Table of Contents

Copyright Statement

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

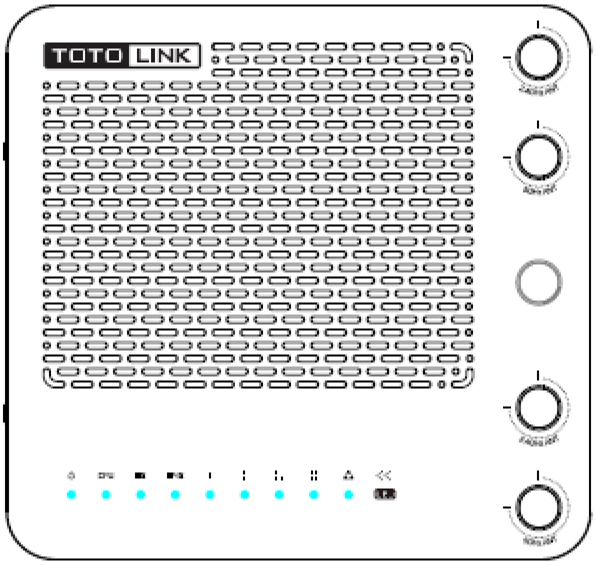
- Complies with IEEE 802.11ac/a/b/g/n standards.
- Delivers 300Mbps data rate on 2.4GHz and 867Mbps on 5GHz simultaneously.
- Advanced MIMO technology ensures greater range and increasing throughput.
- Supports DHCP, Static IP, PPPoE, PPTP and L2TP broadband functions.
- Supports dual access while WAN type is PPPoE, PPTP or L2TP.
- Provides 64/128-bit WEP, WPA, WPA2 and WPA/WPA2(TKIP+AES) security.
- Connects to secure network easily and fast using WPS (one-button).
- Supports IP, MAC, URL filtering and Port Forwarding.

- Universal repeater and WDS make WiFi extension simple.

2.3 Panel Layout

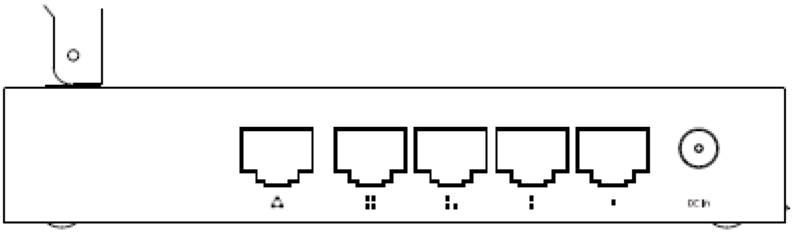
2.3.1 Front Panel

The front panel of this router consists of 10 LEDs, which is designed to indicate connection status.



POWER	This indicator lights blue when the router powered on, otherwise it is off.
CPU	When the router powered on, this indicator keeps lighting blue.
2.4G	This indicator lights blue when the 2.4G wireless connection enabled.
5G	This indicator lights blue when the 5G wireless connection enabled.
WAN	When the WAN port is connected successfully the indicator lights blue.
	While transmitting or receiving data through the WAN port the indicator blinks blue.
1/2/3/4 LAN	When the LAN port has a successful connection, the indicator lights blue.
	While transmitting or receiving data through the LAN port the indicator blinks blue.

The figure below shows the rear panel of this router.



DC IN	This socket is used to connect the power adapter.
ON/OFF	This slide switch is used to power on or off the wireless router.
1/2/3/4 LAN	This port is used to connect the router to local PC.
WAN	This port is used to connect the router to the Internet.
RST-WPS	There is a RST-WPS button on the rear panel. Press the button for more than 5 seconds, the router will restore factory settings. If press the button less than 5 seconds, the router will establish Wi-Fi protected settings automatically.

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.

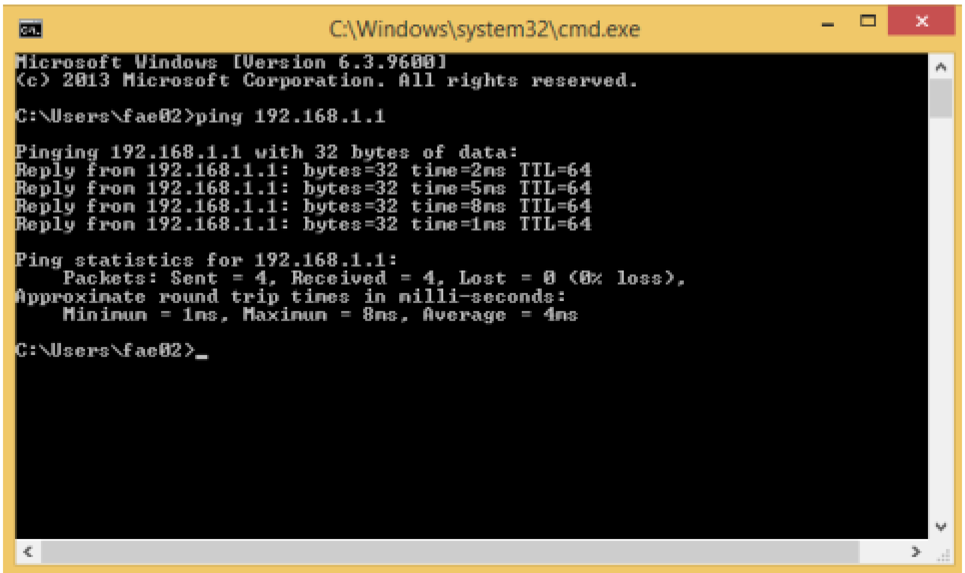
- **Configure the IP address manually**

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.

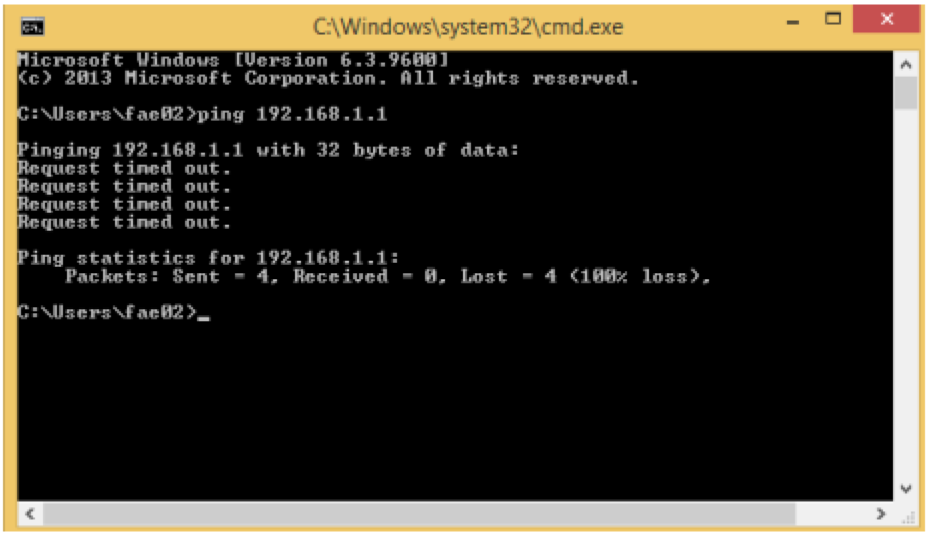
Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. Open a command prompt, and type in **ping 192**.168.1.1, then press Enter.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\fae02>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=8ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 4ms

C:\Users\fae02>_
```

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.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\fae02>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:\Users\fae02>_
```

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?

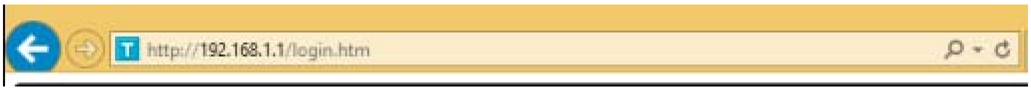
Since the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

4. CONNECTING TO INTERNET

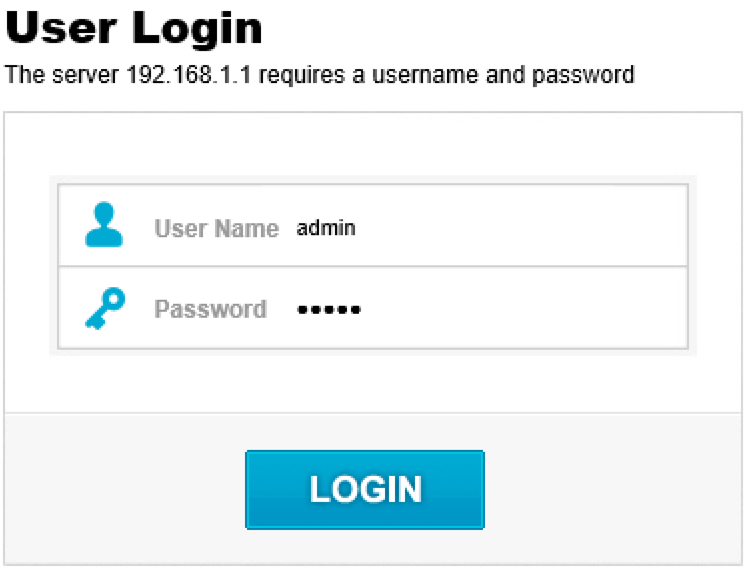
This chapter introduces how to configure the basic functions of your router so that you can surf the Internet.

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.



User Login

The server 192.168.1.1 requires a username and password

User Name admin

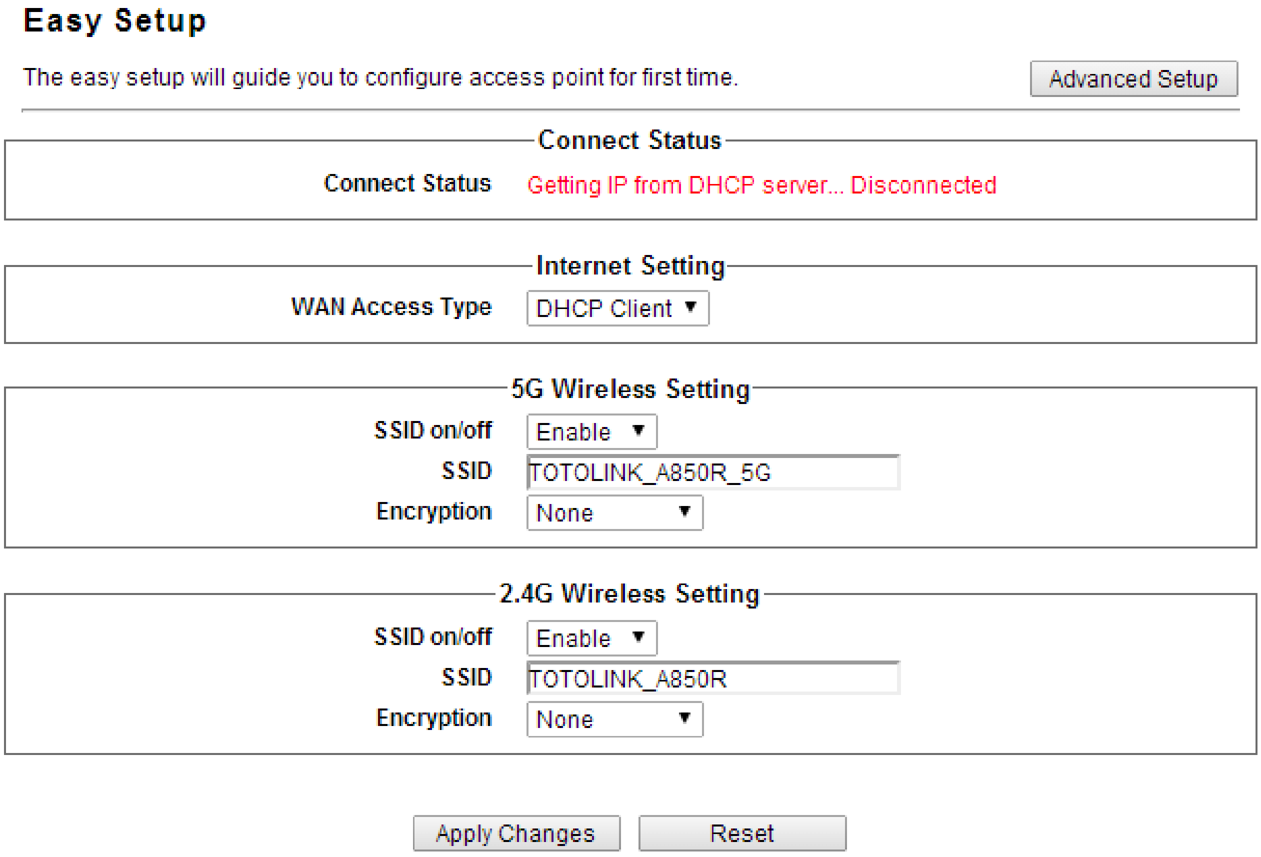
Password ●●●●●

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.



Easy Setup

The easy setup will guide you to configure access point for first time.

Connect Status

Connect Status Getting IP from DHCP server... Disconnected

Internet Setting

WAN Access Type DHCP Client

5G Wireless Setting

SSID on/off Enable

SSID TOTOLINK_A850R_5G

Encryption None

2.4G Wireless Setting

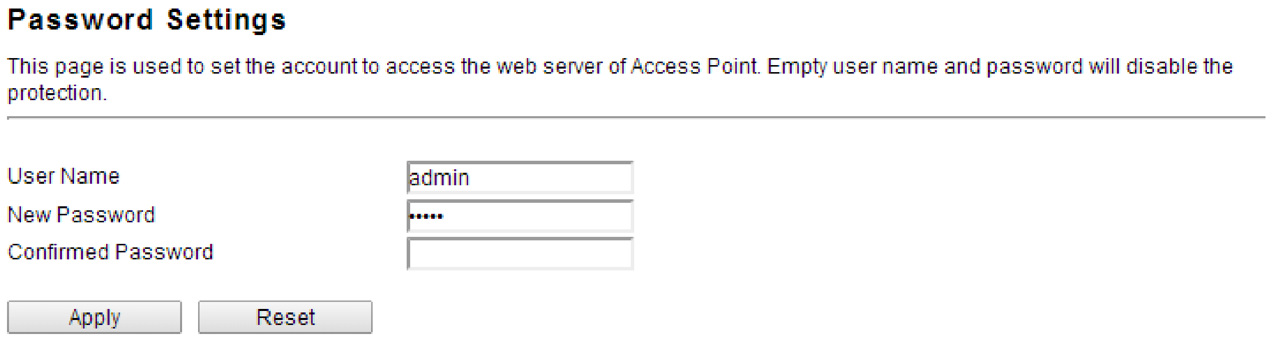
SSID on/off Enable

SSID TOTOLINK_A850R

Encryption None

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.



Password Settings

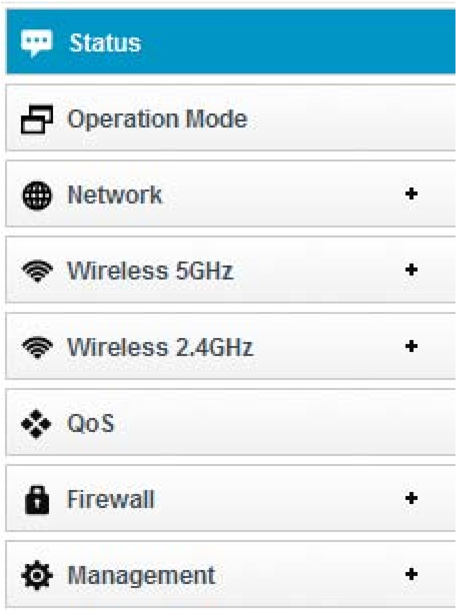
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name	admin
New Password	•••••
Confirmed Password	

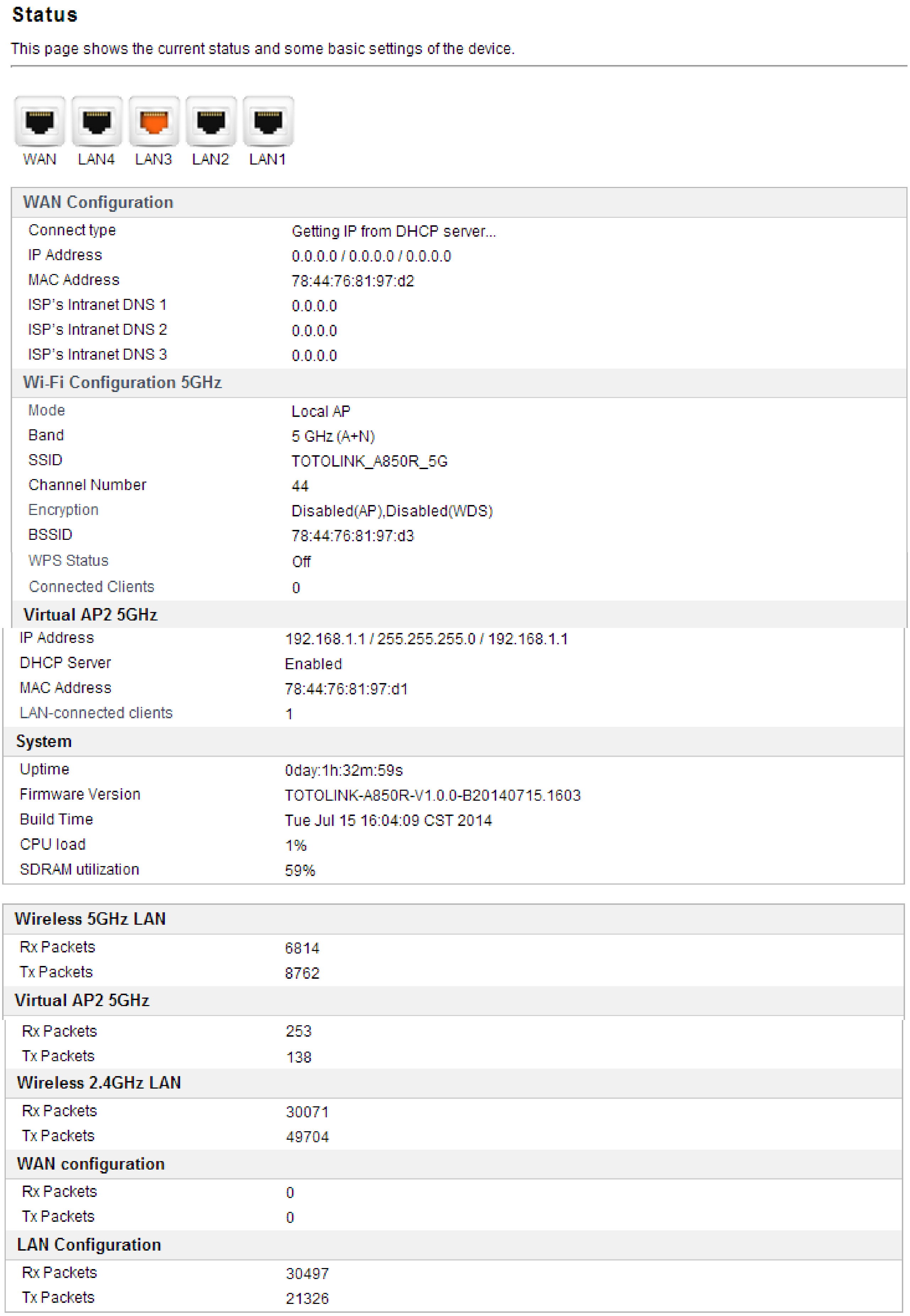
User Name: type in the name that you use to login the web interface of the router.
New Password: new password is used for administrator authentication.
Confirm Password: new password should be re-entered to verify its accuracy.

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

4.3 Status



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



Status

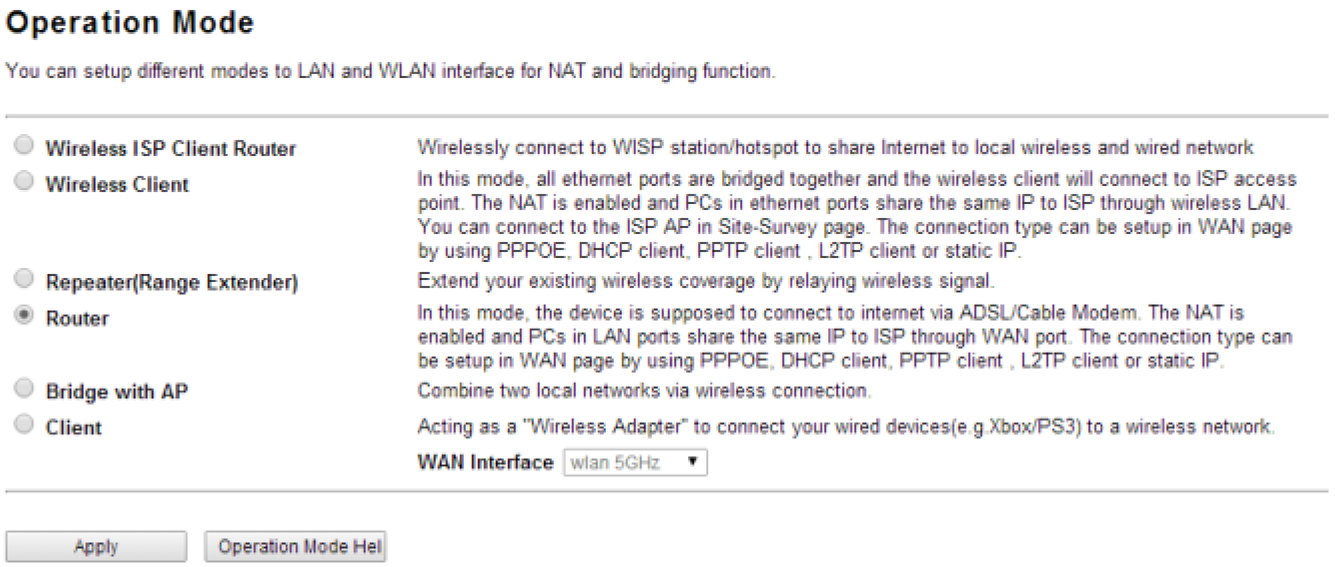
This page shows the current status and some basic settings of the device.

