Table of Contents

Copyright Statement

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

1. ABOUT THIS GUIDE

Thank you very much for purchasing this Wireless N ADSL Modem Router. This guide will introduce the features of the Modem Router and tell you how to connect and setup the router. Please follow the instructions in this guide to avoid affecting the Modem Router's performance by improper operation.

1.1 Navigation of the User's Guide

Product Overview: Describes functions, features and appearance of the Modem Router.

Hardware Installation: Describes the hardware installation and configuration of your PC.

Connecting to Internet: Tells how you can setup the Modem Router quickly to access Internet.

Advanced Settings: Lists all technical functions including Interface Setup, Advanced Setup, Access Management and Maintenance.

2. PRODUCT OVERVIEW

2.1 Introduction

This device is a Wireless ADSL Modem Router which integrates functions of high speed ADSL Modem, wireless router and 4-port switch. It complies with the most advanced IEEE 802.11n standard and can deliver up to 300Mbps wireless data rate. It also supports the latest ADSL 2/2+ standards to provide higher performance for users and make the transmission coverage wider than other devices.

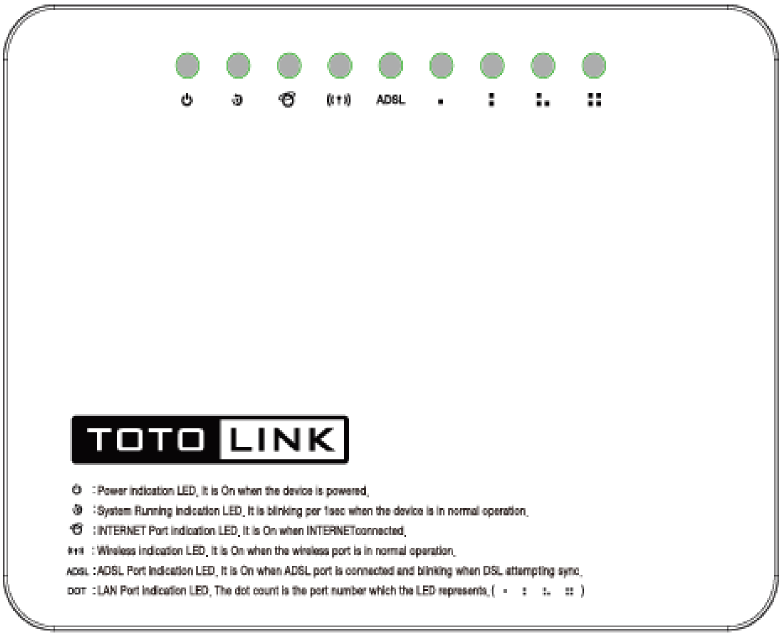
2.2 Features

- Complies with IEEE 802.11n/g/b standards for 2.4GHz Wireless LAN.
- Up to 300Mbps data rate for Wi-Fi network.
- Combines functions of high speed ADSL Modem, wireless router and 4-port switch.
- Supports both ADSL and LAN broadband access.
- Provides 64/128-bit WEP, WPA, WPA2 and WPA/WPA2 (TKIP+AES) security.
- Supports PVC detecting automatically.
- Supports IPv6 protocol.
- The IP, MAC and URL filtering makes access and time control more flexibly.
- Repeater and WDS function for easy WiFi expansion.
- QoS function allocates network bandwidth reasonably.
- WiFi on/off and Power on/off buttons make configuration simple.
- IGMP multicast and IGMP proxy are supported.
- Supports both ADSL and WAN broadband access.

2.3 Panel Layout

2.3.1 Front Panel

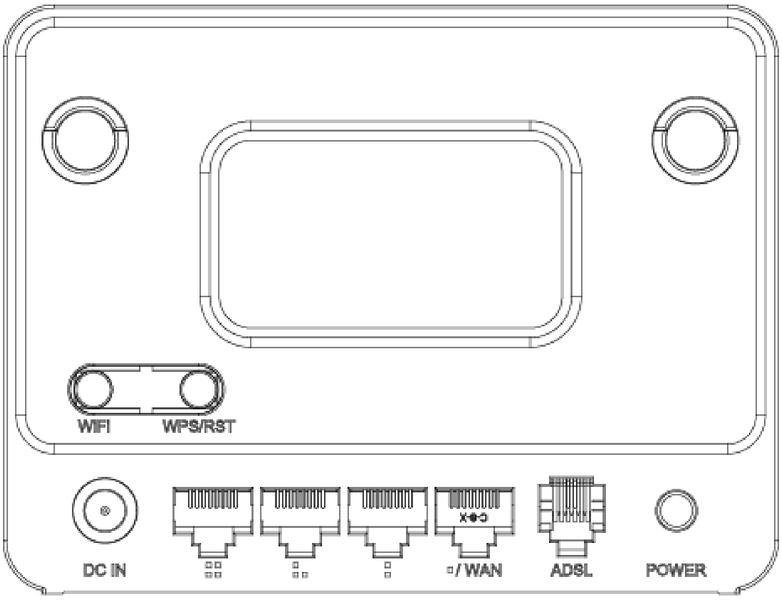
The front panel of Modem Router consists of 9 LEDs, which is designed to indicate connection status.


ADSL
TOTO LINK
: Power indication LED, It is On when the device is powered,
: System Running indication LED, It is blinking per 1sec when the device is in normal operation,
: INTERNET Port indication LED, It is On when INTERNETconnected,
: Wireless indication LED, It is On when the wireless port is in normal operation,
ADSL : ADSL Port indication LED, It is On when ADSL port is connected and blinking when DSL attempting sync,
DOT : LAN Port indication LED, The dot count is the port number which the LED represents,( )

POWER	This indicator lights blue when the router powered on, otherwise it is off.
CPU	When the router powered on, this indicator keeps lighting.
ADSL	It is on when ADSL port is connected and blinking when there are data transmitting.
Internet	It is on when Internet is connected.
WLAN	This indicator lights when the wireless connection enabled.
1/2/3/4 LAN	When the LAN port has a successful connection, the indicator lights.
	While transmitting or receiving data through the LAN port the indicator blinks.

2.3.2 Rear Panel

The figure below shows the rear panel of Modem Router.



DC IN	This socket is used to connect the power adapter.
WiFi ON/OFF	This slide switch is used to turn on or turn off WiFi.
ADSL	This RJ11 ADSL port is used to connect to ADSL modem
Power ON/OFF	Turn on or turn off the router by the switch.
2/3/4 LAN	This port is used to connect the router to local PC.
1 LAN/WAN	This port is where you will connect the DSL/cable Modem, Ethernet or local PC.
WPS/RST	**WPS:** If you have client devices you can press this button to quickly establish secured connections between this router and client devices.
	RST: There is a RST button on the opposite side of the rear panel which is used to reset the router to factory default settings. Press the button for more than 5 seconds, the router will restore factory settings.

3. HARDWARE INSTALLATION

3.1 Hardware Installation

For the first time you use this ADSL Router, wired connection is recommended to setup the router. Please follow below steps to build correct connections through provided UTP cables.

Step1: Connect Modem Router's ADSL port to external Filter's (provided by your ISP) ADSL port.

Step 2: Connect your PC's network interface to any one LAN port of Modem Router.

Step 3: Plug the Power adapter into the router and then into an outlet.

Step 4: Power on the Router and turn on your PC.

3.2 Check the Installation

The control LEDs of the Modem 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 external filter, the Power, CPU, ADSL and LAN ports LEDs of the Modem Router will light up indicating a normal status.

2. After a few seconds, the LAN LED indicators without connection go out and WLAN indicator will light up.

3.3 Set up PC

The default IP address of the Router is 192.168.0.1, 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.

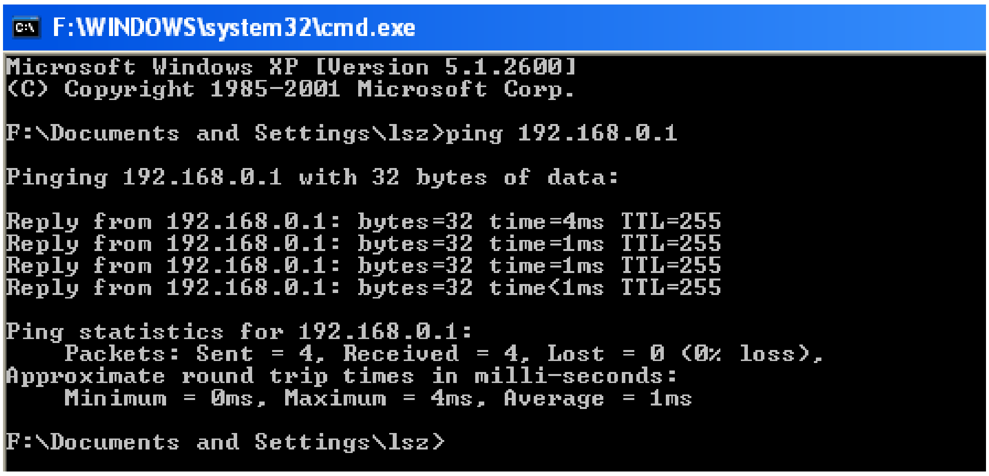
◆ **Configure the IP address manually**

1. Set up the TCP/IP Protocol for your PC.
2. Configure the network parameters. The IP address is 192.168.0.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.0.1 (Router's default IP address).

◆ **Obtain an IP address automatically**

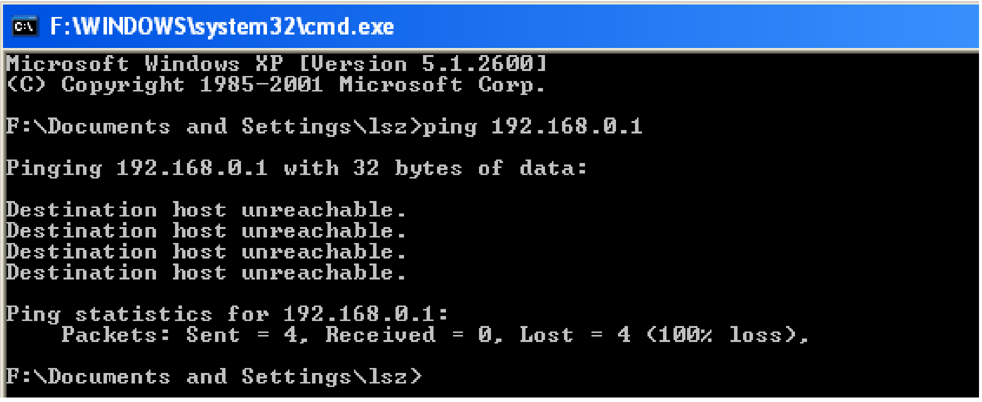
1. Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.
2. Power off the Router and PC. Then turn on the Router and restart the PC. The built-in DHCP server will assign IP address for the PC.

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 192.168.0.1**, then press **Enter.**



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lsz>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=4ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

F:\Documents and Settings\lsz>
```

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



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lsz>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

F:\Documents and Settings\lsz>
```

If the result displayed is similar to that shown in the above figure, it means that your PC has not connected to the Router successfully. Please check it following below steps:

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

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

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

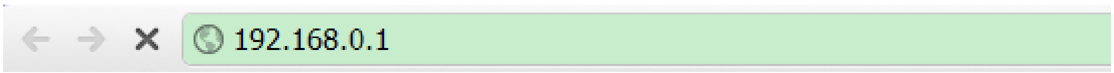
Since the Router's IP address is 192.168.0.1, your PC's IP address must be within the range of 192.168.0.2 ~ 192.168.0.254, the Gateway must be 192.168.0.1.

4. EASY SETUP

This chapter introduces how to **Easy Setup** the Modem Router so that users can easily finish the settings step by step following with the guide to access Internet.

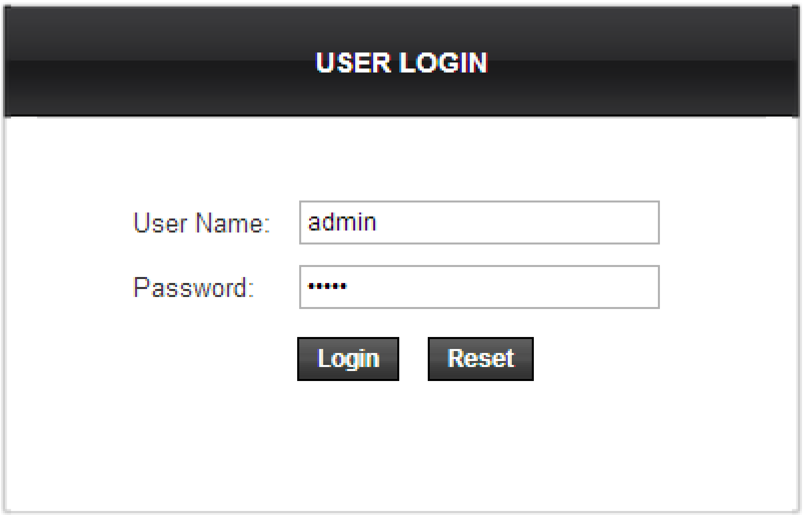
4.1 Accessing Web page

Connect to the Modem Router by typing **http://192.168.0.1** in the address field of Web Browser. Then press **Enter** key.



192.168.0.1

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



USER LOGIN

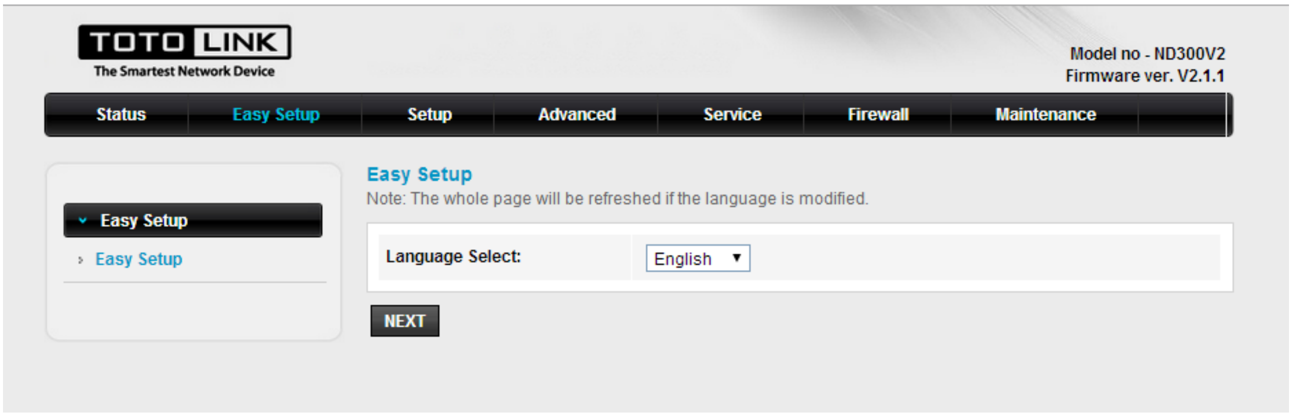
User Name: admin

Password: •••••

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

> ***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 Modem Router. First, you can see the **Easy Setup** page.



Model no - ND300V2
Firmware ver. V2.1.1

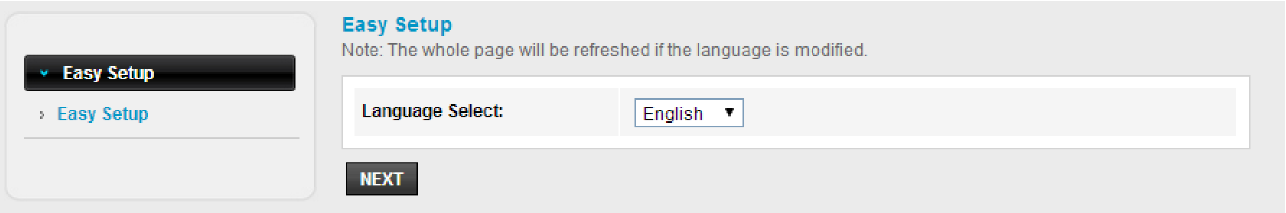
Easy Setup

Note: The whole page will be refreshed if the language is modified.

Language Select: English ▼

4.2 Easy Setup

Easy Setup is provided as part of the web configuration utility. Users can follow the introductions to finish the basic settings of the Modem Router step by step.
Select language at first and click **NEXT** button.



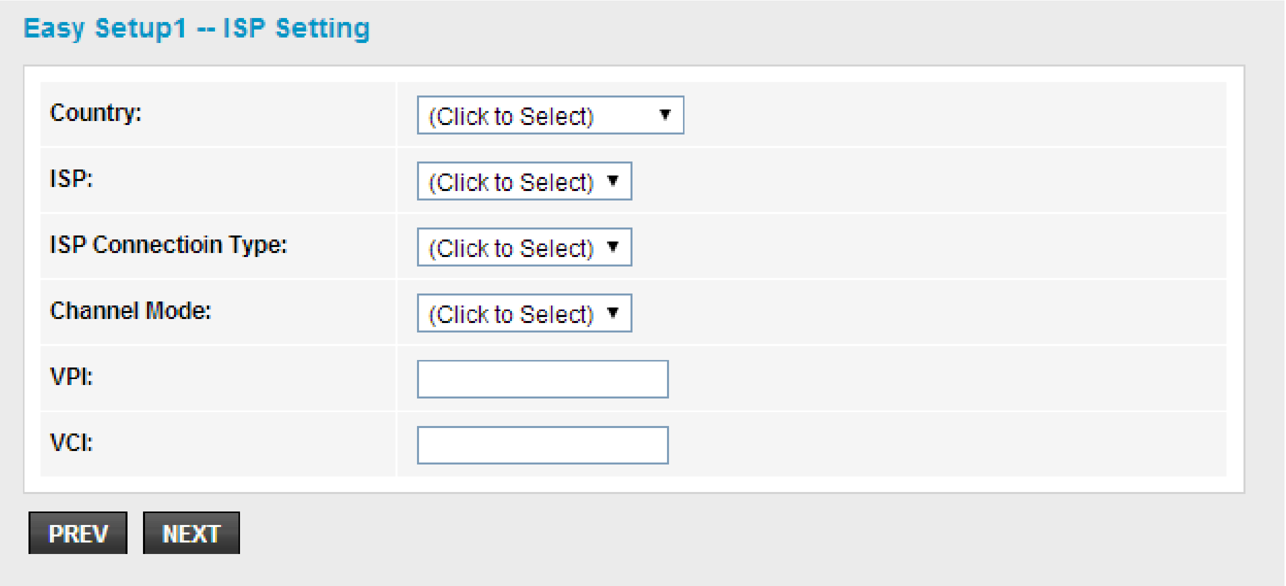
Easy Setup

Note: The whole page will be refreshed if the language is modified.

Language Select: English ▼

4.2.1 ISP Setting

You’re required to choose one ISP Connection Type, after configuration is finished, please click **NEXT** to continue the setting.



Easy Setup1 -- ISP Setting

Country:	(Click to Select) ▼
ISP:	(Click to Select) ▼
ISP Connectioin Type:	(Click to Select) ▼
Channel Mode:	(Click to Select) ▼
VPI:	
VCI:	

Country: please select the correct country name.
ISP Connection Type: there are five ISP connection type supported: PPPoE, PPPoA,

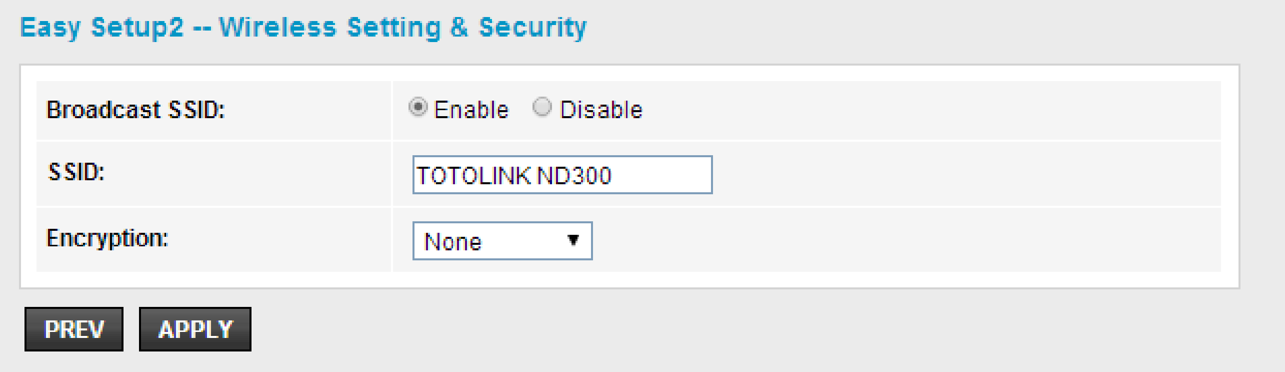
Dynamic IP, Static IP and Bridge.

VPI: Virtual Path Identifier, this is based on the region you are living, generally provided by ISP.

VCI: Virtual Channel Identifier, this is based on the region you are living, generally provided by ISP.

4.2.2 Wireless Setting& Security

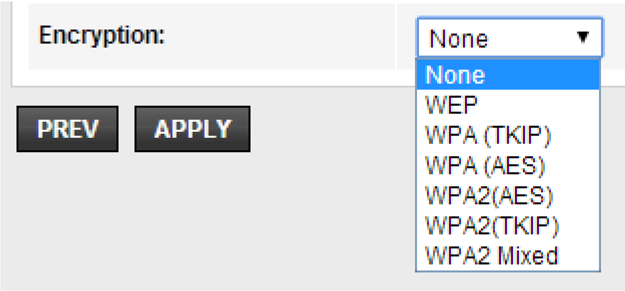
In this page, you can disable or enable SSID broadcast, change the Wireless SSID and also the encryption mode, after changing settings, please click **APPLY** to finish easy setup.



Easy Setup2 -- Wireless Setting & Security

Broadcast SSID:	● Enable ○ Disable
SSID:	TOTOLINK ND300
Encryption:	None

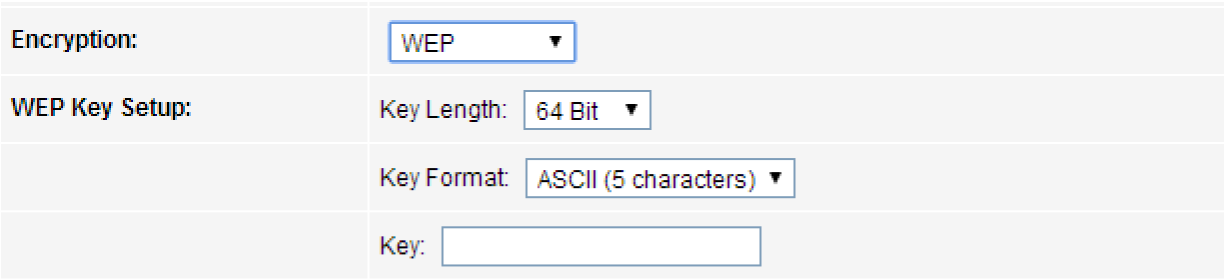
Encryption: choose an encryption method for this wireless network, WEP, WPA, WPA2 and WPA2 Mixed can be selected here.



Encryption: None

1. WEP

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes.



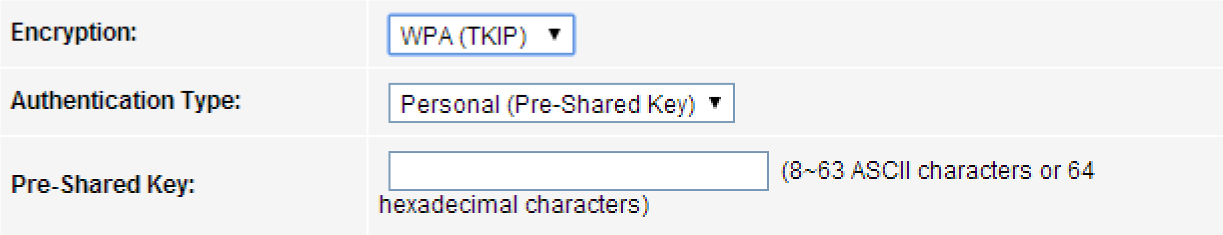
Encryption:	WEP
WEP Key Setup:	Key Length: 64 Bit
	Key Format: ASCII (5 characters)
	Key:

2. 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.

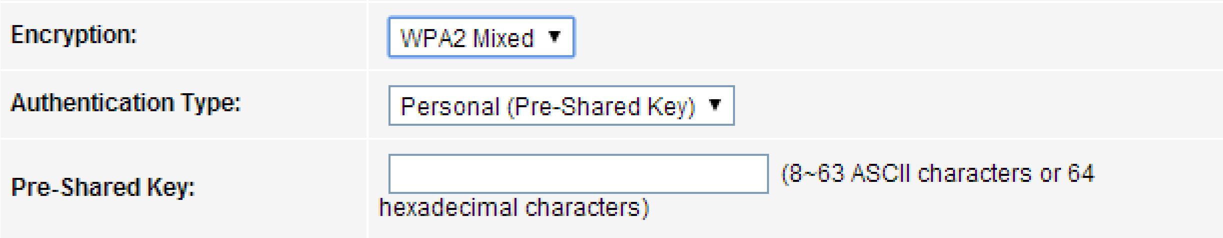


Encryption:	WPA (TKIP) ▼
Authentication Type:	Personal (Pre-Shared Key) ▼
Pre-Shared Key:	(8~63 ASCII characters or 64 hexadecimal characters)

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…”).

2. WPA2-Mixed (Recommended)

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

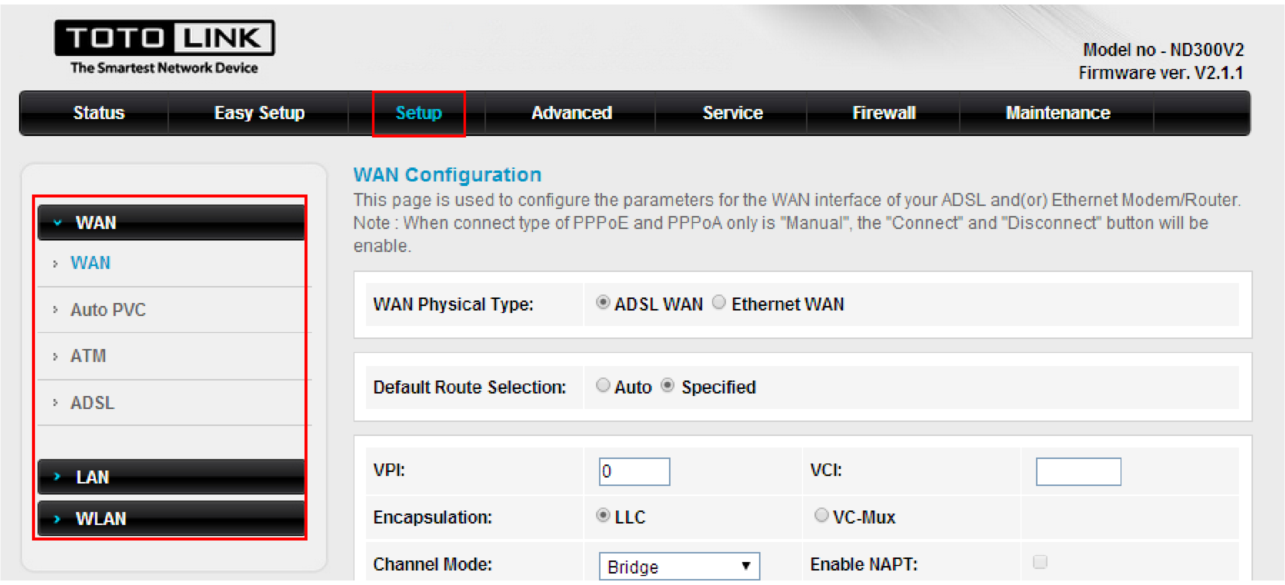


Encryption:	WPA2 Mixed ▼
Authentication Type:	Personal (Pre-Shared Key) ▼
Pre-Shared Key:	(8~63 ASCII characters or 64 hexadecimal characters)

5. ADVANCED SETUP

5.1 Setup

This setup interface allows you to configure WAN, LAN and WLAN settings.



