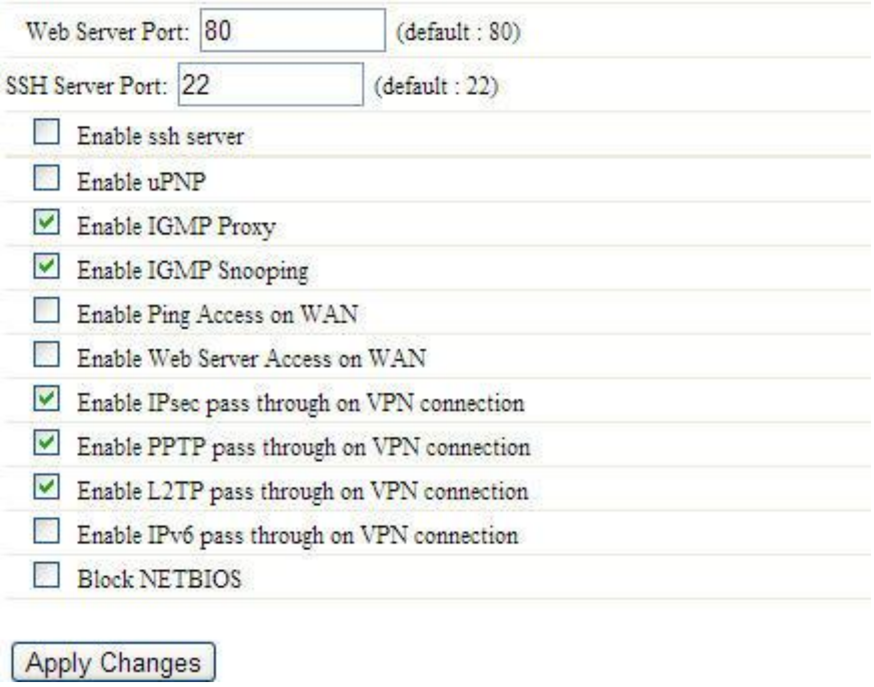
Attain DNS Automatically: choose this option you don't need to set the DNS by yourself.

Set DNS Manually: you will have to type in the DNS address by yourself.

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.

5.3.2 Advanced Settings

This page is used to configure the parameters for TCP/IP.



Web Server Port: 80 (default : 80)

SSH Server Port: 22 (default : 22)

□ Enable ssh server

□ Enable uPNP

☑ Enable IGMP Proxy

☑ Enable IGMP Snooping

□ 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

□ Enable IPv6 pass through on VPN connection

□ Block NETBIOS

Web Server Port: enter your web Server port. By default, it is 80.

SSH Server Port: SSH means Secure Shell, it is the security protocol based on Application Layer and Transport Layer. Please enter the ssh server port.

Enable ssh server: choose the check box to enable ssh server.

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.

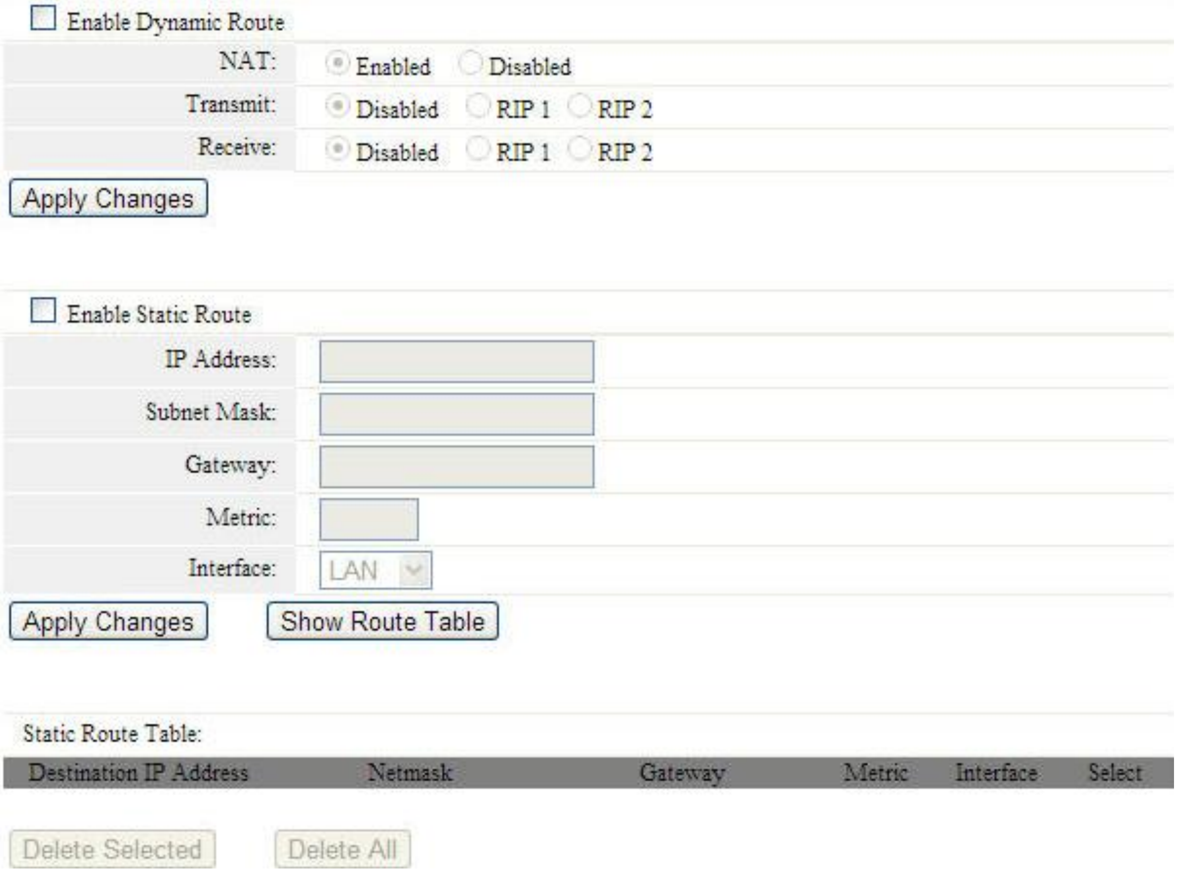
Enable IGMP Proxy: IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. If you select this checkbox, the application of multicast will be executed through WAN port. In addition,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

Enable IGMP Snooping: if you enable this function, multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.

Enable Ping Access on WAN: enable users use Ping command to access WAN.
Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN services of this Router to allow VPN tunnel pass through as well as the appropriate NAT settings, such as DMZ or open port:
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Enable IPv6 pass through on VPN connection

5.3.3 Route Settings

This page is used to setup dynamic routing protocol or edit static route entry.



□ Enable Dynamic Route

NAT: ● Enabled ○ Disabled

Transmit: ● Disabled ○ RIP 1 ○ RIP 2

Receive: ● Disabled ○ RIP 1 ○ RIP 2

□ Enable Static Route

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: LAN

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select

Enable Dynamic Route

You may want to set up your router to route computers or devices on your network to other local networks through other routers. If other routers support dynamic routing such as RIP (Routing Information Protocol), you can enable this feature on your router to automatically learn the required routes to reach those networks. It is required that the same dynamic routing protocol and version is also enabled on the other routers in order your router and the other users to exchange information about the network. Select the checkbox to enable Dynamic Route function.

Note: *Configuring this feature assumes that you have some general networking knowledge.*

NAT: by default, this option is selected. Detailed information about this parameter refers to the discussion before.

Transmit: allows your router to send out network information to other routers so other routers can dynamically build routes to your network.

Disabled—Disable sending routing information from your router to other routers.
RIP1—Sends out routing information to other routers using the RIP version 1 protocol.
RIP2—Sends out routing information to other routers using the RIP version 2 protocol.

Receive: allows your router to receive network information from other routers so your router can build routes to other networks.

Disabled—Disable receiving routing information from other router to your router.
RIP1—Receive routing information from other routers using the RIP version 1 protocol.
RIP2—Receive routing information from other routers using the RIP version 2 protocol.

Enable Static Route: this part allows you to specify that a specific target IP addresses passes through a determined gateway manually.

IP Address: type in the target network IP.

Subnet Mask: type in the Netmask.