WAN Configuration	
Connect type	Getting IP from DHCP server...
IP Address	0.0.0.0 / 0.0.0.0 / 0.0.0.0
MAC Address	78:44:76:81:97:d2
ISP's Intranet DNS 1	0.0.0.0
ISP's Intranet DNS 2	0.0.0.0
ISP's Intranet DNS 3	0.0.0.0
Wi-Fi Configuration 5GHz	
Mode	Local AP
Band	5 GHz (A+N)
SSID	TOTOLINK_A850R_5G
Channel Number	44
Encryption	Disabled(AP),Disabled(WDS)
BSSID	78:44:76:81:97:d3
WPS Status	Off
Connected Clients	0
Virtual AP2 5GHz	
IP Address	192.168.1.1 / 255.255.255.0 / 192.168.1.1
DHCP Server	Enabled
MAC Address	78:44:76:81:97:d1
LAN-connected clients	1
System	
Uptime	0day:1h:32m:59s
Firmware Version	TOTOLINK-A850R-V1.0.0-B20140715.1603
Build Time	Tue Jul 15 16:04:09 CST 2014
CPU load	1%
SDRAM utilization	59%

Wireless 5GHz LAN	
Rx Packets	6814
Tx Packets	8762
Virtual AP2 5GHz	
Rx Packets	253
Tx Packets	138
Wireless 2.4GHz LAN	
Rx Packets	30071
Tx Packets	49704
WAN configuration	
Rx Packets	0
Tx Packets	0
LAN Configuration	
Rx Packets	30497
Tx Packets	21326

4.4 Operation Mode

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



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

○ Wireless ISP Client Router — Wirelessly connect to WISP station/hotspot to share Internet to local wireless and wired network

○ Wireless Client — 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 can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

○ Repeater(Range Extender) — Extend your existing wireless coverage by relaying wireless signal.

● Router — 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, PPTP client , L2TP client or static IP.

○ Bridge with AP — Combine two local networks via wireless connection.

○ Client — Acting as a "Wireless Adapter" to connect your wired devices(e.g.Xbox/PS3) to a wireless network.

WAN Interface: wlan 5GHz ▼

1. Wireless ISP Client Router
In this mode, it will wirelessly connect to WISP station/hotspot to share Internet to local wireless and wired network.

2. Wireless Client
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 can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

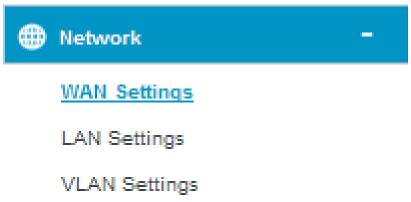
3. Repeater (Range Extender)
In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners. It is good for extending your existing wireless coverage by relaying wireless signal.

4. Router
In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The Wireless port share the same IP to ISP through Ethernet WAN port .The Wireless port acts the same as a LAN port while at AP Router mode. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

5. Bridge with AP
In this mode, the device can be used to combine multiple local networks together to the same one via wireless connections, especially for a home or office where separated networks can’t be connected easily together with a cable.

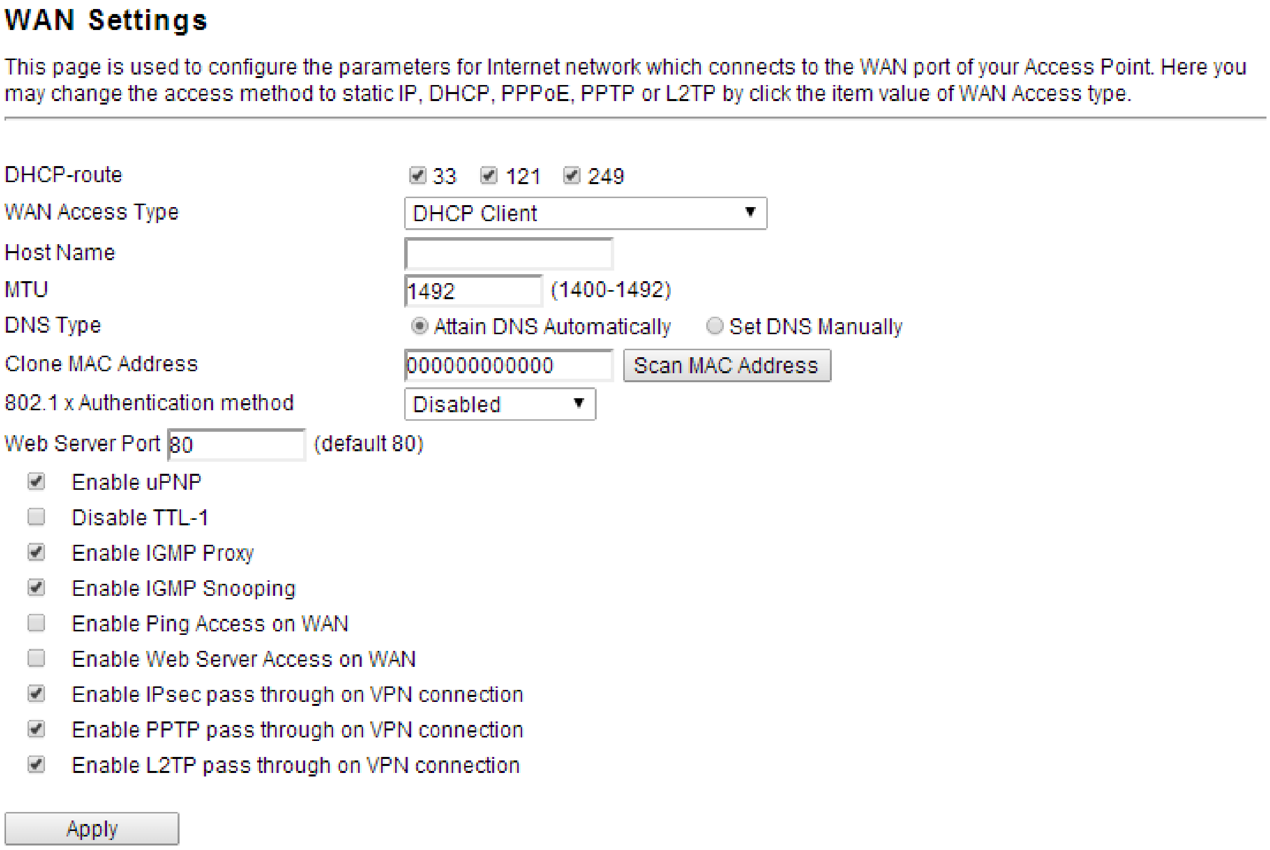
6. Client
In this mode, the device can be connected to another device via Ethernet port and act as a "Wireless Adapter" to connect your wired device to a wireless network.

4.5 Network



4.5.1 WAN Settings

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



WAN Settings

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

DHCP-route	☑ 33 ☑ 121 ☑ 249
WAN Access Type	DHCP Client ▼
Host Name	
MTU	1492 (1400-1492)
DNS Type	● Attain DNS Automatically ○ Set DNS Manually
Clone MAC Address	000000000000 Scan MAC Address
802.1 x Authentication method	Disabled ▼

Web Server Port 80 (default 80)

☑ Enable uPNP
□ Disable TTL-1
☑ 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 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.

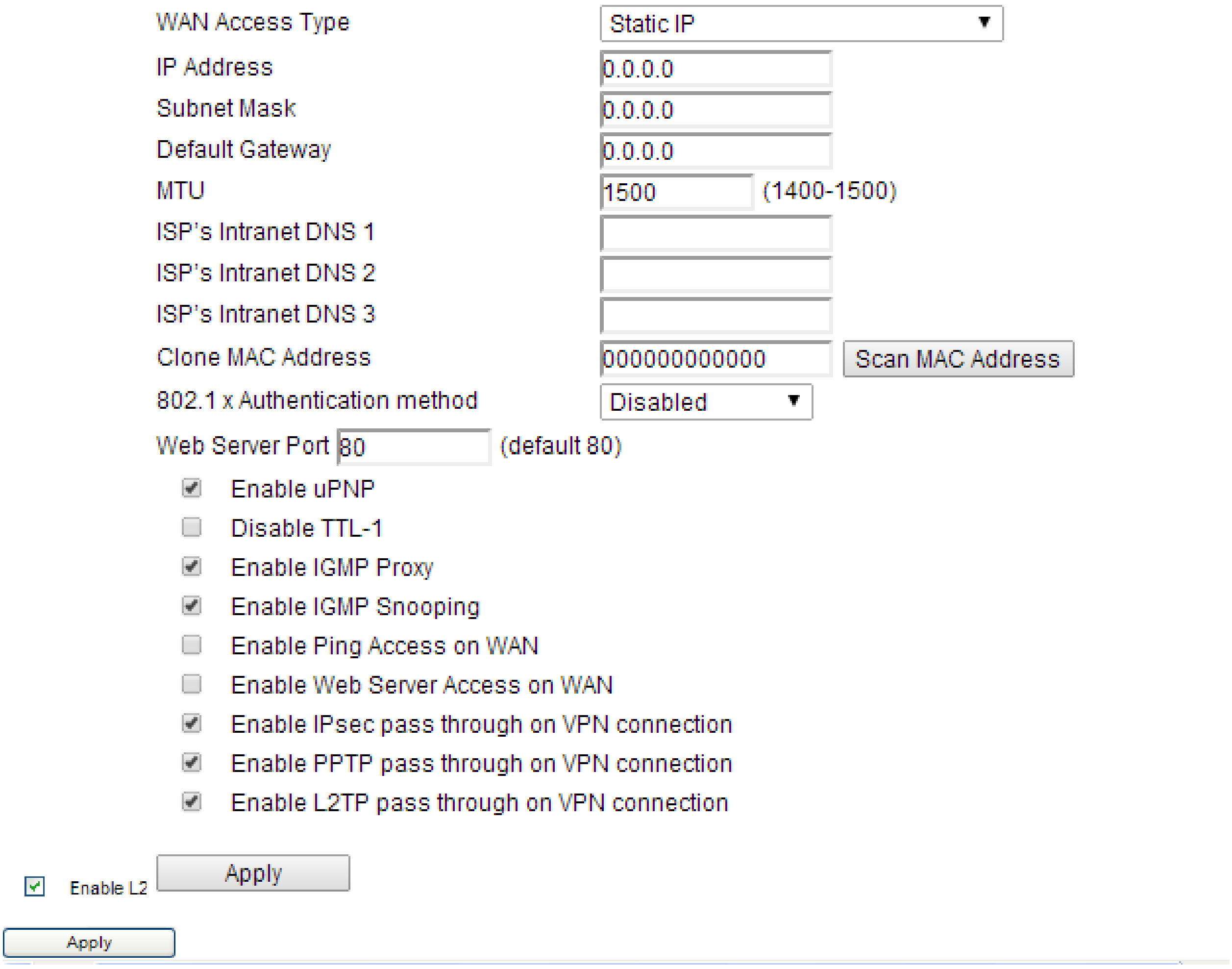
Enable PPTP pass through on VPN connection: PPTP pass through is a technique for allowing PPTP packets to pass through a NAT router.

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

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.



WAN Access Type	Static IP ▼
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MTU	1500 (1400-1500)
ISP's Intranet DNS 1	
ISP's Intranet DNS 2	
ISP's Intranet DNS 3	
Clone MAC Address	000000000000 Scan MAC Address
802.1 x Authentication method	Disabled ▼

Web Server Port 80 (default 80)

☑ Enable uPNP

□ Disable TTL-1

☑ 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 L2 Apply

Apply

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.

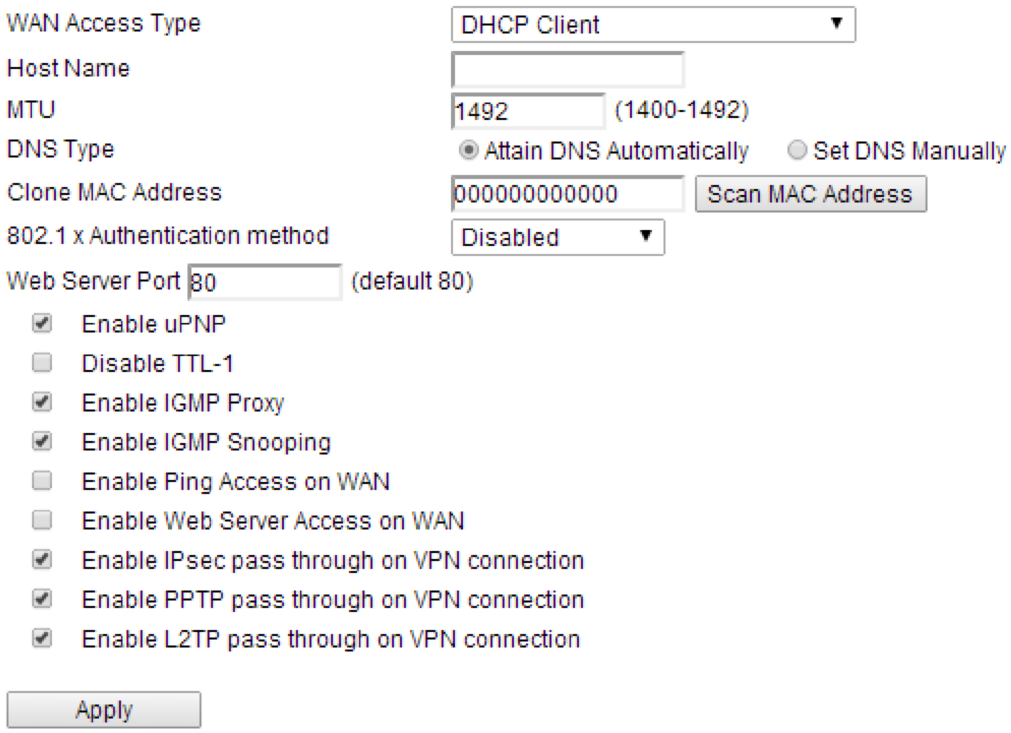
Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination 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.



WAN Access Type	DHCP Client ▼
Host Name	
MTU	1492 (1400-1492)
DNS Type	● Attain DNS Automatically ○ Set DNS Manually
Clone MAC Address	000000000000 Scan MAC Address
802.1 x Authentication method	Disabled ▼

Web Server Port 80 (default 80)

☑ Enable uPNP

☐ Disable TTL-1

☑ 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

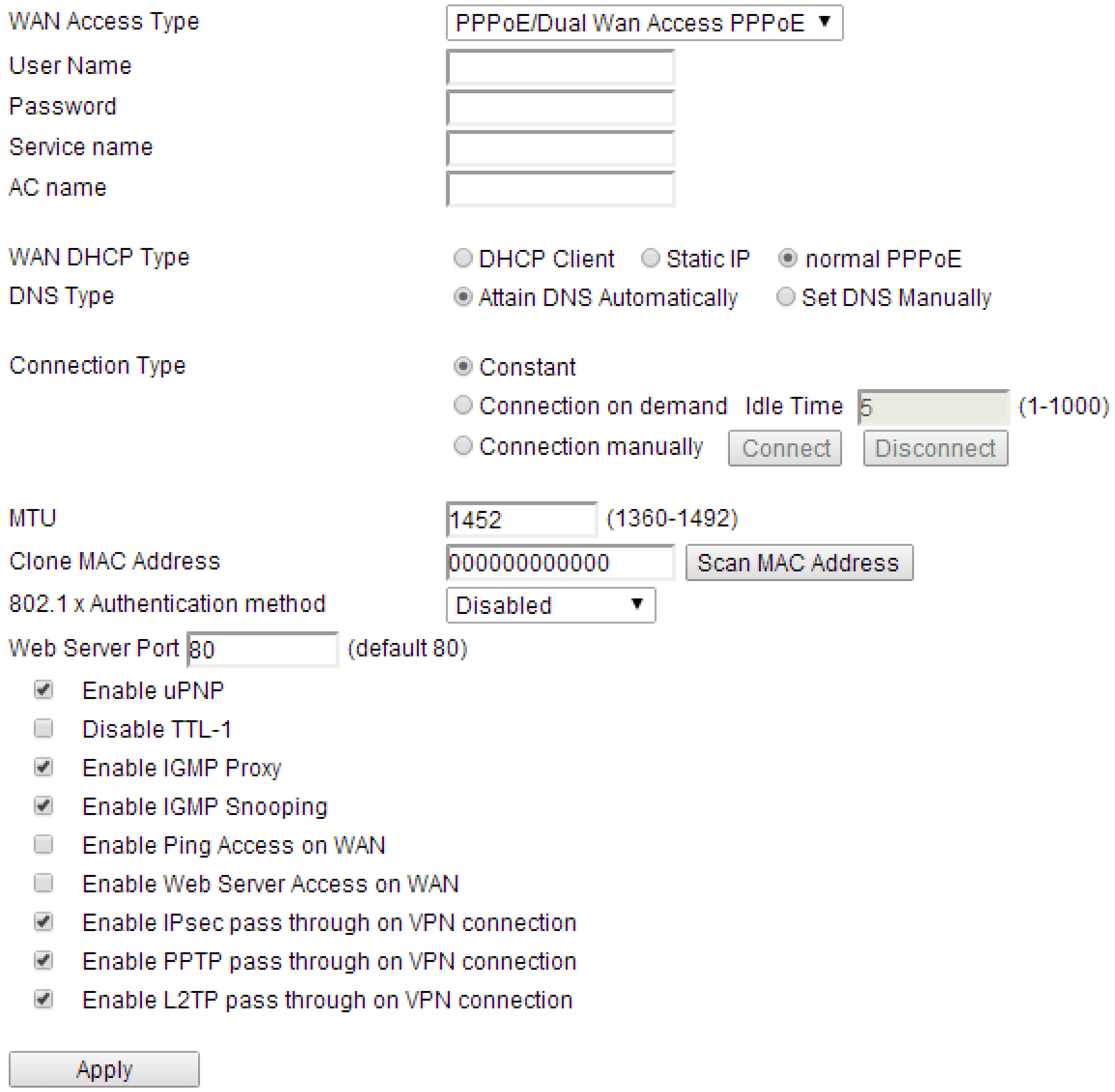
Host Name: the name of your computer, online neighbors will identify the computer according to the name.

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.



WAN Access Type	PPPoE/Dual Wan Access PPPoE ▼
User Name	
Password	
Service name	
AC name	
WAN DHCP Type	○ DHCP Client ○ Static IP ● normal PPPoE
DNS Type	● Attain DNS Automatically ○ Set DNS Manually
Connection Type	● Constant ○ Connection on demand Idle Time 5 (1-1000) ○ Connection manually Connect Disconnect
MTU	1452 (1360-1492)
Clone MAC Address	000000000000 Scan MAC Address
802.1 x Authentication method	Disabled ▼

Web Server Port 80 (default 80)

☑ Enable uPNP

□ Disable TTL-1

☑ 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

Apply

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.

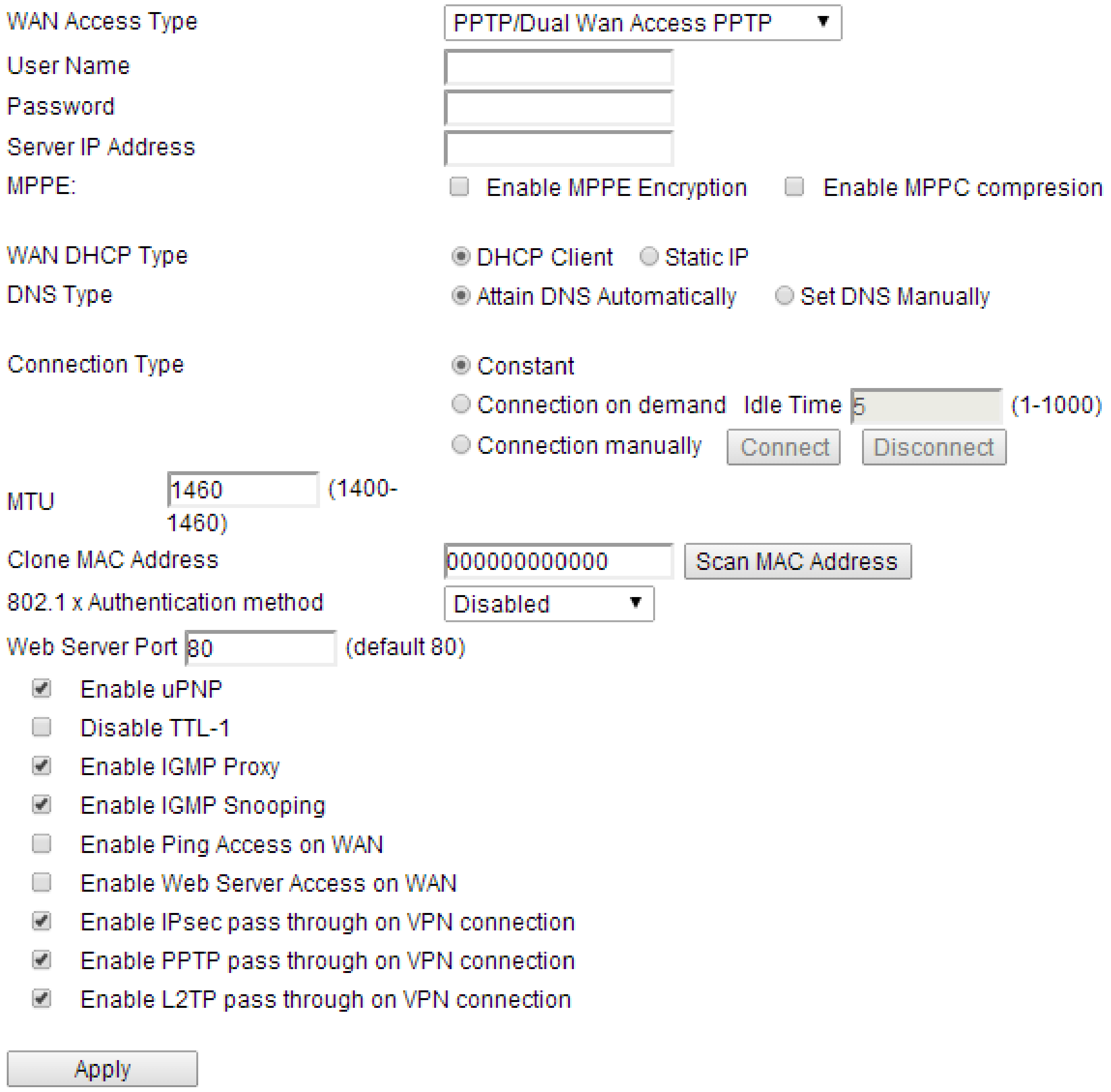
- **Continuous**: the connection can be re-established automatically.
- **Connection on demand**: the Internet connection can be terminated automatically after a specified inactivity period (idle time).
- **Manual:** you can click **Connect** or **Disconnect** button to connect/disconnect immediately.

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.