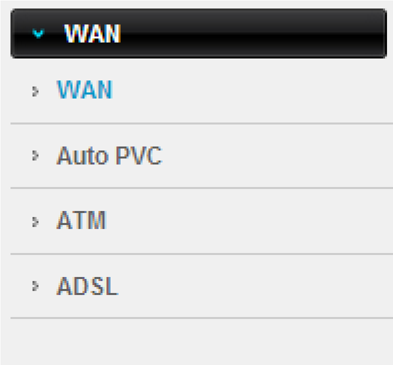
Model no - ND300V2
Firmware ver. V2.1.1

WAN Configuration

This page is used to configure the parameters for the WAN interface of your ADSL and(or) Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

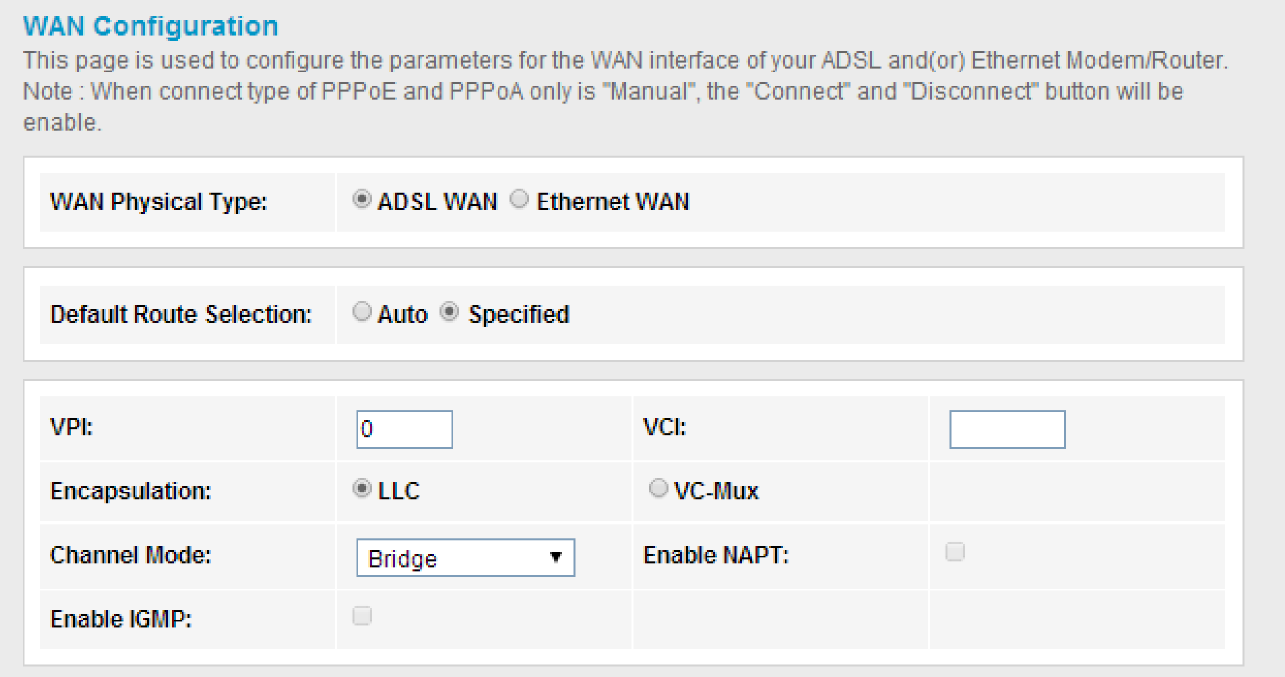
WAN Physical Type:	● ADSL WAN ○ Ethernet WAN		
Default Route Selection:	○ Auto ● Specified		
VPI:	0	VCI:	
Encapsulation:	● LLC	○ VC-Mux	
Channel Mode:	Bridge ▼	Enable NAPT:	□

5.1.1 WAN



5.1.1.1 WAN

The ADSL router provides ADSL WAN or Ethernet WAN for you to connect to Internet. Select one type accordingly and enter the parameters provided by your ISP.



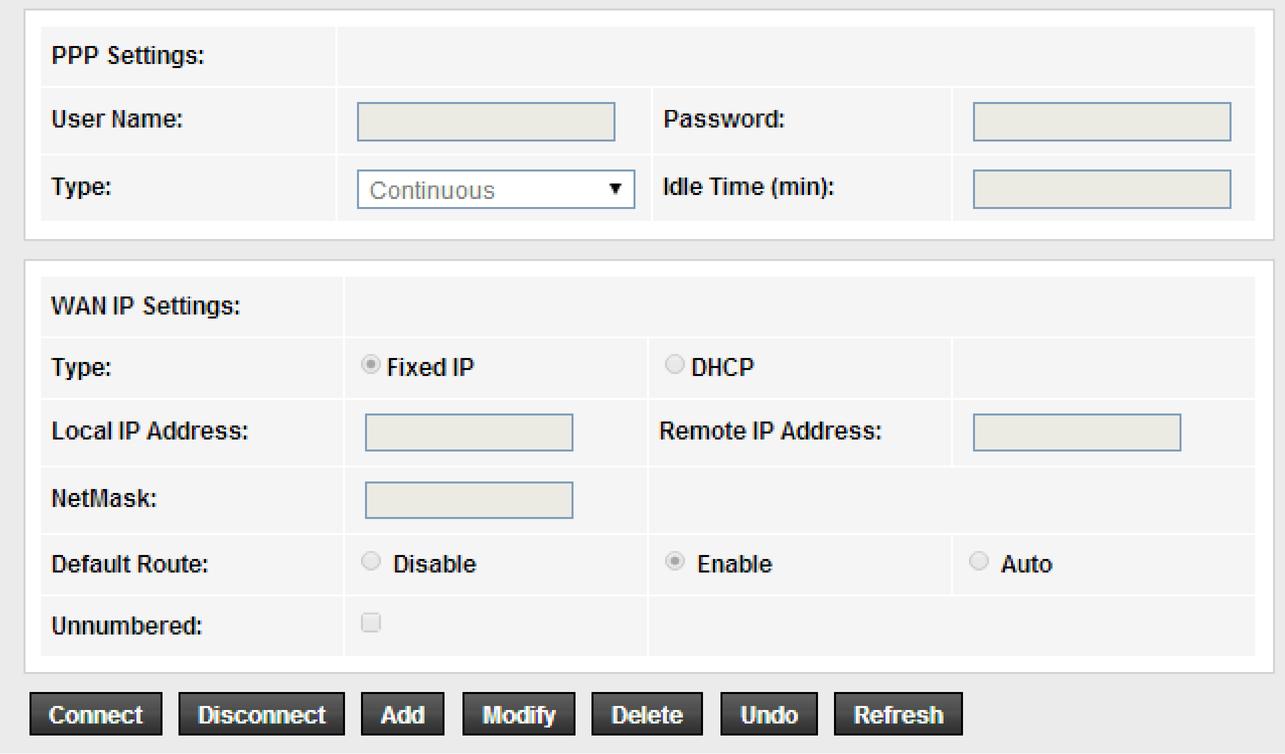
WAN Configuration

This page is used to configure the parameters for the WAN interface of your ADSL and(or) Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

WAN Physical Type:	● ADSL WAN ○ Ethernet WAN

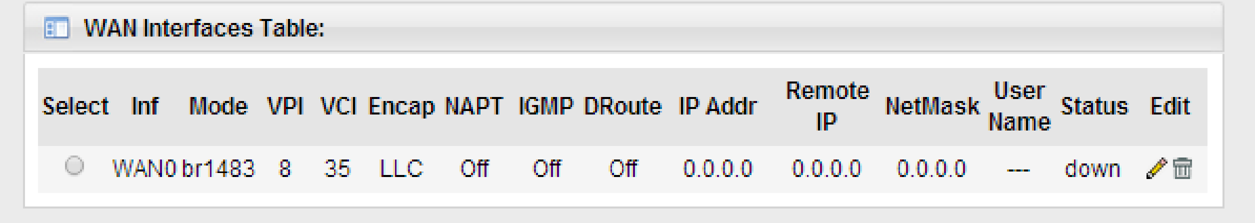
Default Route Selection:	○ Auto ● Specified

VPI:	0	VCI:	
Encapsulation:	● LLC	○ VC-Mux	
Channel Mode:	Bridge ▼	Enable NAPT:	□
Enable IGMP:	□		



PPP Settings:			
User Name:		Password:	
Type:	Continuous ▼	Idle Time (min):	

WAN IP Settings:			
Type:	● Fixed IP	○ DHCP	
Local IP Address:		Remote IP Address:	
NetMask:			
Default Route:	○ Disable	● Enable	○ Auto
Unnumbered:	□		

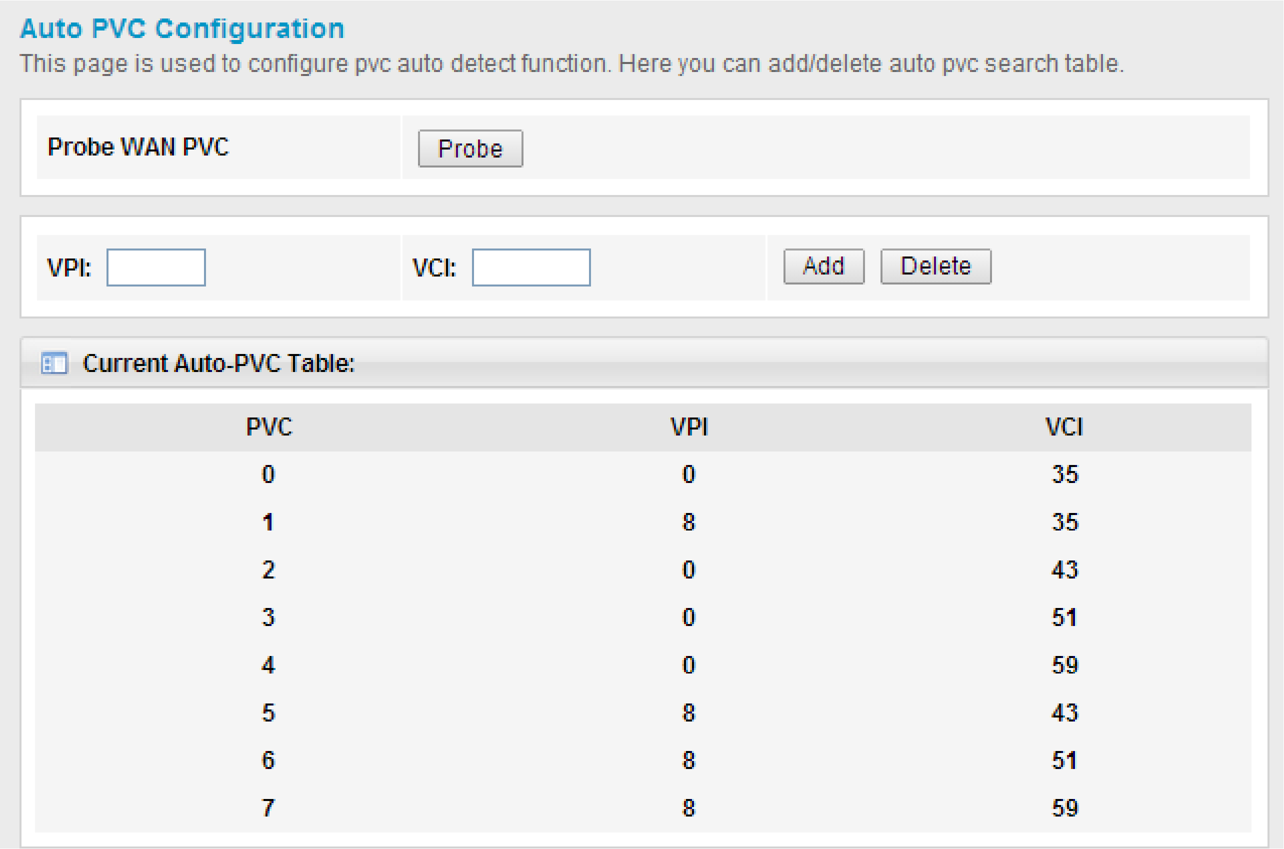


WAN Interfaces Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IGMP	DRoute	IP Addr	Remote IP	NetMask	User Name	Status	Edit
○	WAN0	br1483	8	35	LLC	Off	Off	Off	0.0.0.0	0.0.0.0	0.0.0.0	---	down	✎ 🗑

5.1.1.2 Auto PVC

PVC auto detecting can be setup in this page.



Auto PVC Configuration

This page is used to configure pvc auto detect function. Here you can add/delete auto pvc search table.

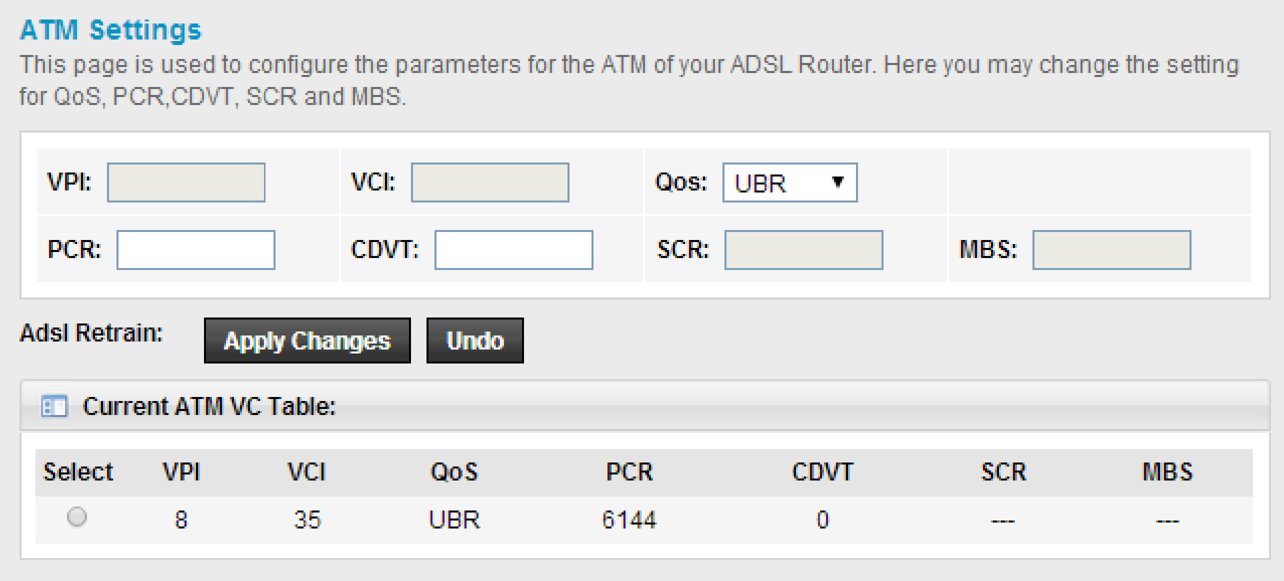
Current Auto-PVC Table:

PVC	VPI	VCI
0	0	35
1	8	35
2	0	43
3	0	51
4	0	59
5	8	43
6	8	51
7	8	59

VPI: Virtual Path Identifier, this is based on the region you are living, generally provided by ISP.

VCI: Virtual Channel Identifier, this is based on the region you are living, generally provided by ISP.

5.1.1.3 ATM



ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for QoS, PCR,CDVT, SCR and MBS.

Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	8	35	UBR	6144	0	---	---

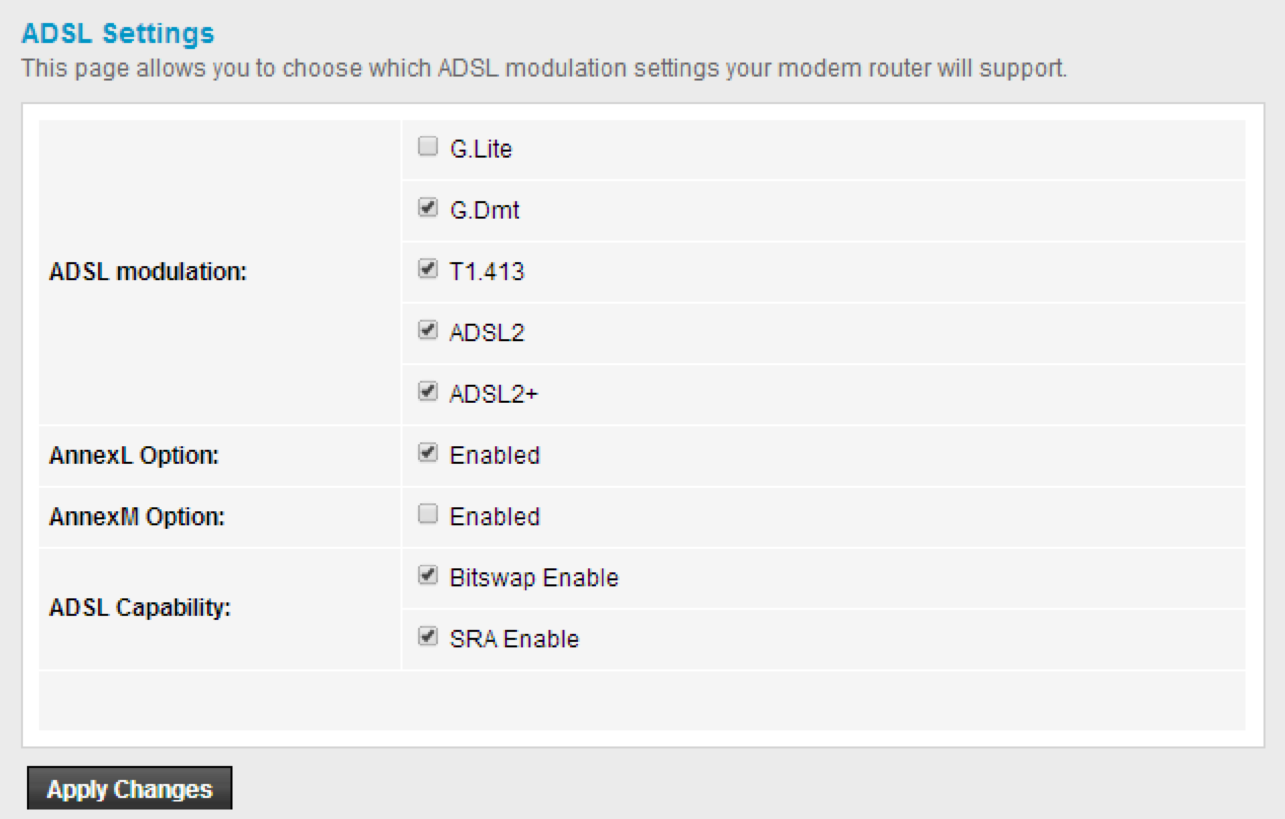
VPI: Virtual Path Identifier, this is based on the region you are living, generally provided by ISP.

VCI: Virtual Channel Identifier, this is based on the region you are living, generally provided by ISP.

ATM QoS: Choose the ATM QoS type provided by your ISP. By default, it is UBR selected.

5.1.1.4 ADSL

This interface allows you to choose some ADSL parameters that your modem router will support. You could keep the default value.

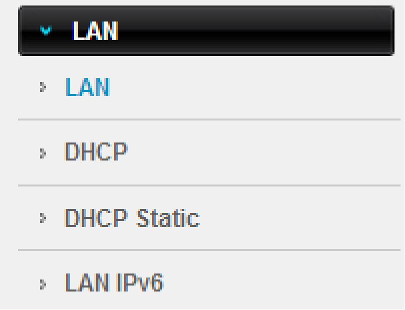


ADSL Settings

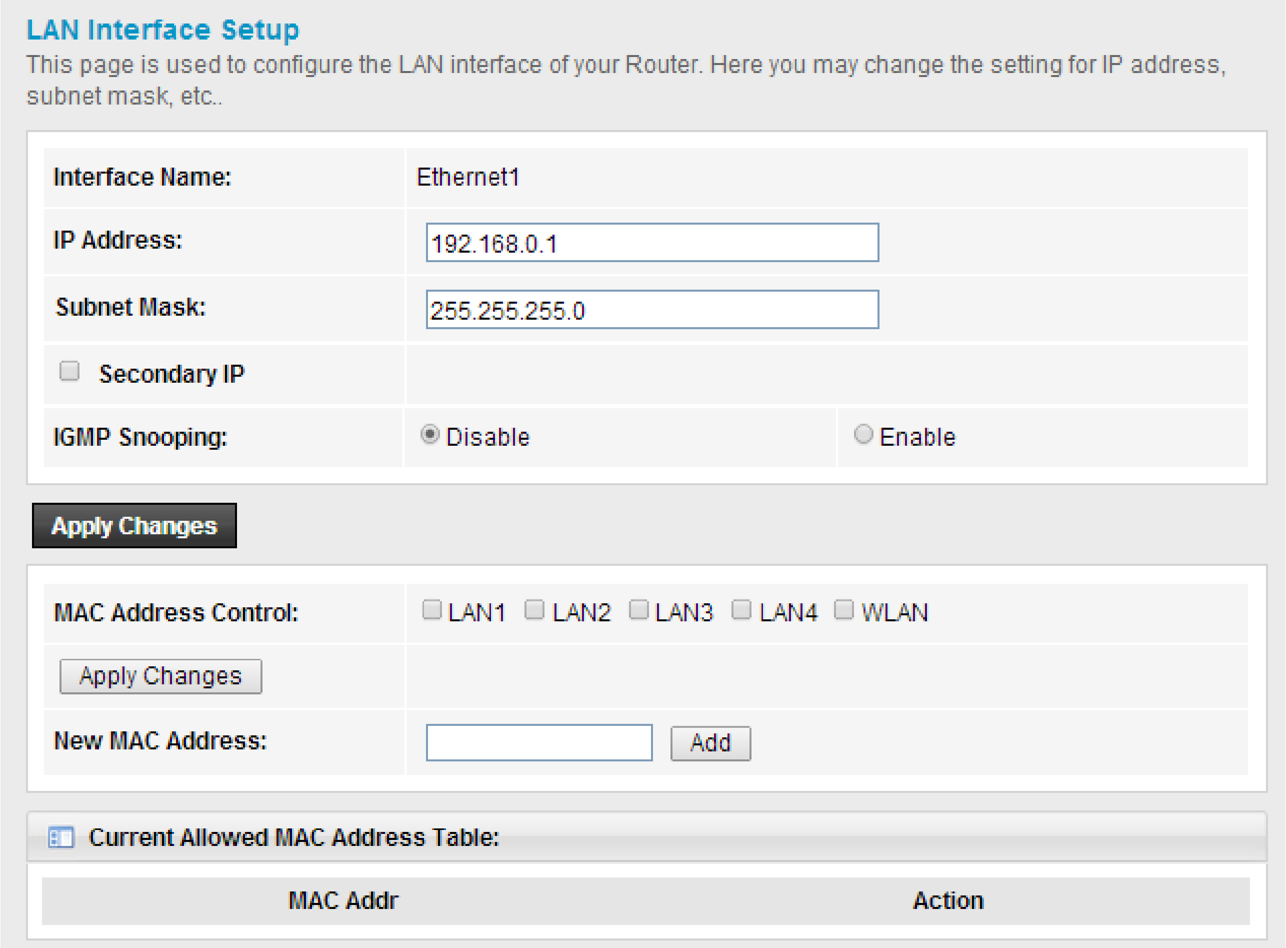
This page allows you to choose which ADSL modulation settings your modem router will support.

ADSL modulation:	☐ G.Lite
	☑ G.Dmt
	☑ T1.413
	☑ ADSL2
	☑ ADSL2+
AnnexL Option:	☑ Enabled
AnnexM Option:	☐ Enabled
ADSL Capability:	☑ Bitswap Enable
	☑ SRA Enable

5.1.2 LAN



5.1.2.1 LAN



LAN Interface Setup

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP address, subnet mask, etc..

Interface Name:	Ethernet1	
IP Address:	192.168.0.1	
Subnet Mask:	255.255.255.0	
□ Secondary IP		
IGMP Snooping:	● Disable	○ Enable

MAC Address Control:	□ LAN1 □ LAN2 □ LAN3 □ LAN4 □ WLAN
Apply Changes	
New MAC Address:	Add

Current Allowed MAC Address Table:

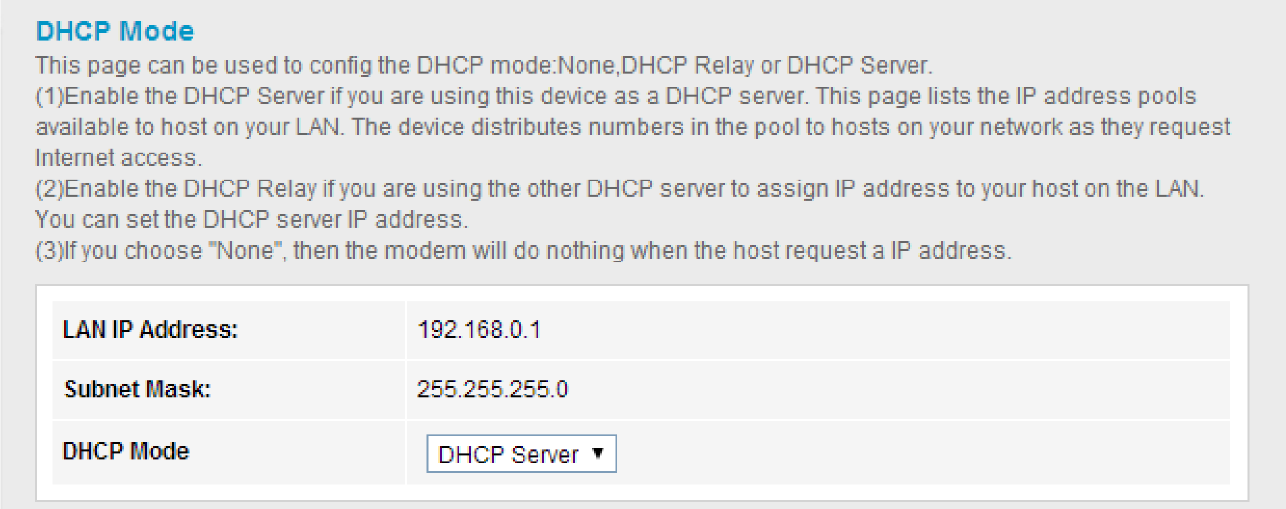
MAC Addr	Action

IP Address: IP Address of this ADSL Router. By default, it is 192.168.0.1. You can change it as well.

Subnet Mask: Subnet Mask of this ADSL Router is 255.255.255.0. Please just keep the value.

5.1.2.2 DHCP

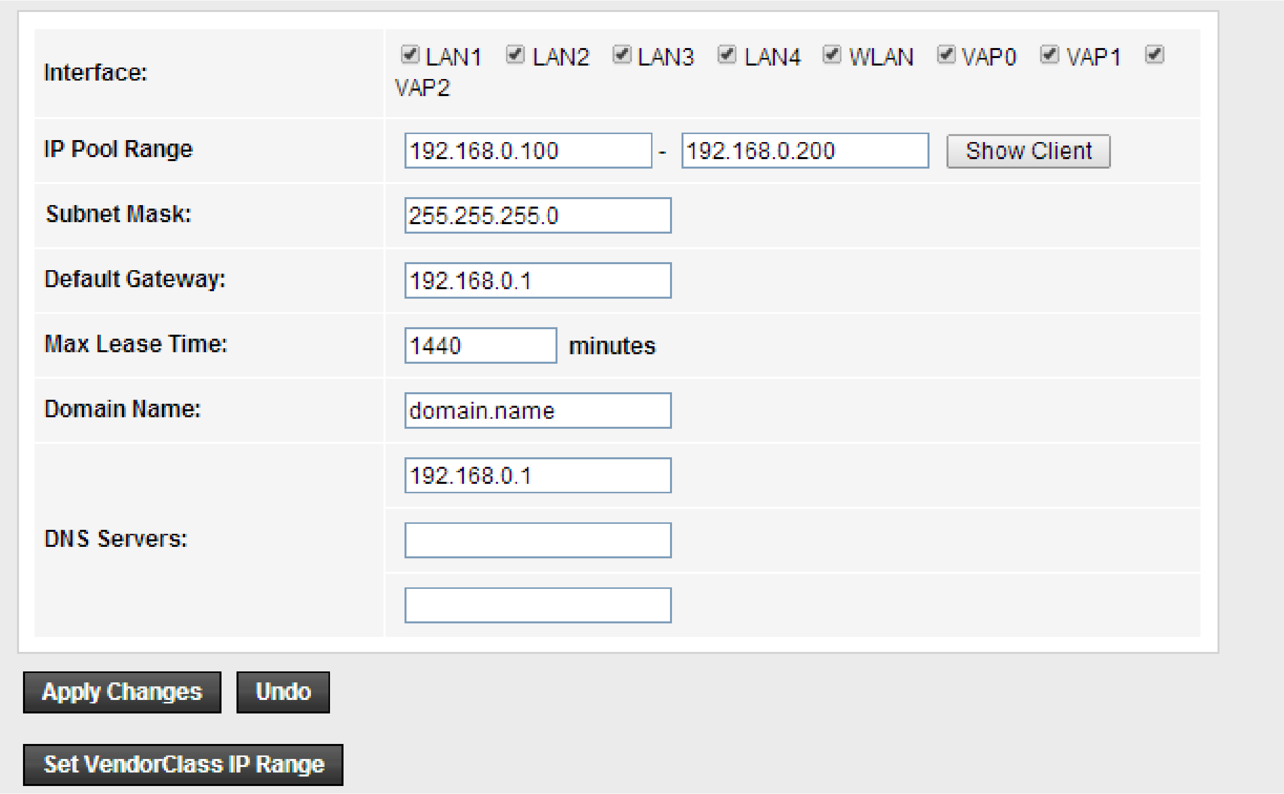
Dynamic Host Configuration Protocol. DHCP service will supply IP settings to computers which are connected to this Router and configured to obtain IP settings automatically.



DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address.
(3)If you choose "None", then the modem will do nothing when the host request a IP address.