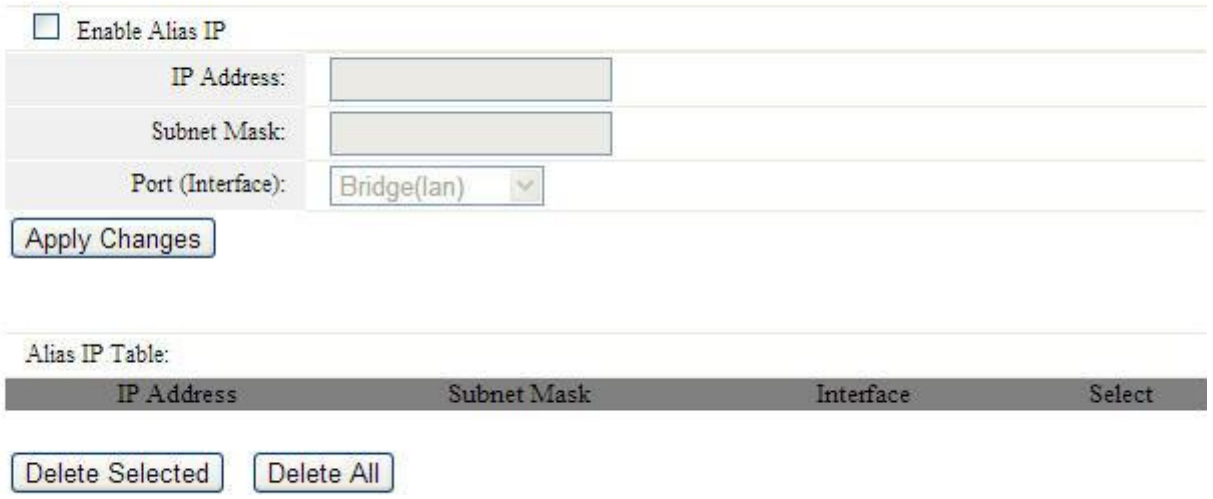
Gateway: type in the Gateway IP.

Metric: enter the metric or priority of the route. The metric range is 1 to 15, the lowest number 1 being the highest priority.

Interface: click the drop-down list and select the interface on your router where the route is active.

Static Route Table: this table will list the detailed information about the target network IP.

5.3.4 Alias IP



□ Enable Alias IP

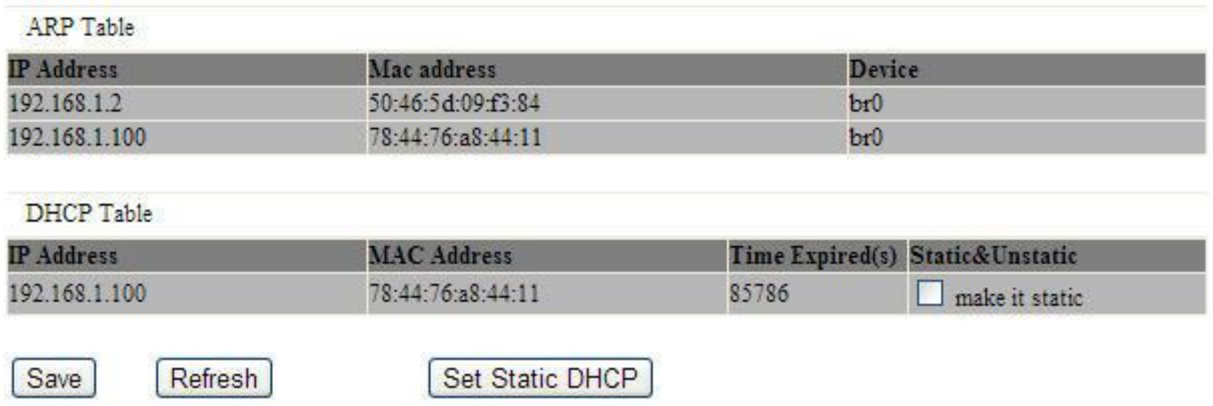
IP Address:	
Subnet Mask:	
Port (Interface):	Bridge(lan)

Alias IP Table:

IP Address	Subnet Mask	Interface	Select

Alias IP means virtual IP. You can choose to enable this function according to your requirement.

5.3.5 DHCP Clients & ARP Table



ARP Table

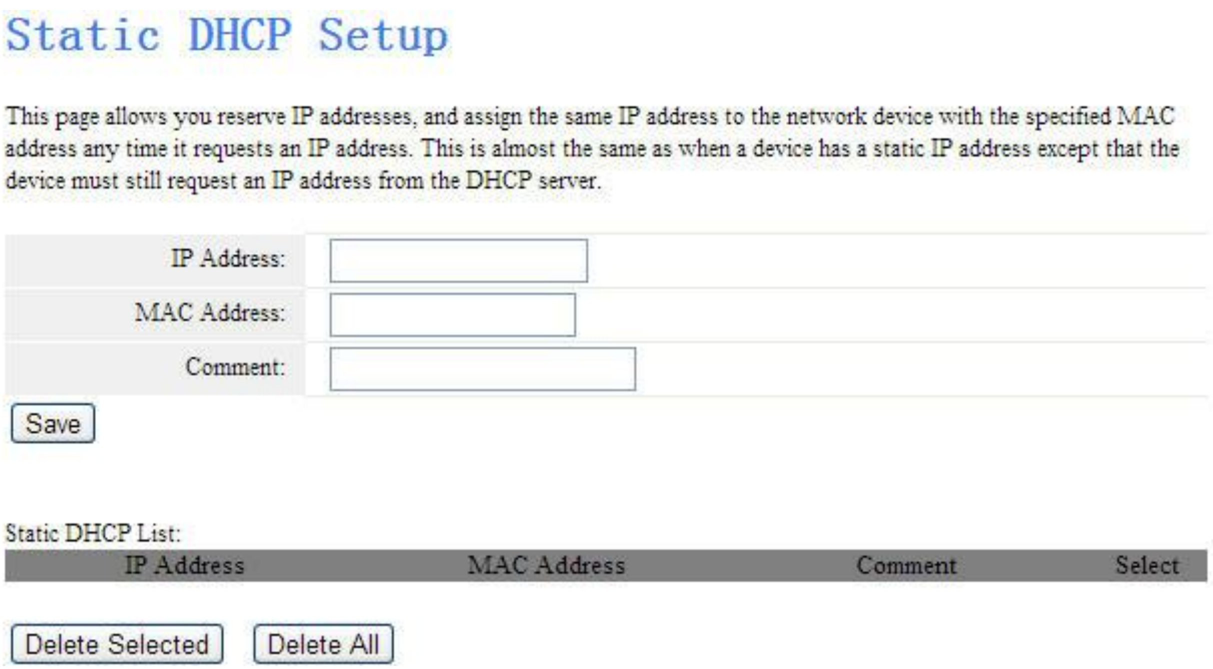
IP Address	Mac address	Device
192.168.1.2	50:46:5d:09:f3:84	br0
192.168.1.100	78:44:76:a8:44:11	br0

DHCP Table

IP Address	MAC Address	Time Expired(s)	Static&Unstatic
192.168.1.100	78:44:76:a8:44:11	85786	□ make it static

ARP means address resolution protocol. This table will show you detailed information about the ARP request your router has detected.
DHCP Table presents the DHCP information. You can also click the Set Static DHCP button to set parameters for Static DHCP.

This page allows you 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.



Static DHCP Setup

This page allows you 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. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

IP Address:	
MAC Address:	
Comment:	

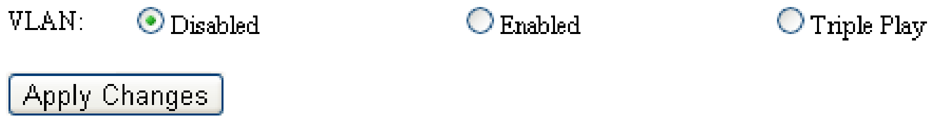
Static DHCP List:

IP Address	MAC Address	Comment	Select

IP Address: shows the IP address of selected MAC address.