4.5.1.4 PPTP

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



WAN Access Type: PPTP/Dual Wan Access PPTP ▼

User Name:

Password:

Server IP Address:

MPPE: □ Enable MPPE Encryption □ Enable MPPC compresion

WAN DHCP Type: ● DHCP Client ○ Static IP

DNS Type: ● Attain DNS Automatically ○ Set DNS Manually

Connection Type: ● Constant
○ Connection on demand Idle Time 5 (1-1000)
○ Connection manually [Connect] [Disconnect]

MTU 1460 (1400-1460)

Clone MAC Address 000000000000 [Scan MAC Address]

802.1 x Authentication method: Disabled ▼

Web Server Port 80 (default 80)

☑ Enable uPNP
□ Disable TTL-1
☑ 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

[Apply]

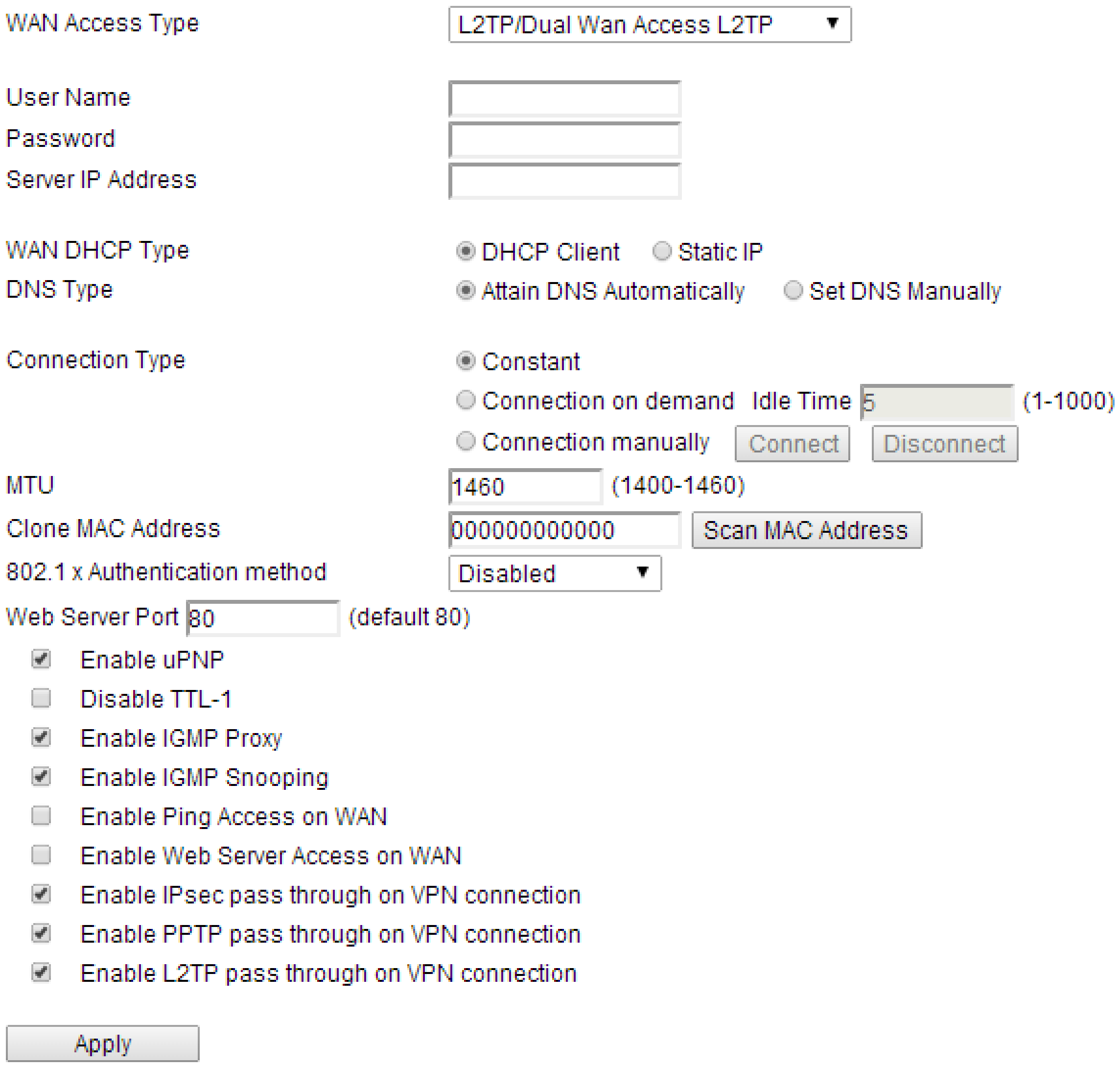
MPPE: You can enable MPPE Encryption or MPPC compression here. MPPE provides link encryption. Link encryption encrypts data as it passes between the calling and answering routers. MPPC provides a method to negotiate and utilize compression protocols over PPP encapsulated links.

WAN DHCP type: it's available only for PPTP connection. If your ISP provides an extra type to connect to a local area network such as **DHCP Client/Static IP**, you should select the type and enter the right parameters provided by ISP to enable the secondary connection.

DNS Type: 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 while you select the DHCP client mode. Besides, it is Set DNS type while you select the Static IP.

4.5.1.5 L2TP

You should select L2TP option if ISP provides a L2TP connection and enter the following parameters. Please refer to PPPoE configuration if there are the same parameters.



WAN Access Type: L2TP/Dual Wan Access L2TP ▼

User Name:

Password:

Server IP Address:

WAN DHCP Type: ● DHCP Client ○ Static IP

DNS Type: ● Attain DNS Automatically ○ Set DNS Manually

Connection Type: ● Constant
○ Connection on demand Idle Time 5 (1-1000)
○ Connection manually [Connect] [Disconnect]

MTU: 1460 (1400-1460)

Clone MAC Address: 000000000000 [Scan MAC Address]

802.1 x Authentication method: Disabled ▼

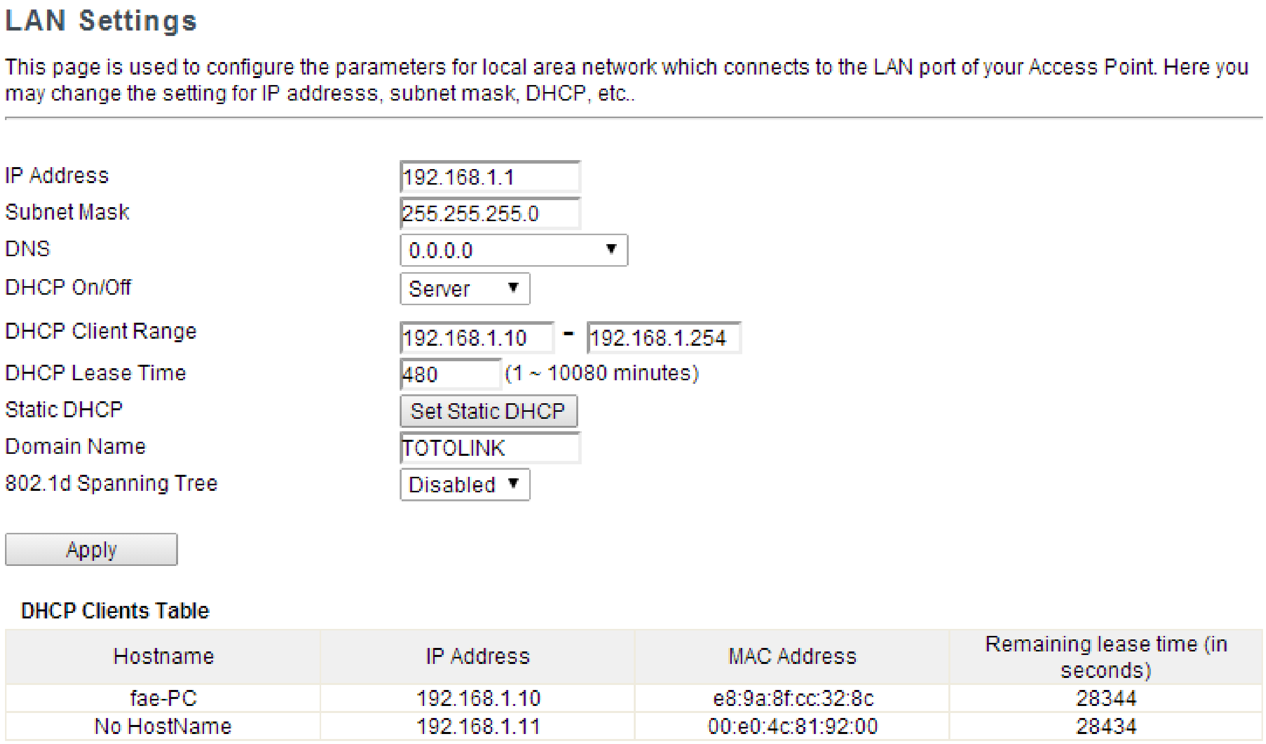
Web Server Port 80 (default 80)

☑ Enable uPNP
□ Disable TTL-1
☑ 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

[Apply]

4.5.2 LAN Settings

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 Settings

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

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DNS	0.0.0.0 ▼
DHCP On/Off	Server ▼
DHCP Client Range	192.168.1.10 - 192.168.1.254
DHCP Lease Time	480 (1 ~ 10080 minutes)
Static DHCP	Set Static DHCP
Domain Name	TOTOLINK
802.1d Spanning Tree	Disabled ▼

DHCP Clients Table

Hostname	IP Address	MAC Address	Remaining lease time (in seconds)
fae-PC	192.168.1.10	e8:9a:8f:cc:32:8c	28344
No HostName	192.168.1.11	00:e0:4c:81:92:00	28434

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.

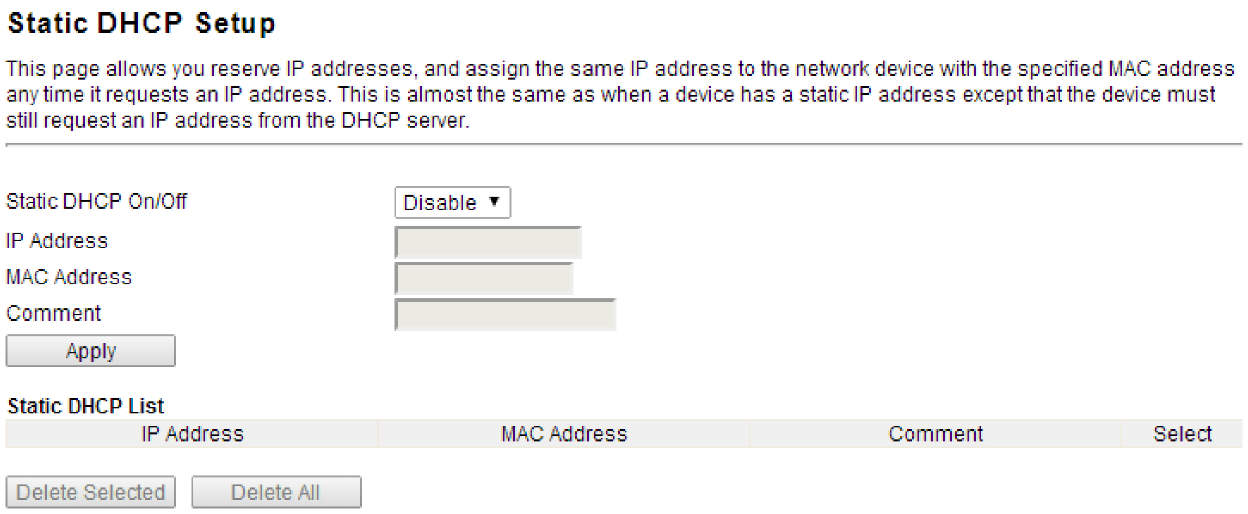
DHCP Client Range: the range of IP addresses that will be assigned to each computer connected with the router.

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.

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.



Static DHCP Setup

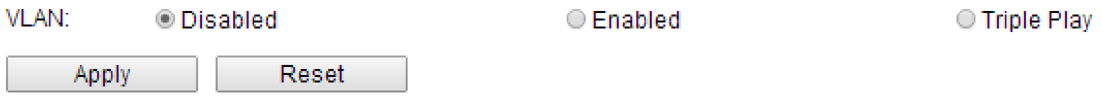
This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

Static DHCP On/Off	Disable ▼
IP Address	
MAC Address	
Comment	

Static DHCP List

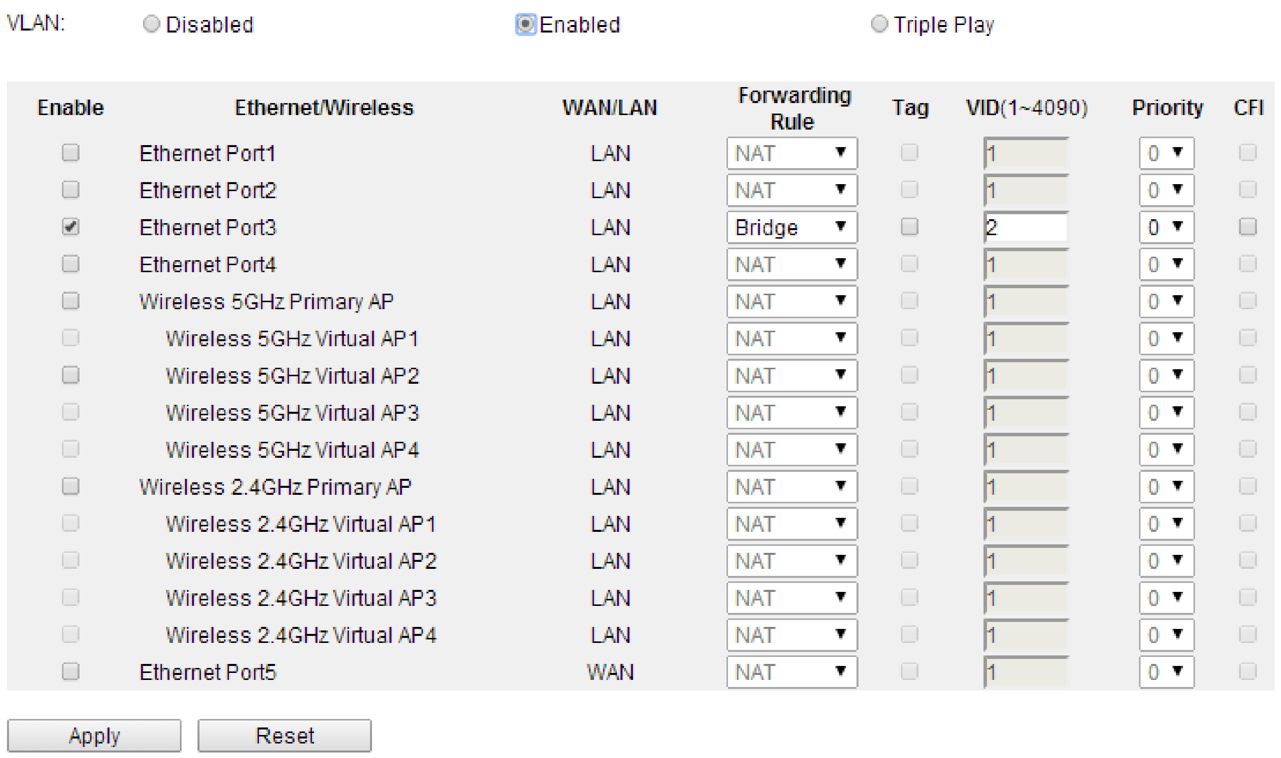
IP Address	MAC Address	Comment	Select

4.5.4 VLAN Settings



VLAN: ● Disabled ○ Enabled ○ Triple Play

VLAN means Virtual Local Area Network, 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.



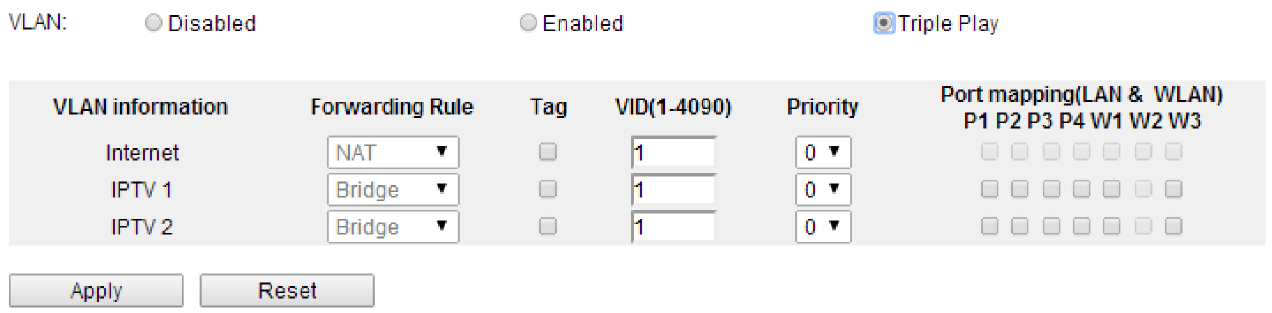
VLAN: ○ Disabled ● Enabled ○ Triple Play

Enable	Ethernet/Wireless	WAN/LAN	Forwarding Rule	Tag	VID(1~4090)	Priority	CFI
□	Ethernet Port1	LAN	NAT	□	1	0	□
□	Ethernet Port2	LAN	NAT	□	1	0	□
☑	Ethernet Port3	LAN	Bridge	□	2	0	□
□	Ethernet Port4	LAN	NAT	□	1	0	□
□	Wireless 5GHz Primary AP	LAN	NAT	□	1	0	□
□	Wireless 5GHz Virtual AP1	LAN	NAT	□	1	0	□
□	Wireless 5GHz Virtual AP2	LAN	NAT	□	1	0	□
□	Wireless 5GHz Virtual AP3	LAN	NAT	□	1	0	□
□	Wireless 5GHz Virtual AP4	LAN	NAT	□	1	0	□
□	Wireless 2.4GHz Primary AP	LAN	NAT	□	1	0	□
□	Wireless 2.4GHz Virtual AP1	LAN	NAT	□	1	0	□
□	Wireless 2.4GHz Virtual AP2	LAN	NAT	□	1	0	□
□	Wireless 2.4GHz Virtual AP3	LAN	NAT	□	1	0	□
□	Wireless 2.4GHz Virtual AP4	LAN	NAT	□	1	0	□
□	Ethernet Port5	WAN	NAT	□	1	0	□

Enabled: 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: 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.
CFI: enable the CFI function which indicates whether MAC is encapsulated by standard format.

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

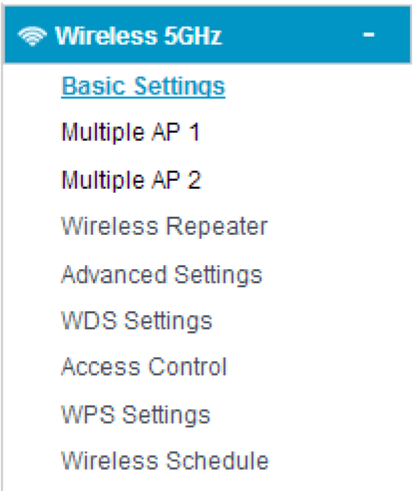
When you choose Triple Play, this configuration page is shown below



VLAN: ○ Disabled ○ Enabled ● Triple Play

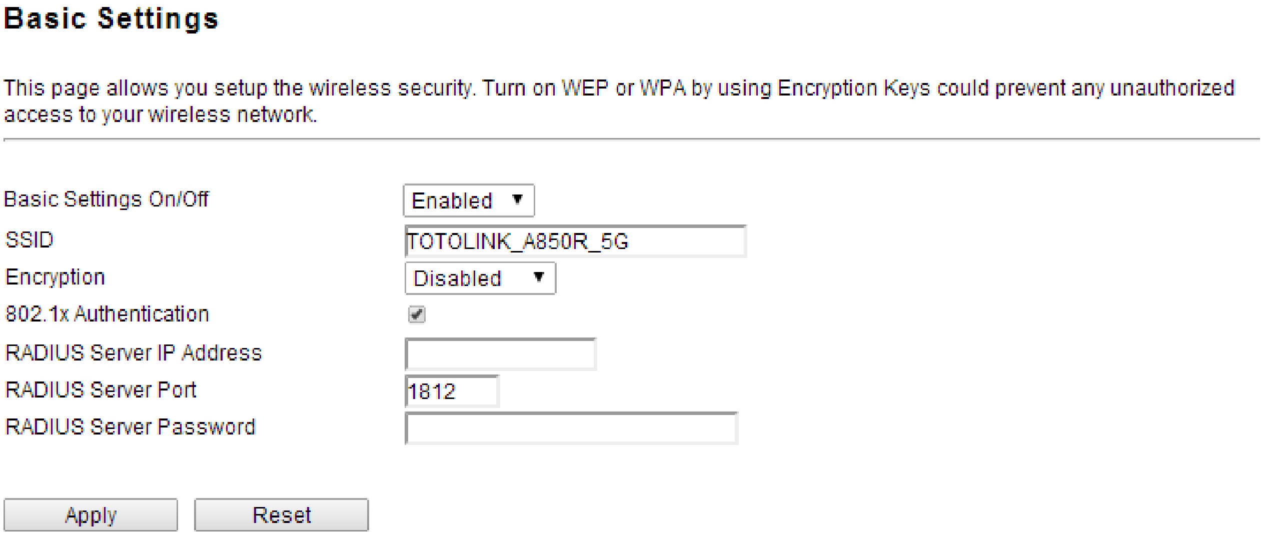
VLAN information	Forwarding Rule	Tag	VID(1-4090)	Priority	Port mapping(LAN & WLAN) P1	P2	P3	P4	W1	W2	W3
Internet	NAT	□	1	0	□	□	□	□	□	□	□
IPTV 1	Bridge	□	1	0	□	□	□	□	□	□	□
IPTV 2	Bridge	□	1	0	□	□	□	□	□	□	□

4.6 Wireless 5GHZ



4.6.1 Basic Settings

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

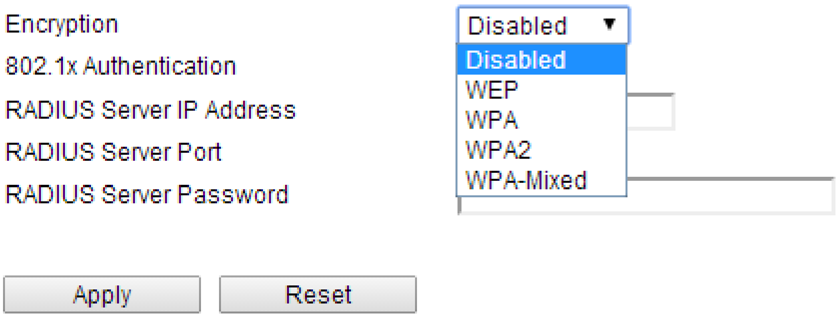


Basic Settings

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

Basic Settings On/Off	Enabled ▼
SSID	TOTOLINK_A850R_5G
Encryption	Disabled ▼
802.1x Authentication	☑
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

Encryption: This router supports Disabled, WEP, WPA, WPA2, WPA-Mixed security options. By default, it is disabled. Please select one according to the Access Point security policy for a secure network.