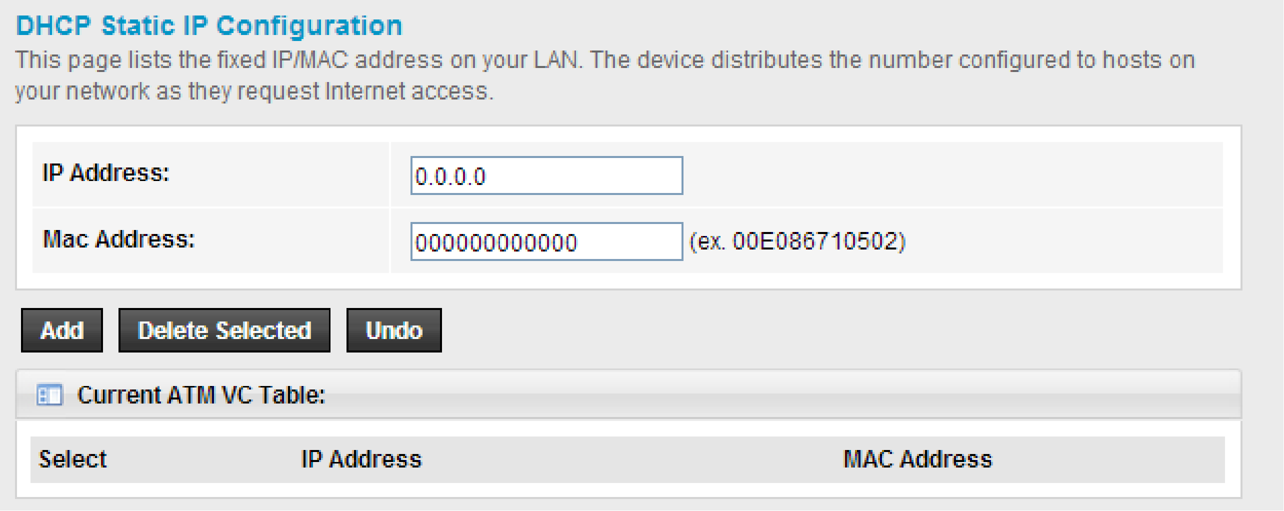
LAN IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
DHCP Mode	DHCP Server ▾



Interface:	☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN ☑ VAP0 ☑ VAP1 ☑ VAP2
IP Pool Range	192.168.0.100 - 192.168.0.200
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Max Lease Time:	1440 minutes
Domain Name:	domain.name
DNS Servers:	192.168.0.1

IP Pool Range: enter an IP address for the DHCP server. Since the default IP address of the Modem Router is 192.168.0.1, the IP pool range is from 192.168.1.100 to 192.168.1.200.

5.1.2.3 DHCP Static



DHCP Static IP Configuration

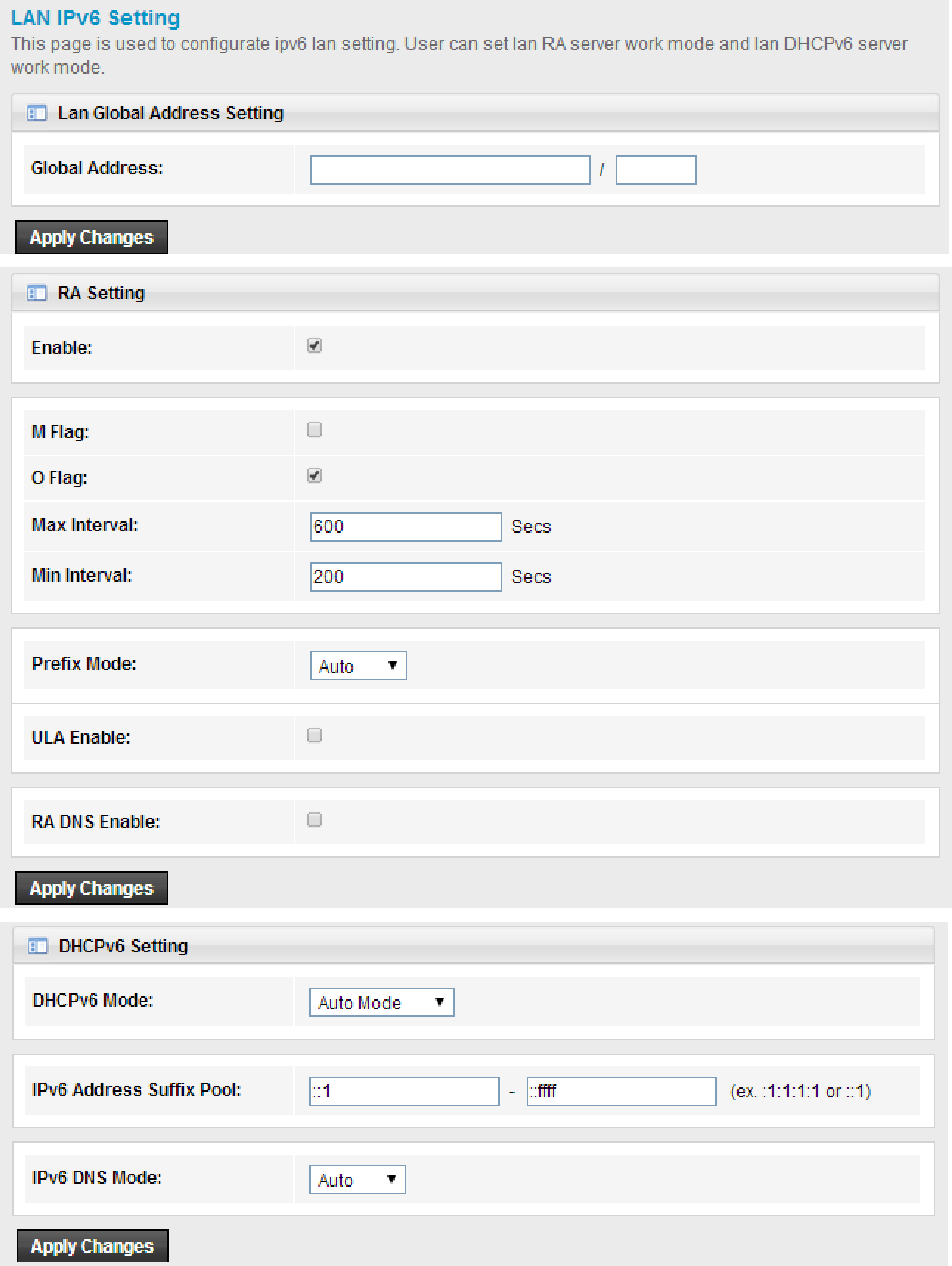
This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

IP Address:	0.0.0.0
Mac Address:	000000000000 (ex. 00E086710502)

Current ATM VC Table:

Select	IP Address	MAC Address

5.1.2.4 LAN IPv6



LAN IPv6 Setting

This page is used to configurate ipv6 lan setting. User can set lan RA server work mode and lan DHCPv6 server work mode.

Lan Global Address Setting

Global Address: ______ / ______

RA Setting

Enable: ☑

M Flag: □

O Flag: ☑

Max Interval: 600 Secs

Min Interval: 200 Secs

Prefix Mode: Auto ▼

ULA Enable: □

RA DNS Enable: □

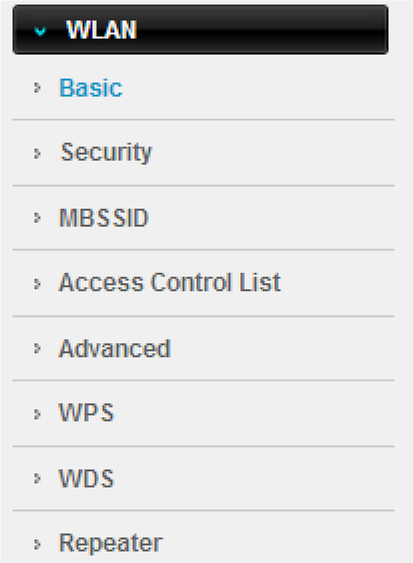
DHCPv6 Setting

DHCPv6 Mode: Auto Mode ▼

IPv6 Address Suffix Pool: ::1 - ::ffff (ex. :1:1:1:1 or ::1)

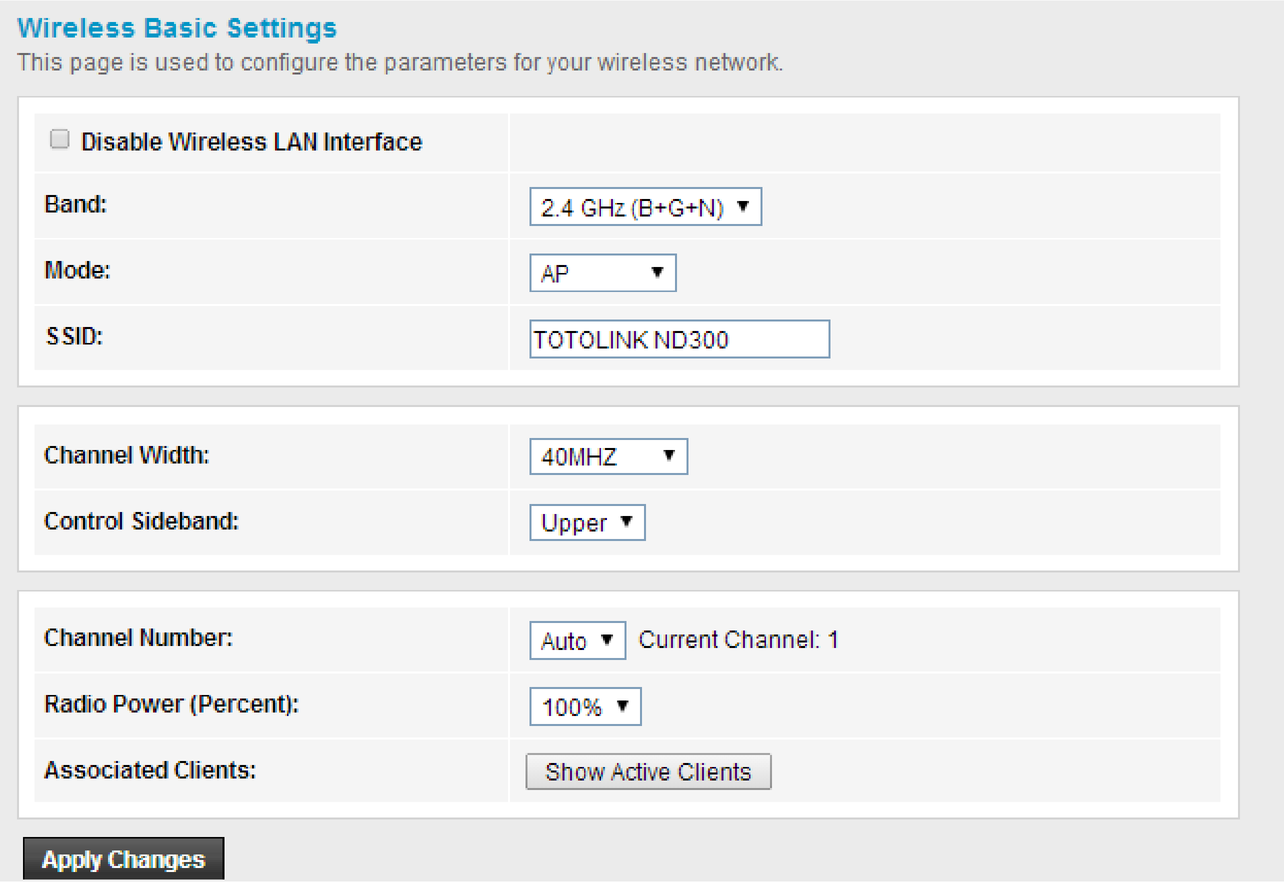
IPv6 DNS Mode: Auto ▼

5.1.3 WLAN



5.1.3.1 Basic

On this page, you could configure the parameters for Wireless LAN client that may connect to your Access Point.



Wireless Basic Settings

This page is used to configure the parameters for your wireless network.

□ Disable Wireless LAN Interface	
Band:	2.4 GHz (B+G+N) ▼
Mode:	AP ▼
SSID:	TOTOLINK ND300
Channel Width:	40MHZ ▼
Control Sideband:	Upper ▼
Channel Number:	Auto ▼ Current Channel: 1
Radio Power (Percent):	100% ▼
Associated Clients:	Show Active Clients

Band: Specifies the standards this Modem Router complies with. Generally, it is 2.4GHz (B+G+N) selected

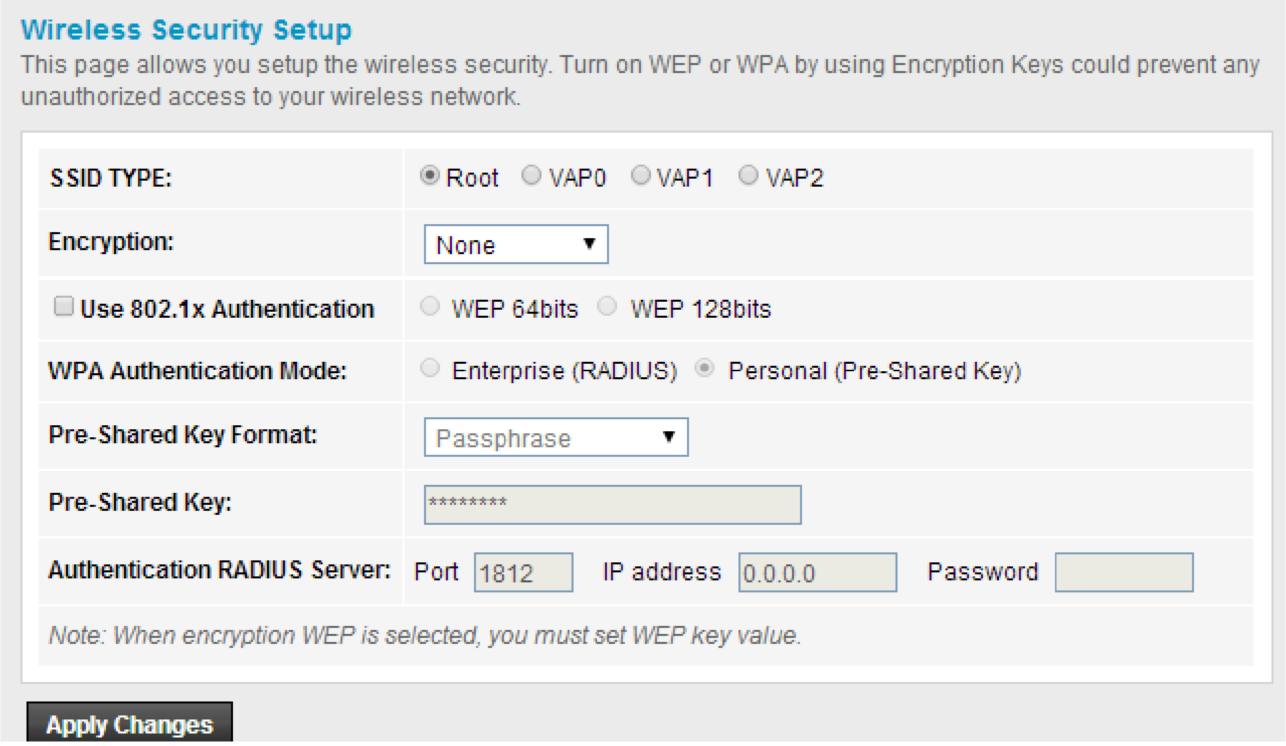
SSID: This is your wireless network name. Others can access Internet wirelessly by searching for this SSID and connecting to it.

Channel Bandwidth: this is the spectral width of the radio channel.

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

5.1.3.2 Security

You can setup wireless security in this page. Setup different encryptions for different SSIDs so that makes your wireless network more secure.



Wireless Security Setup

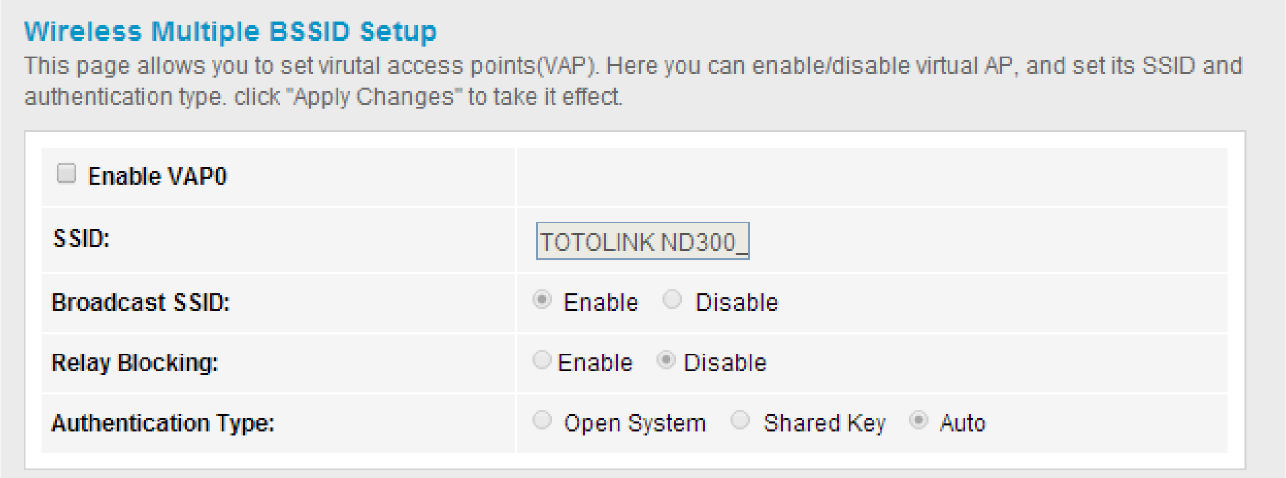
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE:	● Root ○ VAP0 ○ VAP1 ○ VAP2
Encryption:	None ▾
□ Use 802.1x Authentication	○ WEP 64bits ○ WEP 128bits
WPA Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
Pre-Shared Key Format:	Passphrase ▾
Pre-Shared Key:	********
Authentication RADIUS Server:	Port 1812 IP address 0.0.0.0 Password

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

5.1.3.3 MBSSID

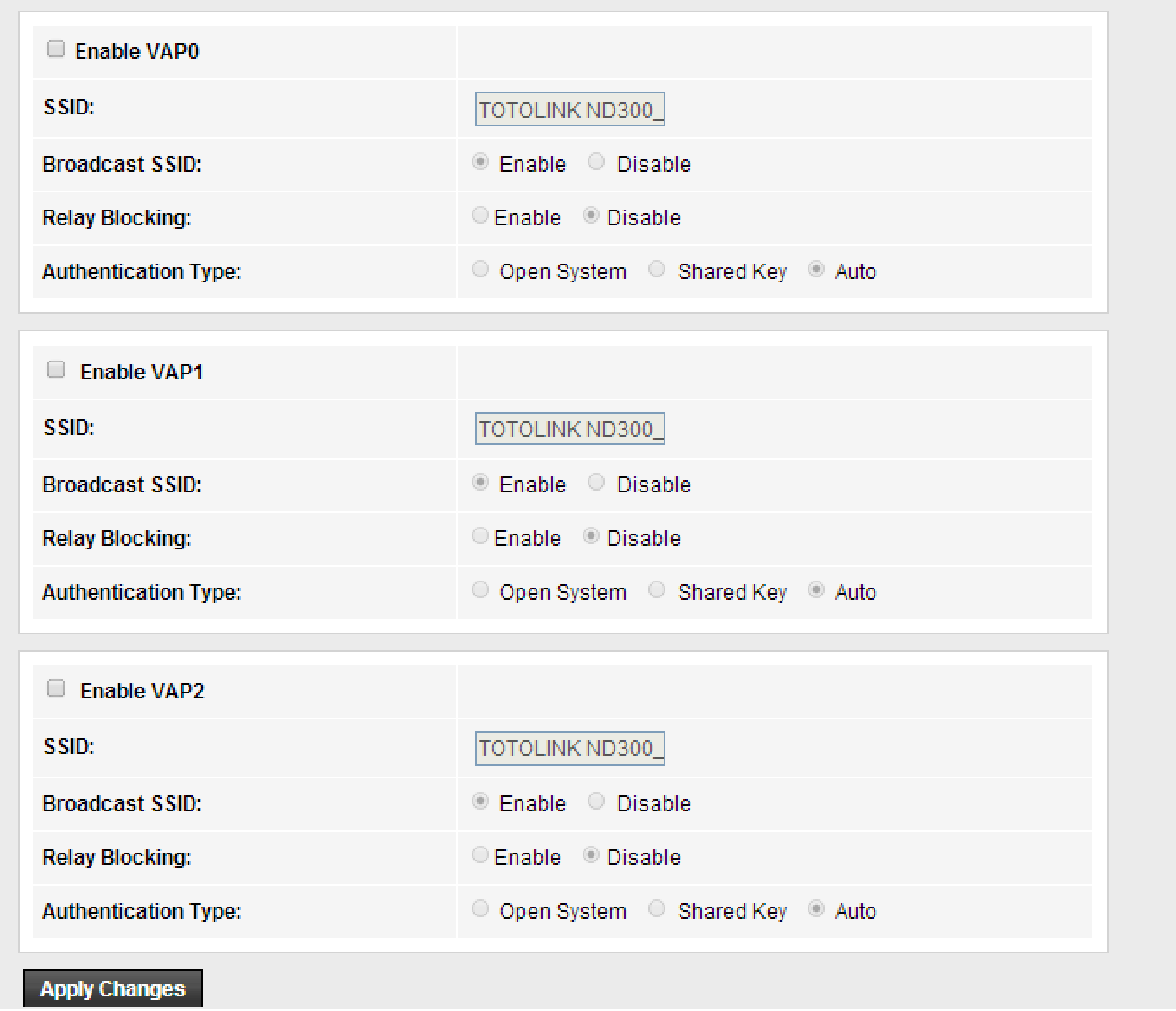
In this page, you can enable and set multiple VAP function. It is practical to set different SSID with encryption for different clients or friends.



Wireless Multiple BSSID Setup

This page allows you to set virutal access points(VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click "Apply Changes" to take it effect.

□ Enable VAP0	
SSID:	TOTOLINK ND300_
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto



□ Enable VAP0

SSID: TOTOLINK ND300_

Broadcast SSID: ● Enable ○ Disable

Relay Blocking: ○ Enable ● Disable

Authentication Type: ○ Open System ○ Shared Key ● Auto

□ Enable VAP1

SSID: TOTOLINK ND300_

Broadcast SSID: ● Enable ○ Disable

Relay Blocking: ○ Enable ● Disable

Authentication Type: ○ Open System ○ Shared Key ● Auto

□ Enable VAP2

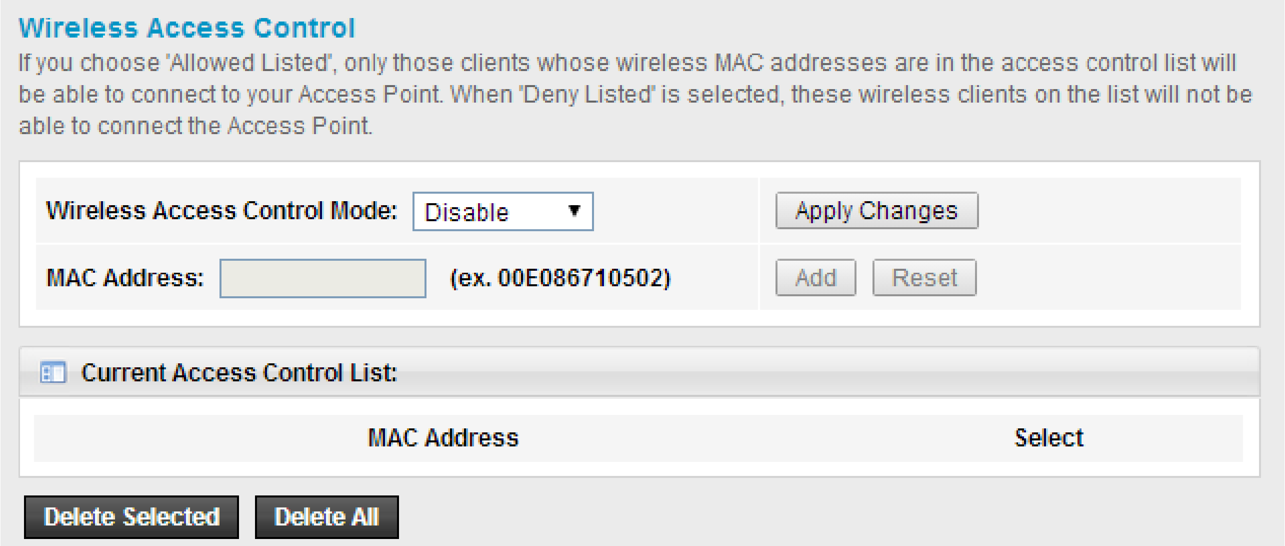
SSID: TOTOLINK ND300_

Broadcast SSID: ● Enable ○ Disable

Relay Blocking: ○ Enable ● Disable

Authentication Type: ○ Open System ○ Shared Key ● Auto

5.1.3.4 Access Control List



Wireless Access Control

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

Wireless Access Control Mode: Disable

MAC Address: (ex. 00E086710502)

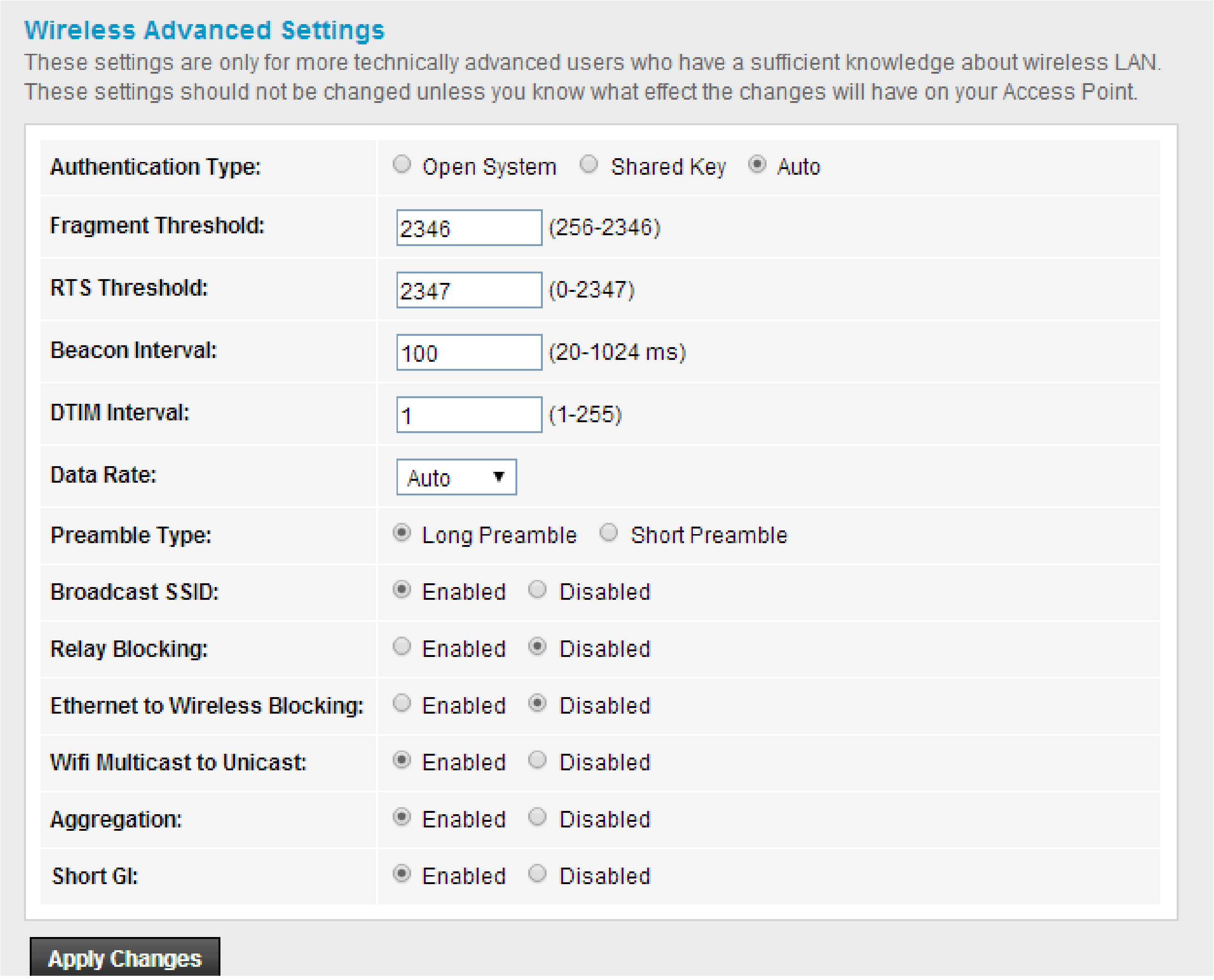
Current Access Control List:

MAC Address	Select

Mode: you could choose to allow or deny the following addresses entered by you.

MAC Address: enter the MAC address that you want to deny or allow.

5.1.3.5 Advanced Settings



Wireless Advanced Settings

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

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
DTIM Interval:	1 (1-255)
Data Rate:	Auto ▼
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
Relay Blocking:	○ Enabled ● Disabled
Ethernet to Wireless Blocking:	○ Enabled ● Disabled
Wifi Multicast to Unicast:	● Enabled ○ Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled

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 0-2347 bytes. The default value is 2347, which means that RTS is disabled.