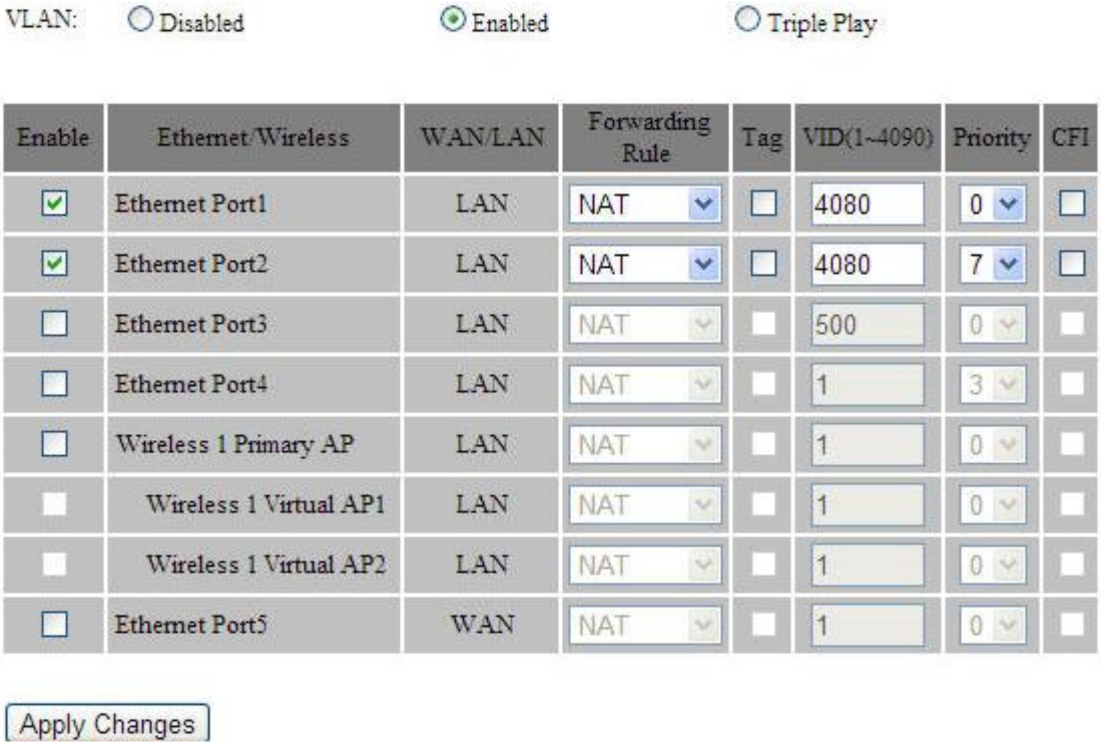
MAC Address: choose the MAC address that you want to bind.

5.3.6 VLAN



VLAN: ● Disabled ○ Enabled ○ Triple Play

VLAN means Virtual LAN, this function 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. VLANs address issues such as scalability, security, and network management.



VLAN: ○ Disabled ● Enabled ○ Triple Play

Enable	Ethernet/Wireless	WAN/LAN	Forwarding Rule	Tag	VID(1~4090)	Priority	CFI
☑	Ethernet Port1	LAN	NAT	□	4080	0	□
☑	Ethernet Port2	LAN	NAT	□	4080	7	□
□	Ethernet Port3	LAN	NAT	□	500	0	□
□	Ethernet Port4	LAN	NAT	□	1	3	□
□	Wireless 1 Primary AP	LAN	NAT	□	1	0	□
□	Wireless 1 Virtual AP1	LAN	NAT	□	1	0	□
□	Wireless 1 Virtual AP2	LAN	NAT	□	1	0	□
□	Ethernet Port5	WAN	NAT	□	1	0	□

For example, if the VLAN is configured as above diagram. Both port 1 and port 2 are the member port of VLAN 4080, it means that port 1 and port 2 can communicate with each other, port 1 and port 3 can NOT communicate with each other.

Ethernet/Wireless: specifies the WAN port and wireless AP.

WAN/LAN: defines the WAN port or LAN port.

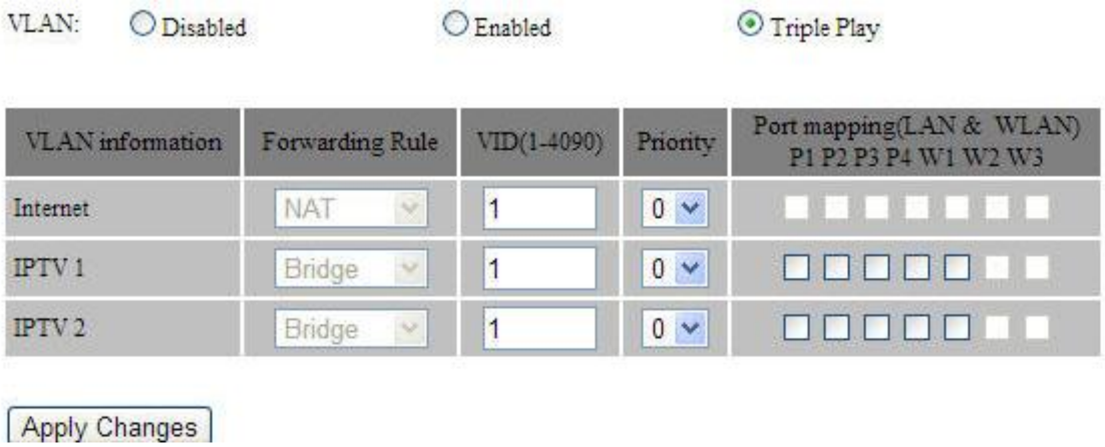
Forwarding Rule: VLAN feature also support forwarding rule as bridge and NAT between LAN port and WAN port.

Tag: enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out. Please type the tag value and specify the priority for the packets sending by LAN.

VID: type the value as the VLAN ID number. The range is from 1 to 4090.

Priority: Type the packet priority number for such VLAN. The range is from 0 to 7.

If you choose **Triple Play**, you will see the following form:



VLAN: ○ Disabled ○ Enabled ● Triple Play

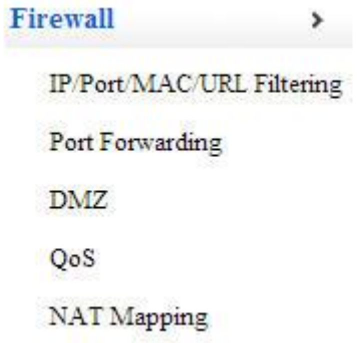
VLAN information	Forwarding Rule	VID(1-4090)	Priority	Port mapping(LAN & WLAN) P1 P2 P3 P4 W1 W2 W3
Internet	NAT	1	0	□ □ □ □ □ □ □
IPTV 1	Bridge	1	0	□ □ □ □ □ □ □
IPTV 2	Bridge	1	0	□ □ □ □ □ □ □

Some customers require AP support VOIP, IPTV and so on. So we add this Triple Play.

After the VLAN settings, please click **Apply Changes** to finish TCP/IP Settings.

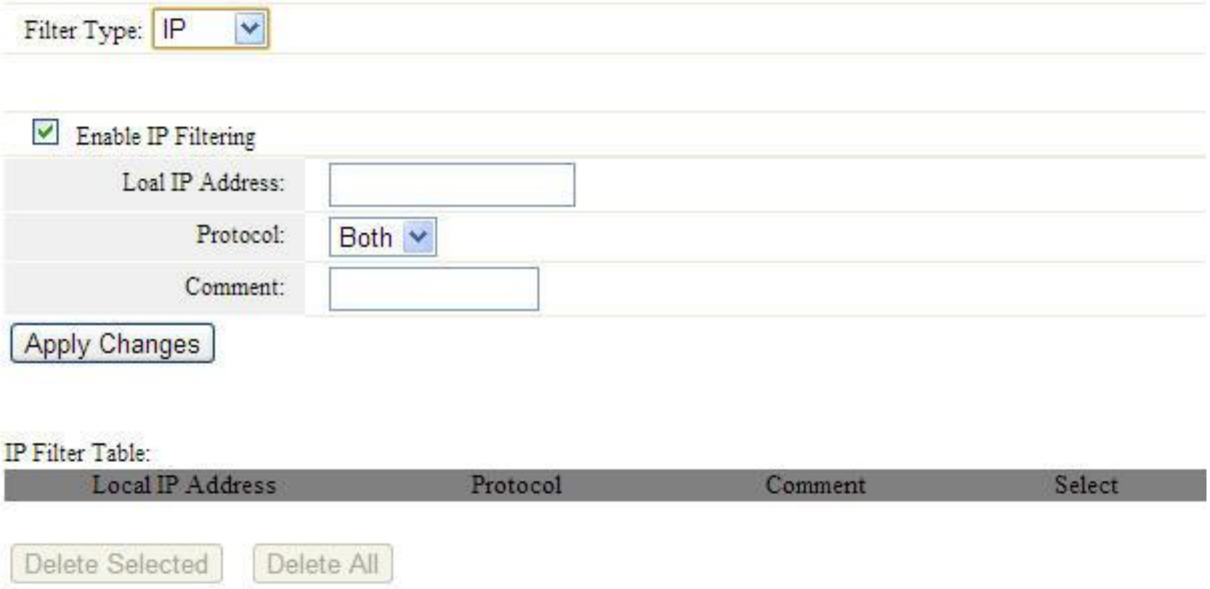
5.4 Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. 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.