Encryption: Disabled

802.1x Authentication

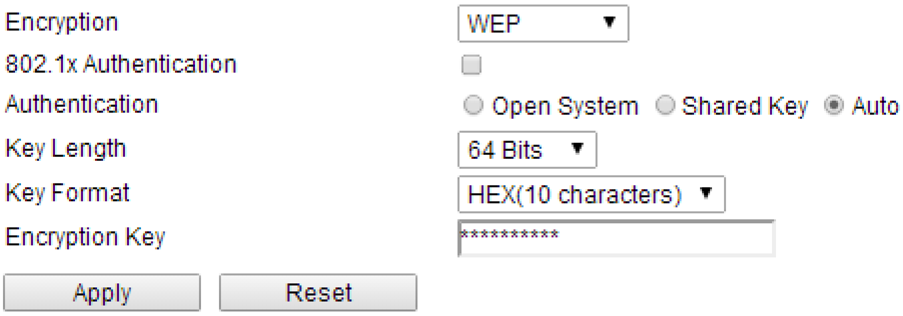
RADIUS Server IP Address

RADIUS Server Port

RADIUS Server Password

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 Bits

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.)

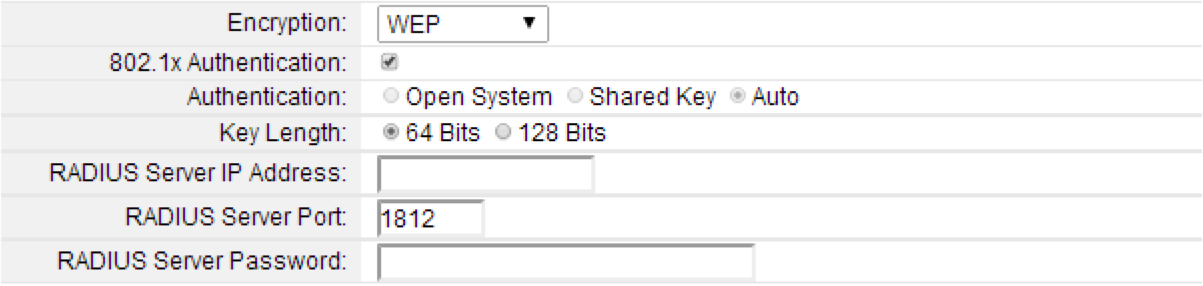
128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

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 802.1x Authentication, 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.

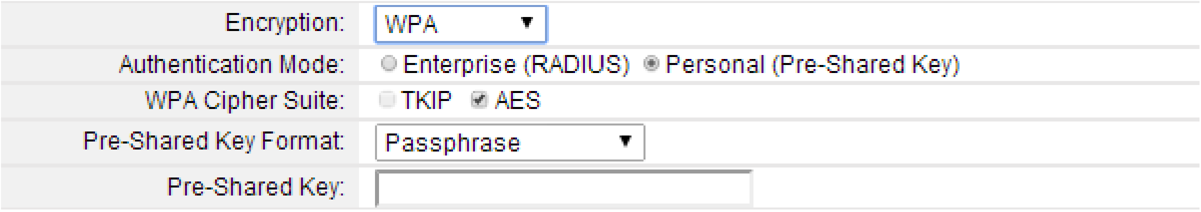
> **RADIUS:** Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet Service Provider. It is the most common method of authenticating and authorizing dial-up and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

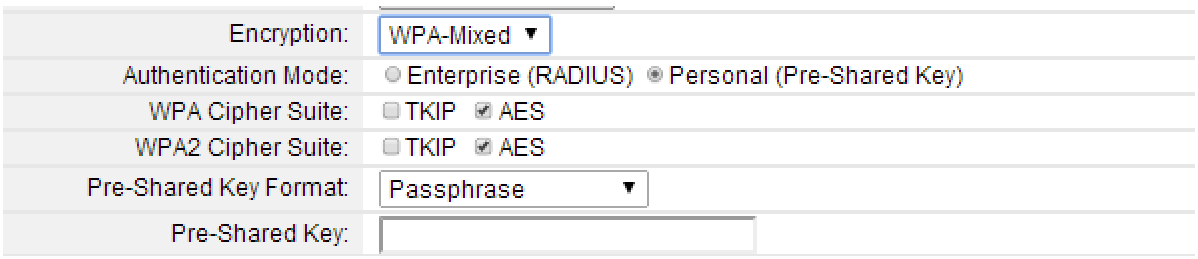


Encryption:	WPA ▼
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	□ TKIP ☑ AES
Pre-Shared Key Format:	Passphrase ▼
Pre-Shared Key:	

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

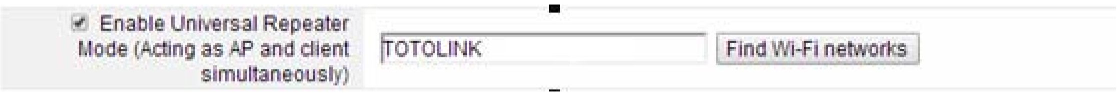
This option mixes WPA/WPA2 together. It will provide the best security for your router.



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.*

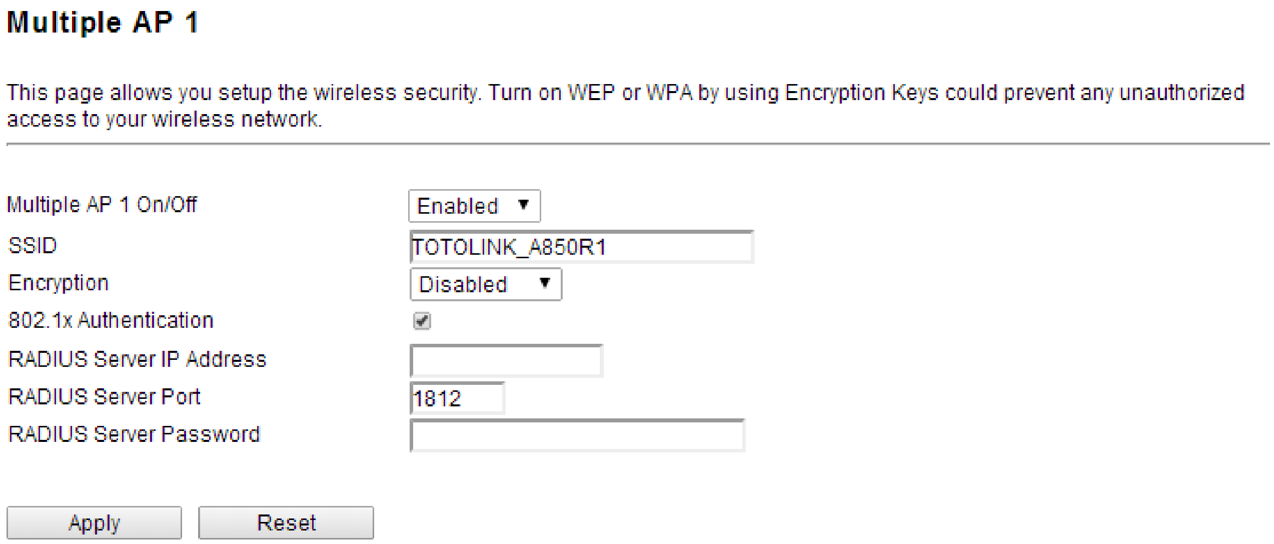
Enable Universal Repeater Mode: enable the repeater mode and search for wireless networks in range on all the supported channels while device is operating in Access Point.



☑ Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK

4.6.2 Wireless AP1

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



Multiple AP 1

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

Multiple AP 1 On/Off	Enabled ▼
SSID	TOTOLINK_A850R1
Encryption	Disabled ▼
802.1x Authentication	☑
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

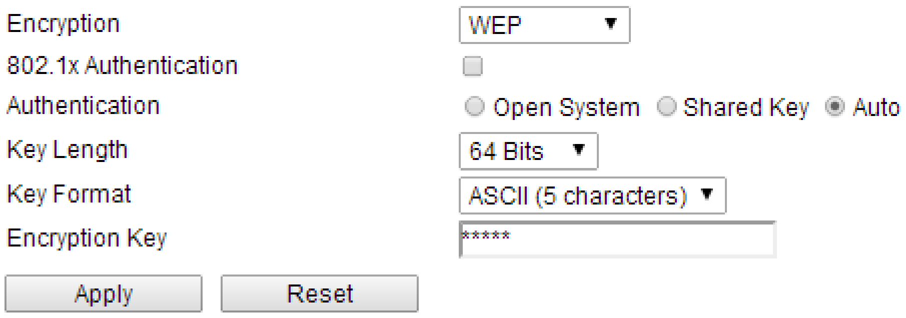
Encryption: This router supports WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.

Encryption: Disabled

Disabled
WEP
WPA
WPA2
WPA-Mixed

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 Bits
Key Format	ASCII (5 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.

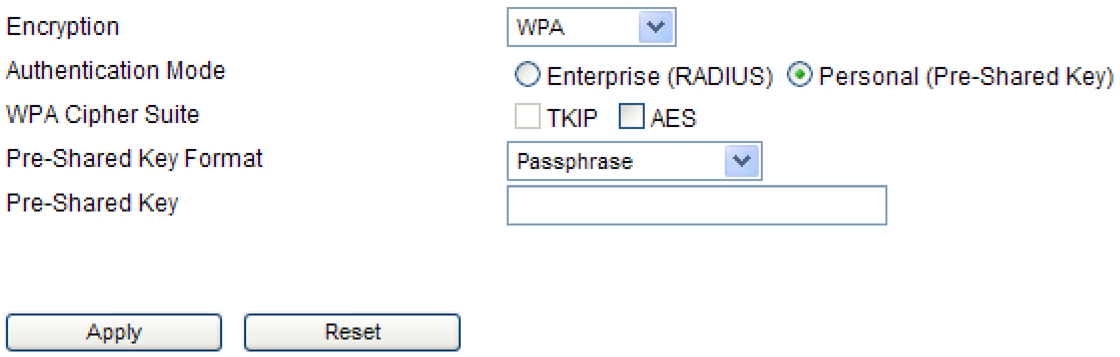
2) WPA/WPA2

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.

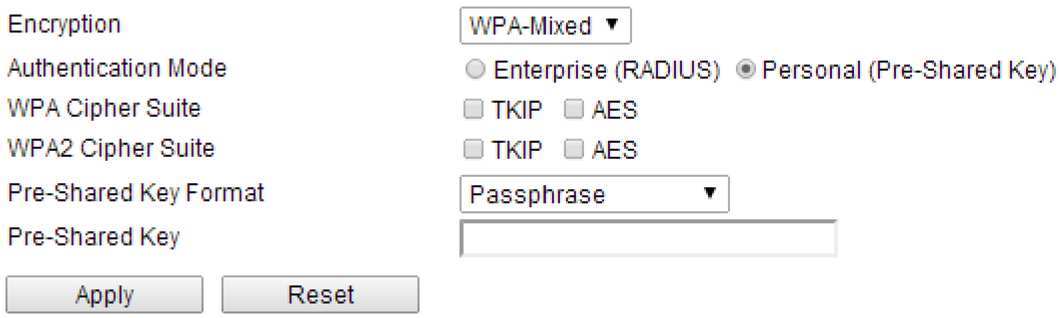


Encryption	WPA
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

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…”).

3) WPA Mixed

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

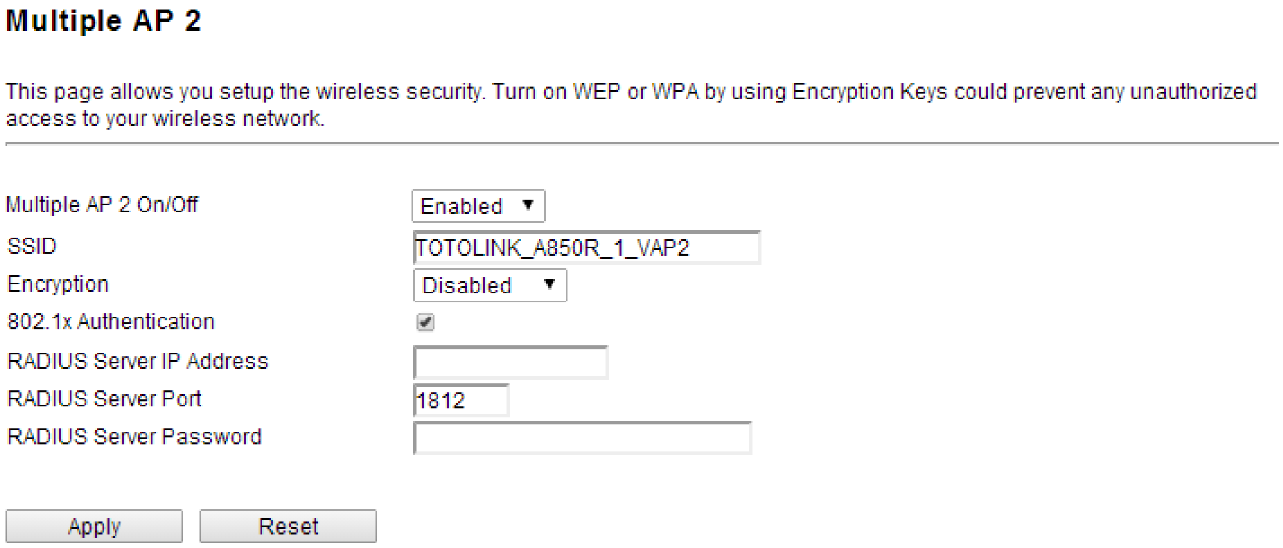


Encryption	WPA-Mixed
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
WPA2 Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

***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.*

4.6.3 Wireless AP2

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

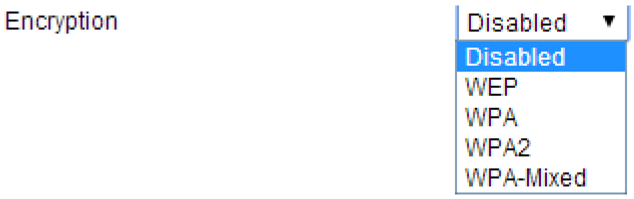


Multiple AP 2

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

Multiple AP 2 On/Off	Enabled ▼
SSID	TOTOLINK_A850R_1_VAP2
Encryption	Disabled ▼
802.1x Authentication	☑
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

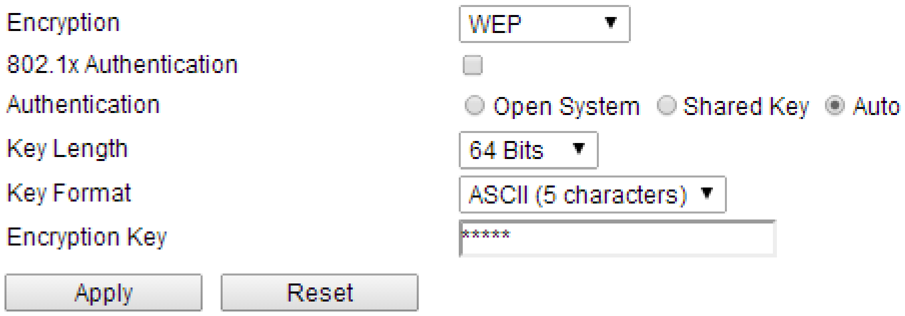
Encryption: This router supports WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.



Encryption: Disabled ▼

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 Bits ▼
Key Format	ASCII (5 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.

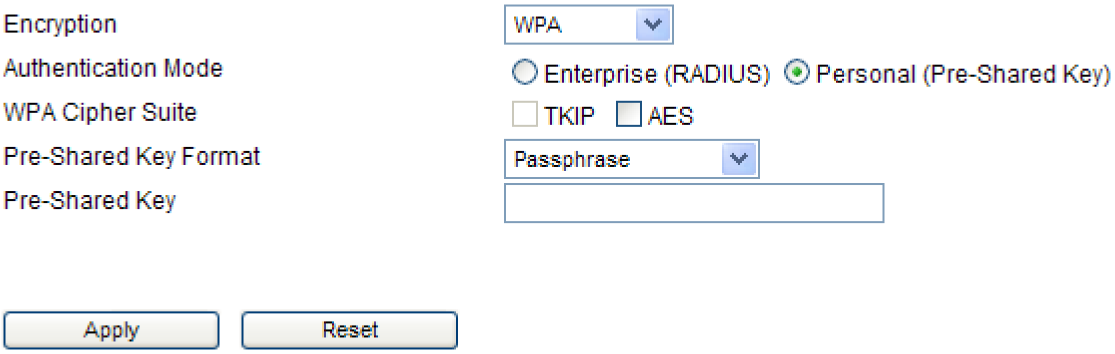
2) WPA/WPA2

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.

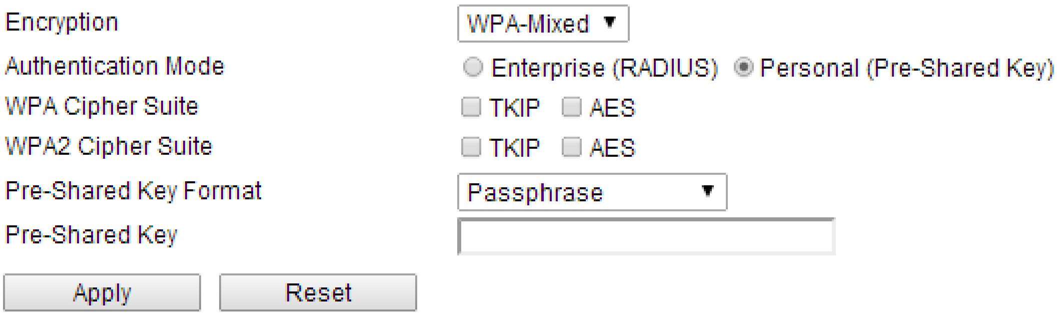


Encryption	WPA
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

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…”).

3) WPA Mixed

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

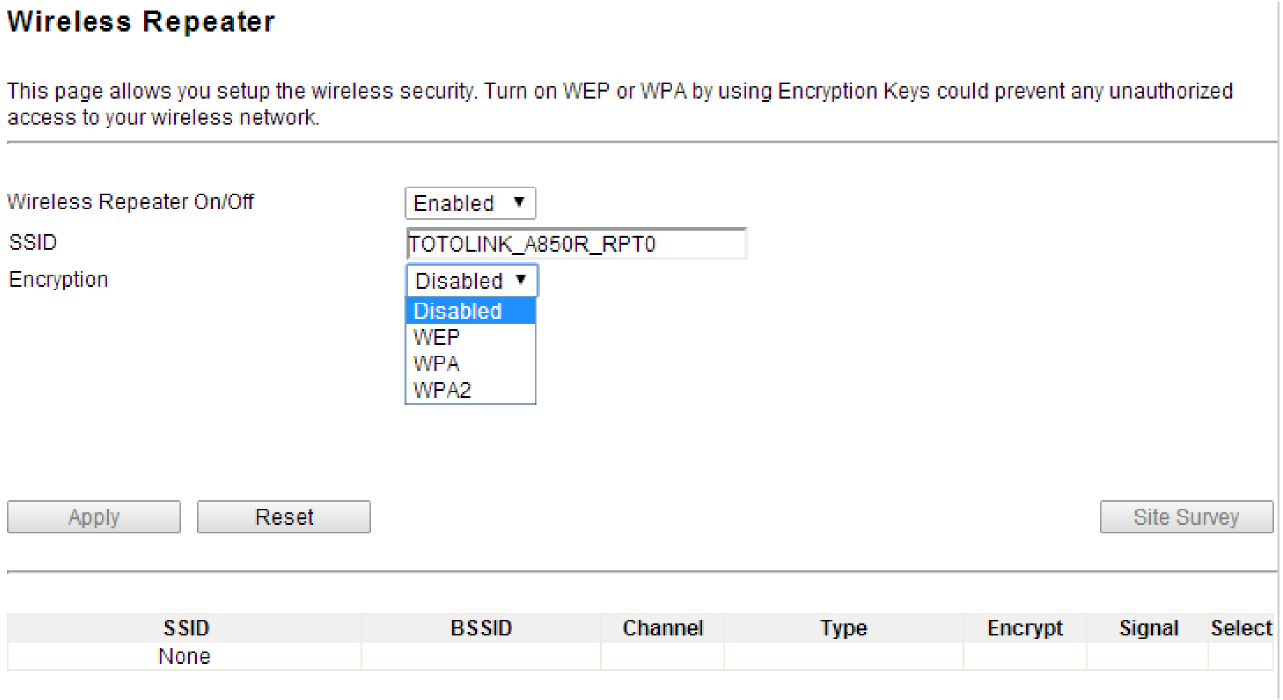


Encryption	WPA-Mixed
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
WPA2 Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

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.*

4.6.4 Wireless Repeater

The Repeater methods can help you to expand the wireless coverage and allow more terminals to access Internet.