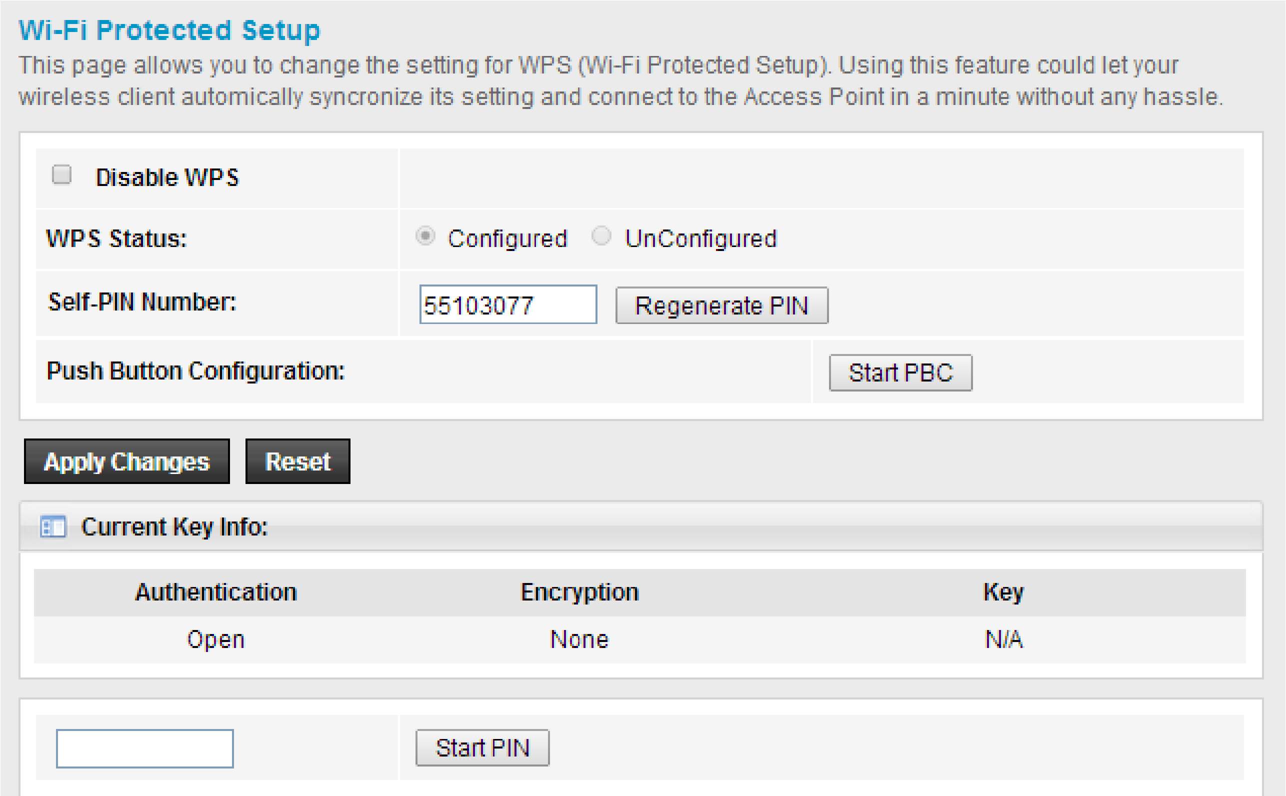
Beacon Interval: By default, it is set to 100ms. Higher Beacon interval will improve the device’s wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

Data Rates: you can choose the wireless data rate. This router provides three options. Be default, it is Default (1-2-5.5-11Mbps).**TX Power:** display the data transmission rate power.

Preamble type: it 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.

5.1.3.6 WPS

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.



Wi-Fi Protected Setup

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.

□ Disable WPS

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 55103077

Current Key Info:

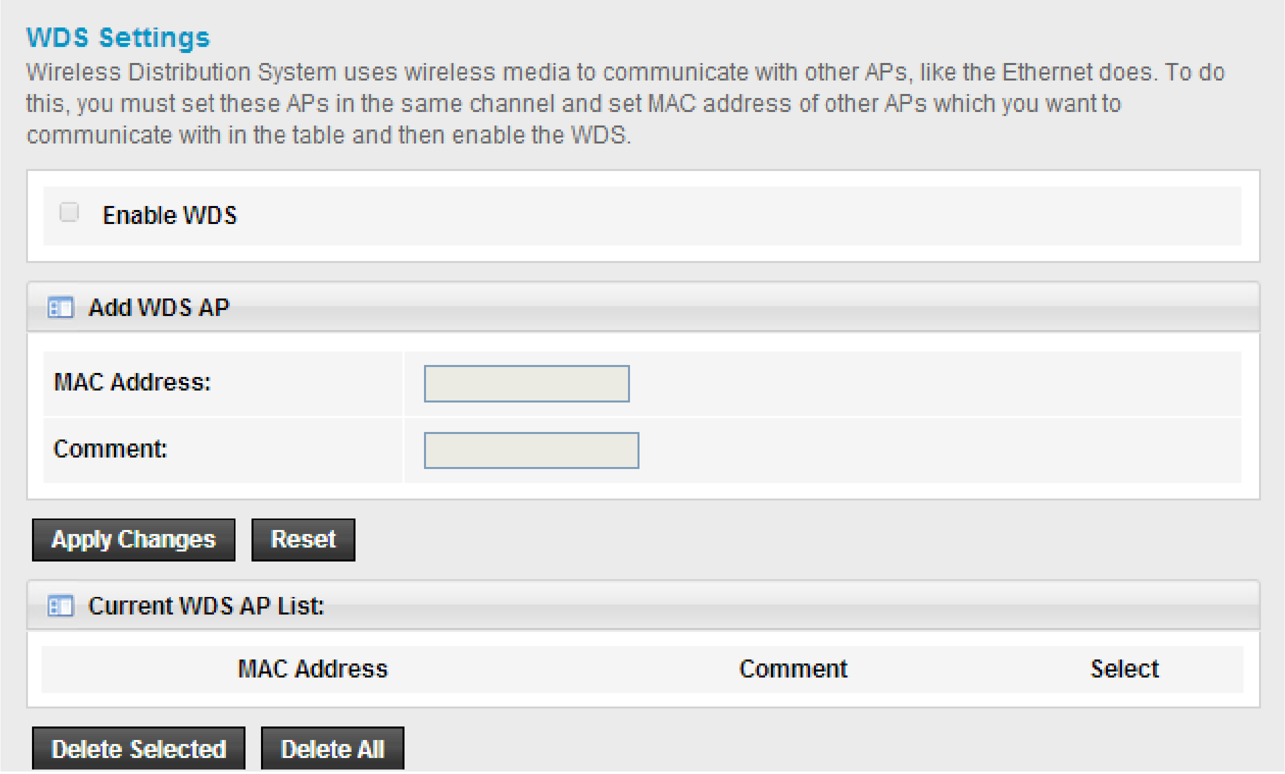
Authentication	Encryption	Key
Open	None	N/A

5.1.3.7 WDS

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

- Provide bridge traffic between two LANs though the air.
- 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.

☐ Enable WDS

Add WDS AP

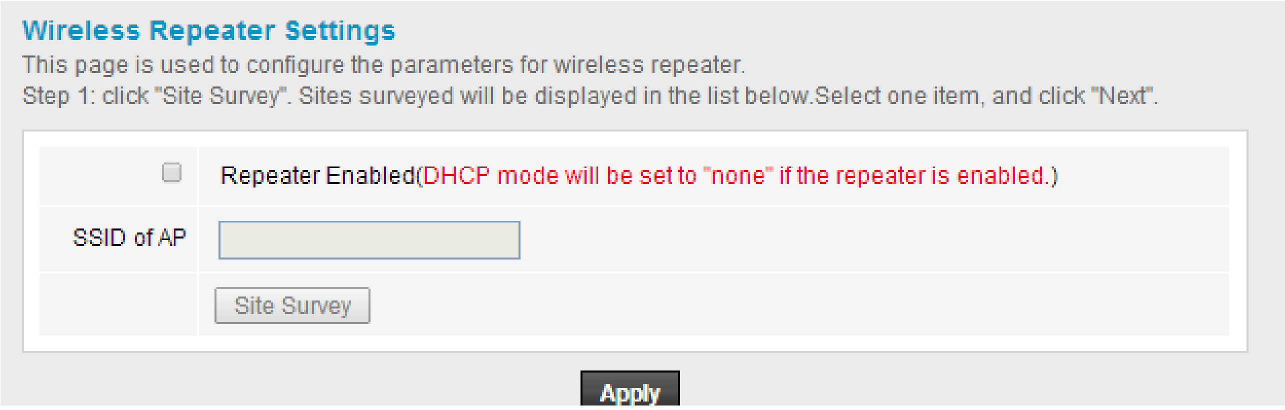
MAC Address:	
Comment:	

Current WDS AP List:

MAC Address	Comment	Select

5.1.3.8 Repeater

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

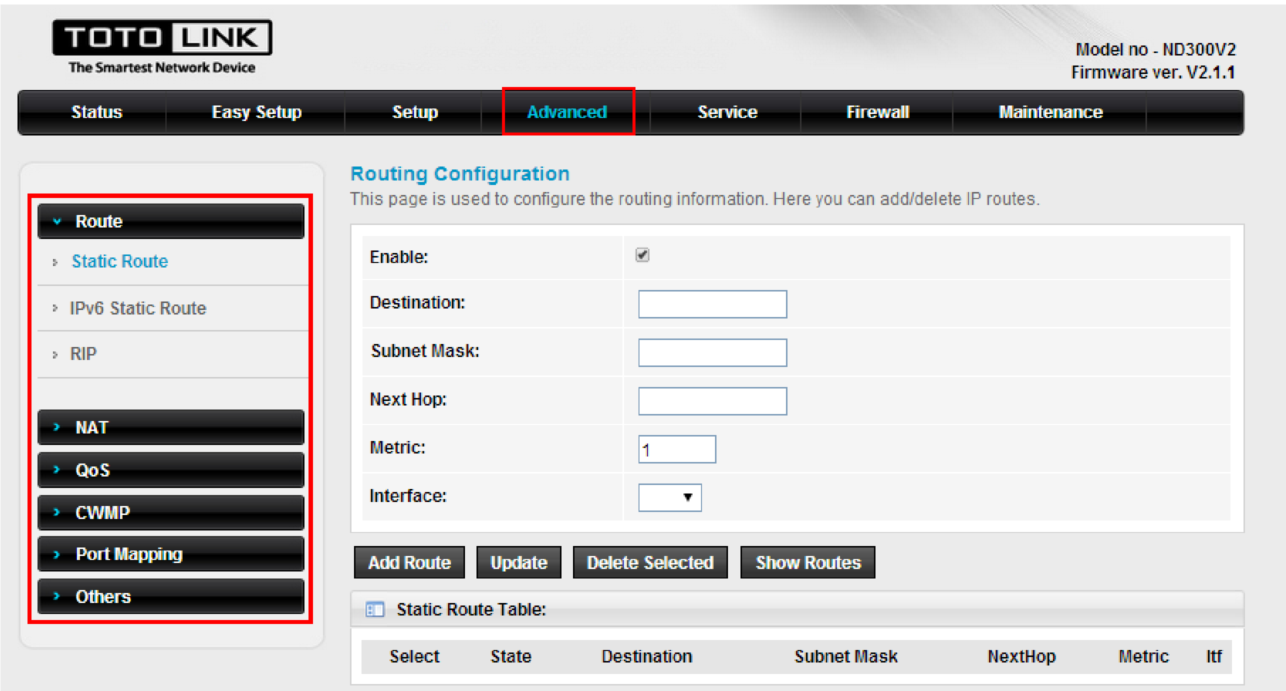


Wireless Repeater Settings

This page is used to configure the parameters for wireless repeater.
Step 1: click "Site Survey". Sites surveyed will be displayed in the list below.Select one item, and click "Next".

☐	Repeater Enabled(DHCP mode will be set to "none" if the repeater is enabled.)
SSID of AP	

5.2 Advanced



Routing Configuration

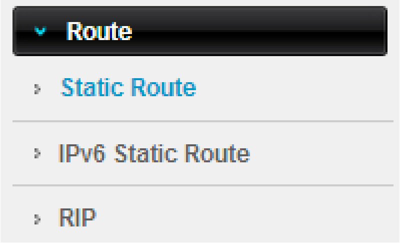
This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	1
Interface:	▾

Static Route Table:

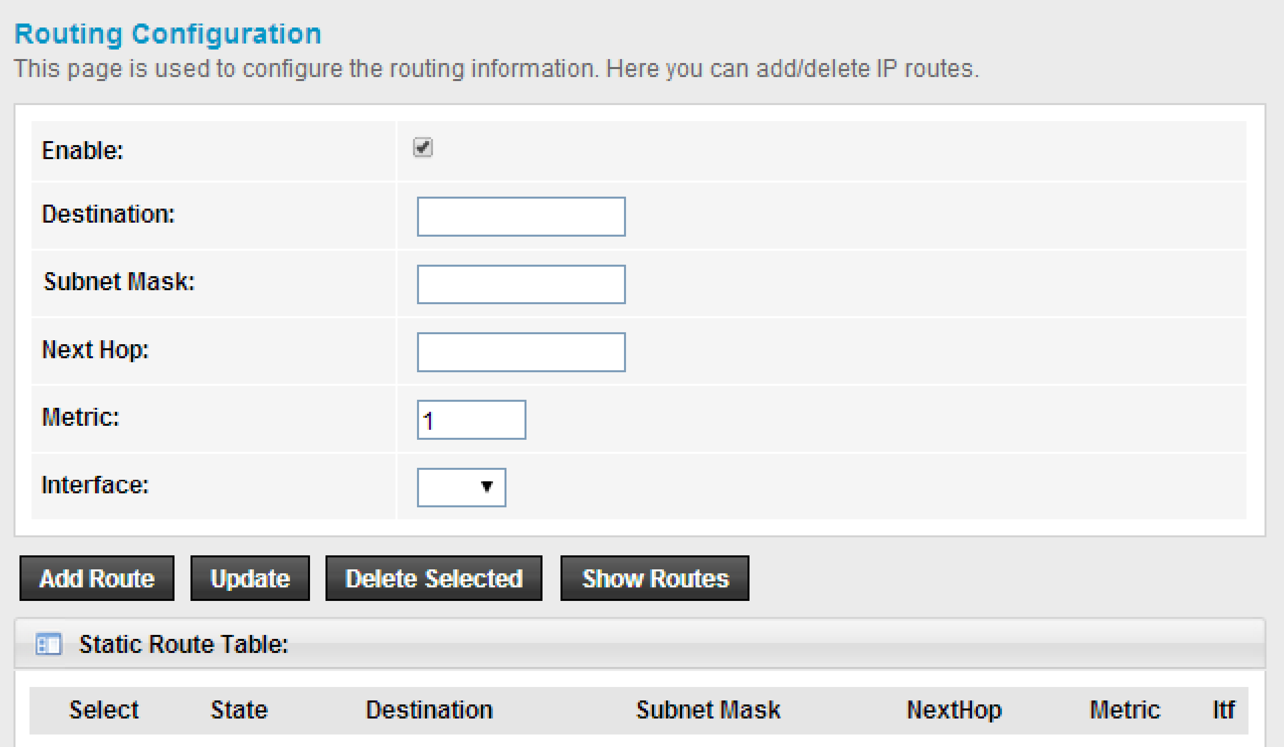
Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

5.2.1 Route



5.2.1.1 Static Route

This page allows you to specify that a specific target IP addresses passes through a determined gateway manually.



Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	1
Interface:	▼

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

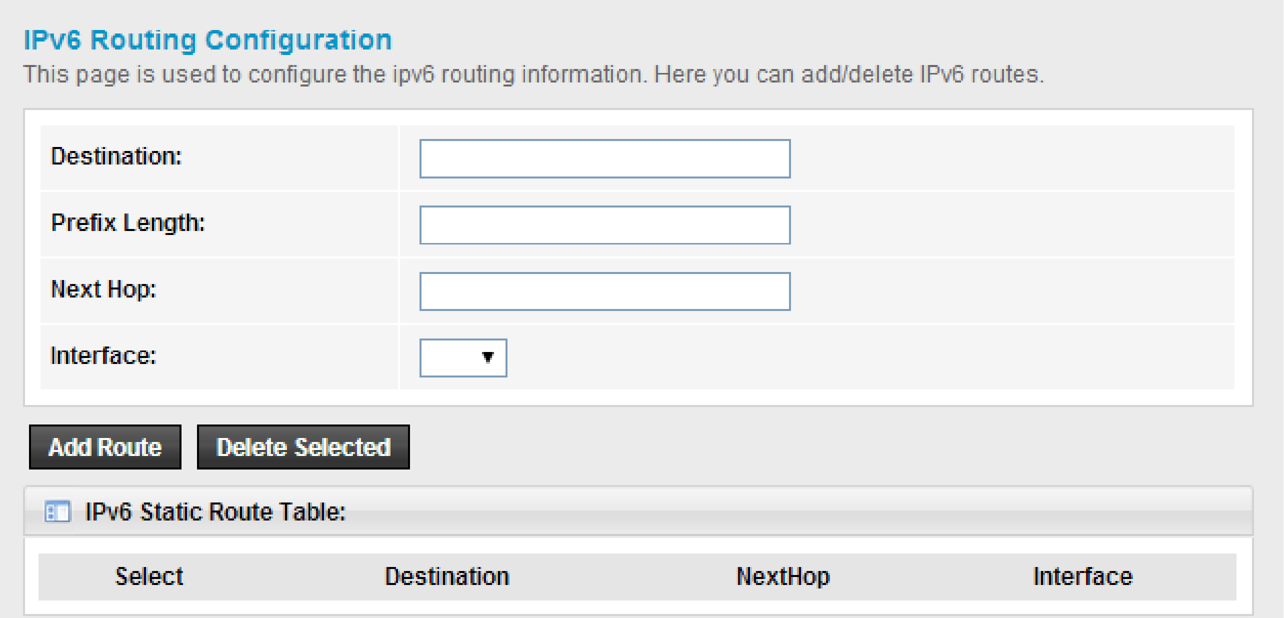
Destination: This is the address of the network or host that you want to assign to a static route.

Subnet Mask: This value determines which portion of an IP Address is the network portion, and which portion is the host portion.

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

5.2.1.2 IPv6 Static Route

This page allows you to configure a static route to an Internet Protocol version 6 (IPv6) network.



IPv6 Routing Configuration

This page is used to configure the ipv6 routing information. Here you can add/delete IPv6 routes.

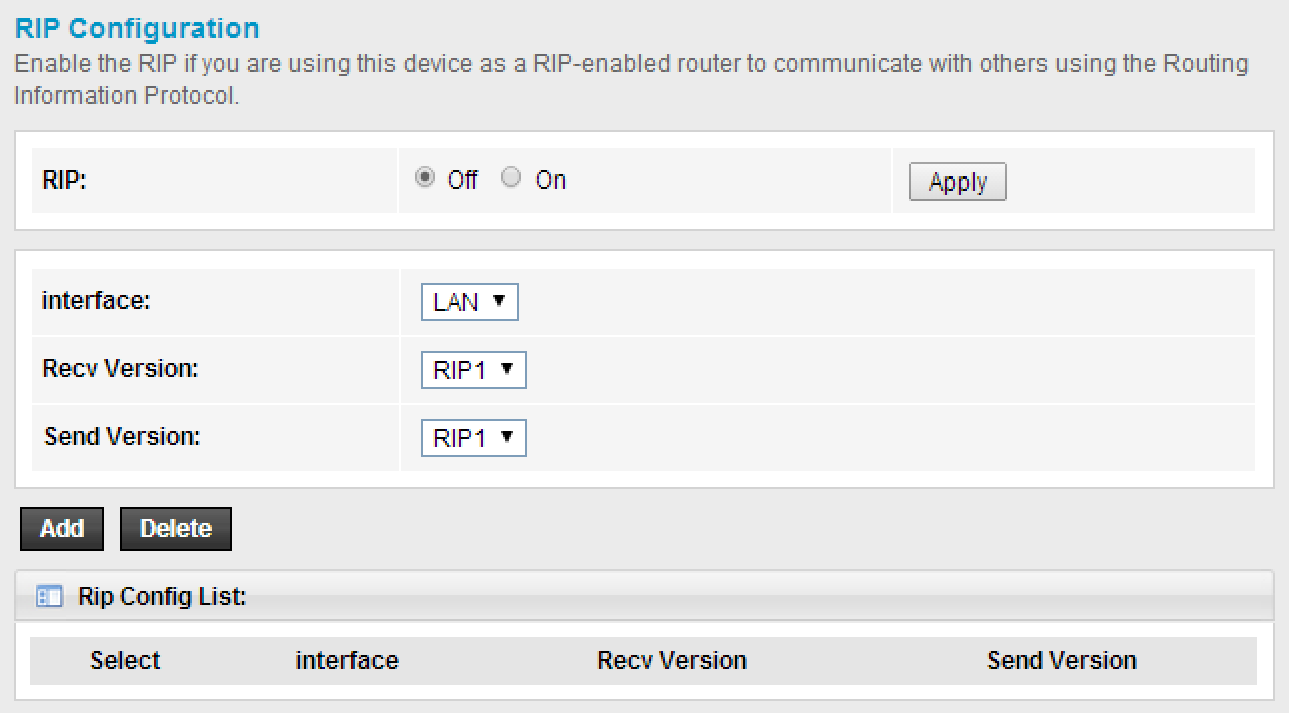
Destination:	
Prefix Length:	
Next Hop:	
Interface:	▼

IPv6 Static Route Table:

Select	Destination	NextHop	Interface

5.2.1.3 RIP

RIP means Routing Information Protocol.



RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.

RIP: ● Off ○ On

interface: LAN

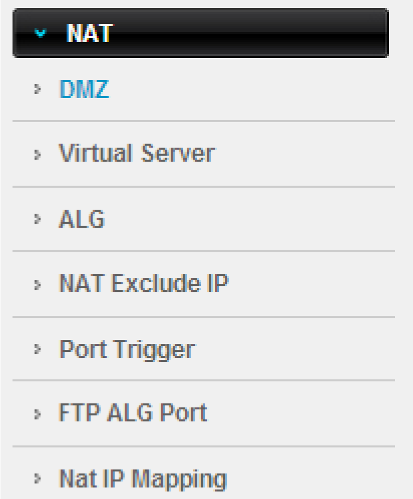
Recv Version: RIP1

Send Version: RIP1

Rip Config List:

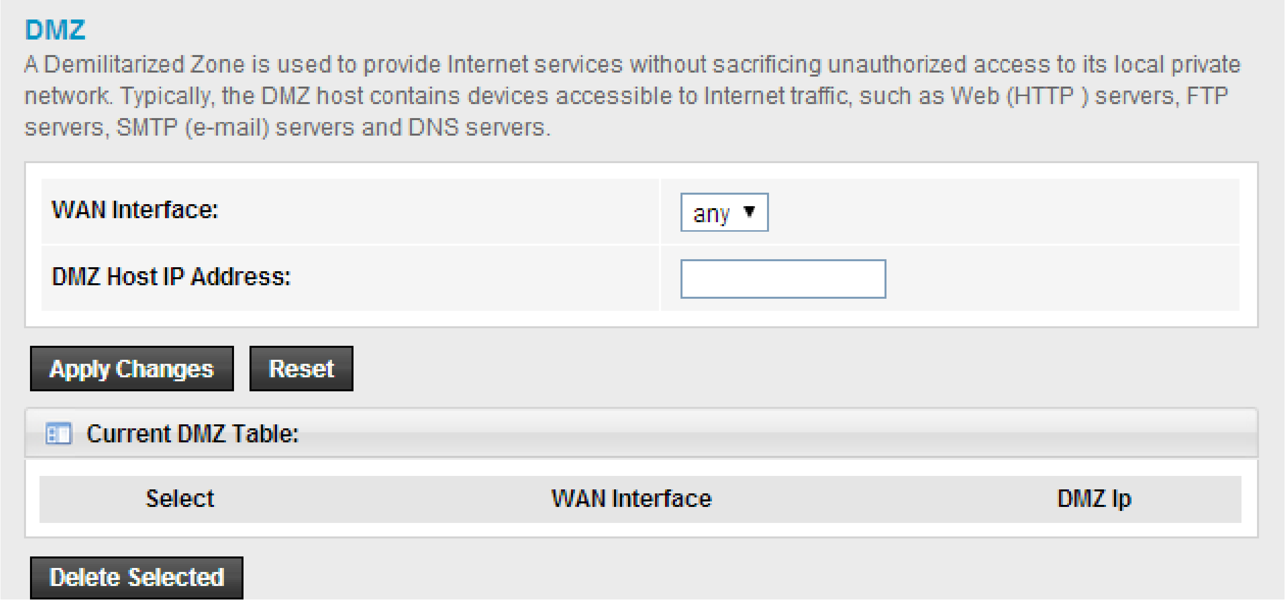
Select	interface	Recv Version	Send Version

5.2.2 NAT



5.2.2.1 DMZ

DMZ means Demilitarized Zone. It can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security.



DMZ

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.

WAN Interface:	any ▾
DMZ Host IP Address:	

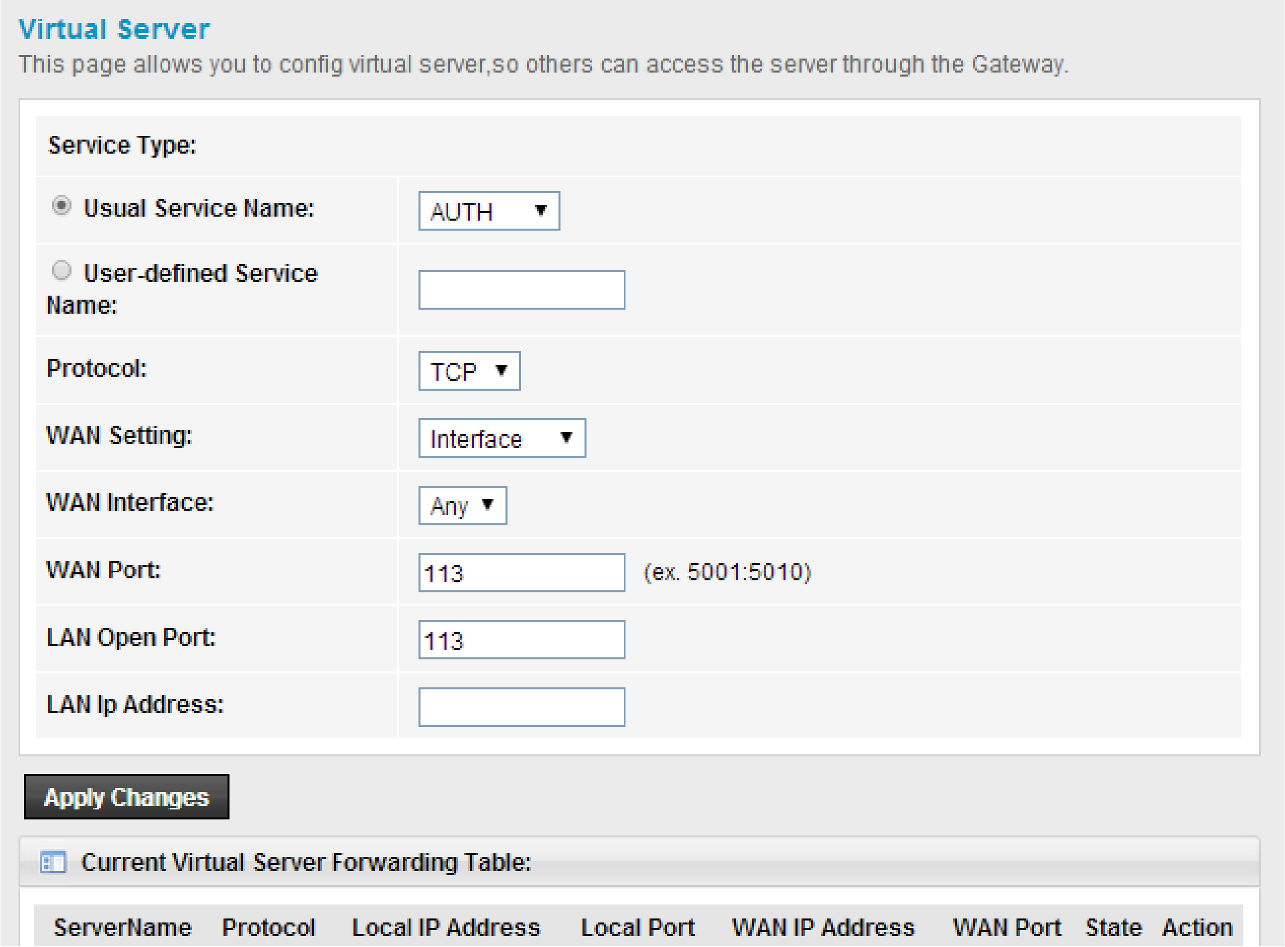
Current DMZ Table:

Select	WAN Interface	DMZ Ip

DMZ Host IP Address: Type in the DMZ Host IP address.