5.4.1 IP/Port/MAC/URL Filtering

5.4.1.1 IP Filtering


Filter Type: IP

☑ Enable IP Filtering

Loal IP Address:

Protocol: Both

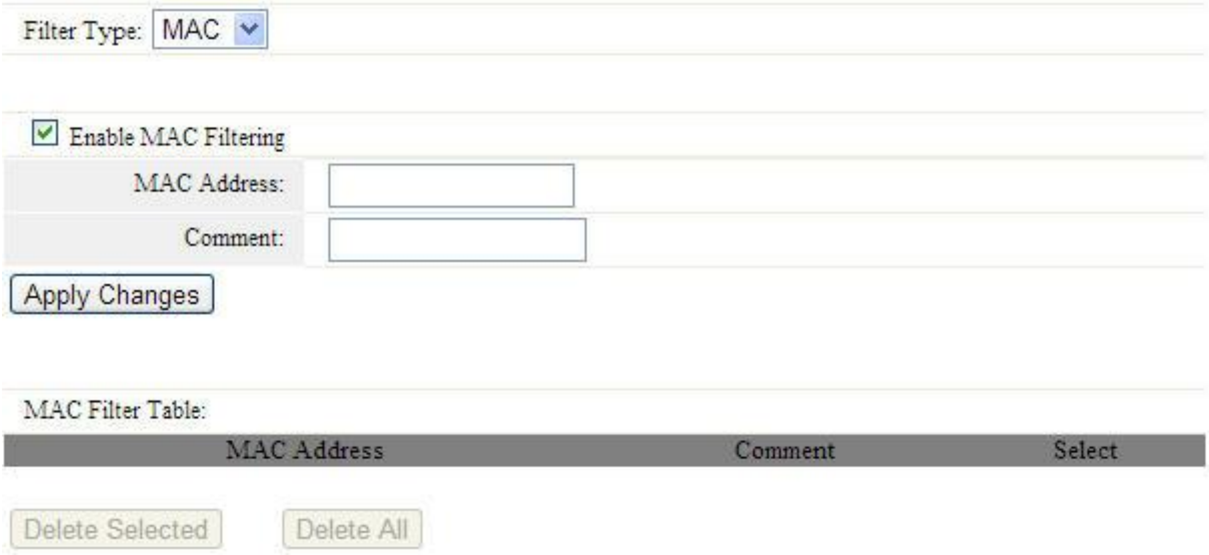
Comment:

IP Filter Table:

Local IP Address	Protocol	Comment	Select

Enable IP filtering: you can select this checkbox to enable IP Filtering function.
Local IP Address: the IP address that you want to filter.
Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP.
Comment: describe the reason why you want to filter the IP address. Just few words are saved there usually.
IP Filter Table: this table will list the detailed information about the IP addresses that will be filtered.

5.4.1.2 MAC Filtering


Filter Type: MAC

☑ Enable MAC Filtering

MAC Address:

Comment:

MAC Filter Table:

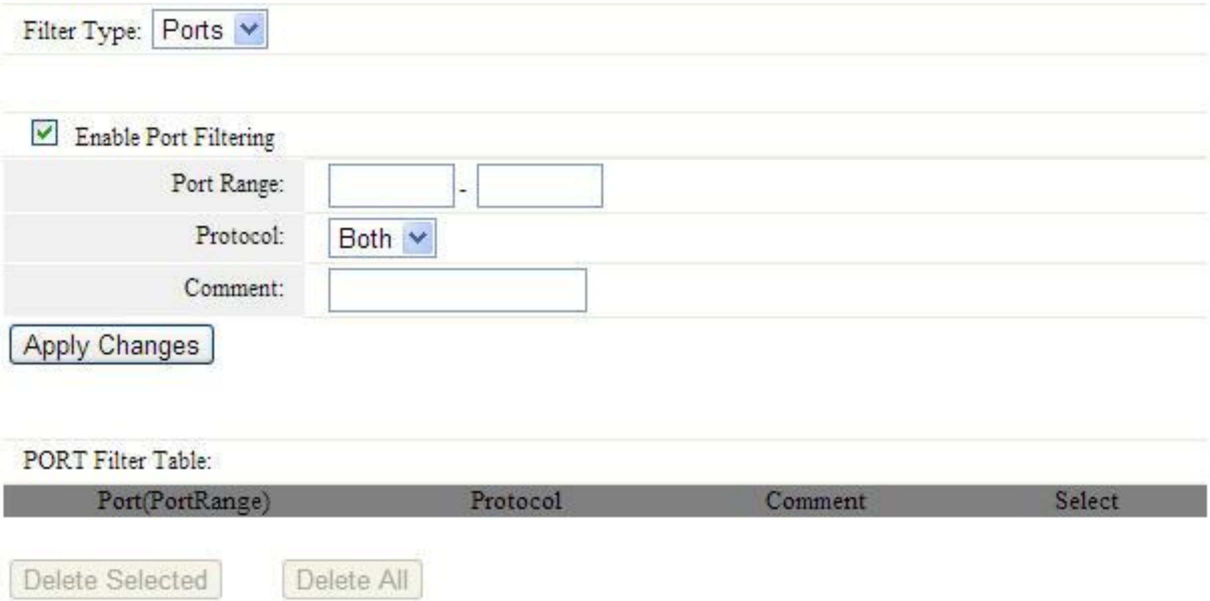
MAC Address	Comment	Select

Enable MAC Filtering: you can select this checkbox 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.

MAC Filter Table: this table will list the detailed information about the MAC addresses that will be filtered.

5.4.1.3 Port Filtering



Filter Type: Ports

☑ Enable Port Filtering

Port Range:	-
Protocol:	Both
Comment:	

PORT Filter Table:

Port(PortRange)	Protocol	Comment	Select

Enable Port Filtering: you can select this checkbox to enable Port Filtering function.

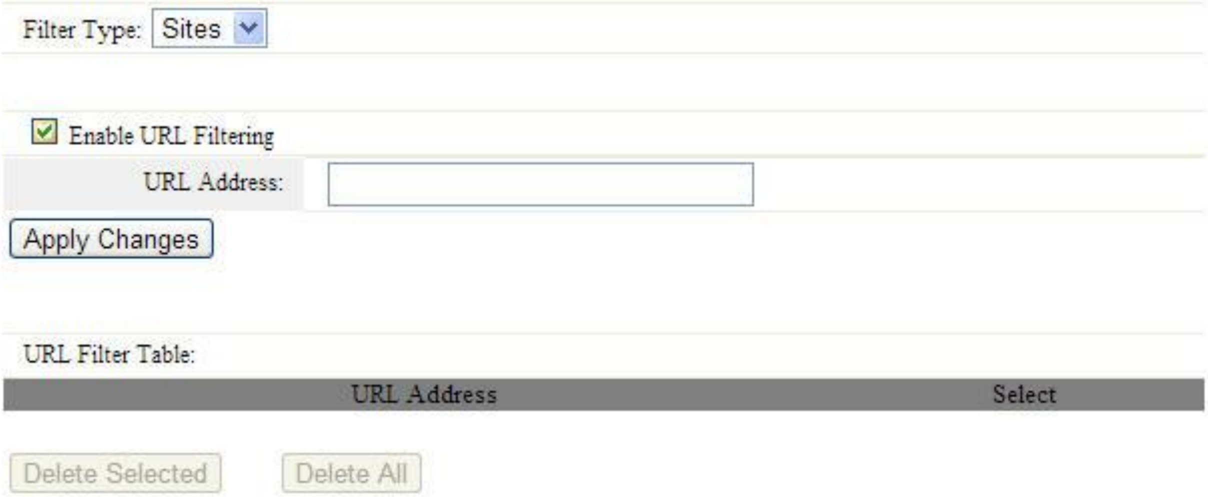
Port Range: the Port range that you want to filter.

Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.

Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP.

PORT Filter Table: this table will list the detailed information about the ports that will be filtered.