Wireless Repeater

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

Wireless Repeater On/Off: Enabled

SSID: TOTOLINK_A850R_RPT0

Encryption: Disabled

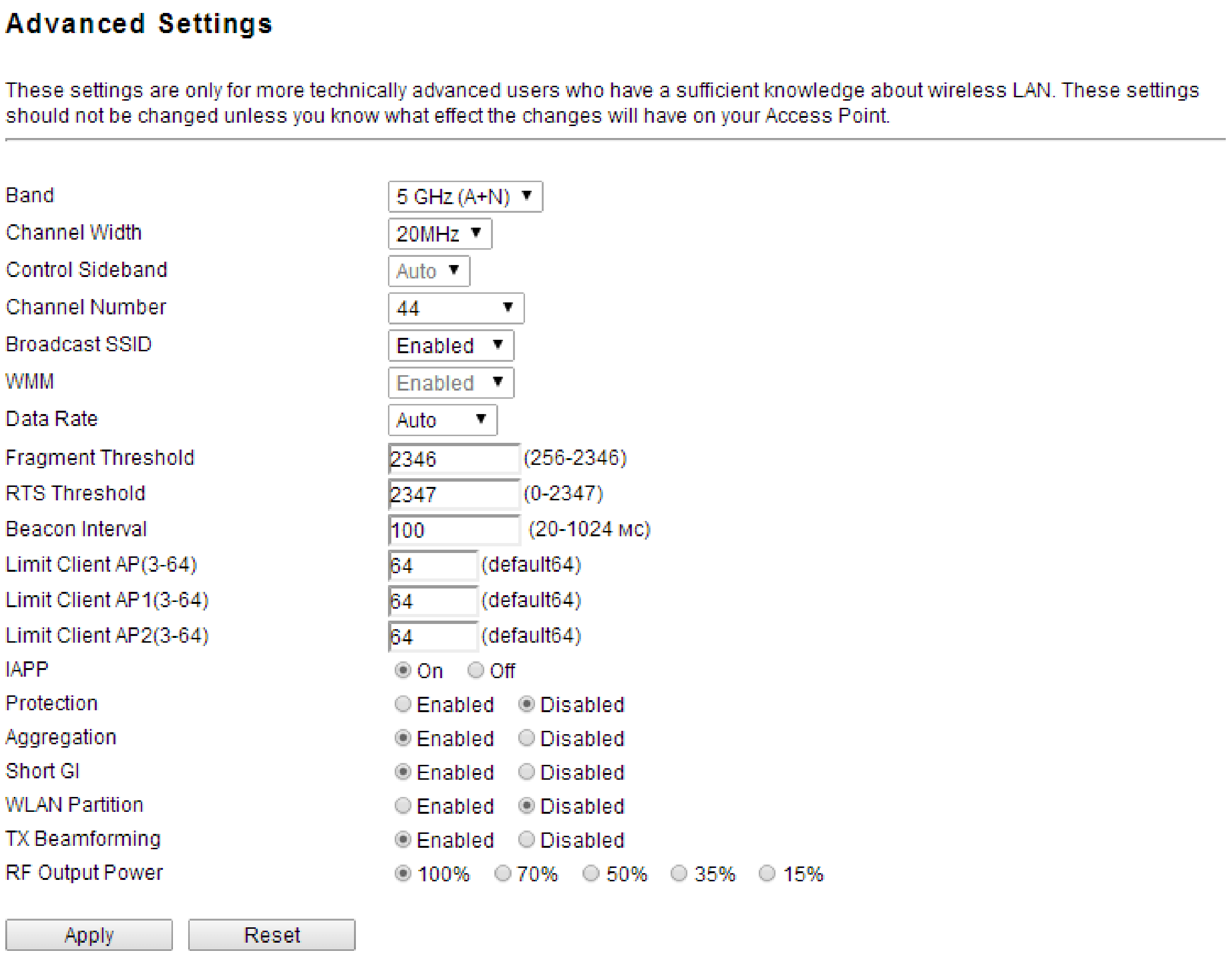
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
None						

Wireless Repeater Network Name (SSID): Click **Scan AP** to choose the SSID you want to implement the repeater function.

Encryption: please refer to **Wireless Basic Settings**.

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.



Advanced Settings

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

Band	5 GHz (A+N) ▼
Channel Width	20MHz ▼
Control Sideband	Auto ▼
Channel Number	44 ▼
Broadcast SSID	Enabled ▼
WMM	Enabled ▼
Data Rate	Auto ▼
Fragment Threshold	2346 (256-2346)
RTS Threshold	2347 (0-2347)
Beacon Interval	100 (20-1024 мс)
Limit Client AP(3-64)	64 (default64)
Limit Client AP1(3-64)	64 (default64)
Limit Client AP2(3-64)	64 (default64)
IAPP	● On ○ Off
Protection	○ Enabled ● Disabled
Aggregation	● Enabled ○ Disabled
Short GI	● Enabled ○ Disabled
WLAN Partition	○ Enabled ● Disabled
TX Beamforming	● Enabled ○ Disabled
RF Output Power	● 100% ○ 70% ○ 50% ○ 35% ○ 15%

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.

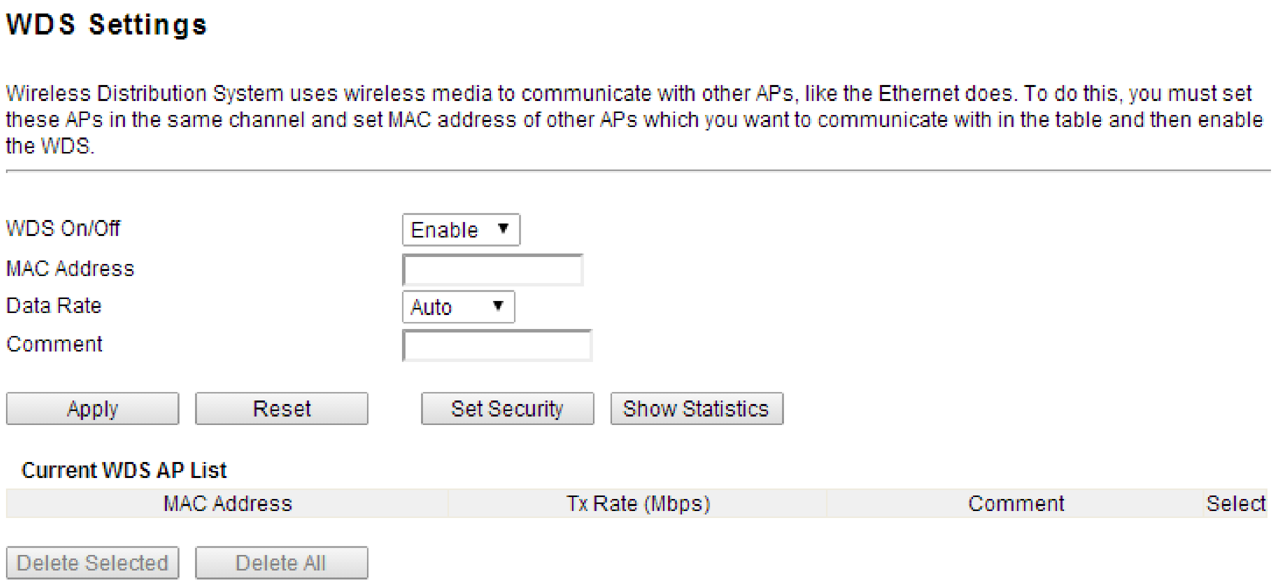
RF Output Power: you can select the output power of the wireless device. The default value is 100%. It will deliver the best performance of the device.

4.6.6 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.



WDS Settings

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

WDS On/Off	Enable
MAC Address	
Data Rate	Auto
Comment	

Current WDS AP List

MAC Address	Tx Rate (Mbps)	Comment	Select

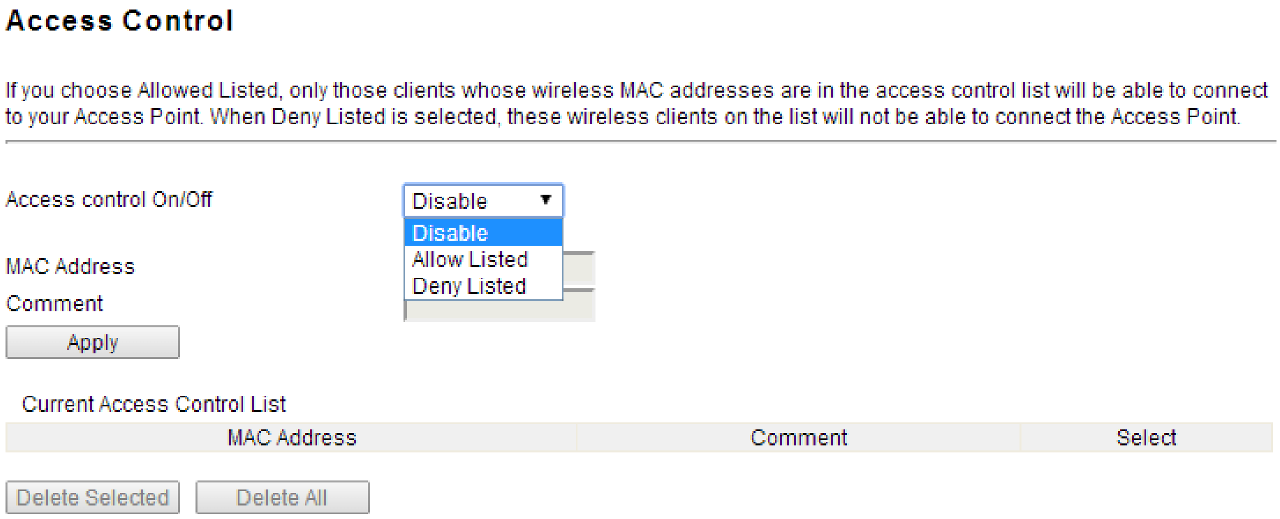
Enable WDS: by default, you can't select the checkbox to enable WDS.

MAC Address: the other AP's MAC Address that you want to communicate with.

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 Access Control



Access Control

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

Access control On/Off	Disable
MAC Address	
Comment	

Current Access Control List

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 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.

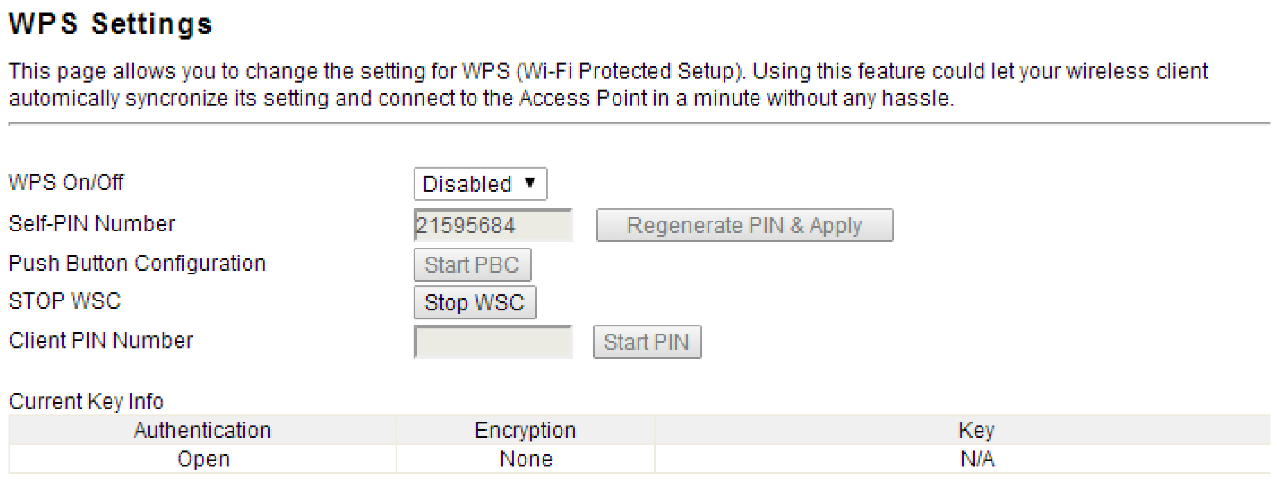
Comment: describe the reason why you allow or deny the access of the MAC Address.

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.

4.6.8 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 Settings

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

WPS On/Off	Disabled ▼
Self-PIN Number	21595684 [Regenerate PIN & Apply]
Push Button Configuration	[Start PBC]
STOP WSC	[Stop WSC]
Client PIN Number	[Start PIN]

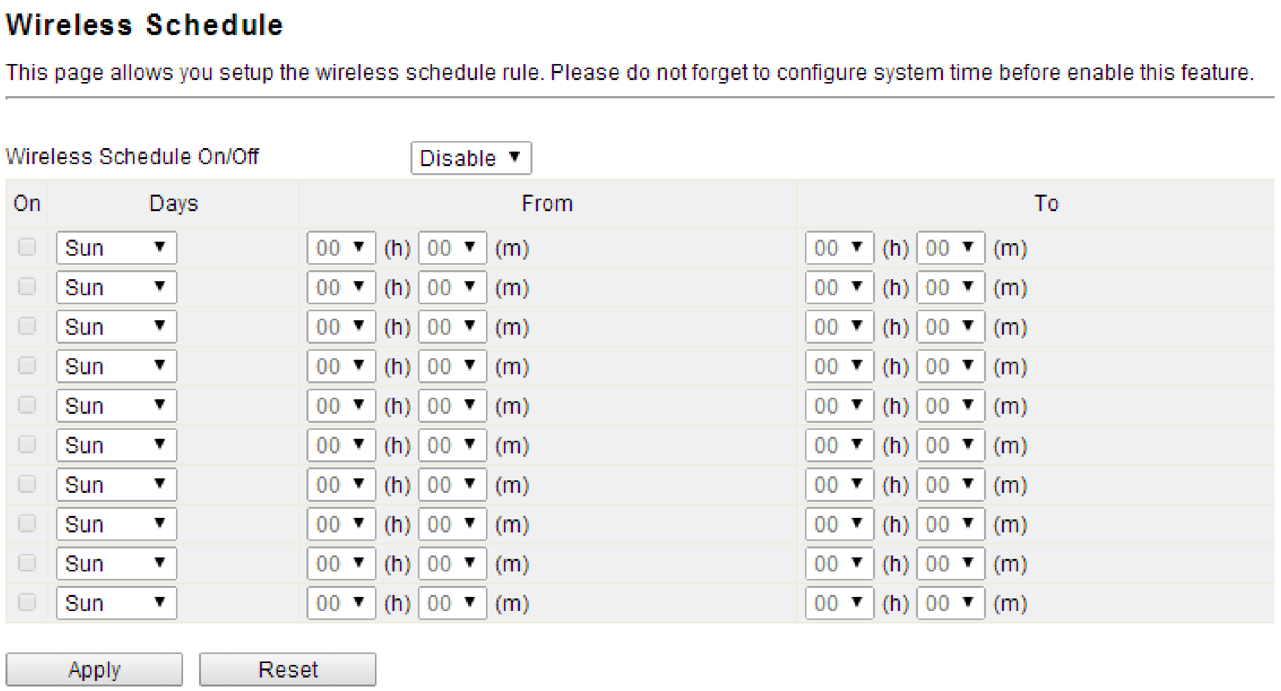
Current Key Info

Authentication	Encryption	Key
Open	None	N/A

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)
Current Key Info: If the wireless security (encryption) function of the router is properly configured, you can see the encryption information on the list.

4.6.9 Wireless 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.



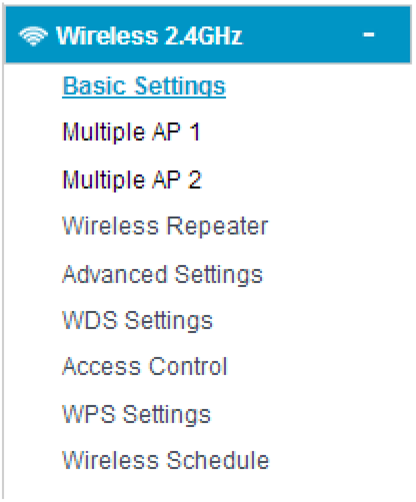
Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Wireless Schedule On/Off: Disable

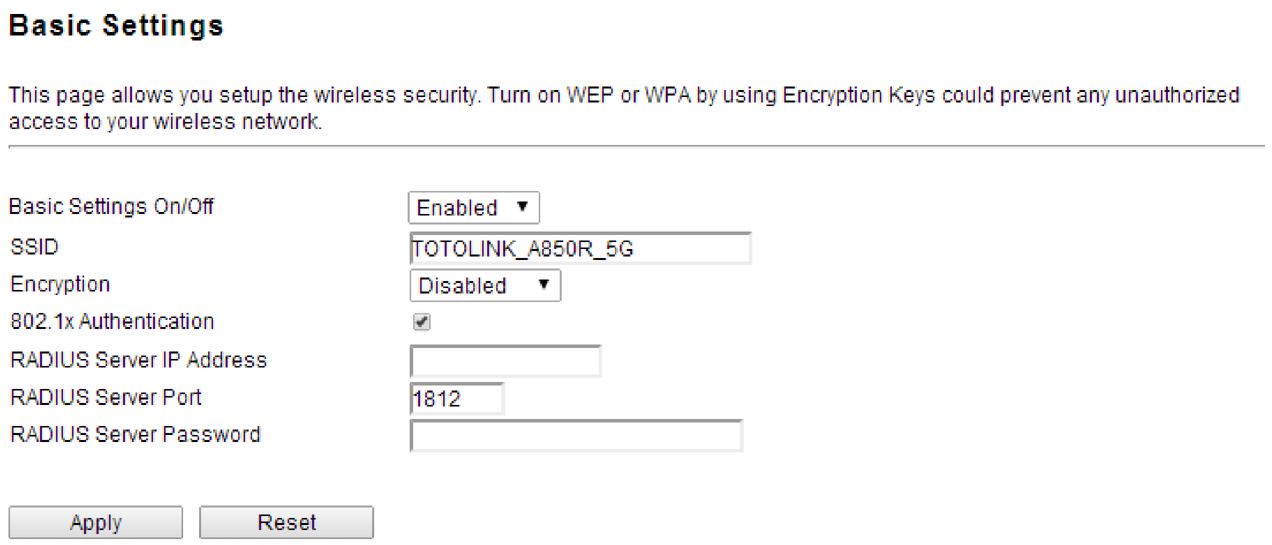
On	Days	From	To
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)
□	Sun	00 (h) 00 (m)	00 (h) 00 (m)

4.7 Wireless 2.4GHZ



4.7.1 Basic Settings

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

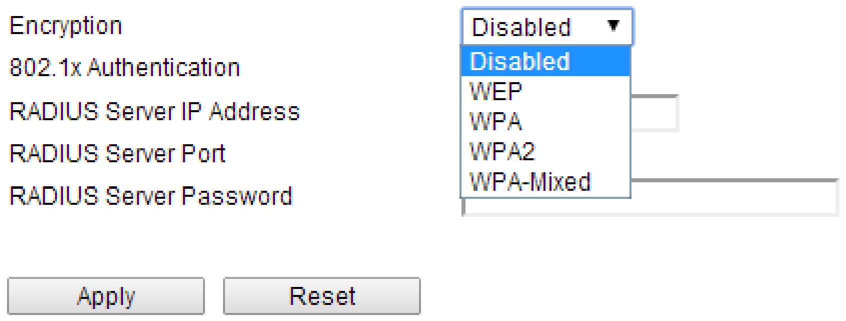


Basic Settings

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

Basic Settings On/Off	Enabled ▼
SSID	TOTOLINK_A850R_5G
Encryption	Disabled ▼
802.1x Authentication	☑
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

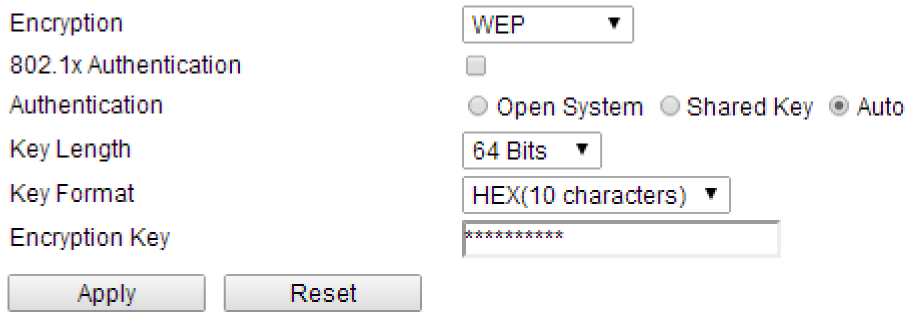
Encryption: This router supports Disabled, WEP, WPA, WPA2, WPA-Mixed security options. By default, it is disabled. Please select one according to the Access Point security policy for a secure network.



Encryption	Disabled ▼
802.1x Authentication	
RADIUS Server IP Address	
RADIUS Server Port	
RADIUS Server Password	

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 Bits ▼
Key Format	HEX(10 characters) ▼
Encryption Key	**********

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

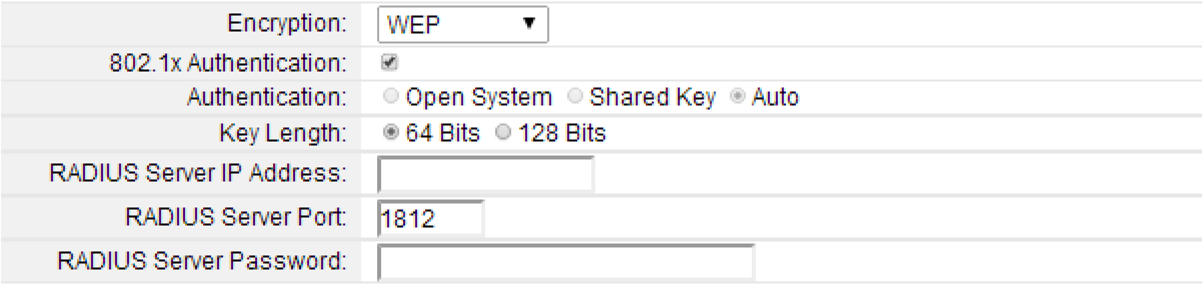
64-bit—For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x414234445.)
128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

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 802.1x Authentication, 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:	

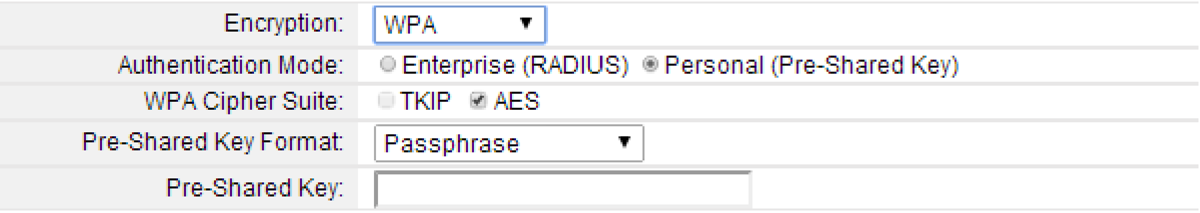
RADIUS Server IP Address: Enter the IP address of RADIUS server.
RADIUS Server Port: the UDP port number that the RADIUS server that is used to authenticate the messages sent between them.
RADIUS Server Password: enter the password.
RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a security 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.