5.2.2.2 Virtual Server

Virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC used for a virtual server must have a static or reserved IP address because its IP address may change when using DHCP function.



Virtual Server

This page allows you to config virtual server,so others can access the server through the Gateway.

Service Type:	
● Usual Service Name:	AUTH ▾
○ User-defined Service Name:	
Protocol:	TCP ▾
WAN Setting:	Interface ▾
WAN Interface:	Any ▾
WAN Port:	113 (ex. 5001:5010)
LAN Open Port:	113
LAN Ip Address:	

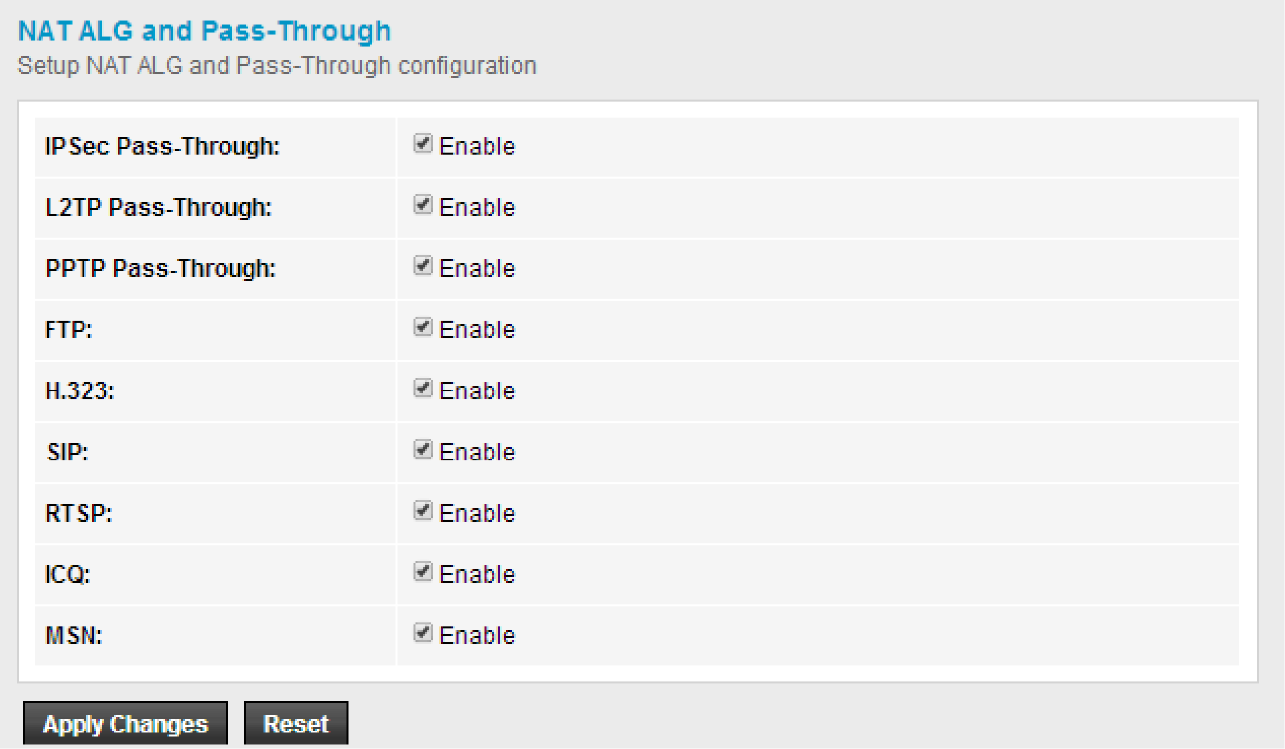
Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action

Protocol: The protocol used for this application, either TCP, or UDP.
Local IP Address: The IP address of the PC running the service application.

5.2.2.3 ALG

Application Layer Gateway consists of a security component that augments a firewall or NAT employed in a computer network.



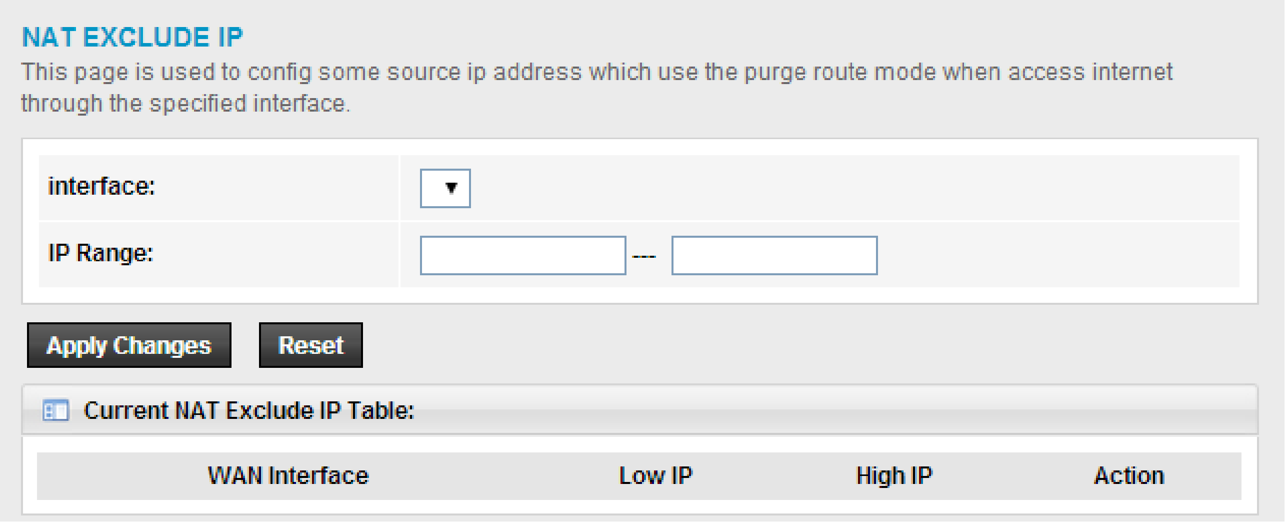
NAT ALG and Pass-Through

Setup NAT ALG and Pass-Through configuration

IPSec Pass-Through:	☑ Enable
L2TP Pass-Through:	☑ Enable
PPTP Pass-Through:	☑ Enable
FTP:	☑ Enable
H.323:	☑ Enable
SIP:	☑ Enable
RTSP:	☑ Enable
ICQ:	☑ Enable
MSN:	☑ Enable

5.2.2.4 NAT Exclude IP

NAT Exclude IP page is help to exclude addresses in the configured network range from being assigned to DHCP clients on the private network.



NAT EXCLUDE IP

This page is used to config some source ip address which use the purge route mode when access internet through the specified interface.

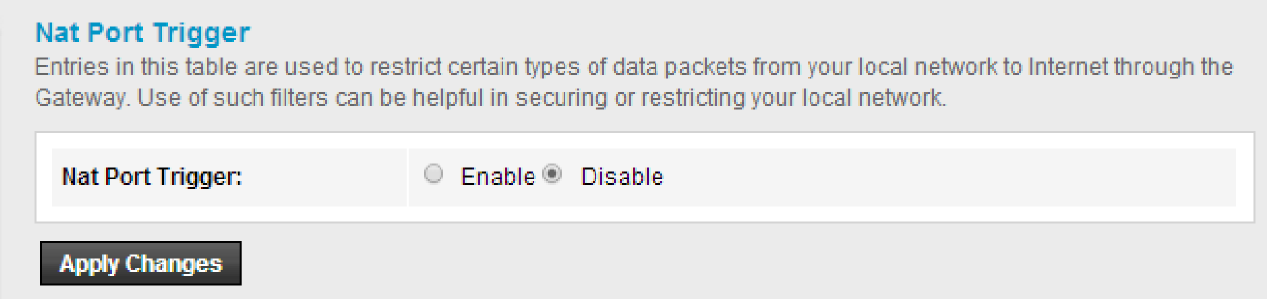
interface:	▼
IP Range:	---

Current NAT Exclude IP Table:

WAN Interface	Low IP	High IP	Action

5.2.2.5 Port Trigger

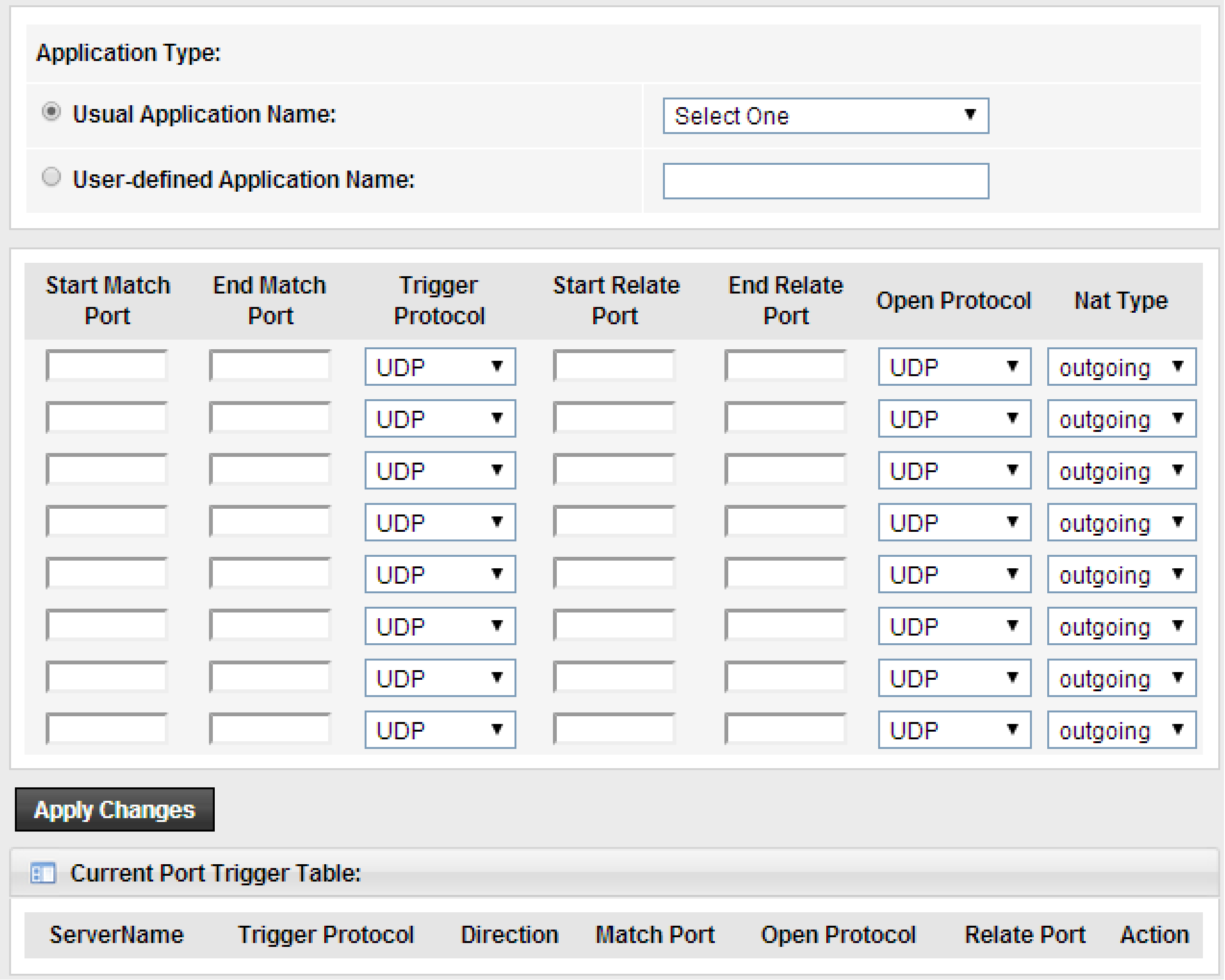
Port Trigger is used to realize that when there comes the Outbound streaming from a specified network port (triggered port), automatically opens the gateway WAN-side interfaces specified port (forwarded port), and the streams will forward to the triggered ports. You can achieve some special purposes by this setting.



Nat Port Trigger

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.

Nat Port Trigger: ○ Enable ● Disable



Application Type:

● Usual Application Name: Select One

○ User-defined Application Name:

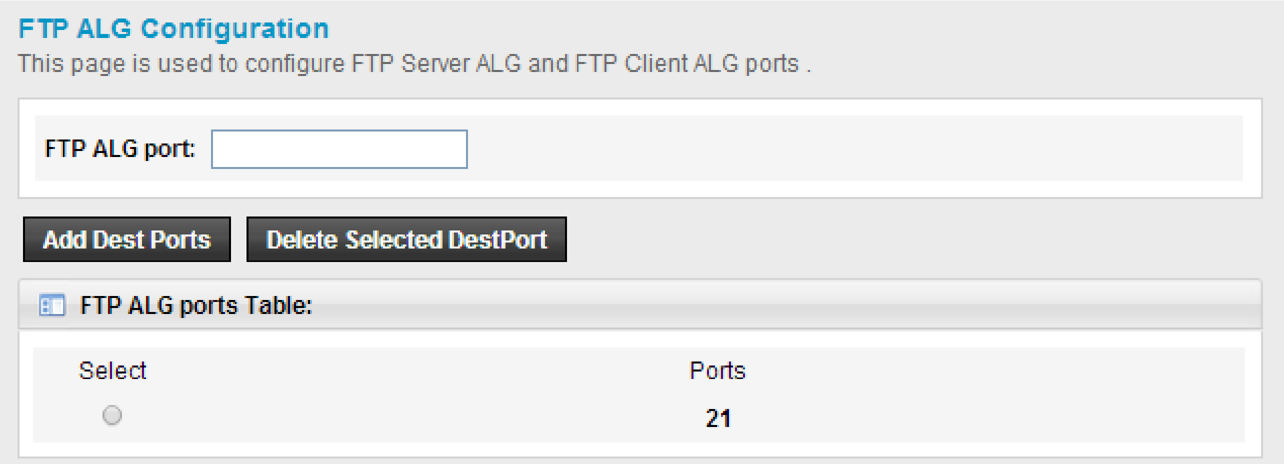
Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing

Current Port Trigger Table:

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action

5.2.2.6 FTP ALG Configuration

FTP ALG may use separate connections for passing control commands and for exchanging data between the client and a remote server. After enabled FTP ALG in ALG page, you can setup FTP ALG Port in this page.



FTP ALG Configuration

This page is used to configure FTP Server ALG and FTP Client ALG ports .

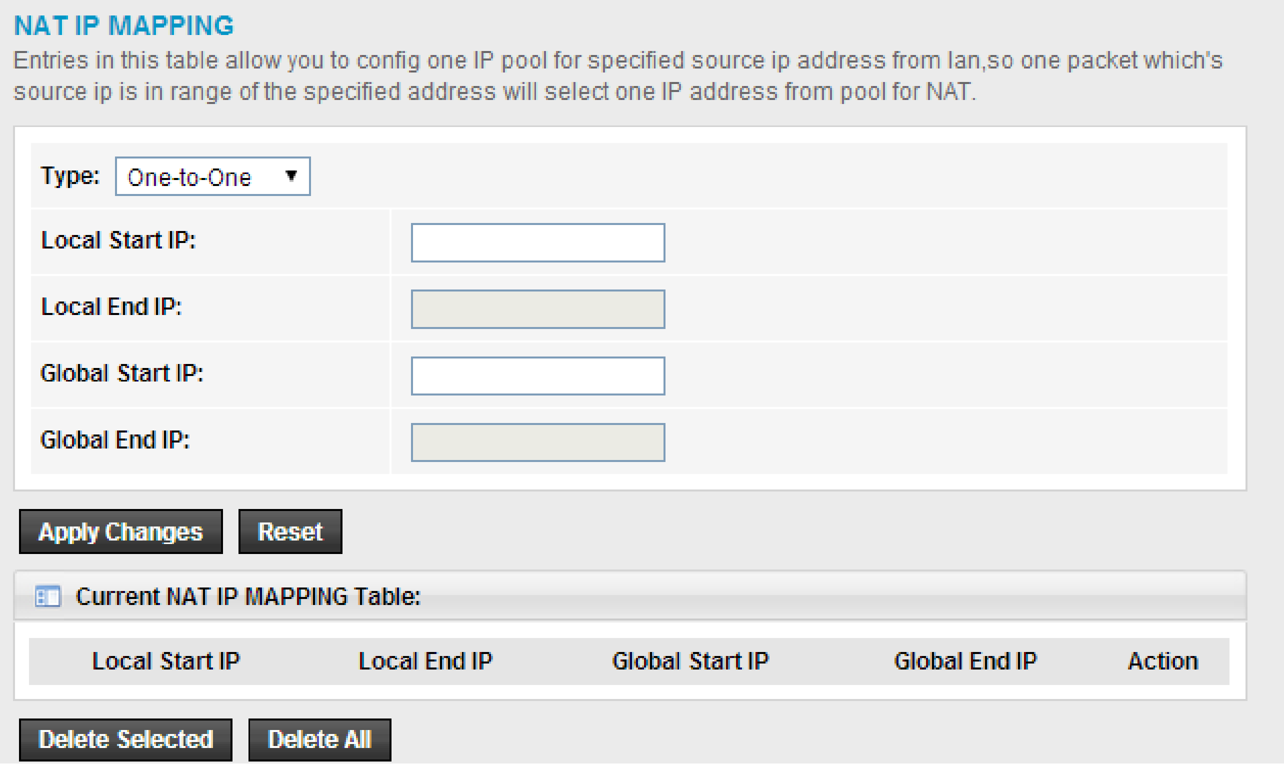
FTP ALG port:	

FTP ALG ports Table:

Select	Ports
○	21

5.2.2.7 NAT IP Mapping

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



NAT IP MAPPING

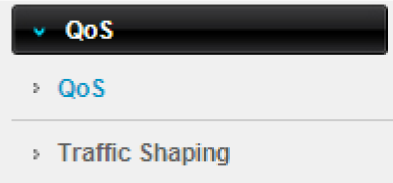
Entries in this table allow you to config one IP pool for specified source ip address from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

Type:	One-to-One
Local Start IP:	
Local End IP:	
Global Start IP:	
Global End IP:	

Current NAT IP MAPPING Table:

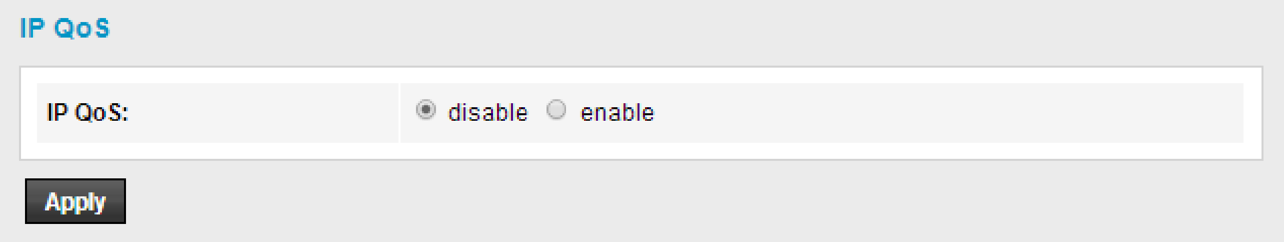
Local Start IP	Local End IP	Global Start IP	Global End IP	Action

5.2.3 QoS



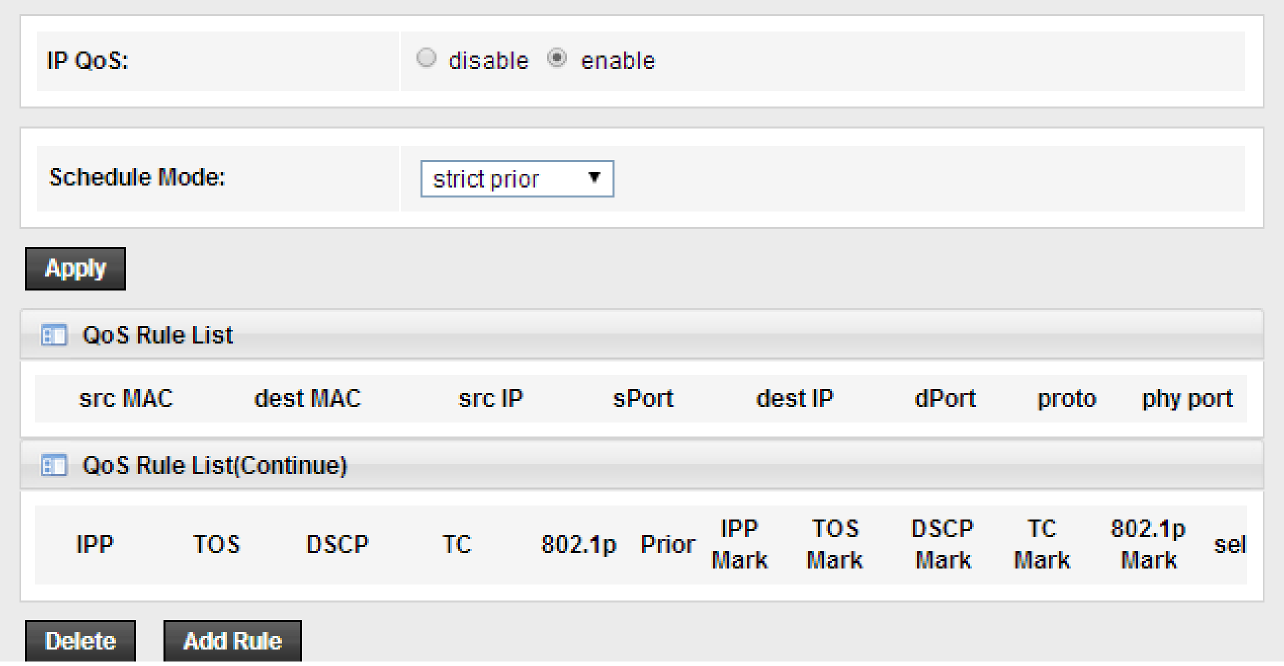
5.2.3.1 QoS

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.



IP QoS

IP QoS: ● disable ○ enable



IP QoS: ○ disable ● enable

Schedule Mode: strict prior ▼

QoS Rule List

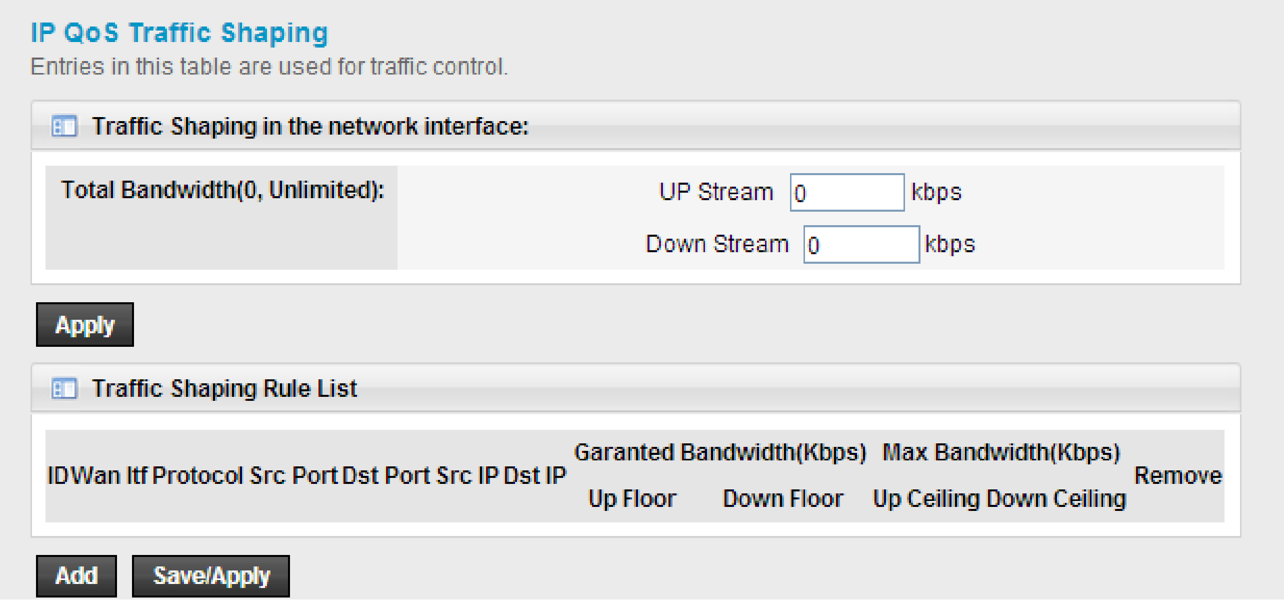
src MAC	dest MAC	src IP	sPort	dest IP	dPort	proto	phy port

QoS Rule List(Continue)

IPP	TOS	DSCP	TC	802.1p	Prior	IPP Mark	TOS Mark	DSCP Mark	TC Mark	802.1p Mark	sel

5.2.3.2 Traffic Shaping

For better traffic control, you can setup upstream and downstream speeds in this page.



IP QoS Traffic Shaping

Entries in this table are used for traffic control.