5.4.1.4 URL Filtering



Filter Type: Sites

☑ Enable URL Filtering

URL Address:	

URL Filter Table:

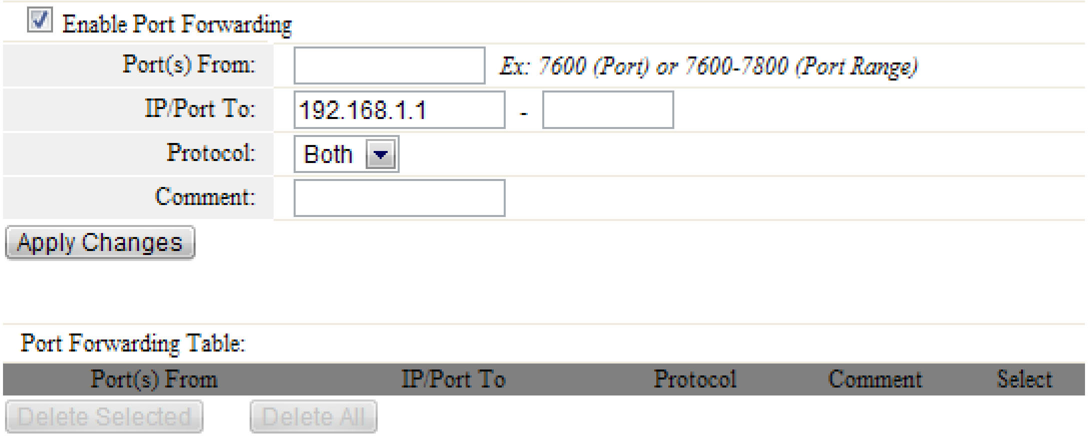
URL Address	Select

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.

URL Filter Table: this table will list the detailed information about the keywords contained in URLs that you don't allow LAN users to access.

5.4.2 Port Fowarding



☑ Enable Port Forwarding

Port(s) From: Ex: 7600 (Port) or 7600-7800 (Port Range)

IP/Port To: 192.168.1.1 -

Protocol: Both

Comment:

Port Forwarding Table:

Port(s) From	IP/Port To	Protocol	Comment	Select

Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side. 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 Port Forwarding: you can select this checkbox to enable Port Forwarding function.

Port(s) From: you can set start port that you want to forward.

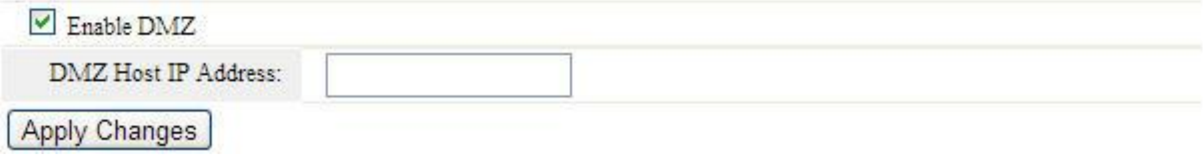
IP/Port To: set the range that you want the port forward to.

Protocol: choose which particular protocol type should be forwarding. Here you can choose UDP/TCP.

Comment: describe the reason why you want to filter the IP address. Just few words are saved there usually.

Port Forwarding Table: this table will list the detailed information about the ports that will be forwarded.

5.4.3 DMZ



☑ Enable DMZ

DMZ Host IP Address:

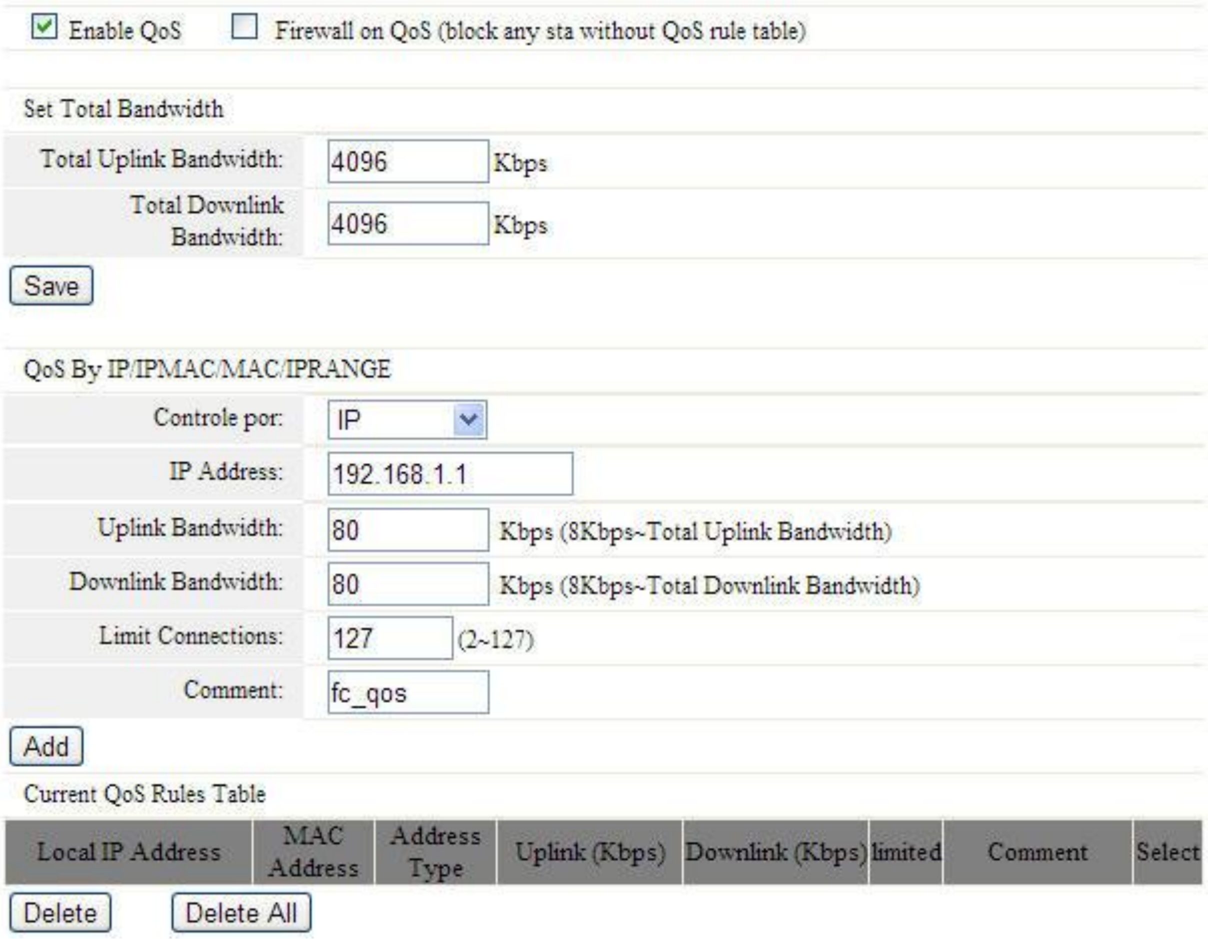
DMZ means Demilitarized Zone. It can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible form 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.

5.4.4 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. Since numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, we need QoS to control the bandwidth use. On this page, you could set the QoS rules.



☑ Enable QoS ☐ Firewall on QoS (block any sta without QoS rule table)

Set Total Bandwidth

Total Uplink Bandwidth:	4096 Kbps
Total Downlink Bandwidth:	4096 Kbps

QoS By IP/IPMAC/MAC/IPRANGE

Controle por:	IP
IP Address:	192.168.1.1
Uplink Bandwidth:	80 Kbps (8Kbps~Total Uplink Bandwidth)
Downlink Bandwidth:	80 Kbps (8Kbps~Total Downlink Bandwidth)
Limit Connections:	127 (2~127)
Comment:	fc_qos

Current QoS Rules Table

Local IP Address	MAC Address	Address Type	Uplink (Kbps)	Downlink (Kbps)	limited	Comment	Select

Enable Qos: check the box if you want to enable QoS function.

Firewall on QoS: enable firewall on QoS function for protecting the security of your network without QoS rule table.

Total Uplink Bandwidth: this option allows you to set the total uplink bandwidth. By default, it is 4096Kbps.

Total Downlink Bandwidth: this allows you to set the total downlink. By default, it is 4096Kbps as well.

QoS By IP/IPMAC/MAC/IPRANGE

Control Port: you can choose from IP, IP+MAC, MAC, IP Range, Network. Here we take IP for example.

IP Address: enter the IP address that you want to adopt this QoS rule.

Uplink Bandwidth: please set the max uplink bandwidth.

Downlink Bandwidth: please set the max downlink bandwidth.