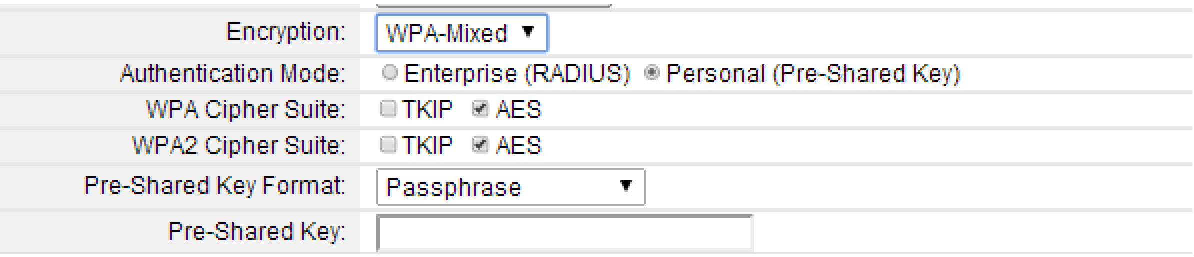


Encryption:	WPA ▼
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	□ TKIP ☑ AES
Pre-Shared Key Format:	Passphrase ▼
Pre-Shared Key:	

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

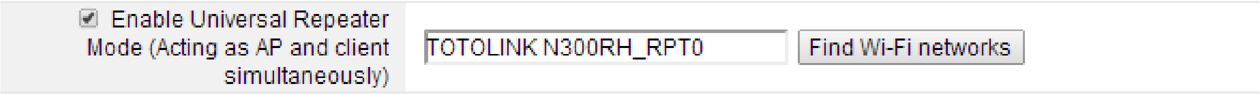
This option mixes WPA/WPA2 together. It will provide the best security for your router.



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.*

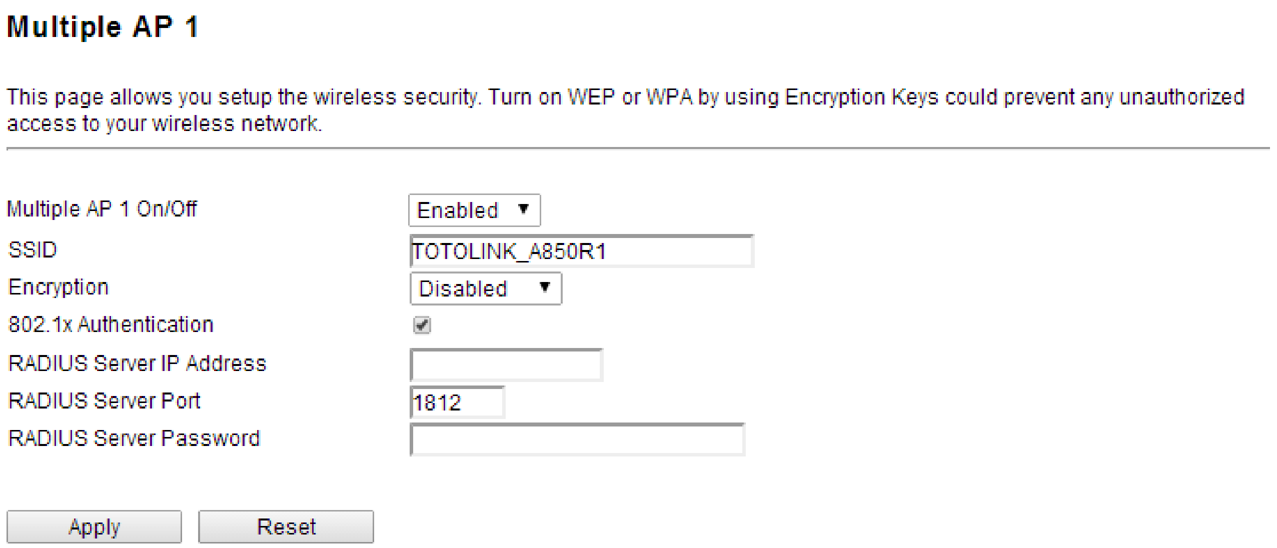
Enable Universal Repeater Mode: enable the repeater mode and search for wireless networks in range on all the supported channels while device is operating in Access Point.



☑ Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK N300RH_RPT0	Find Wi-Fi networks

4.7.2 Wireless AP1

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

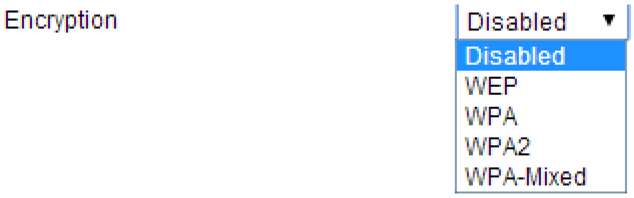


Multiple AP 1

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

Multiple AP 1 On/Off	Enabled ▼
SSID	TOTOLINK_A850R1
Encryption	Disabled ▼
802.1x Authentication	☑
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

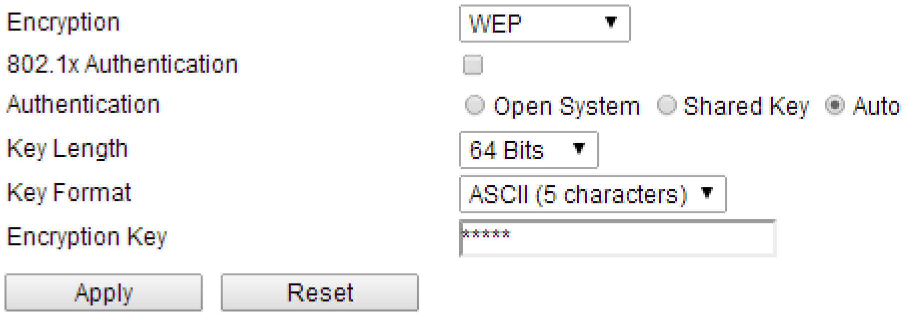
Encryption: This router supports WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.



Encryption: Disabled ▼

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 Bits ▼
Key Format	ASCII (5 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.

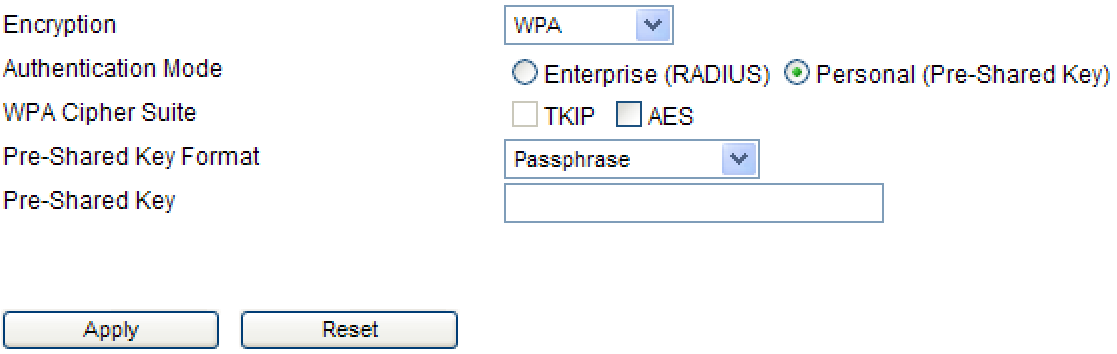
2) WPA/WPA2

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.

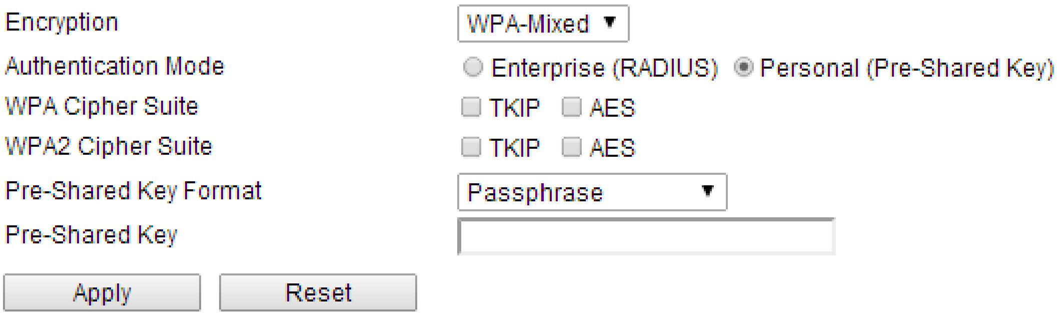


Encryption	WPA
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

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…").

3) WPA Mixed

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

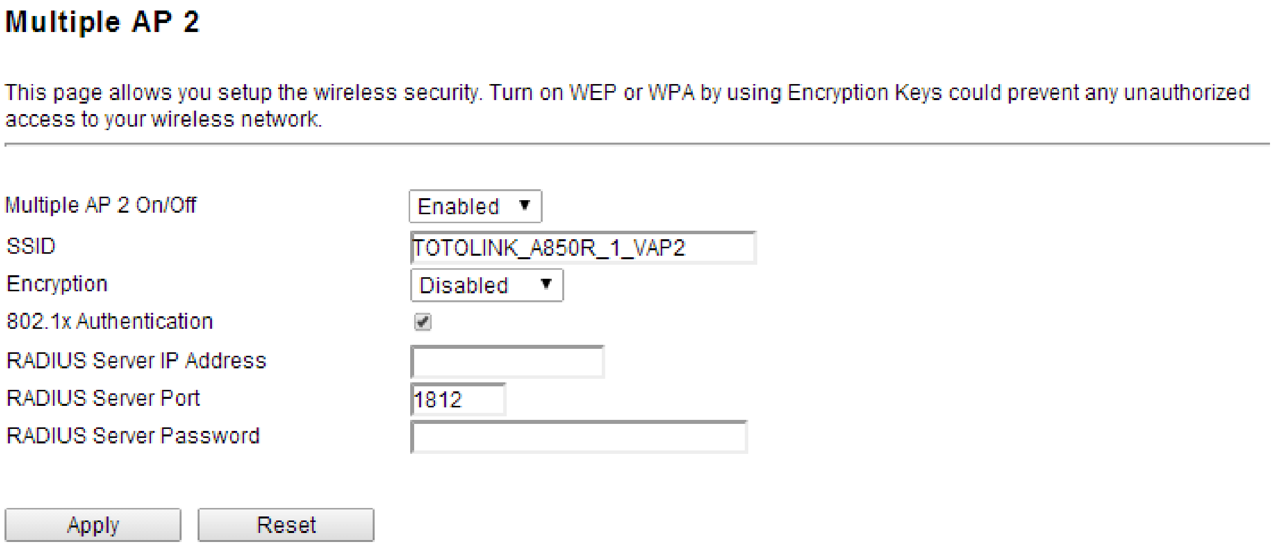


Encryption	WPA-Mixed
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
WPA2 Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

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.*

4.7.3 Wireless AP2

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



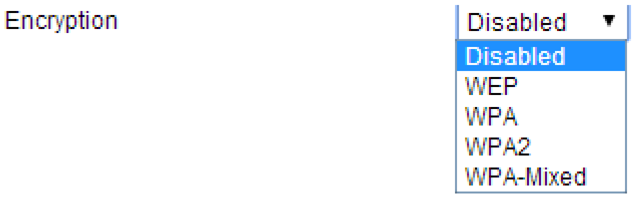
Multiple AP 2

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

Multiple AP 2 On/Off	Enabled ▼
SSID	TOTOLINK_A850R_1_VAP2
Encryption	Disabled ▼
802.1x Authentication	☑
RADIUS Server IP Address	
RADIUS Server Port	1812
RADIUS Server Password	

Apply Reset

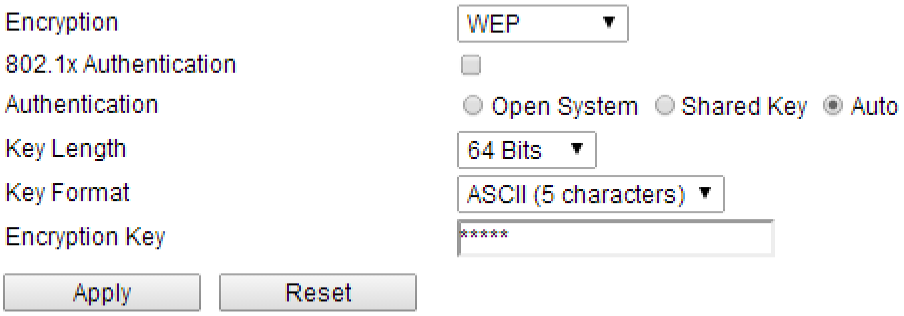
Encryption: This router supports WEP, WPA, WPA2, WPA-Mixed security options. Please select one according to the Access Point security policy.



Encryption Disabled ▼

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 Bits ▼
Key Format	ASCII (5 characters) ▼
Encryption Key	*****

Apply Reset

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.

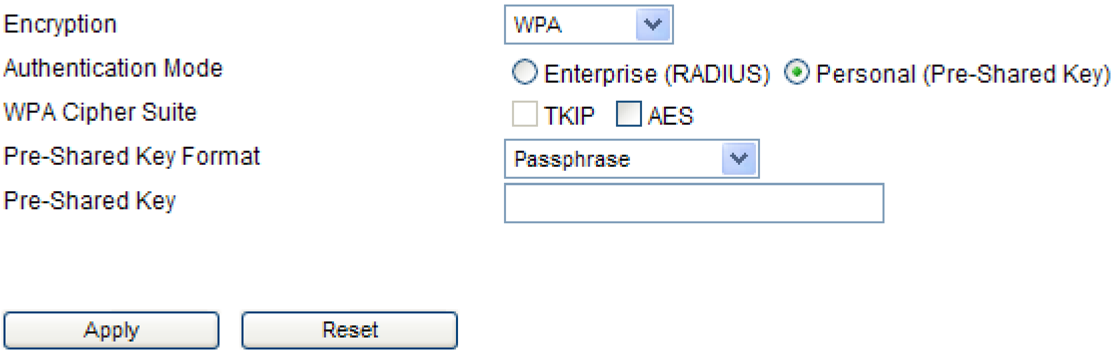
2) WPA/WPA2

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.

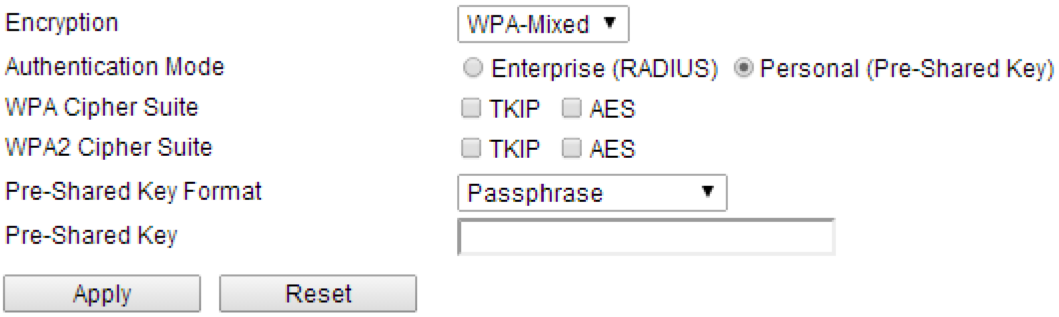


Encryption	WPA
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	□ TKIP □ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

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…”).

3) WPA Mixed

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

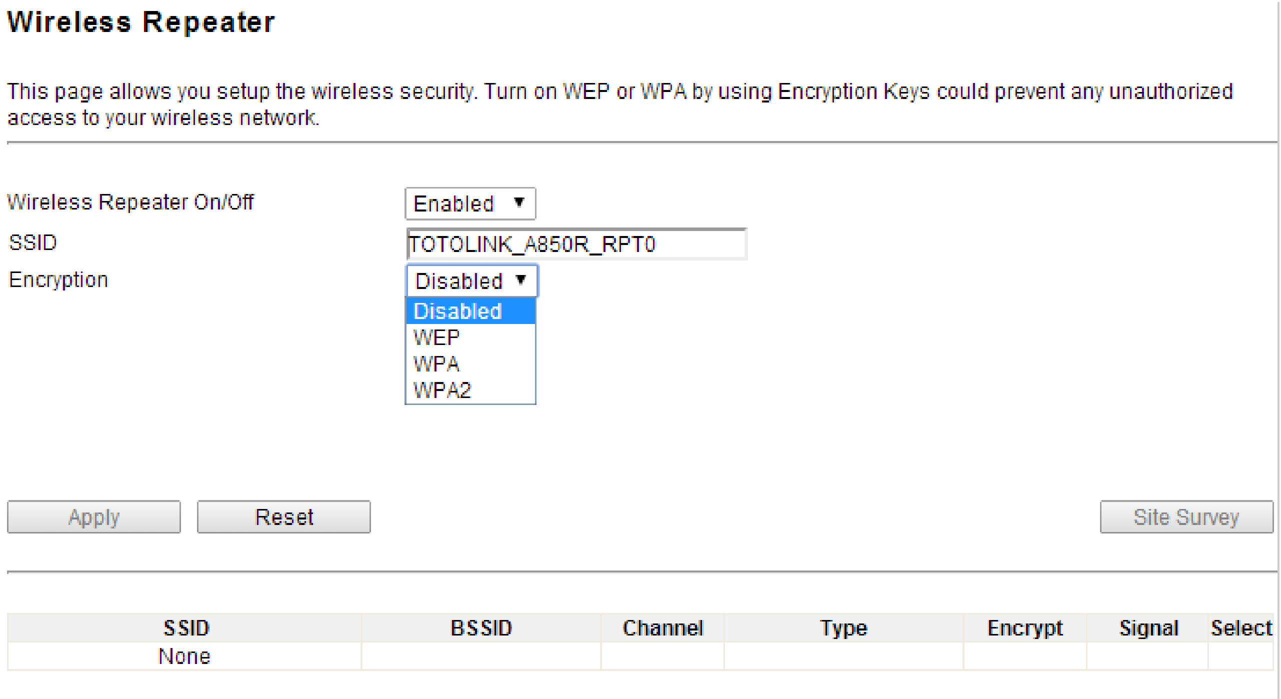


Encryption	WPA-Mixed ▼
Authentication Mode	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite	☐ TKIP ☐ AES
WPA2 Cipher Suite	☐ TKIP ☐ AES
Pre-Shared Key Format	Passphrase ▼
Pre-Shared Key	

***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.*

4.7.4 Wireless Repeater

The Repeater methods can help you to expand the wireless coverage and allow more terminals to access Internet.



Wireless Repeater

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

Wireless Repeater On/Off	Enabled ▼
SSID	TOTOLINK_A850R_RPT0
Encryption	Disabled ▼

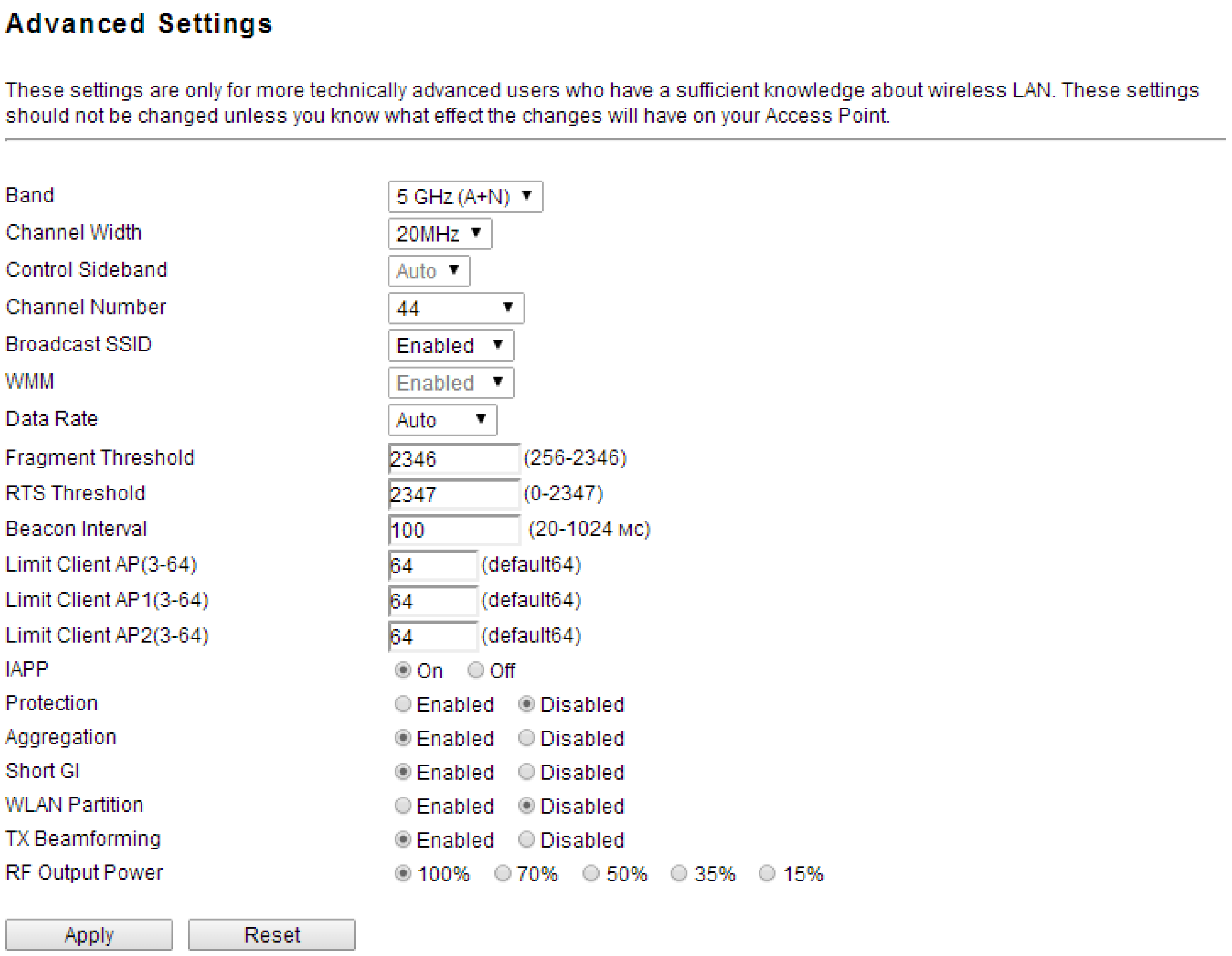
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
None						

Wireless Repeater Network Name (SSID): Click **Scan AP** to choose the SSID you want to implement the repeater function.

Encryption: please refer to **Wireless Basic Settings**.

4.7.5 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.