Traffic Shaping in the network interface:

Total Bandwidth(0, Unlimited): UP Stream 0 kbps

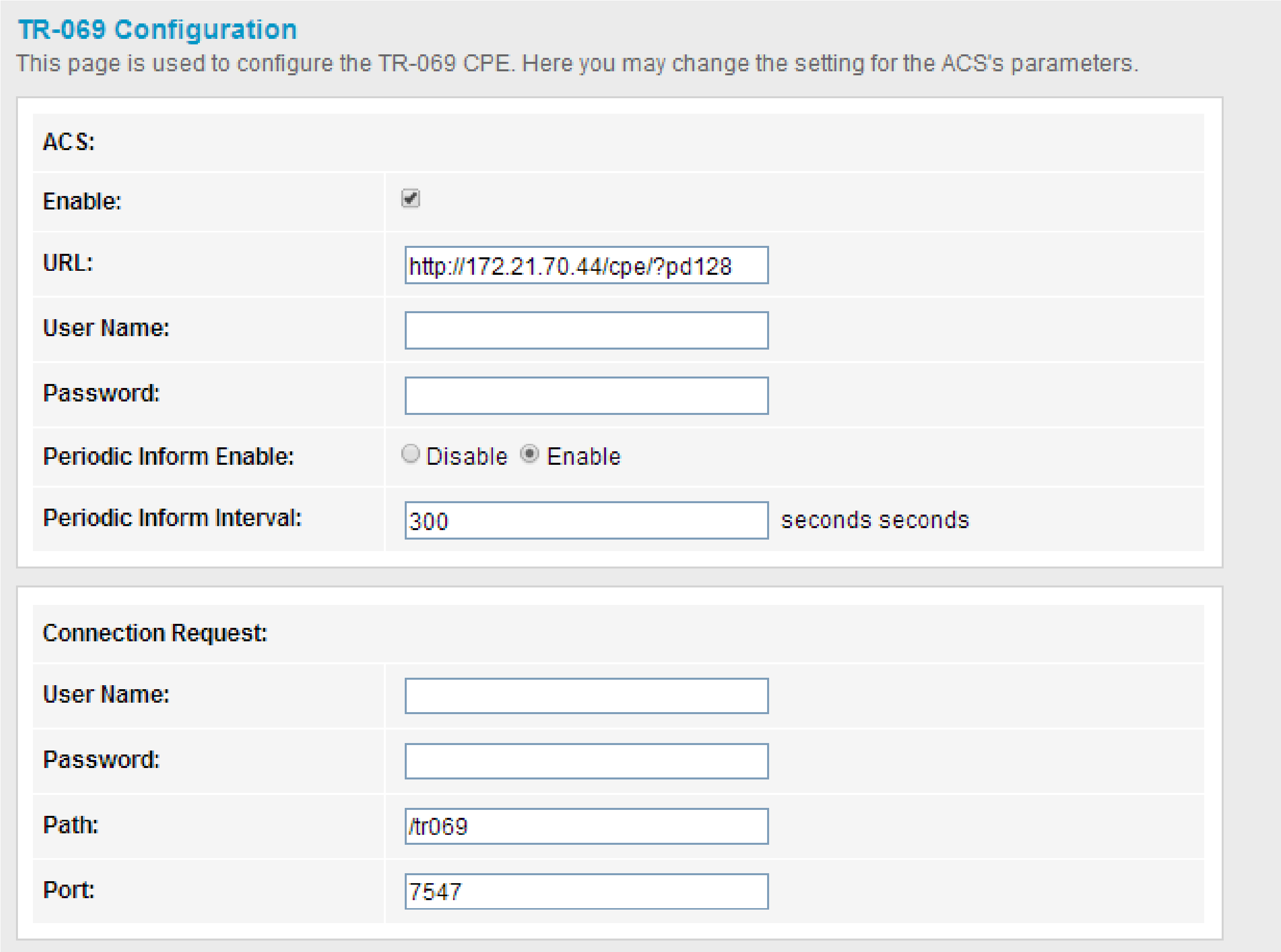
Down Stream 0 kbps

Traffic Shaping Rule List

ID	Wan Itf	Protocol	Src Port	Dst Port	Src IP	Dst IP	Garanted Bandwidth(Kbps)		Max Bandwidth(Kbps)		Remove
							Up Floor	Down Floor	Up Ceiling	Down Ceiling	

5.2.4 CWMP

The Modem Router offers CWMP feature. This function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

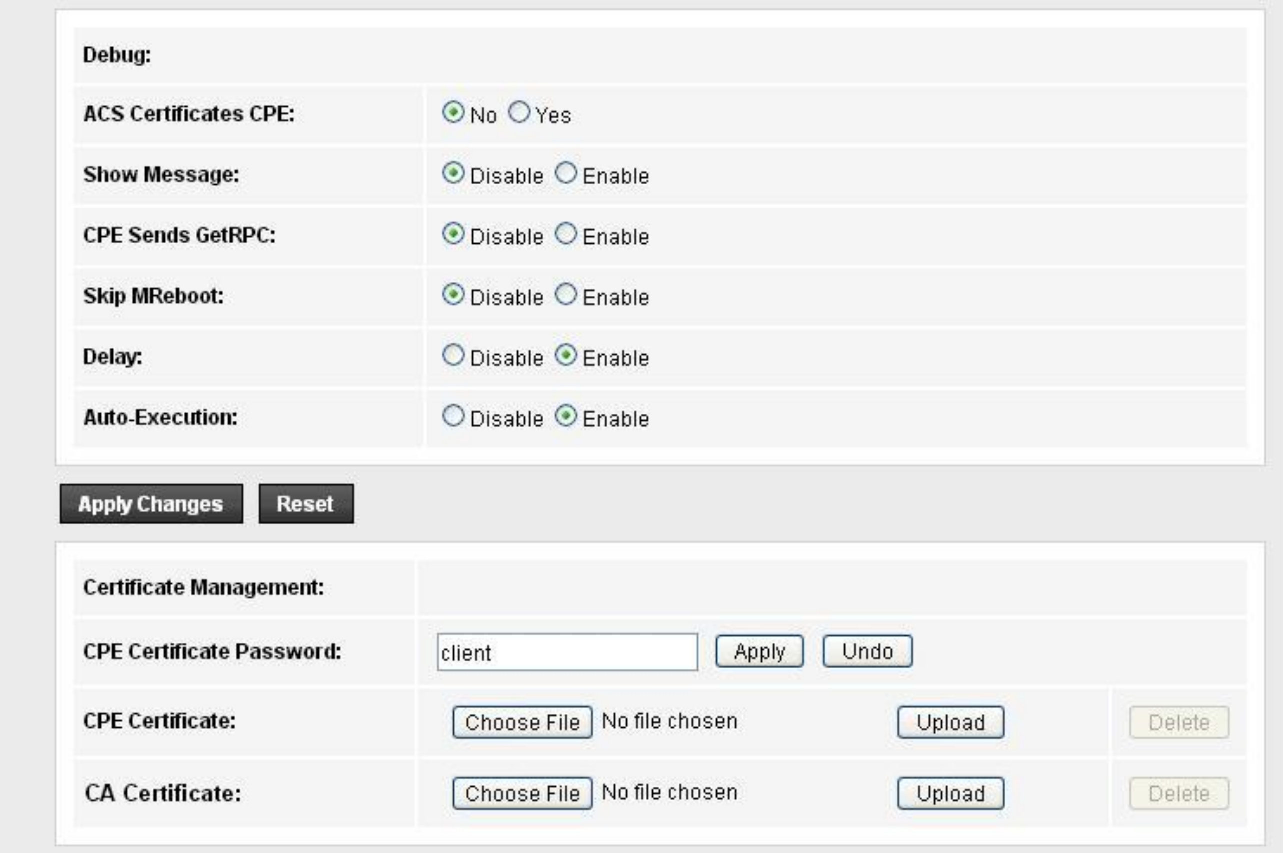


TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

ACS:	
Enable:	☑
URL:	http://172.21.70.44/cpe/?pd128
User Name:	
Password:	
Periodic Inform Enable:	○ Disable ● Enable
Periodic Inform Interval:	300 seconds seconds

Connection Request:	
User Name:	
Password:	
Path:	/tr069
Port:	7547



Debug:		
ACS Certificates CPE:	● No ○ Yes	
Show Message:	● Disable ○ Enable	
CPE Sends GetRPC:	● Disable ○ Enable	
Skip MReboot:	● Disable ○ Enable	
Delay:	○ Disable ● Enable	
Auto-Execution:	○ Disable ● Enable	

Certificate Management:			
CPE Certificate Password:	client	Apply Undo	
CPE Certificate:	Choose File No file chosen	Upload	Delete
CA Certificate:	Choose File No file chosen	Upload	Delete

ACS

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

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

Password: Enter the password to login the ACS server.

Connection Request

User Name: Enter the User Name that provided by the ACS server to login the Modem Router.

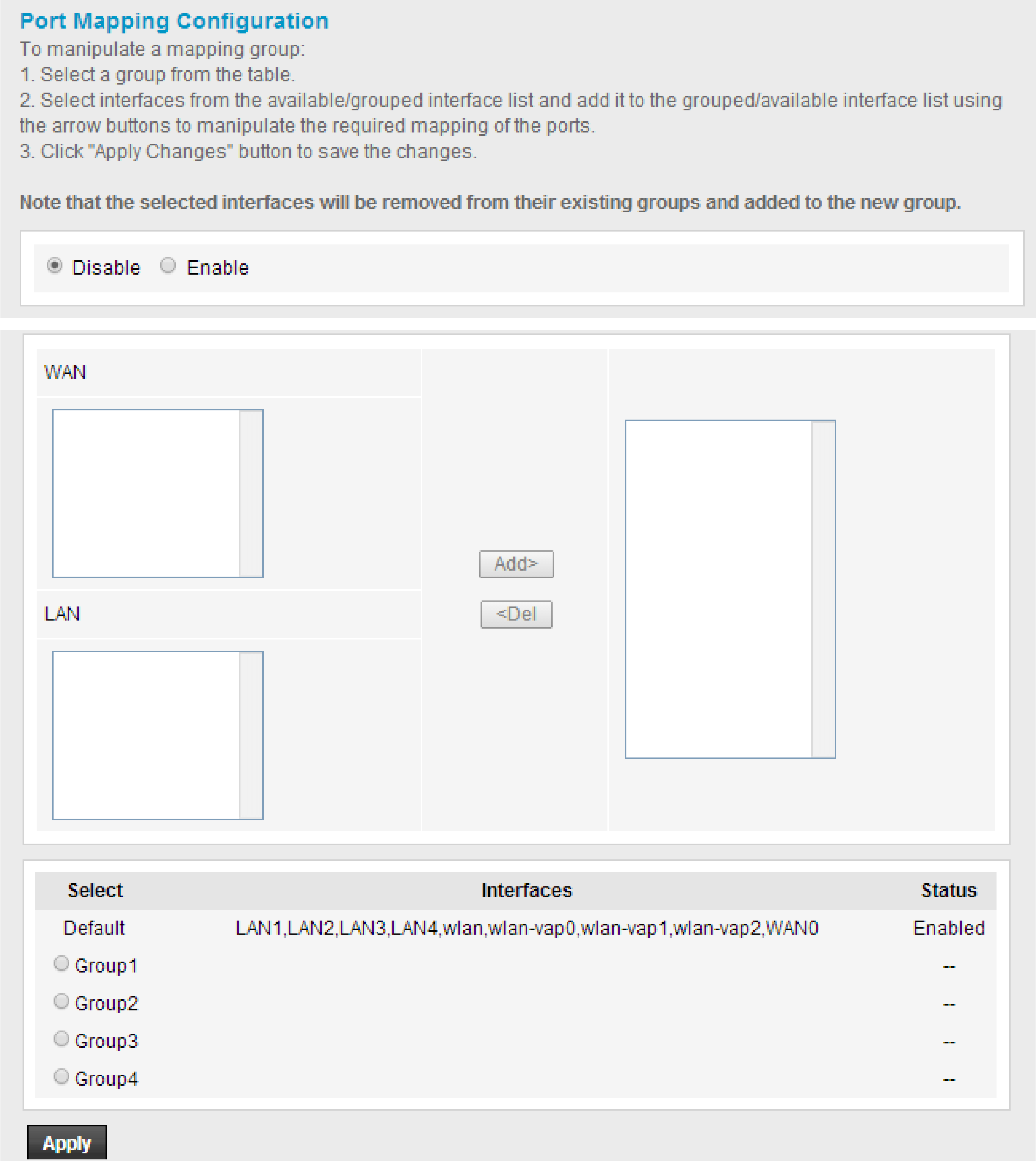
Password: Enter the password that provided by the ACS server to login the Modem Router.

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

Port: Enter the port that connects to the ACS server.

5.2.5 Port Mapping

Port Mapping function allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact it.



Port Mapping Configuration

To manipulate a mapping group:

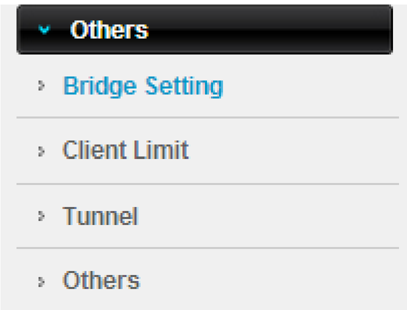
1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

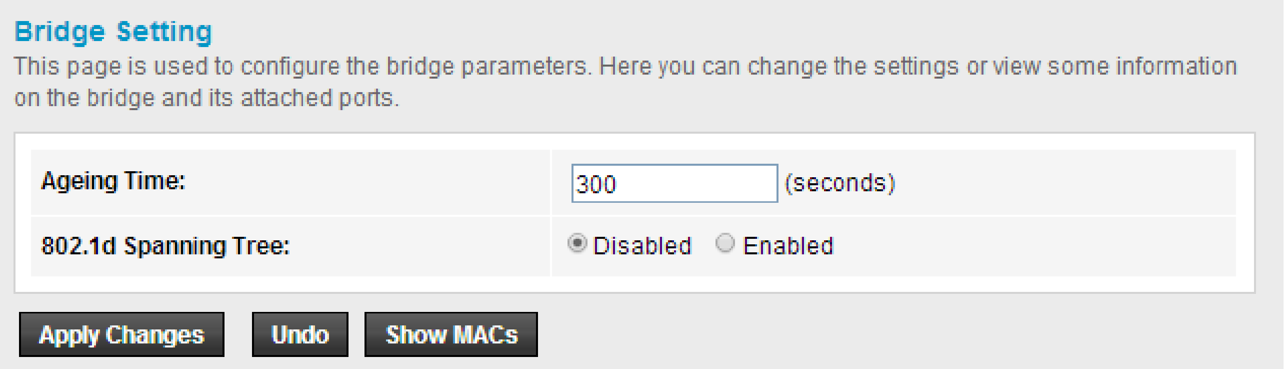
● Disable ○ Enable

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,WAN0	Enabled
○ Group1		--
○ Group2		--
○ Group3		--
○ Group4		--

5.2.6 Others



5.2.6.1 Bridge Setting



Bridge Setting

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

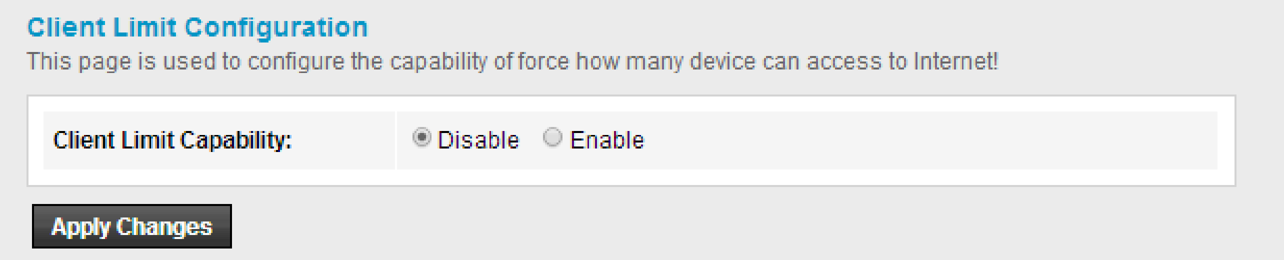
Ageing Time: 300 (seconds)

802.1d Spanning Tree: ● Disabled ○ Enabled

802.1d Spanning Tree: STP is implemented through the exchange of bridge protocol data unit (BPDU) messages between adjacent switches. It helps to ensure a loop-free topology for any bridged Ethernet local area network.

5.2.6.2 Client Limit

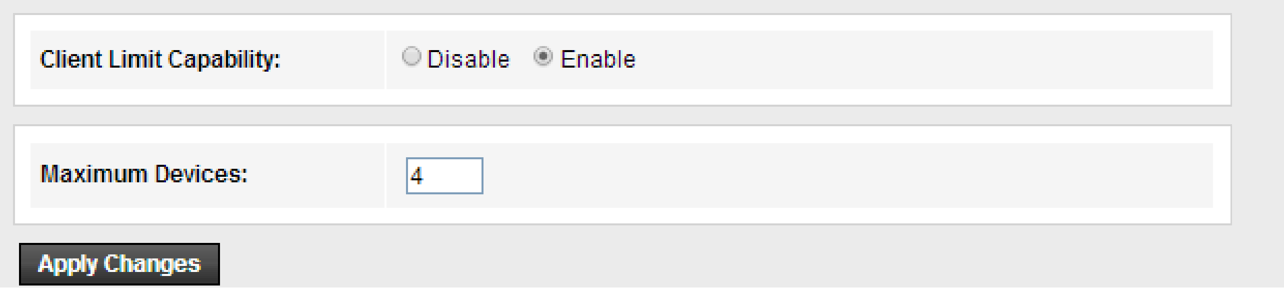
After enabled client limit capability, you can setup the maximum devices that are allowed to access to Internet.



Client Limit Configuration

This page is used to configure the capability of force how many device can access to Internet!

Client Limit Capability: ● Disable ○ Enable

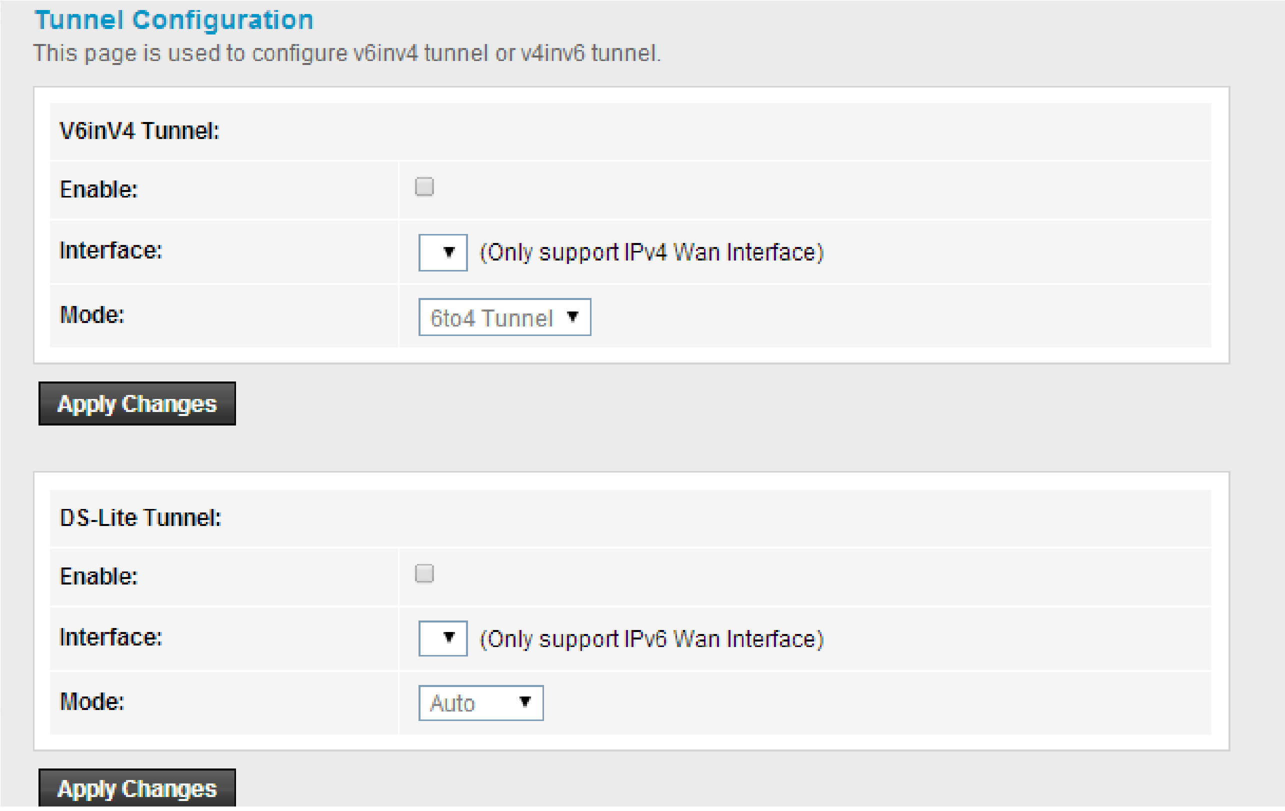


Client Limit Capability: ○ Disable ● Enable

Maximum Devices: 4

5.2.6.3 Tunnel Configuration

V6inv4 tunnel or v4inv6 tunnel can be configured in this page.



Tunnel Configuration

This page is used to configure v6inv4 tunnel or v4inv6 tunnel.

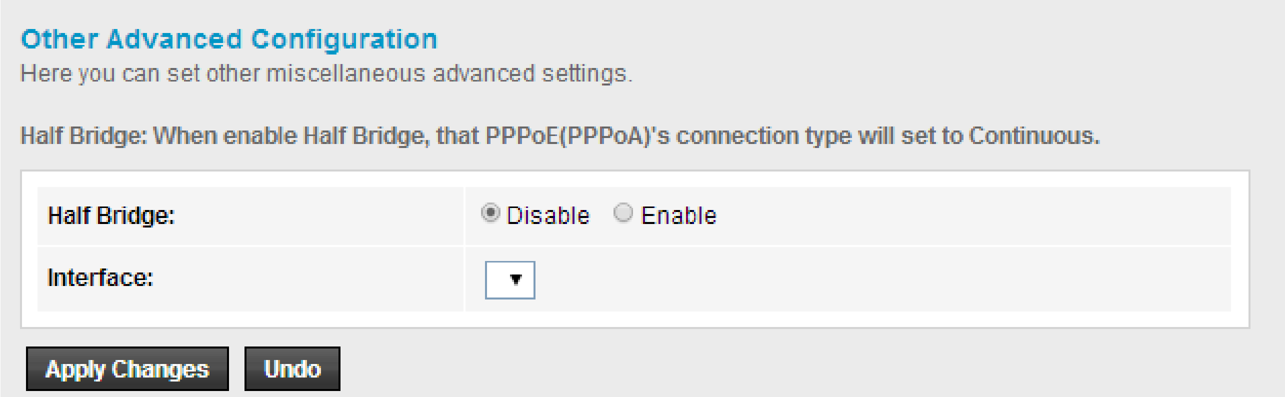
V6inV4 Tunnel:	
Enable:	□
Interface:	▼ (Only support IPv4 Wan Interface)
Mode:	6to4 Tunnel ▼

DS-Lite Tunnel:	
Enable:	□
Interface:	▼ (Only support IPv6 Wan Interface)
Mode:	Auto ▼

V6inV4 is an Internet transition mechanism for migrating from Internet Protocol version 4 (IPv4) to IPv6.

5.2.6.4 Others

In this page you can enable or disable half bridge.



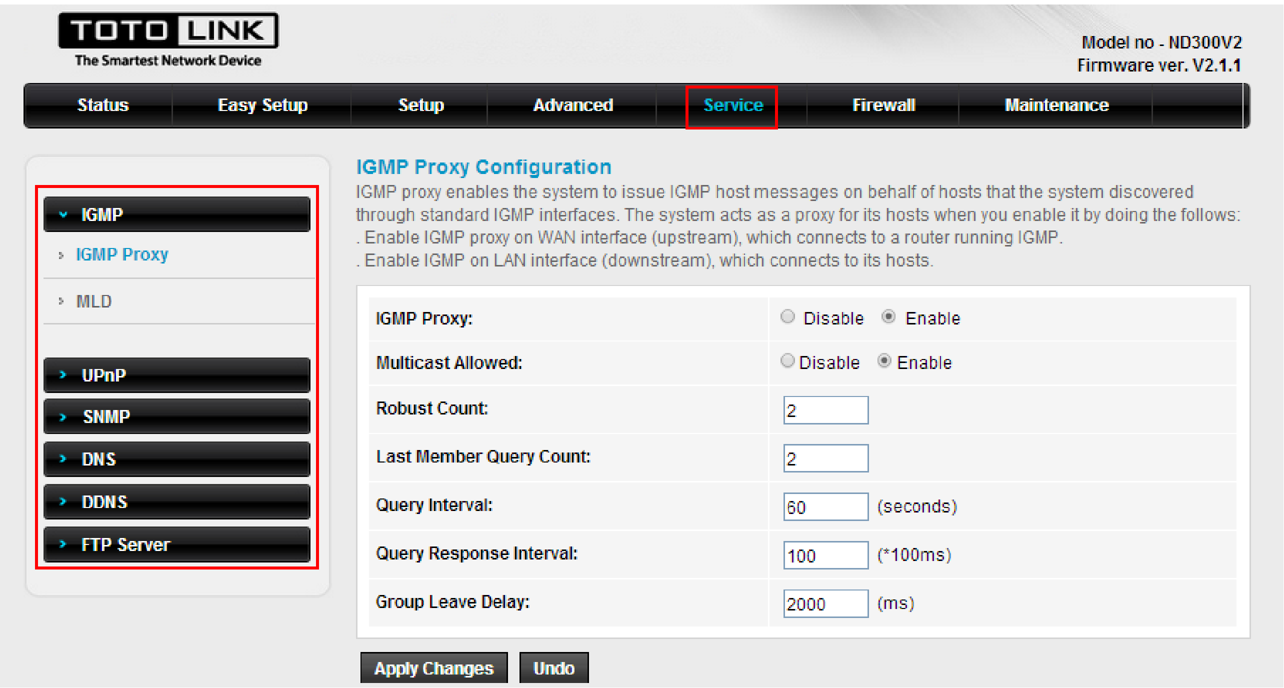
Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to Continuous.

Half Bridge:	● Disable ○ Enable
Interface:	▼

5.3 Service



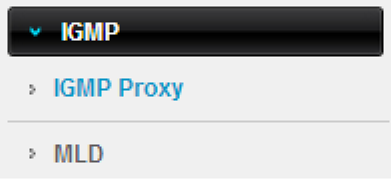
IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:
. Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
. Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy:	○ Disable ● Enable
Multicast Allowed:	○ Disable ● Enable
Robust Count:	2
Last Member Query Count:	2
Query Interval:	60 (seconds)
Query Response Interval:	100 (*100ms)
Group Leave Delay:	2000 (ms)

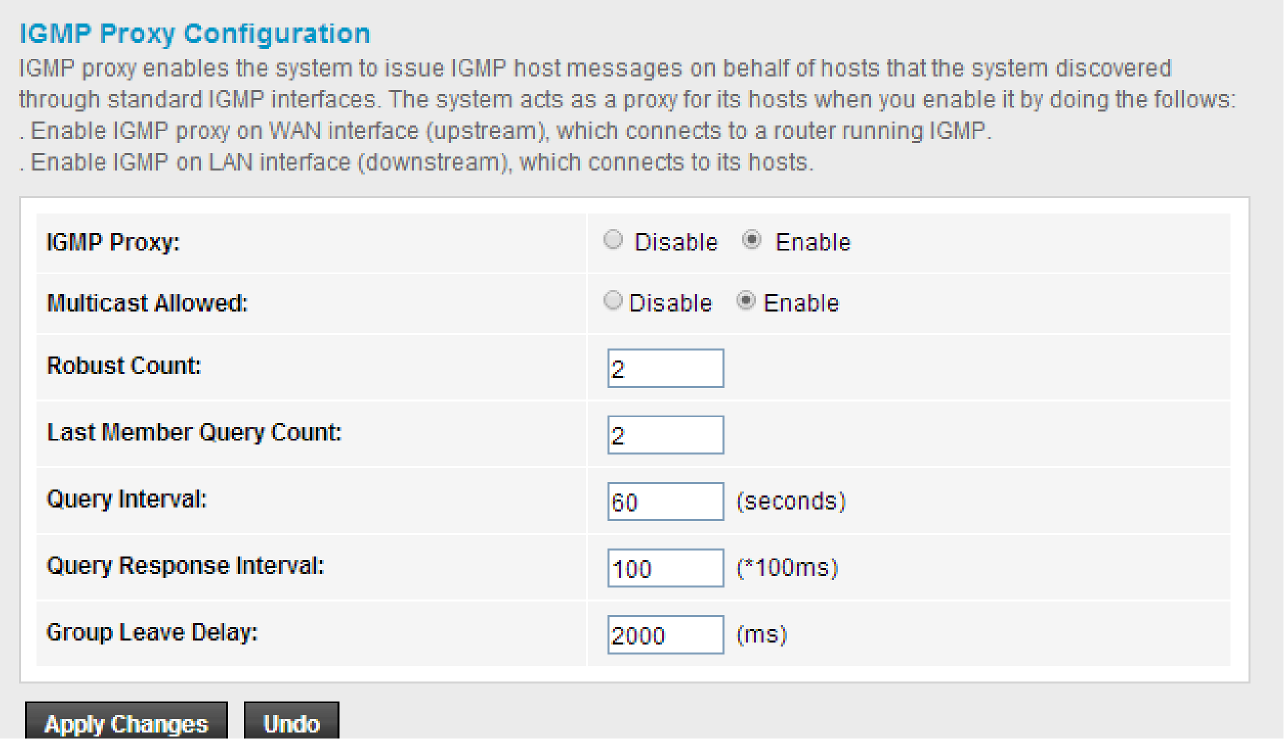
5.3.1 IGMP

IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the Modem Router.



5.3.1.1 IGMP Proxy

IGMP Proxy and Multicast allowed can be configured in this page.



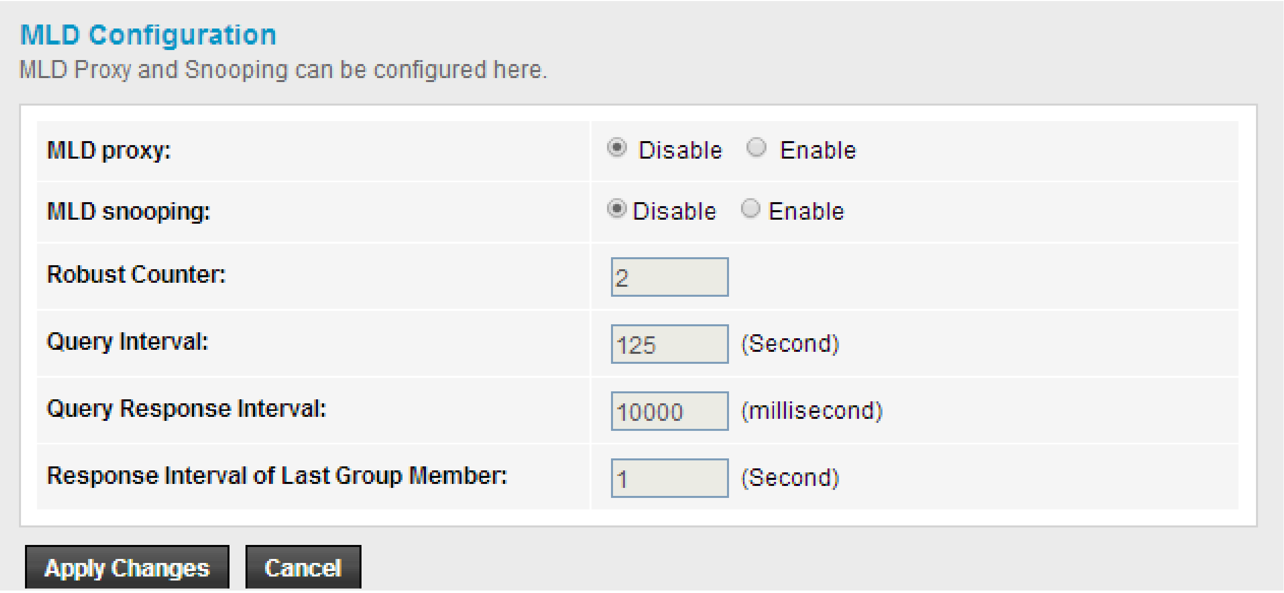
IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:
. Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
. Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy:	○ Disable ● Enable
Multicast Allowed:	○ Disable ● Enable
Robust Count:	2
Last Member Query Count:	2
Query Interval:	60 (seconds)
Query Response Interval:	100 (*100ms)
Group Leave Delay:	2000 (ms)

5.3.1.2 MLD

MLD (Multicast Listener Discovery), it allows the router to find out if there is an IPv6 multicast group listeners on their directly connected network segments.