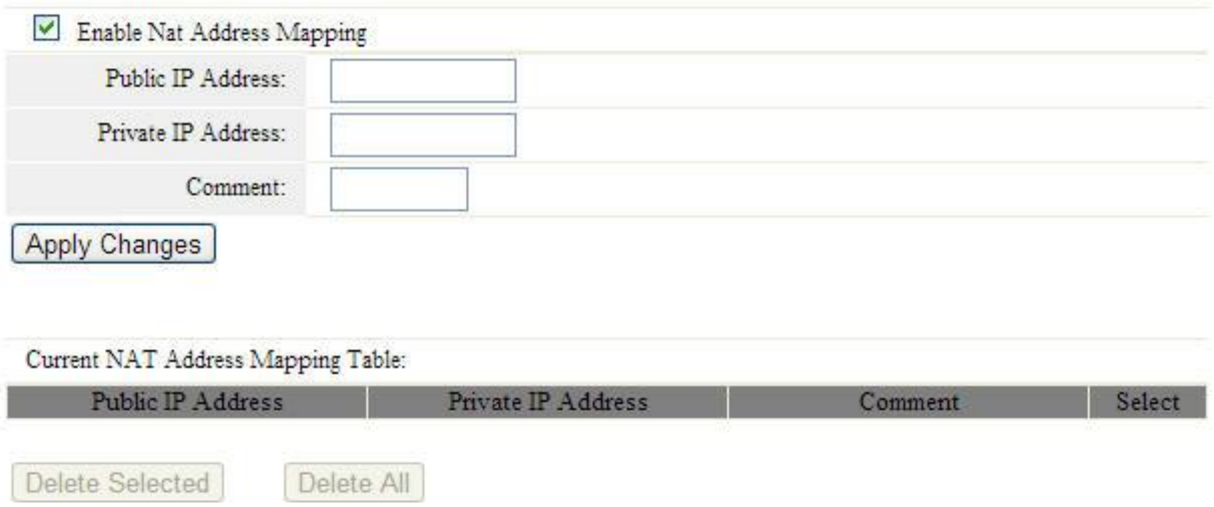
Limit Connections: please set the limit connections for your IP Address.

Comment: enter the reason why you set this QoS rule. Just a few words are ok.

Current QoS Rules Table: this table will show you the current QoS rules you have set.

5.4.5 NAT Mapping

NAT Mapping function is very useful for a domestic network with one wireless router and a few devices with private IP addresses.



☑ Enable Nat Address Mapping

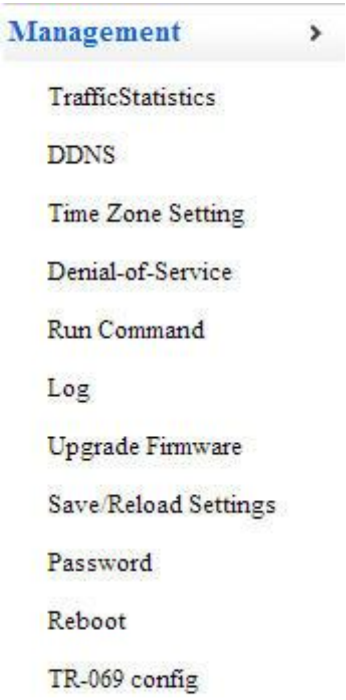
Public IP Address:	
Private IP Address:	
Comment:	

Current NAT Address Mapping Table:

Public IP Address	Private IP Address	Comment	Select

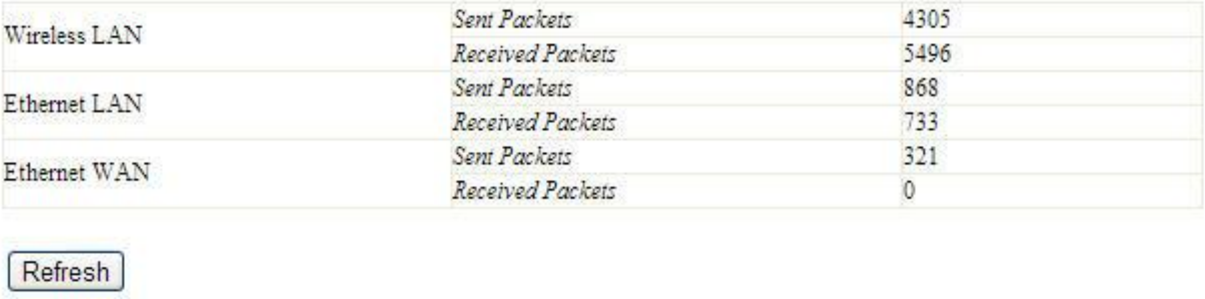
Public IP Address: enter the public IP address provided by corresponding service provider.
Private IP Address: enter the private IP address of your PC.

5.5 Management



5.5.1 Traffic Statistics

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

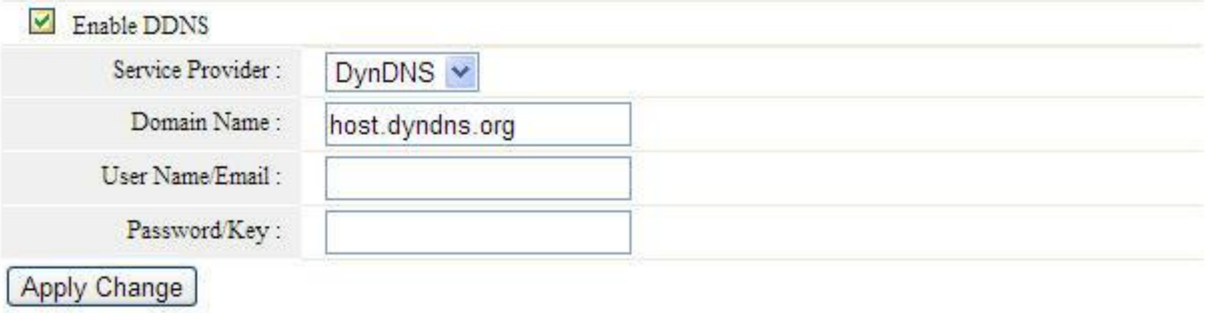


Wireless LAN	*Sent Packets*	4305
	Received Packets	5496
Ethernet LAN	*Sent Packets*	868
	Received Packets	733
Ethernet WAN	*Sent Packets*	321
	Received Packets	0

5.5.2 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. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you user the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. This router supports three service providers: DynDNS, TZO and NOIP.



☑ Enable DDNS

Service Provider :	DynDNS
Domain Name :	host.dyndns.org
User Name/Email :	
Password/Key :	

Enable DDNS: please select this checkbox to enable DDNS function.

Service Provider: choose one service provider where you have applied for free DDNS service.

Domain Name: type in the domain name you registered from the DDNS provider.

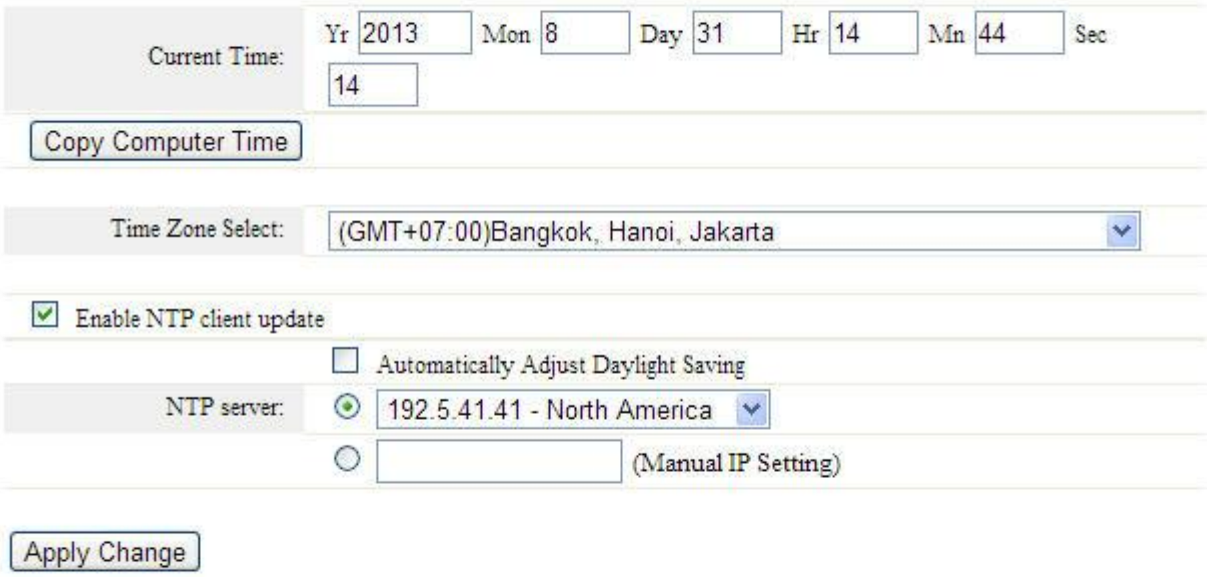
User Name/Email: enter the User Name or Email you registered from the DDNS provider.