Advanced Settings

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

Band	5 GHz (A+N) ▼
Channel Width	20MHz ▼
Control Sideband	Auto ▼
Channel Number	44 ▼
Broadcast SSID	Enabled ▼
WMM	Enabled ▼
Data Rate	Auto ▼
Fragment Threshold	2346 (256-2346)
RTS Threshold	2347 (0-2347)
Beacon Interval	100 (20-1024 мс)
Limit Client AP(3-64)	64 (default64)
Limit Client AP1(3-64)	64 (default64)
Limit Client AP2(3-64)	64 (default64)
IAPP	● On ○ Off
Protection	○ Enabled ● Disabled
Aggregation	● Enabled ○ Disabled
Short GI	● Enabled ○ Disabled
WLAN Partition	○ Enabled ● Disabled
TX Beamforming	● Enabled ○ Disabled
RF Output Power	● 100% ○ 70% ○ 50% ○ 35% ○ 15%

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.

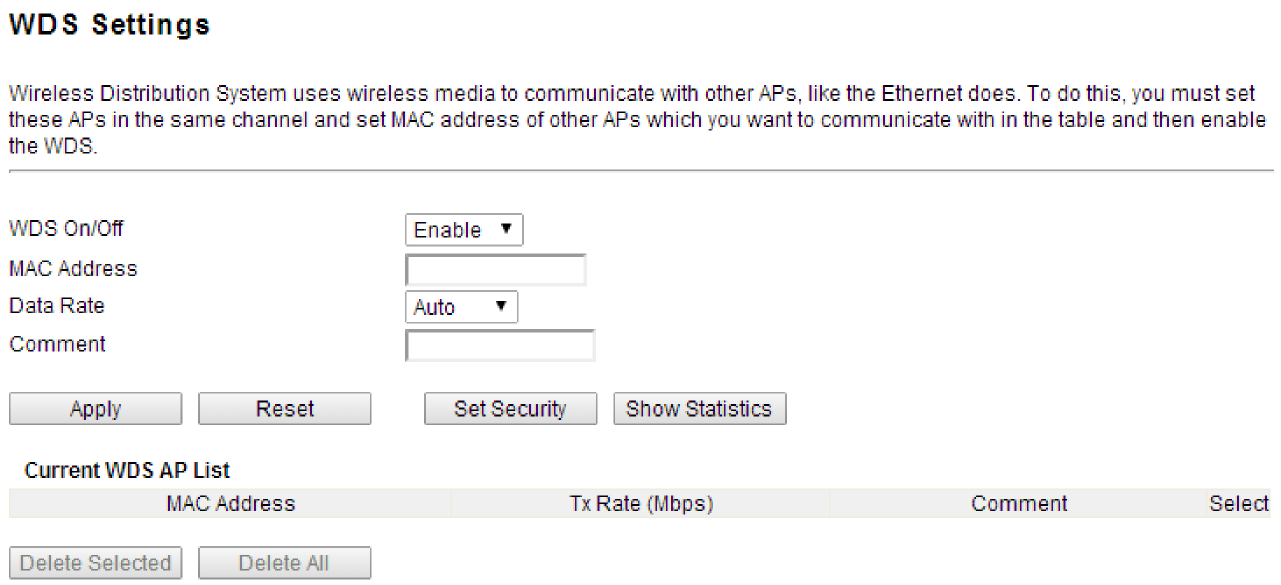
RF Output Power: you can select the output power of the wireless device. The default value is 100%. It will deliver the best performance of the device.

4.7.6 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:

3. Provide bridge traffic between two LANs though the air.
4. 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.


WDS Settings

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

WDS On/Off	Enable
MAC Address	
Data Rate	Auto
Comment	

Current WDS AP List

MAC Address	Tx Rate (Mbps)	Comment	Select

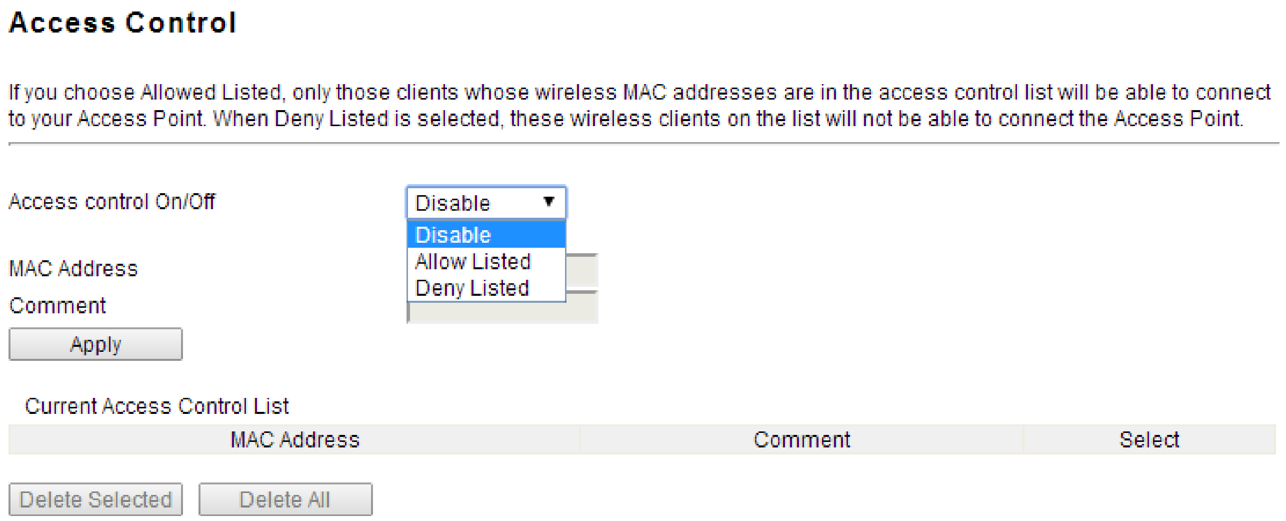
Enable WDS: by default, you can't select the checkbox to enable WDS.

MAC Address: the other AP's MAC Address that you want to communicate with.

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.

4.7.7 Access Control


Access Control

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

Access control On/Off	Disable
MAC Address	
Comment	

Current Access Control List

MAC Address	Comment	Select

By default, Wireless Access Control Mode is disabled.

There are two ways to set the Access Control List:

3. 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.
4. 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.

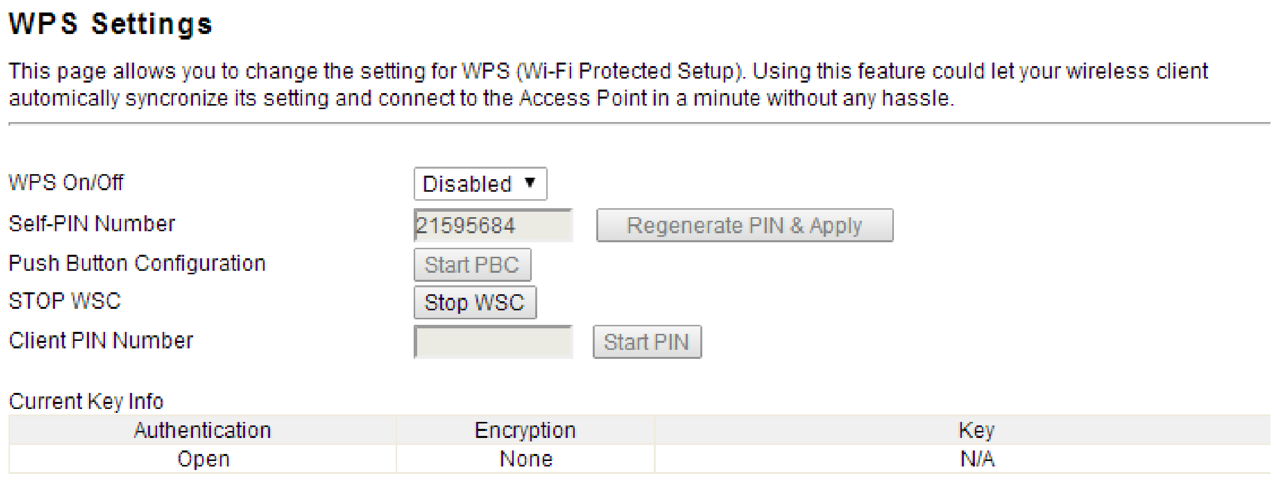
Comment: describe the reason why you allow or deny the access of the MAC Address.

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.

4.7.8 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 Settings

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

WPS On/Off	Disabled ▼
Self-PIN Number	21595684 [Regenerate PIN & Apply]
Push Button Configuration	[Start PBC]
STOP WSC	[Stop WSC]
Client PIN Number	[Start PIN]

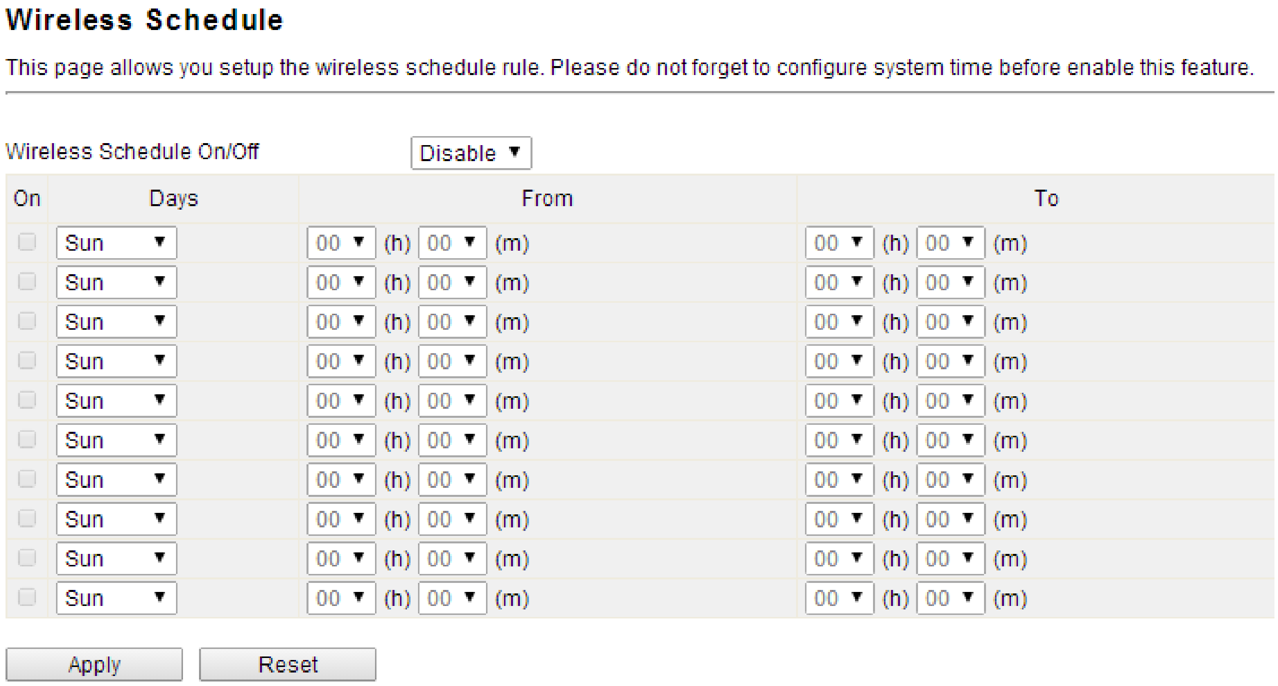
Current Key Info

Authentication	Encryption	Key
Open	None	N/A

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)
Current Key Info: If the wireless security (encryption) function of the router is properly configured, you can see the encryption information on the list.

4.7.9 Wireless 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.



Wireless Schedule

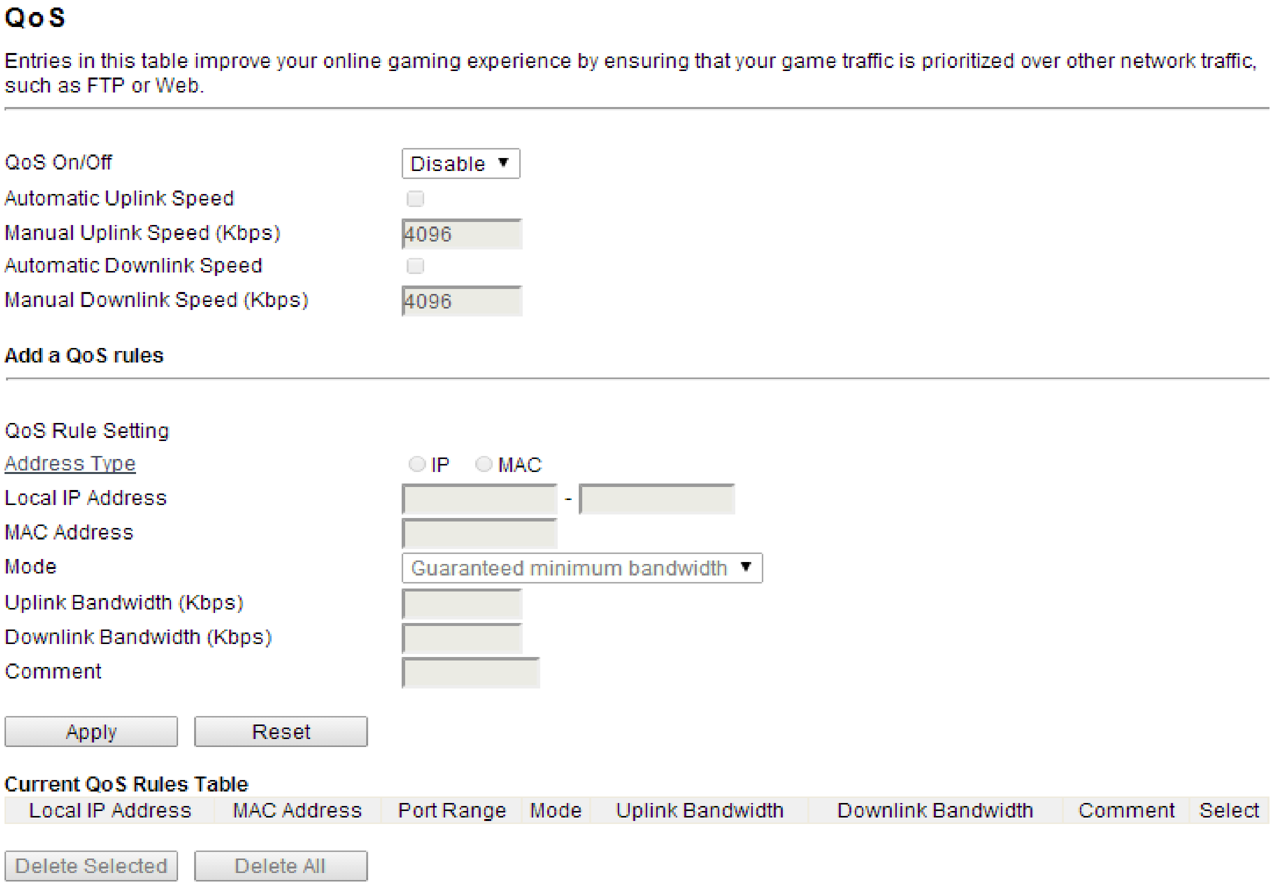
This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Wireless Schedule On/Off	Disable ▼

On	Days	From	To
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)
□	Sun ▼	00 ▼ (h) 00 ▼ (m)	00 ▼ (h) 00 ▼ (m)

4.8 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.



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

QoS On/Off	Disable ▼
Automatic Uplink Speed	□
Manual Uplink Speed (Kbps)	4096
Automatic Downlink Speed	□
Manual Downlink Speed (Kbps)	4096

Add a QoS rules

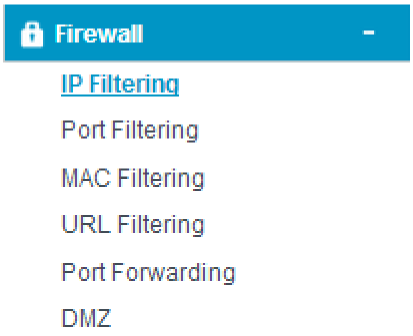
QoS Rule Setting	
Address Type	○ IP ○ MAC
Local IP Address	-
MAC Address	
Mode	Guaranteed minimum bandwidth ▼
Uplink Bandwidth (Kbps)	
Downlink Bandwidth (Kbps)	
Comment	

Current QoS Rules Table

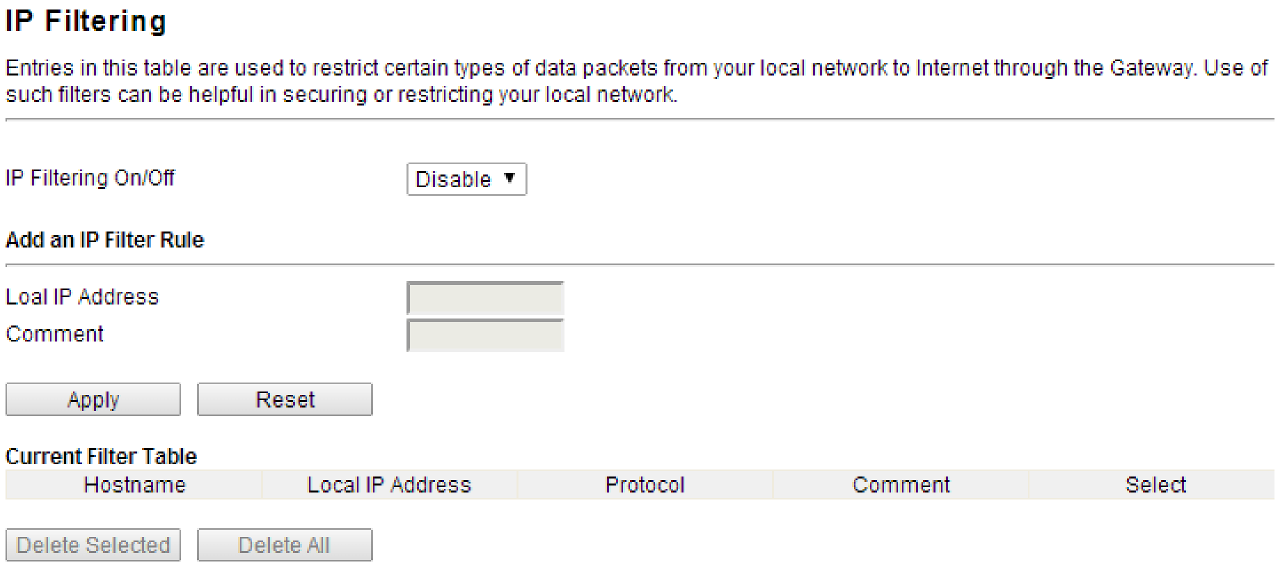
Local IP Address	MAC Address	Port Range	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

4.9 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.



4.9.1 IP Filtering



IP Filtering

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

IP Filtering On/Off: Disable ▼

Add an IP Filter Rule

Loal IP Address

Comment

Apply | Reset

Current Filter Table

Hostname	Local IP Address	Protocol	Comment	Select

Delete Selected | Delete All

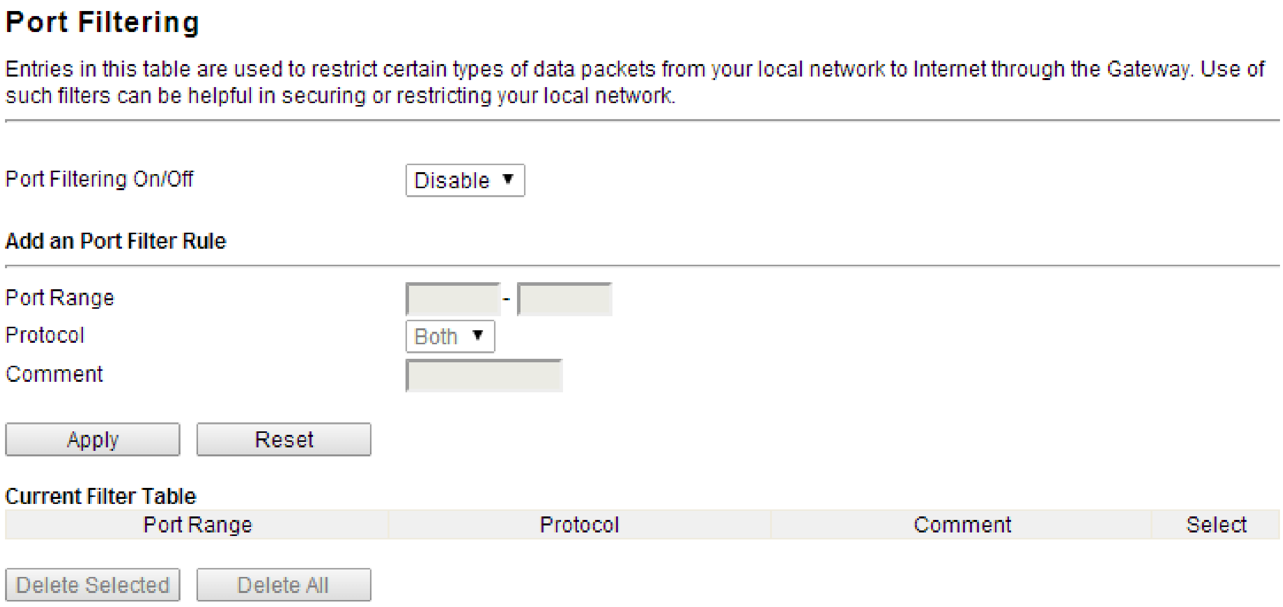
IP filtering On/Off: you can select this checkbox to enable IP Filtering function.

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.