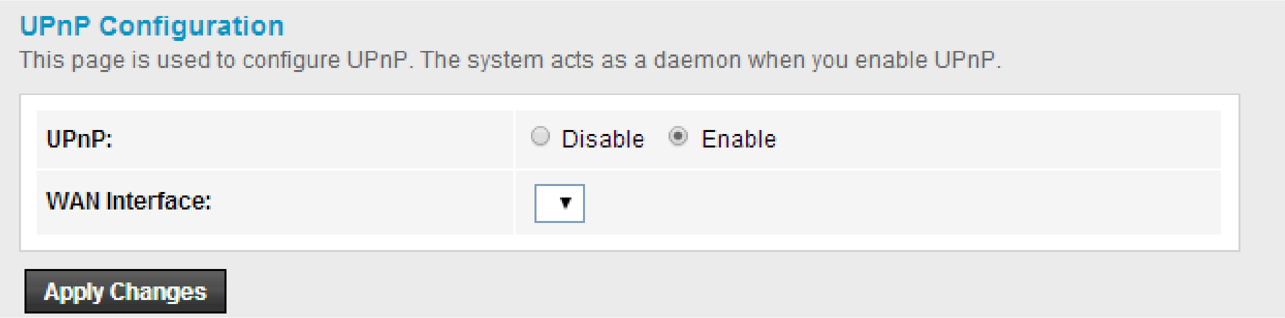
MLD Configuration

MLD Proxy and Snooping can be configured here.

MLD proxy:	● Disable ○ Enable
MLD snooping:	● Disable ○ Enable
Robust Counter:	2
Query Interval:	125 (Second)
Query Response Interval:	10000 (millisecond)
Response Interval of Last Group Member:	1 (Second)

5.3.2 UPnP

The Universal Plug and Play (UPnP) devices can be automatically discovered by the UPnP service application on the LAN.



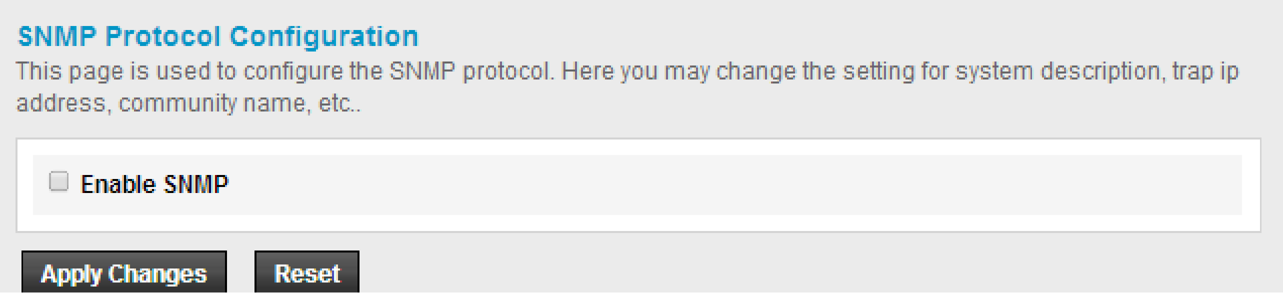
UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

UPnP:	○ Disable ● Enable
WAN Interface:	▼

5.3.3 SNMP

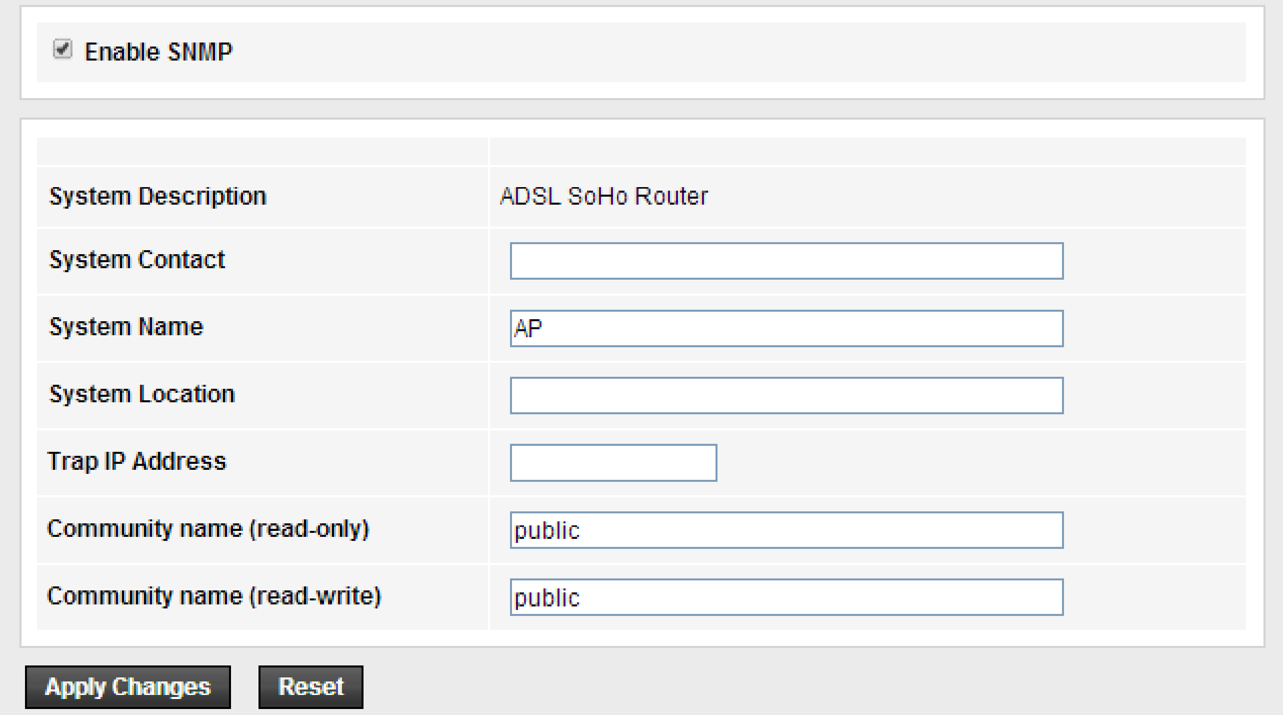
Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.



SNMP Protocol Configuration

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc..

□ Enable SNMP

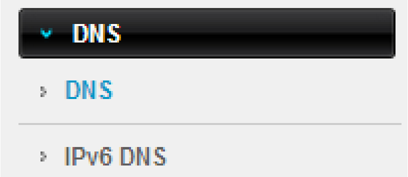


☑ Enable SNMP

System Description	ADSL SoHo Router
System Contact	
System Name	AP
System Location	
Trap IP Address	
Community name (read-only)	public
Community name (read-write)	public

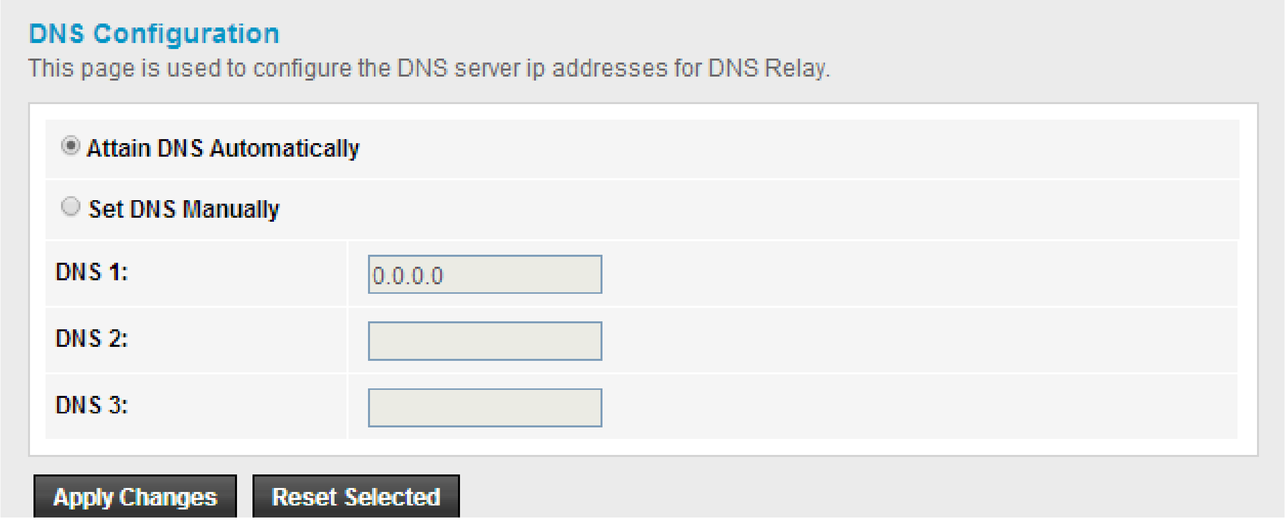
System Name/ Location: set the administrator name and physical location.

5.3.4 DNS



5.3.4.1 DNS

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



DNS Configuration

This page is used to configure the DNS server ip addresses for DNS Relay.

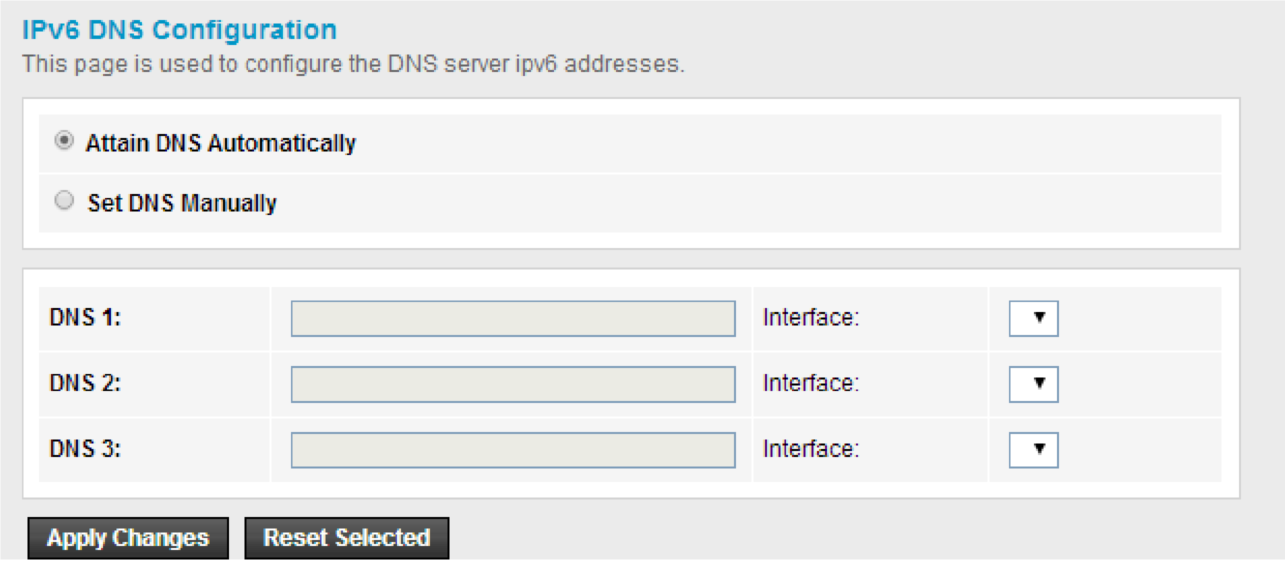
● Attain DNS Automatically

○ Set DNS Manually

DNS 1:	0.0.0.0
DNS 2:	
DNS 3:	

5.3.4.2 IPv6 DNS

This page allows you to configure the DNS server IPv6 address.



IPv6 DNS Configuration

This page is used to configure the DNS server ipv6 addresses.

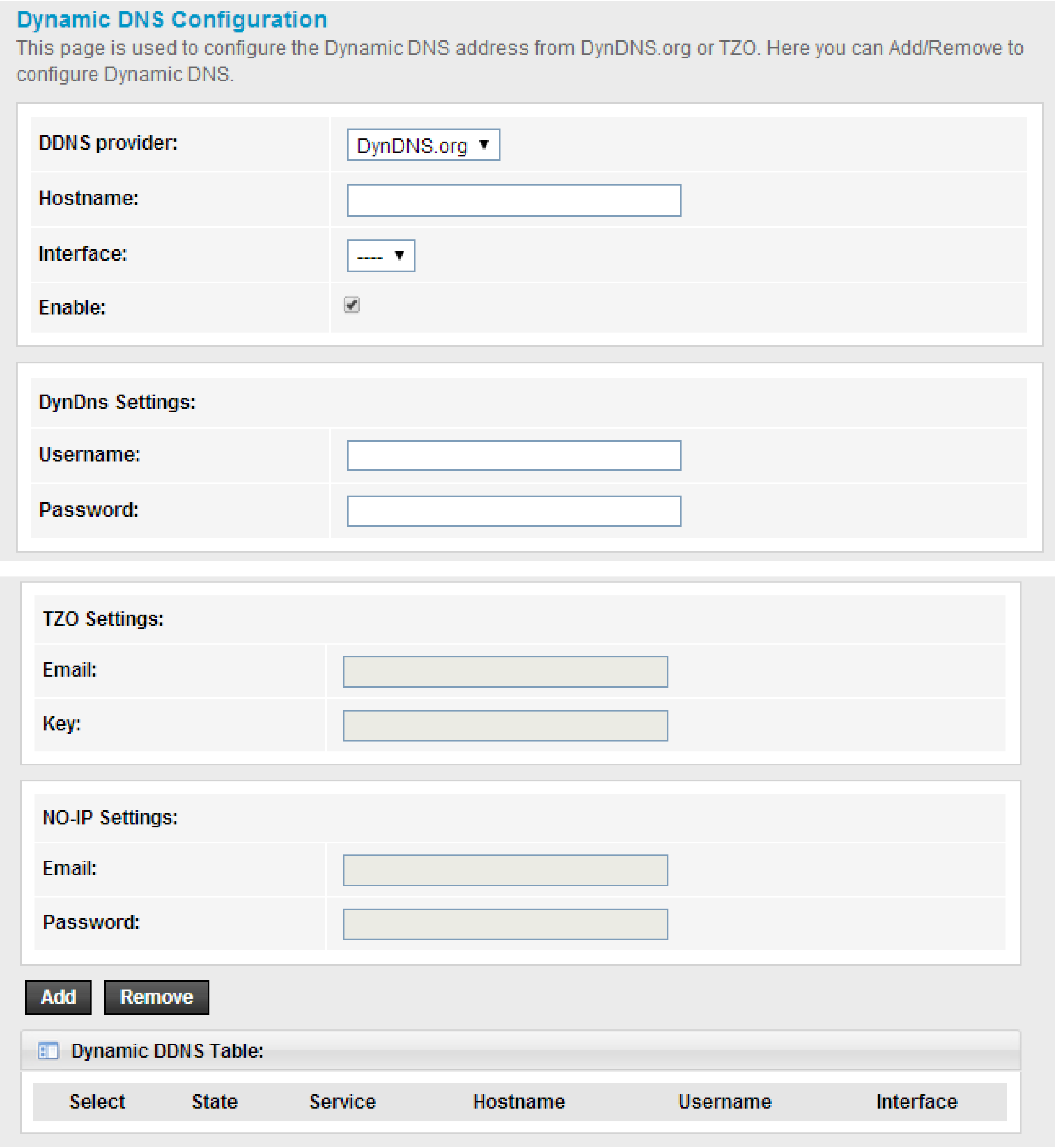
● Attain DNS Automatically

○ Set DNS Manually

DNS 1:		Interface:	▼
DNS 2:		Interface:	▼
DNS 3:		Interface:	▼

5.3.5 DDNS

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



Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

DDNS provider:	DynDNS.org ▼
Hostname:	
Interface:	---- ▼
Enable:	☑

DynDns Settings:	
Username:	
Password:	

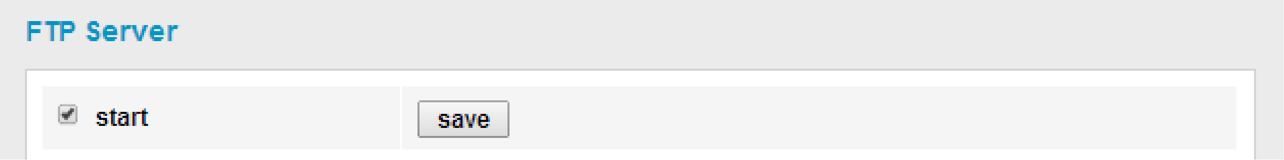
TZO Settings:	
Email:	
Key:	

NO-IP Settings:	
Email:	
Password:	

Dynamic DDNS Table:

Select	State	Service	Hostname	Username	Interface

5.3.6 FTP Server

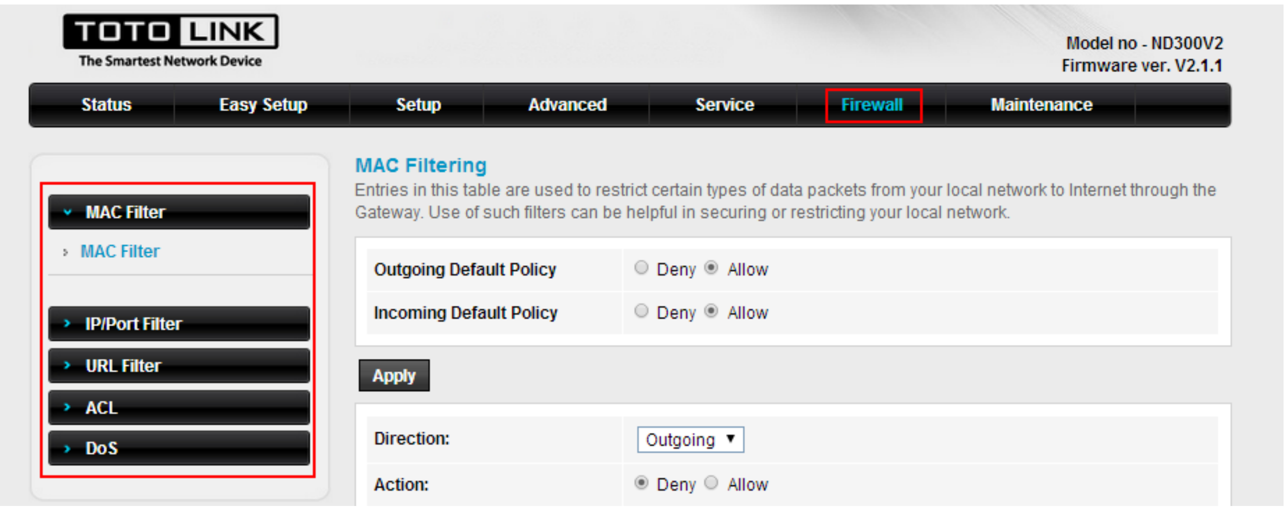


FTP Server

☑ start save

5.4 Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of this router helps to protect your local network against attack from unauthorized access.



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.

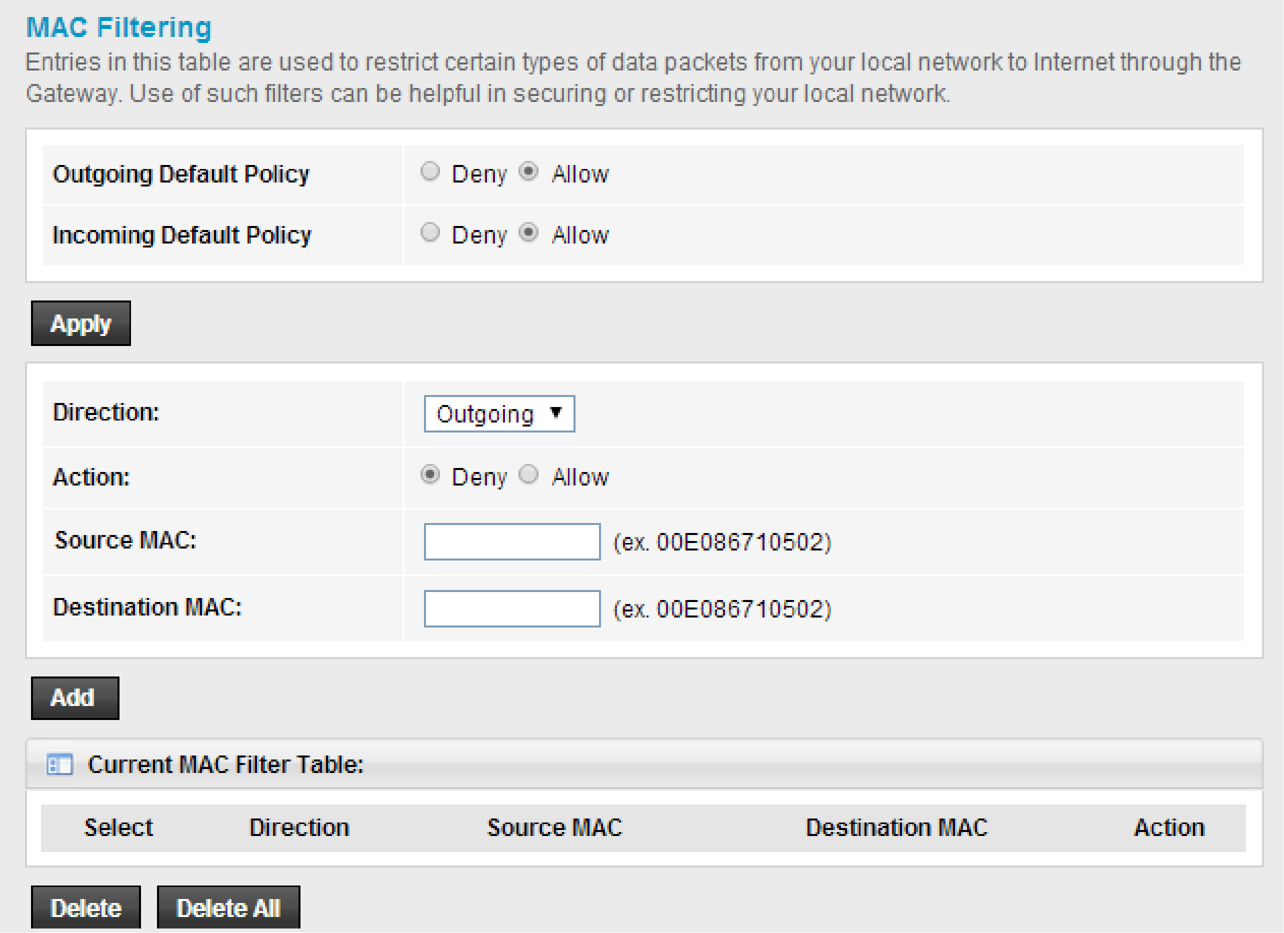
Outgoing Default Policy	○ Deny ● Allow
Incoming Default Policy	○ Deny ● Allow

Apply

Direction:	Outgoing ▾
Action:	● Deny ○ Allow

5.4.1 MAC Filter

MAC Filter function is useful for restricting certain types of data packets from your local network to Internet through the Gateway.



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.

Outgoing Default Policy	○ Deny ● Allow
Incoming Default Policy	○ Deny ● Allow

Direction:	Outgoing ▼
Action:	● Deny ○ Allow
Source MAC:	(ex. 00E086710502)
Destination MAC:	(ex. 00E086710502)

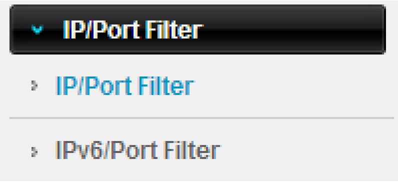
Current MAC Filter Table:

Select	Direction	Source MAC	Destination MAC	Action

Direction: select outgoing or incoming to setup the corresponding value.
Source MAC: enter the starting IP address that you want to deny or allow.

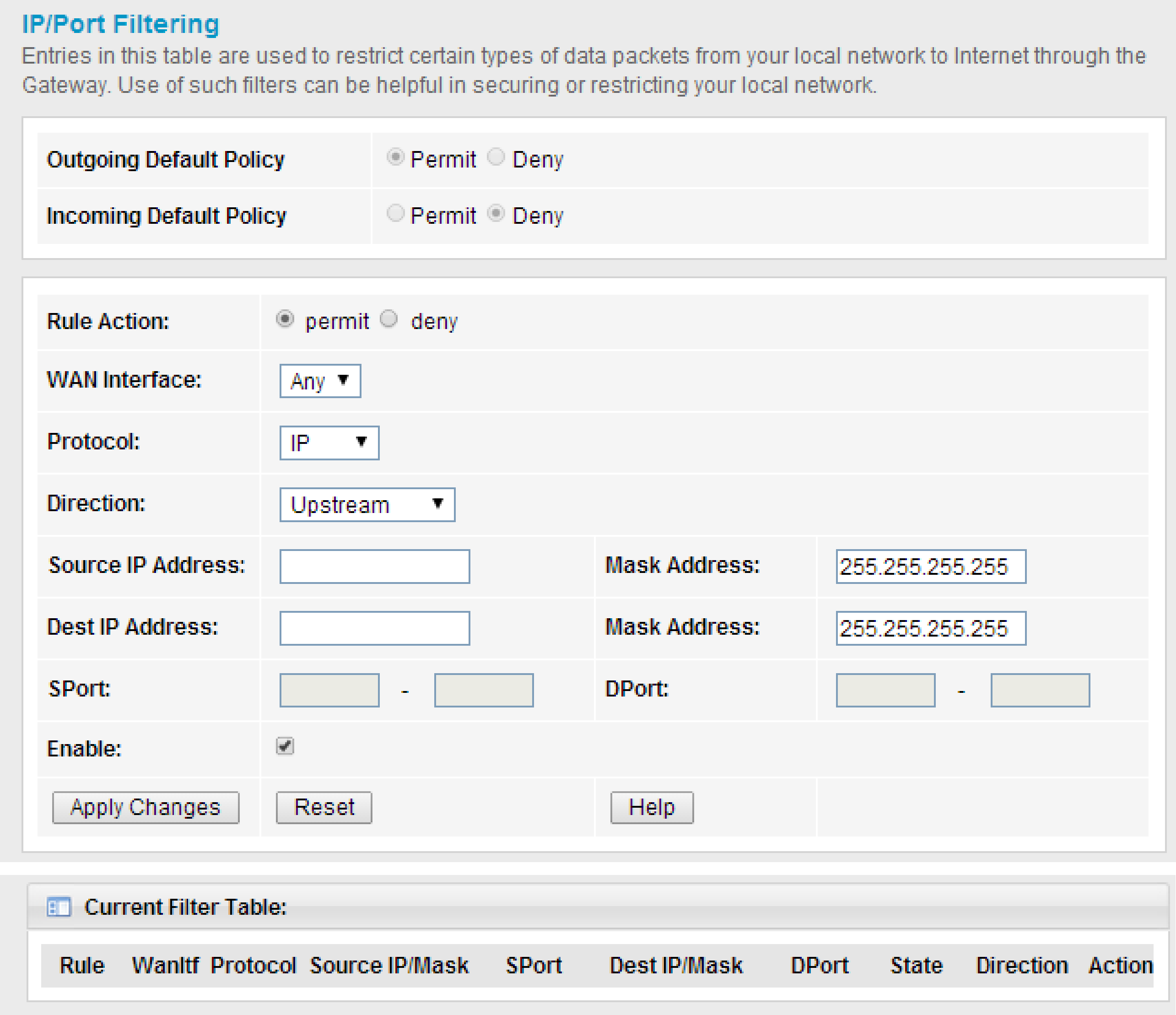
Destination MAC: enter the ending IP address that you want to deny or allow.

5.4.2 IP/Port Filter



5.4.2.1 IP/Port Filter

This page is used to set IP/Port filter rule.



IP/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.