Password/Key: enter the Password or Key you set for the User Name.

Click **Apply Change** to finish the setting.

5.5.3 Time Zone Setting

This page allows you to maintain the system time by synchronizing with a public time server over the Internet. All the parameters setting please refer to **Quick Setup**.



Current Time: Yr 2013 Mon 8 Day 31 Hr 14 Mn 44 Sec 14

Copy Computer Time

Time Zone Select: (GMT+07:00)Bangkok, Hanoi, Jakarta

☑ Enable NTP client update

☐ Automatically Adjust Daylight Saving

NTP server: ● 192.5.41.41 - North America

○ (Manual IP Setting)

Apply Change

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 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 Daylight Saving: if the Time Zone you choose implements daylight saving time, please select this option.

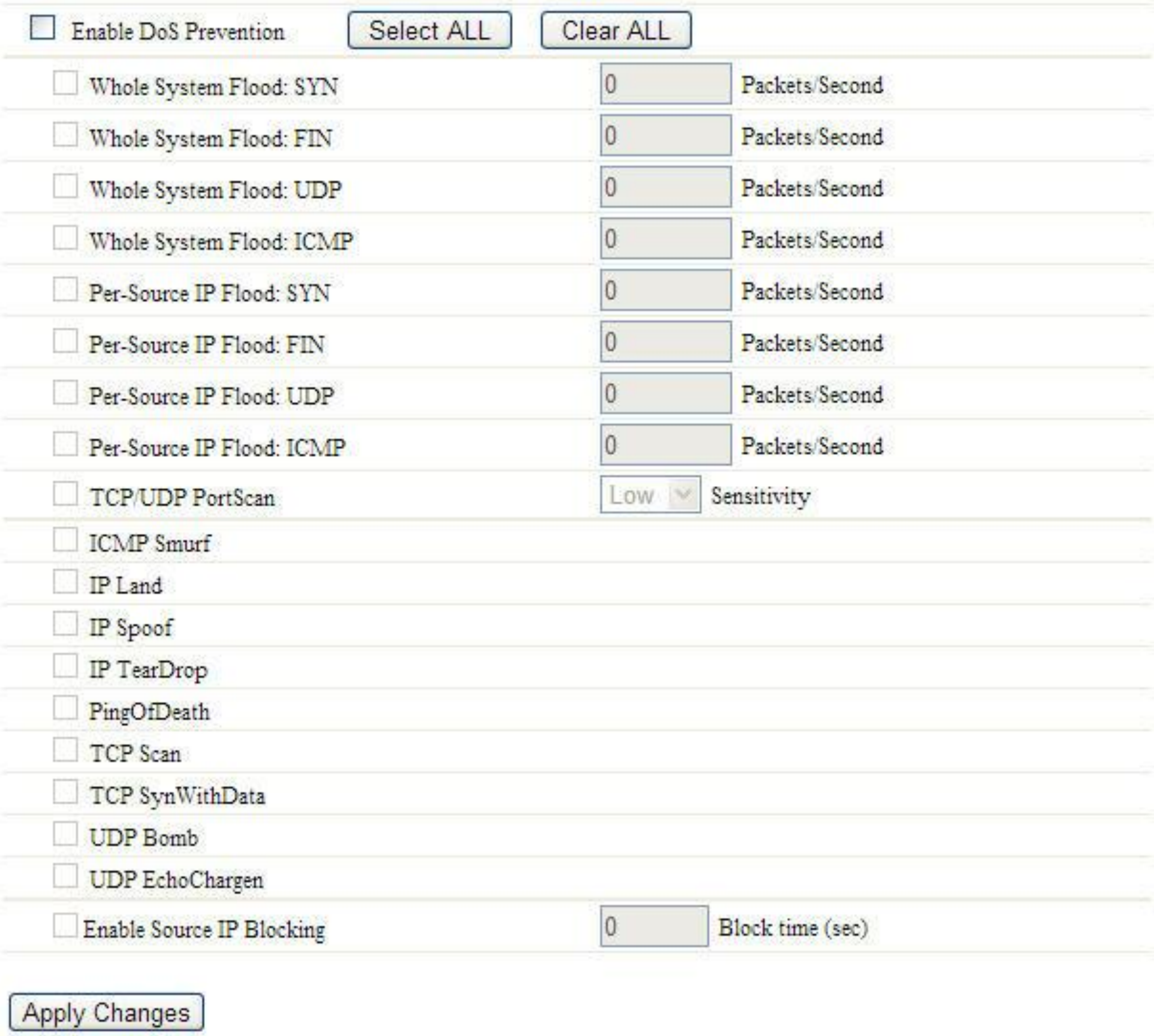
NTP server: Please choose the corresponding NTP server to get right time.

5.5.4 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.

The DoS Prevention function enables the router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also this router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an

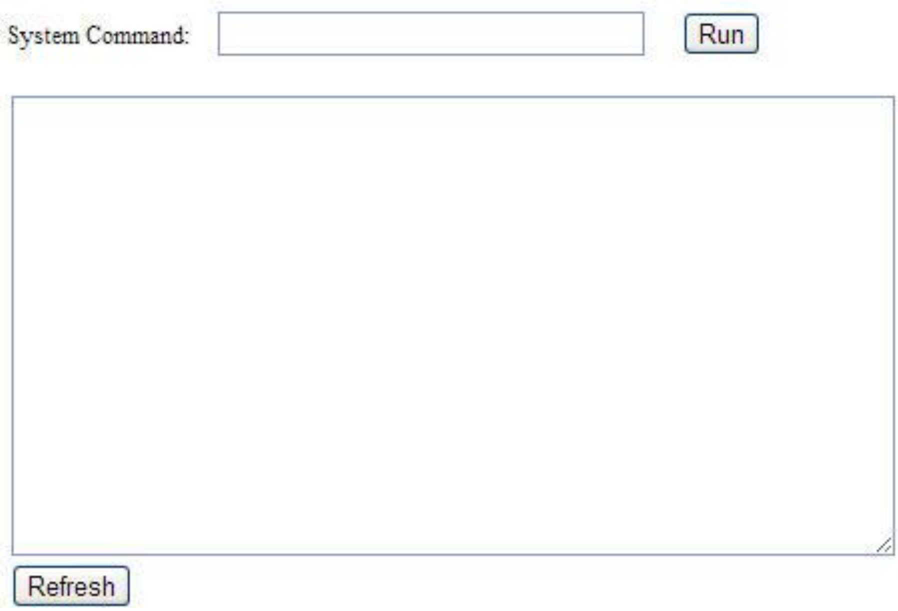


□ Enable DoS Prevention [Select ALL] [Clear ALL]

□ 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)

5.5.5 Run Command

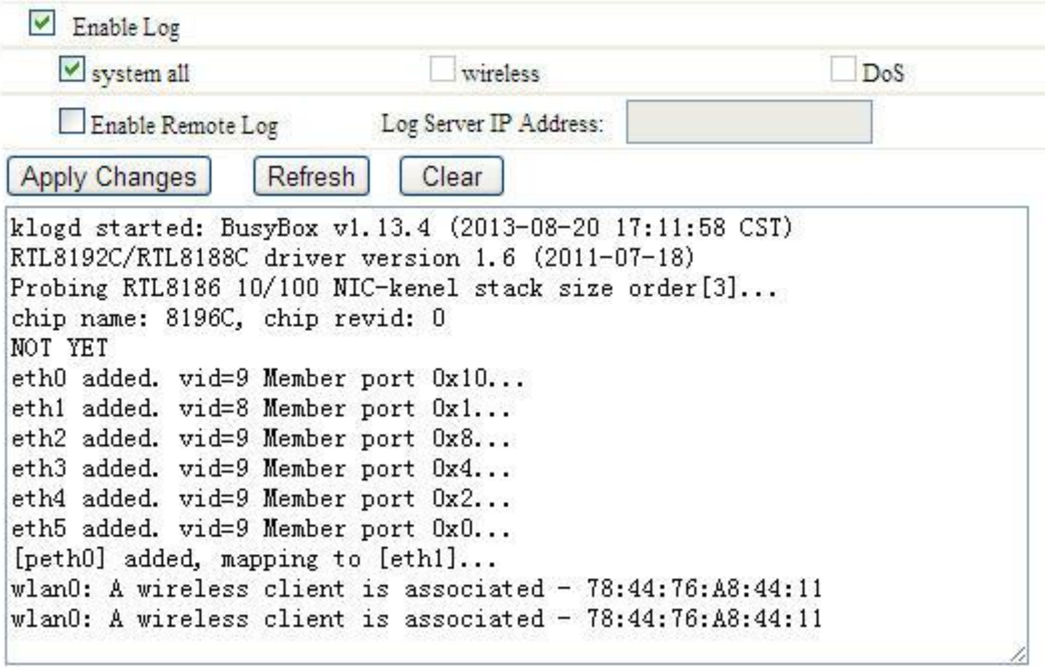
You can run system command in this page, just enter the command in the System Command bar and click Run button.