4.9.2 Port Filtering



Port Filtering

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

Port Filtering On/Off: Disable

Add an Port Filter Rule

Port Range: -

Protocol: Both

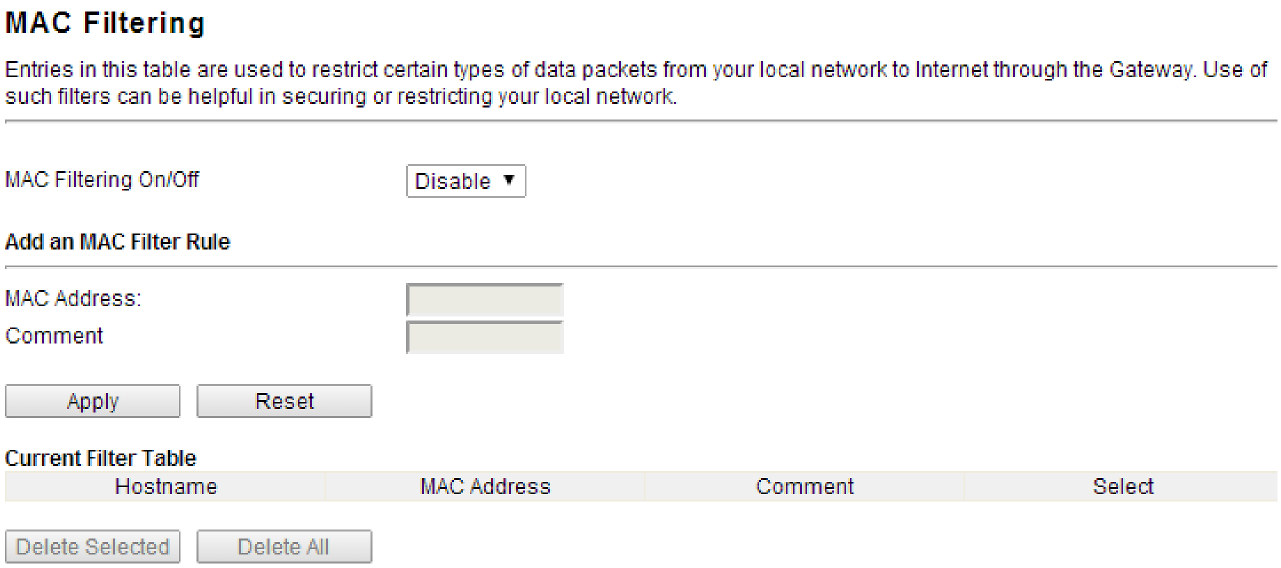
Comment:

Current Filter Table

Port Range	Protocol	Comment	Select

Port Filtering On/Off: 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.

4.9.3 MAC Filtering



MAC Filtering

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

MAC Filtering On/Off: Disable

Add an MAC Filter Rule

MAC Address:

Comment:

Current Filter Table

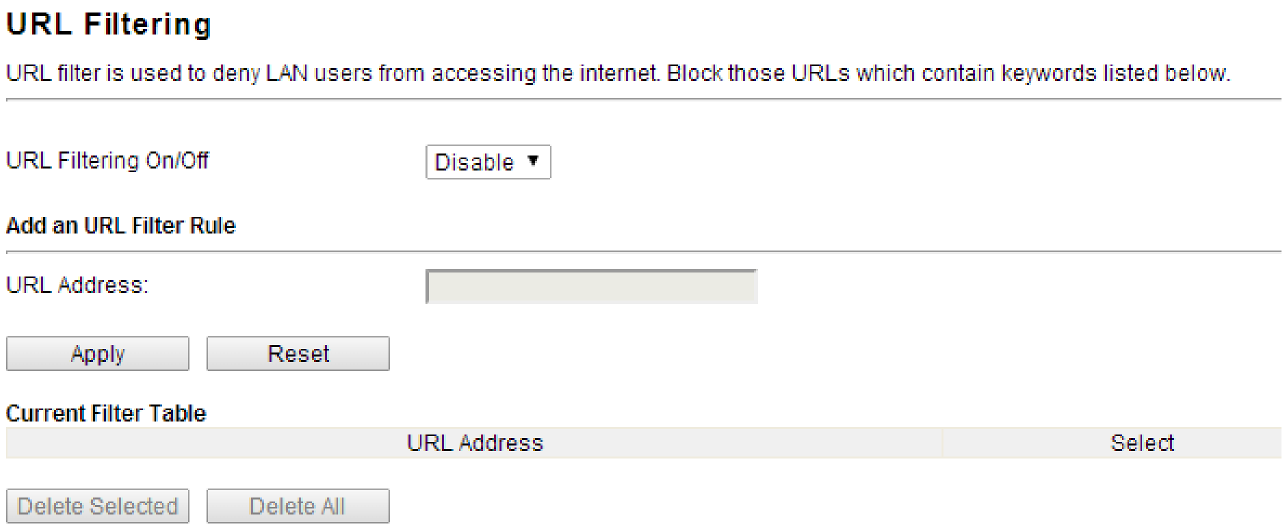
Hostname	MAC Address	Comment	Select

MAC Filtering On/Off: 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.

4.9.4 URL Filtering



URL Filtering

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

URL Filtering On/Off: Disable ▼

Add an URL Filter Rule

URL Address:

Current Filter Table

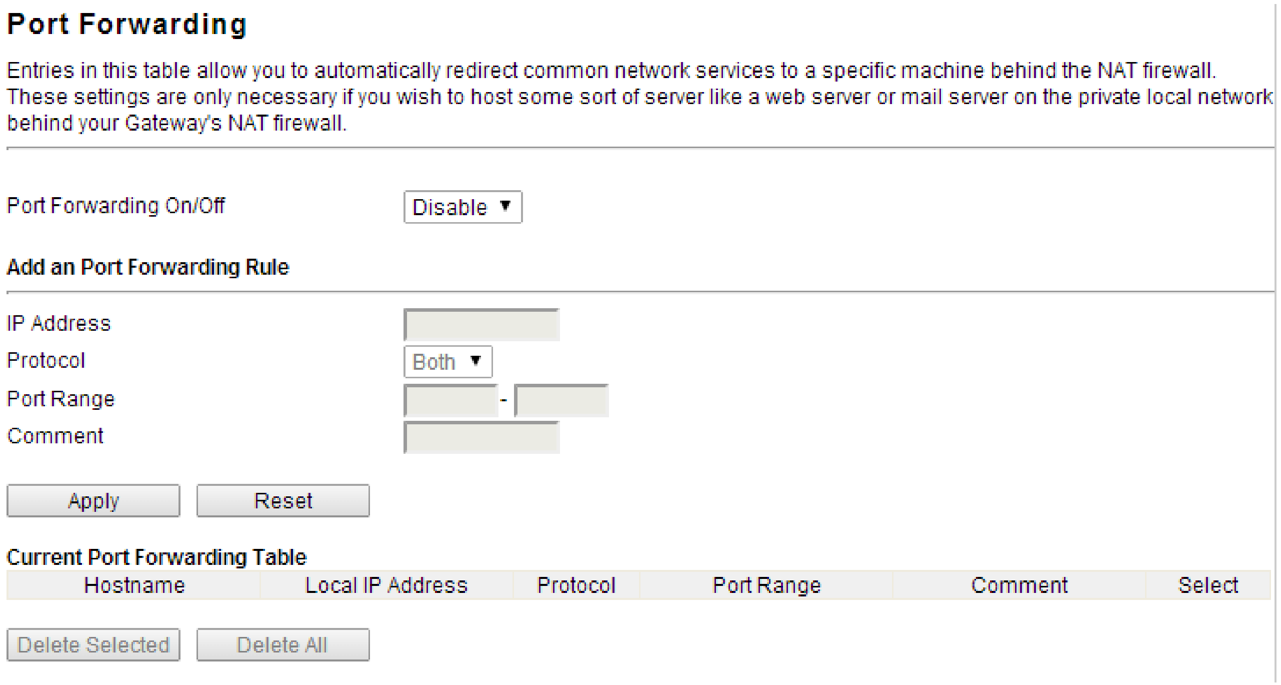
URL Address	Select

URL Filtering On/Off: 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.

4.9.5 Port Forwarding



Port Forwarding

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

Port Forwarding On/Off: Disable ▼

Add an Port Forwarding Rule

IP Address

Protocol: Both ▼

Port Range -

Comment

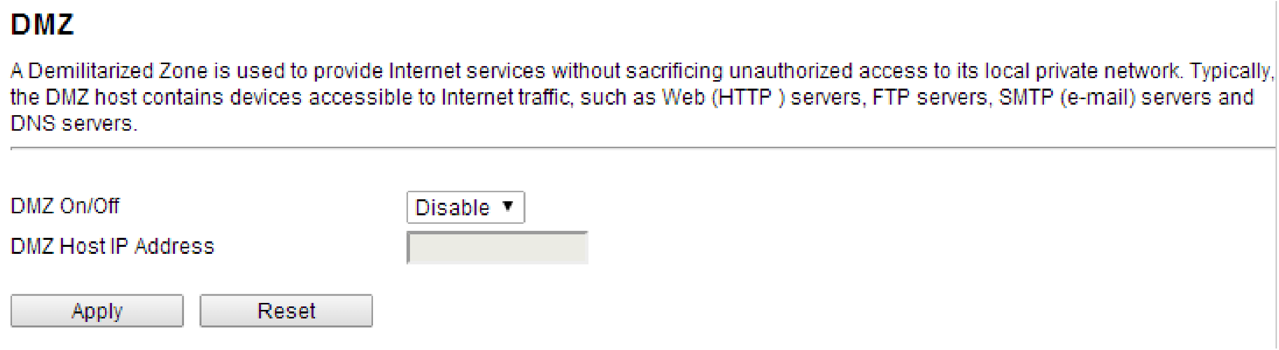
Current Port Forwarding Table

Hostname	Local IP Address	Protocol	Port Range	Comment	Select

Port Forwarding On/Off: you can select this checkbox to enable Port Forwarding function.
IP 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.

4.9.6 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.



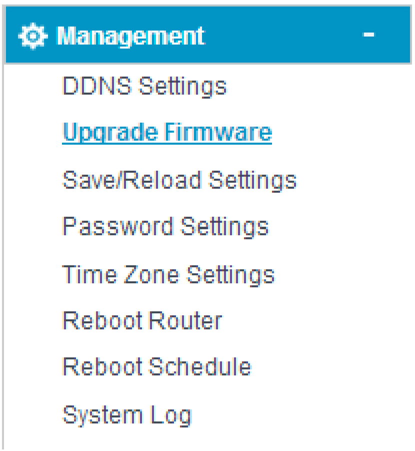
DMZ

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

DMZ On/Off: Disable ▼
DMZ Host IP Address:

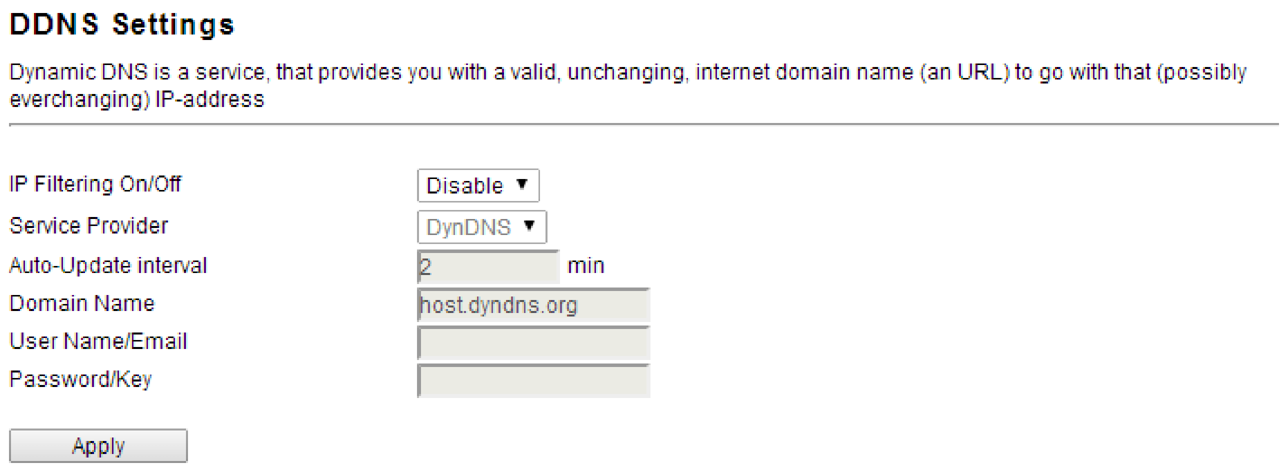
DMZ On/Off: you can select this checkbox to Enable DMZ function.
DMZ Host IP Address: type in the IP address of the DMZ host.

4.10 Management



4.10.1 DDNS Settings

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.



DDNS Settings

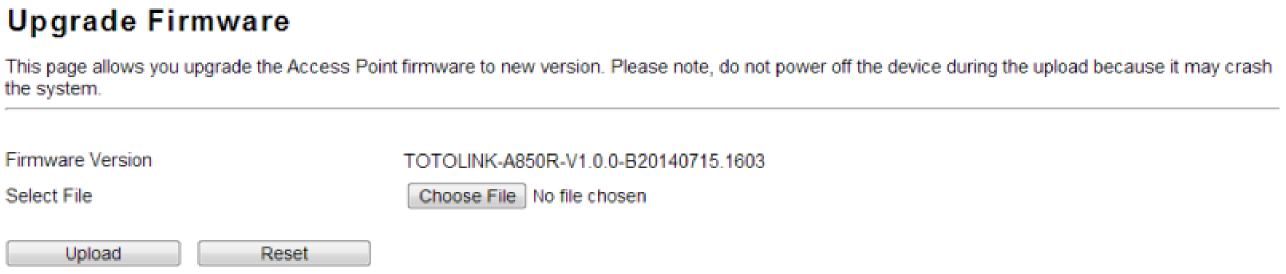
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address

IP Filtering On/Off	Disable ▼
Service Provider	DynDNS ▼
Auto-Update interval	2 min
Domain Name	host.dyndns.org
User Name/Email	
Password/Key	

4.10.2 Upgrade Firmware

New version of firmware will be released to improve the various efficiency or to fix some bugs. Following the steps show below so as to realize upgrading. 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.



Upgrade Firmware

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

Firmware Version	TOTOLINK-A850R-V1.0.0-B20140715.1603
Select File	Choose File No file chosen

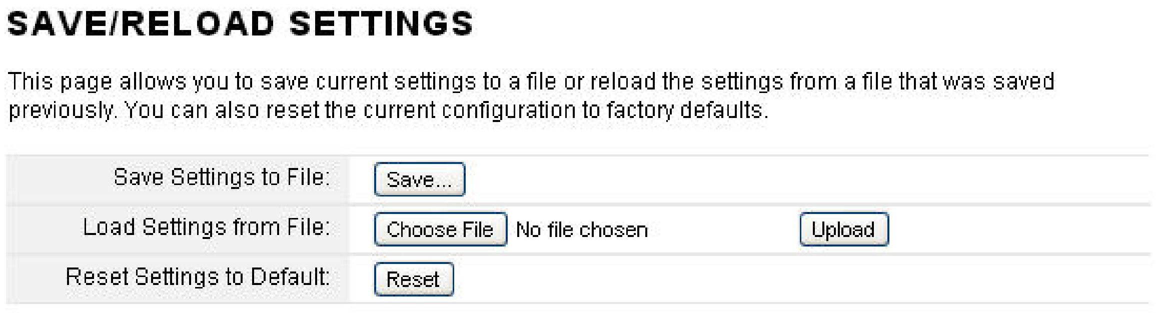
Firmware version: shows the current firmware version.

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

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

4.10.3 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.

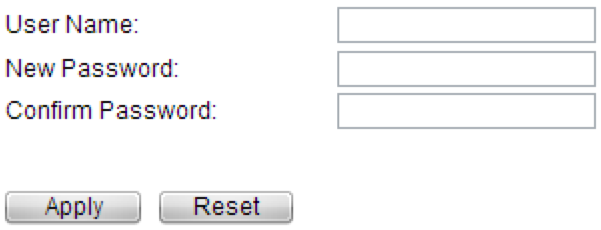


SAVE/RELOAD SETTINGS

This page allows you to save current settings to a file or reload the settings from a file that was saved previously. You can also reset the current configuration to factory defaults.

Save Settings to File:	Save...
Load Settings from File:	Choose File No file chosen Upload
Reset Settings to Default:	Reset

4.10.4 Password Settings



User Name:

New Password:

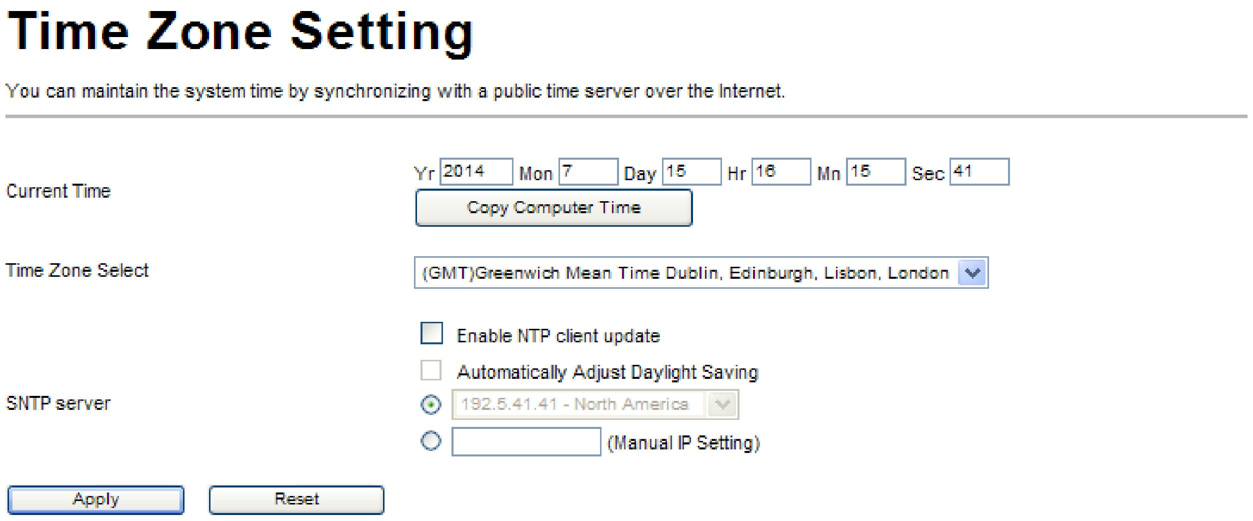
Confirm Password:

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.*

4.10.5 Time Zone Setting

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



Time Zone Setting

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

Current Time: Yr 2014 Mon 7 Day 15 Hr 16 Mn 15 Sec 41

Time Zone Select: (GMT)Greenwich Mean Time Dublin, Edinburgh, Lisbon, London

□ Enable NTP client update

□ Automatically Adjust Daylight Saving

SNTP server: ● 192.5.41.41 - North America

○ (Manual IP Setting)

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.

4.10.6 Reboot Router

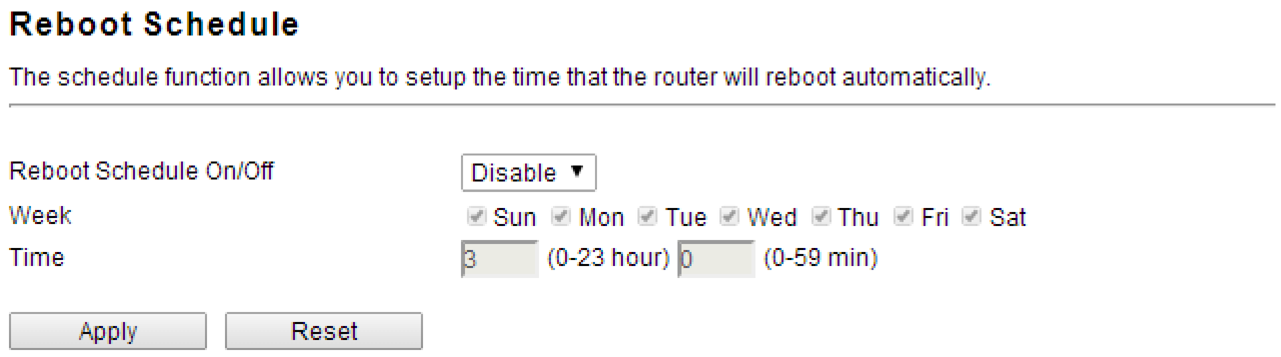
Please click this **Reboot** button to reboot your router quickly.

Reboot Router

Reboot Router [Reboot Router]

4.10.7 Schedule Reboot

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



Reboot Schedule

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

Reboot Schedule On/Off: Disable ▼

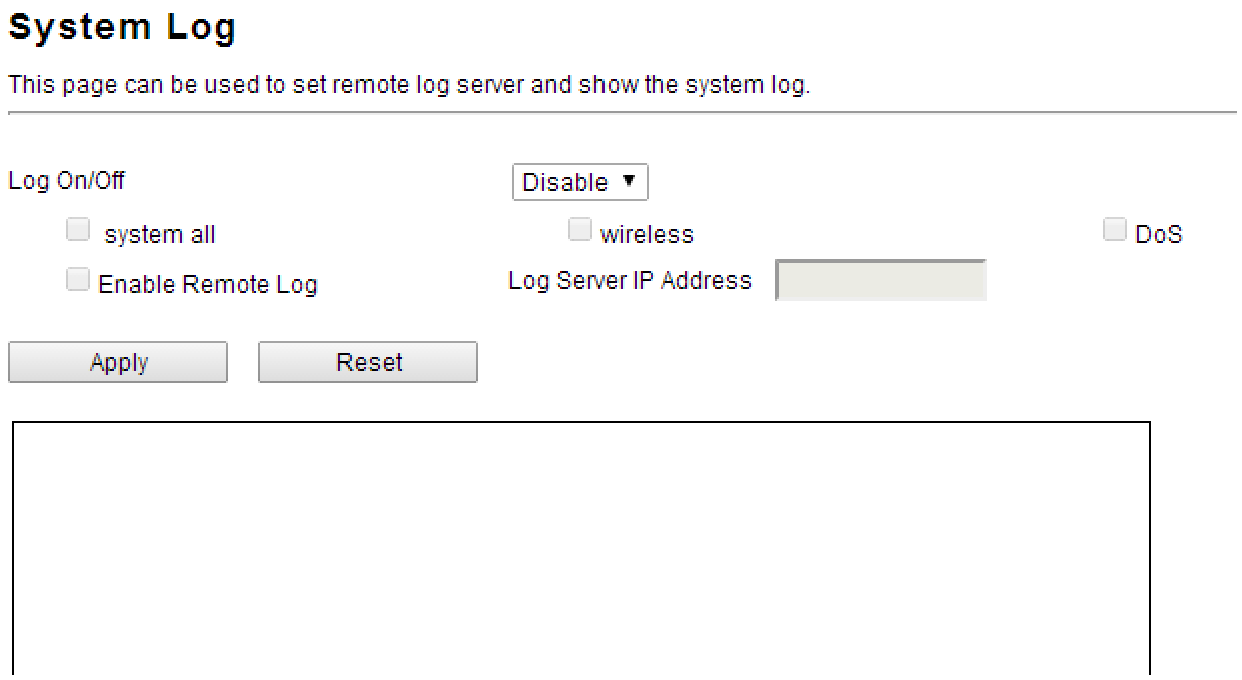
Week: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time: 3 (0-23 hour) 0 (0-59 min)

[Apply] [Reset]

4.10.8 System Log

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



System Log

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

Log On/Off: Disable ▼

□ system all □ wireless □ DoS

□ Enable Remote Log Log Server IP Address

[Apply] [Reset]

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

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

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

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

FCC Statement

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

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

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.