System Command:

5.5.6 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:

```
klogd started: BusyBox v1.13.4 (2013-08-20 17:11:58 CST)
RTL8192C/RTL8188C driver version 1.6 (2011-07-18)
Probing RTL8186 10/100 NIC-kenel stack size order[3]...
chip name: 8196C, chip revid: 0
NOT YET
eth0 added. vid=9 Member port 0x10...
eth1 added. vid=8 Member port 0x1...
eth2 added. vid=9 Member port 0x8...
eth3 added. vid=9 Member port 0x4...
eth4 added. vid=9 Member port 0x2...
eth5 added. vid=9 Member port 0x0...
[peth0] added, mapping to [eth1]...
wlan0: A wireless client is associated - 78:44:76:A8:44:11
wlan0: A wireless client is associated - 78:44:76:A8:44:11
```

Enable Log: this option enables the registration routine of the system log messages. By default it is disabled. Below items including system all, wireless, Dos allows you to choose the log type.

Enable Remote Log: enables the system log remote sending function while System log messages are sent to a remote server.

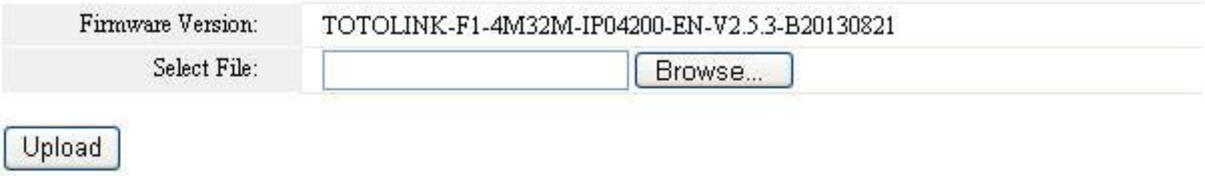
Log Server IP Address: this is the host IP address where system log messages should be sent.

After finished, please click **Apply Changes** to go to next part.

5.5.7 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.



Firmware Version: TOTOLINK-F1-4M32M-IP04200-EN-V2.5.3-B20130821

Select File:

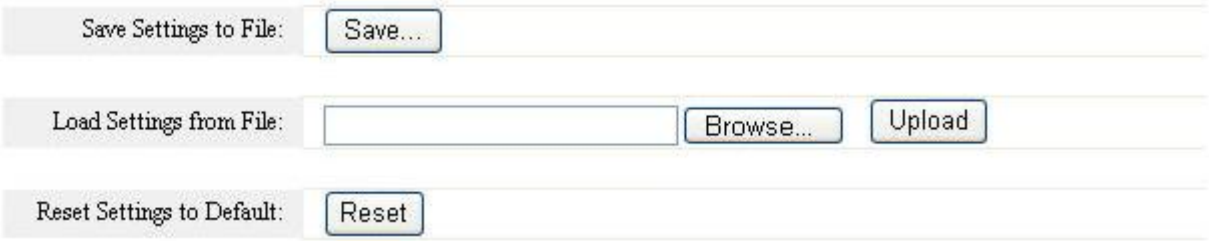
Firmware version: shows the current firmware version.

Select File: click Browse button to select the firmware version you want to upgrade on your computer.

Click **Upload** to upgrade the firmware version.

5.5.8 Save/Reload Setting

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.

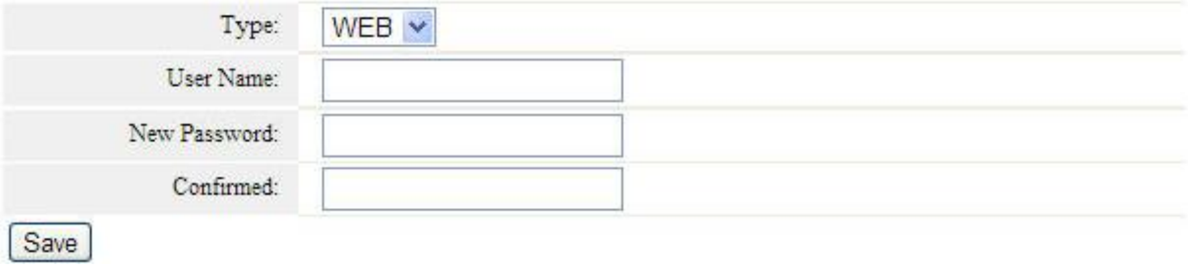


Save Settings to File: click **Save…** button to download the current settings of the Access Point to your computer.

Load Settings to File: if you want to reload the settings from the file saved before, you could click **Choose File** button to choose the right file then click **Upload** button.

Reset Settings to Default: this **Reset** button is provided to allow you to restore the router settings to the default factory settings.

5.5.9 Password



Type: WEB

Type: here you can choose WEB and SSH. If you choose SSH, you don't need to enter the User Name.

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.

Confirmed: new password should be re-entered to verify its accuracy.

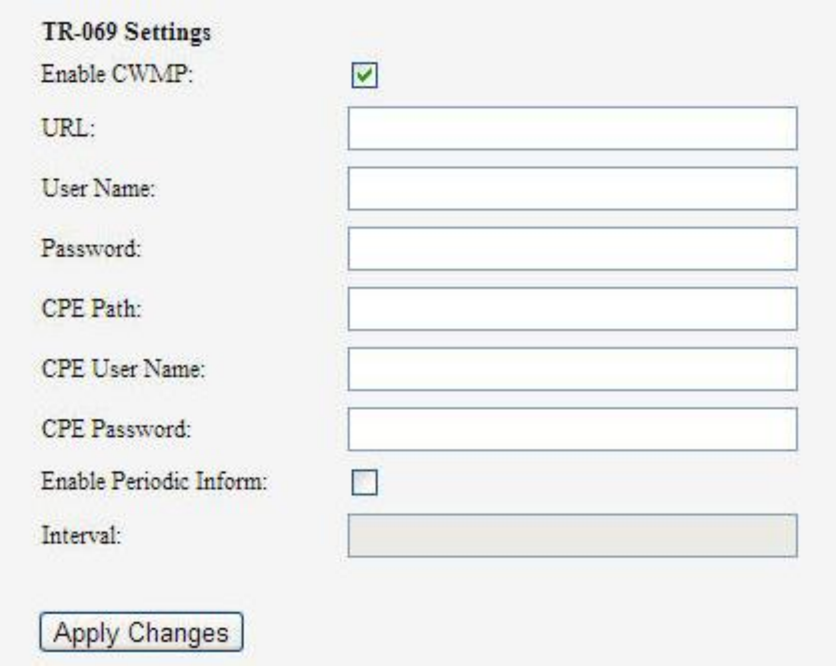
> ***Note:*** *password length is 8 characters maximum, characters after the 8th position will be truncated.*

5.5.10 Reboot

You can just click **Reboot** to restore the router to default factory setting.

5.5.11 TR-069 Config

TR-069 stands for CPE WAN Management Protocol. It is a protocol for communication between Customer Premise Equipment (CPE) and Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions within a common framework. On this page you can configure the TR-069 CPE and change the setting of ACS.



TR-069 Settings

Enable CWMP: ☑

URL:

User Name:

Password:

CPE Path:

CPE User Name:

CPE Password:

Enable Periodic Inform: □

Interval:

Enable CWMP: you can enable or disable this function.

URL: Enter the website of ACS which is provided by your ISP.

User Name: Enter the User Name to login the ACS server.

Password: Enter the password to login the ACS server.

CPE Path: Enter the path that connects to the ACS server.

CPE User Name: enter the CPE Connection Request User Name.

CPE Password: enter CPE Connection Request Password**.**

Enable Periodic inform: if enabled, the information will be informed to ACS server periodically.

Interval: Set the interval time.