Outgoing Default Policy	● Permit ○ Deny
Incoming Default Policy	○ Permit ● Deny

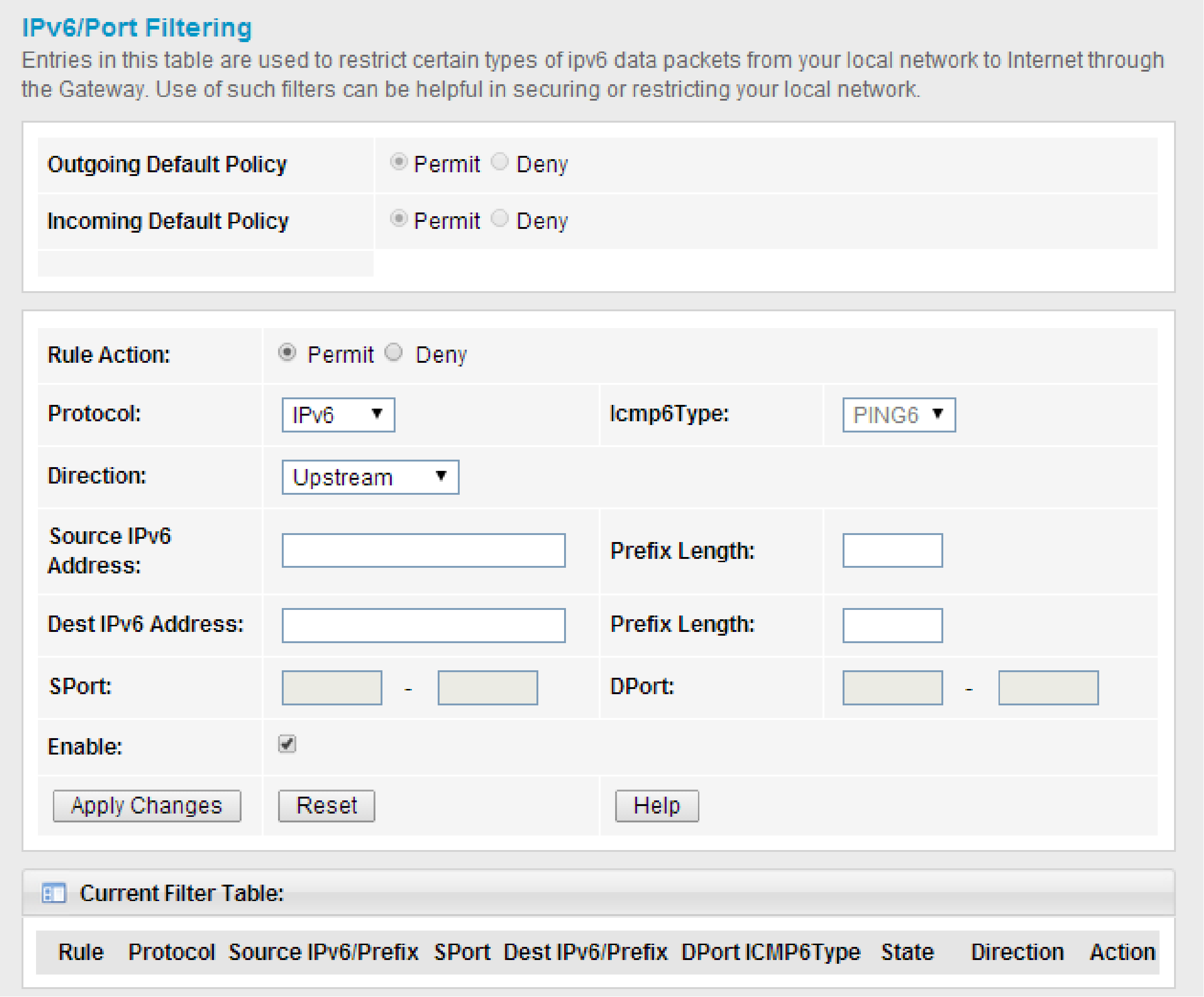
Rule Action:	● permit ○ deny		
WAN Interface:	Any		
Protocol:	IP		
Direction:	Upstream		
Source IP Address:		Mask Address:	255.255.255.255
Dest IP Address:		Mask Address:	255.255.255.255
SPort:	-	DPort:	-
Enable:	☑		
Apply Changes	Reset	Help	

Current Filter Table:

Rule	WanItf	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action

5.4.2.2 IPv6/Port Filter

This page is used to set IPv6/Port filter rule.



IPv6/Port Filtering

Entries in this table are used to restrict certain types of ipv6 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.

Outgoing Default Policy	● Permit ○ Deny
Incoming Default Policy	● Permit ○ Deny

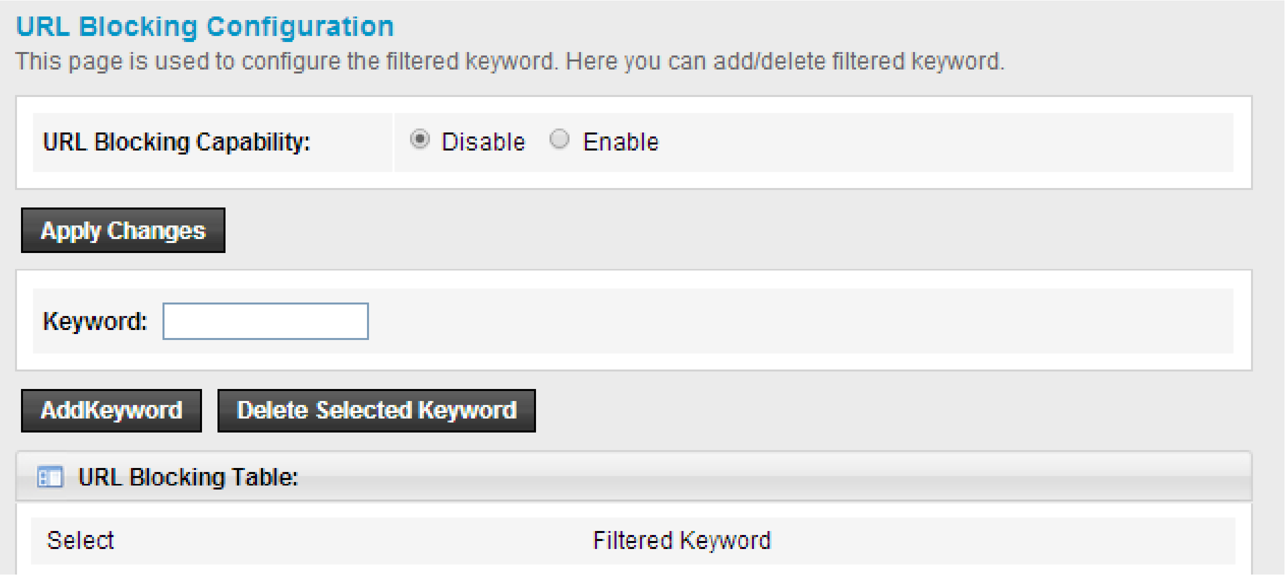
Rule Action:	● Permit ○ Deny		
Protocol:	IPv6 ▼	Icmp6Type:	PING6 ▼
Direction:	Upstream ▼		
Source IPv6 Address:		Prefix Length:	
Dest IPv6 Address:		Prefix Length:	
SPort:	-	DPort:	-
Enable:	☑		

Current Filter Table:

Rule	Protocol	Source IPv6/Prefix	SPort	Dest IPv6/Prefix	DPort	ICMP6Type	State	Direction	Action

5.4.3 URL Filter

This page is used to set URL filter rule. You can active this function and enter URL links that want to filter.



URL Blocking Configuration

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

URL Blocking Capability: ● Disable ○ Enable

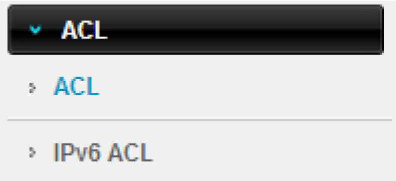
Keyword:

URL Blocking Table:

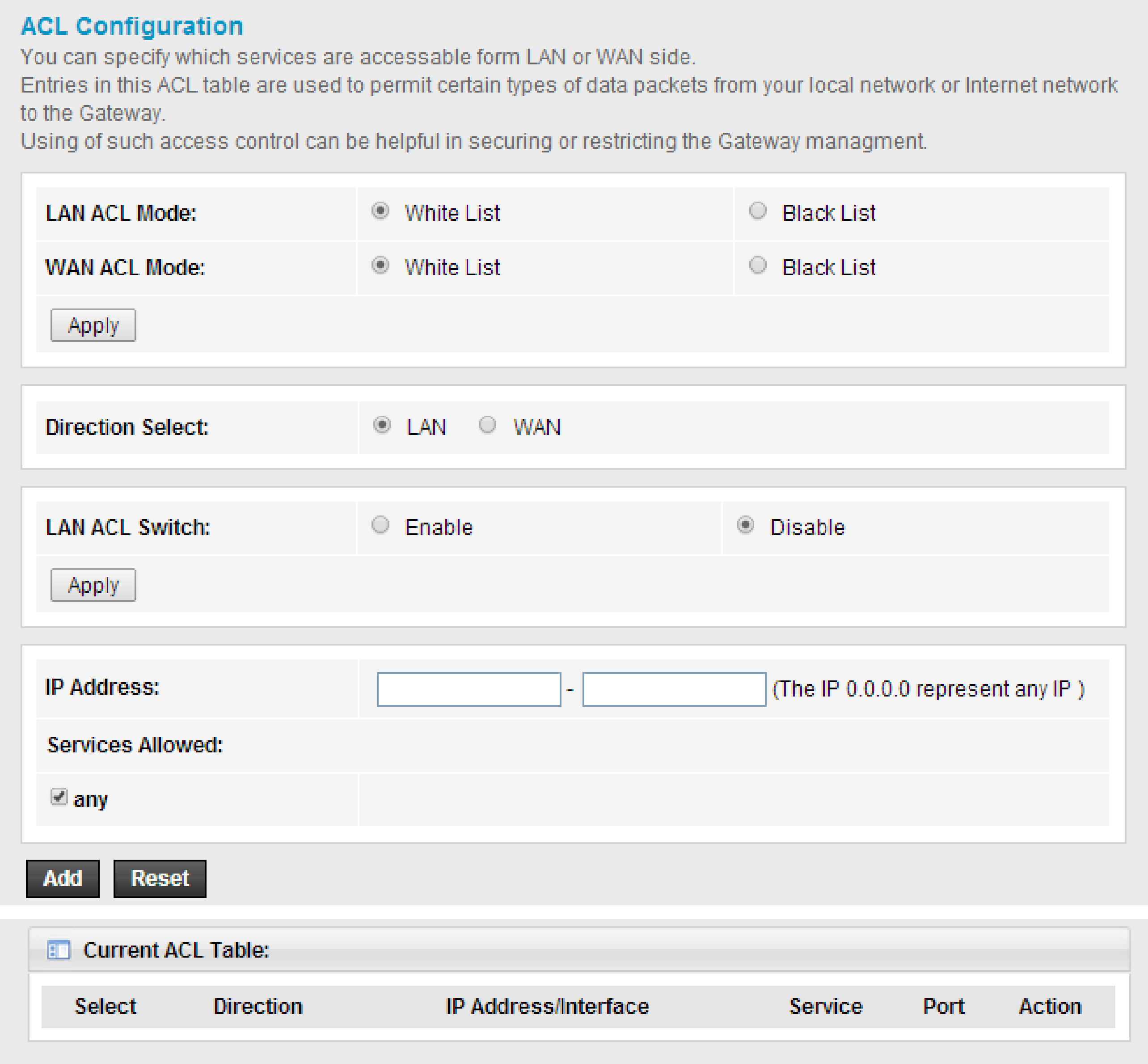
Select	Filtered Keyword

5.4.4 ACL

ACL means Access Control List. This page is used to control the access of this Modem Router.



5.4.4.1 ACL



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

LAN ACL Mode:	● White List	○ Black List
WAN ACL Mode:	● White List	○ Black List
Apply		

Direction Select:	● LAN ○ WAN

LAN ACL Switch:	○ Enable	● Disable
Apply		

IP Address:	[ ] - [ ] (The IP 0.0.0.0 represent any IP)
Services Allowed:	
☑ any	

Add Reset

Current ACL Table:

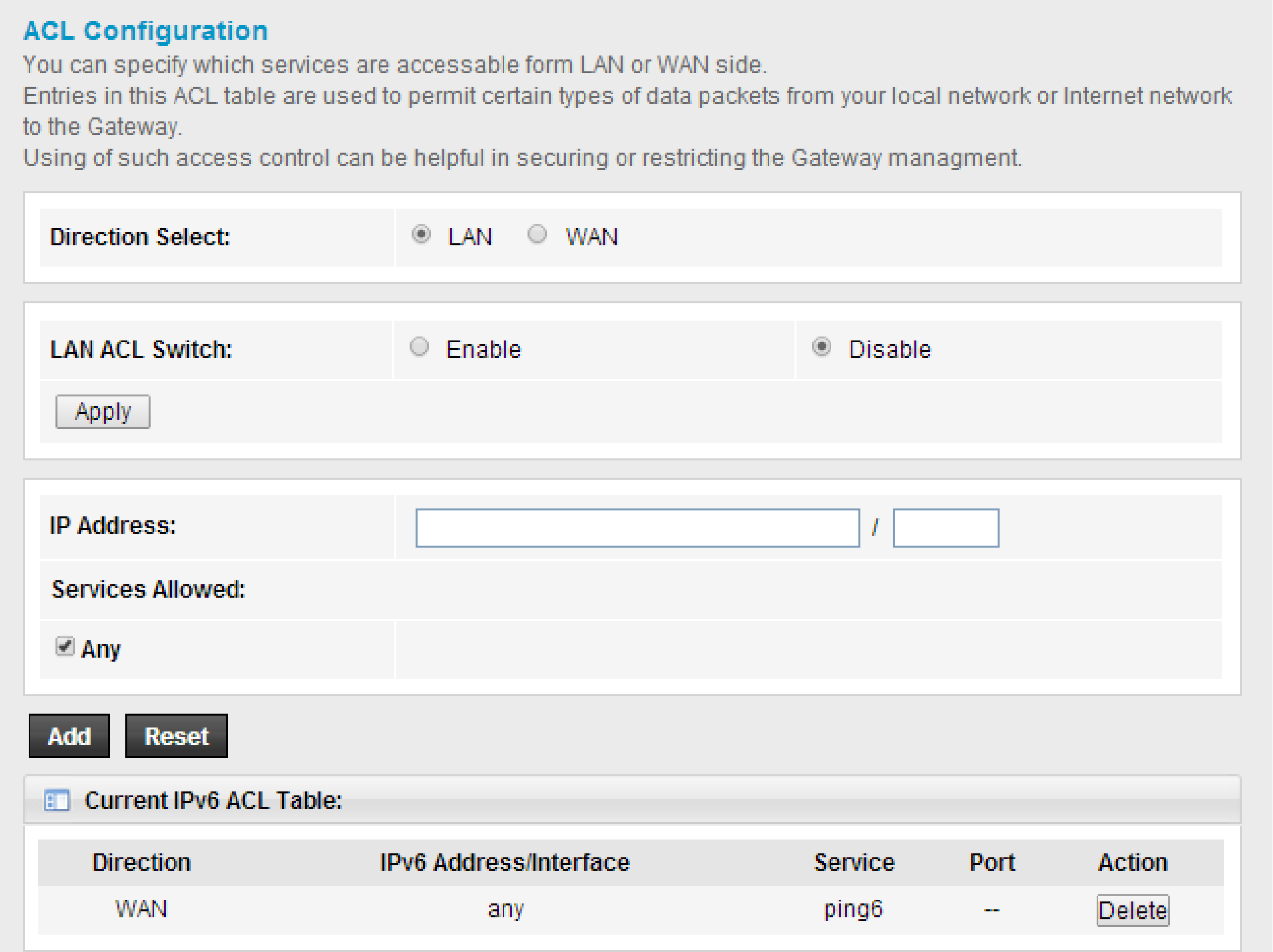
Select	Direction	IP Address/Interface	Service	Port	Action

Direction Select: Set the ACL rule for LAN or WAN.

Secure IP Address: Enter the secure IP address range that you allow to access this Modem Router.

Current ACL Table: This form lists all information about the current ACL rule.

5.4.4.2 IPv6 ACL



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ● LAN ○ WAN

LAN ACL Switch: ○ Enable ● Disable

Apply

IP Address: ______ / ____

Services Allowed:

☑ Any

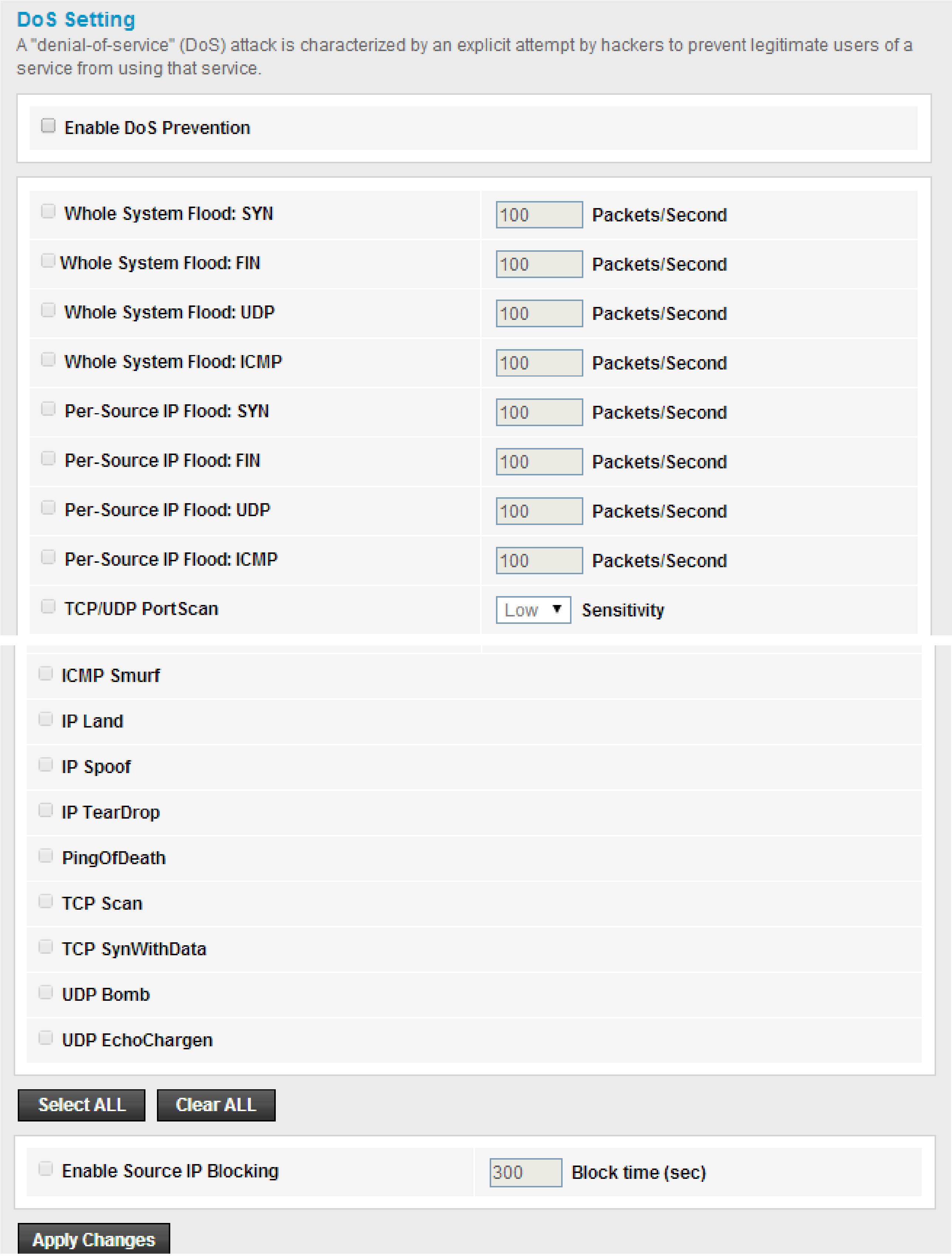
Add Reset

Current IPv6 ACL Table:

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	Delete

5.4.5 DoS

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



DoS Setting

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

☐ Enable DoS Prevention

☐ Whole System Flood: SYN	100 Packets/Second
☐ Whole System Flood: FIN	100 Packets/Second
☐ Whole System Flood: UDP	100 Packets/Second
☐ Whole System Flood: ICMP	100 Packets/Second
☐ Per-Source IP Flood: SYN	100 Packets/Second
☐ Per-Source IP Flood: FIN	100 Packets/Second
☐ Per-Source IP Flood: UDP	100 Packets/Second
☐ Per-Source IP Flood: ICMP	100 Packets/Second
☐ TCP/UDP PortScan	Low ▼ Sensitivity

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

☐ UDP Bomb

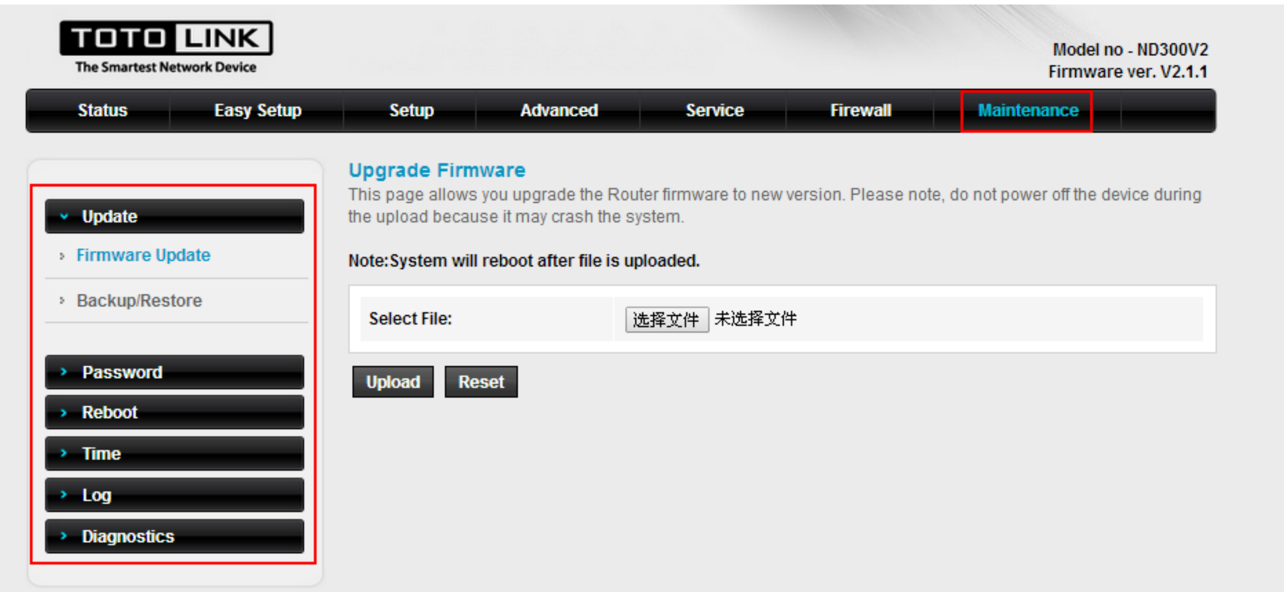
☐ UDP EchoChargen

☐ Enable Source IP Blocking	300 Block time (sec)

5.5 Maintenance

This section includes settings for Administration, Time Zone, Firmware, Log and

Diagnostics.



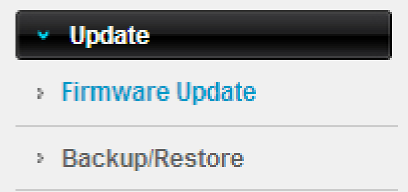
Upgrade Firmware

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

Note:System will reboot after file is uploaded.

Select File: 选择文件 未选择文件

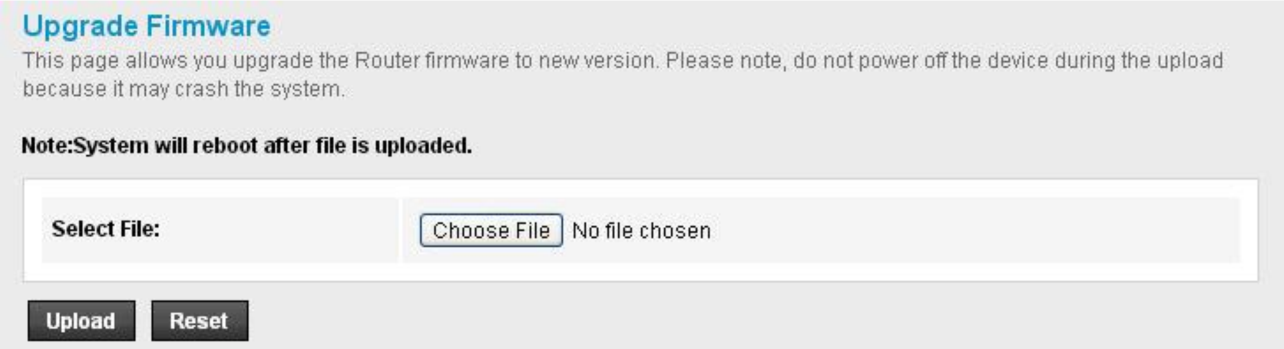
5.5.1 Update



5.5.1.1 Firmware Update

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

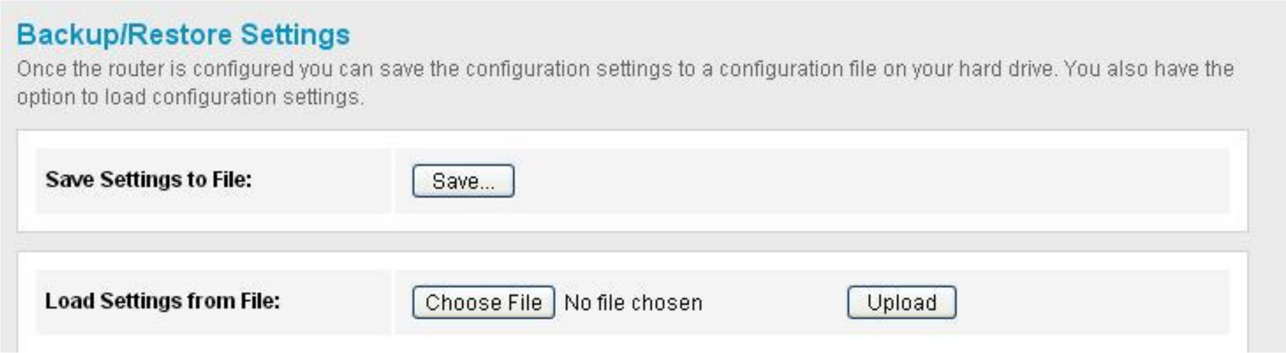
This page allows you upgrade the Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Note:System will reboot after file is uploaded.

Select File: No file chosen

5.5.1.2 Backup/Restore

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



Backup/Restore Settings

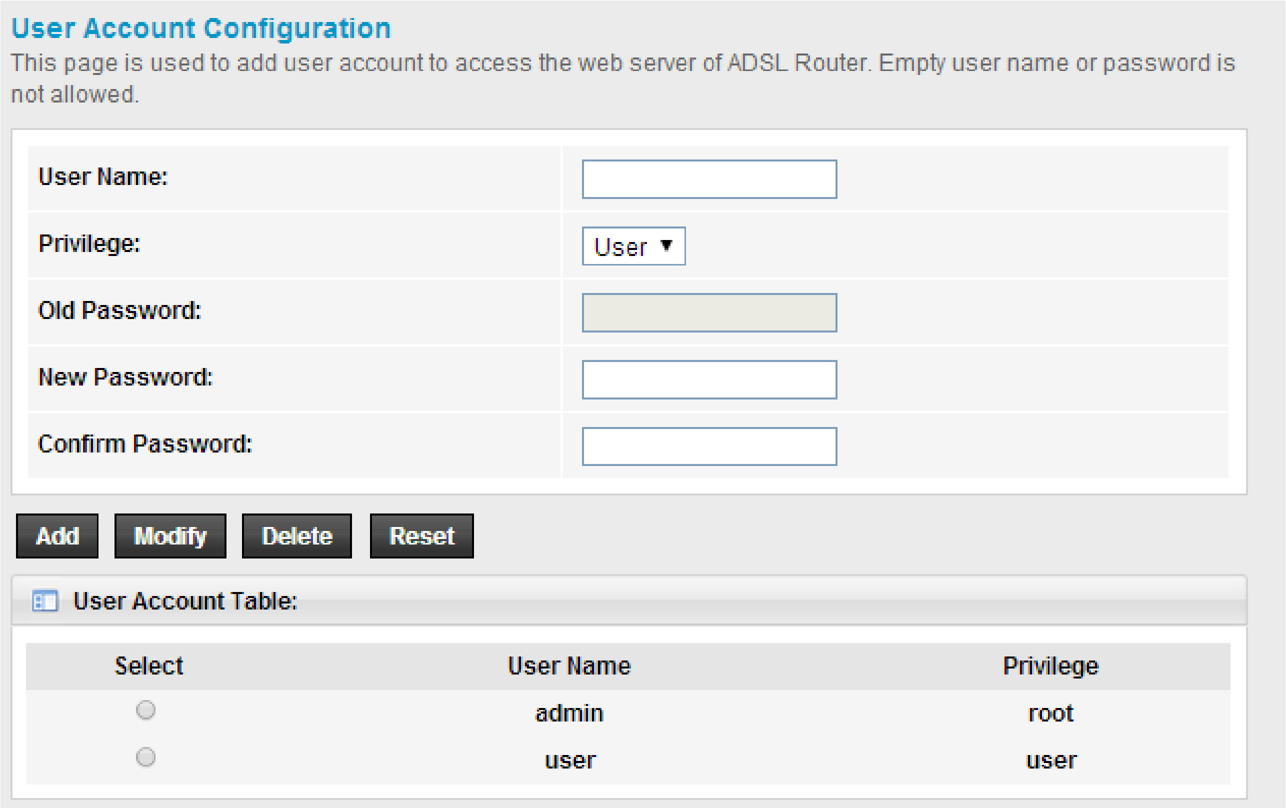
Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.

Save Settings to File:

Load Settings from File: No file chosen

5.5.2 Password

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator’s password should be changed on the very first system setup.



User Account Configuration

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

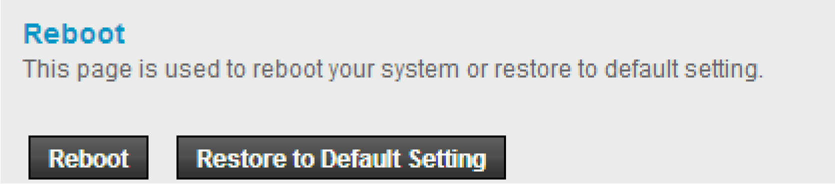
User Name:	
Privilege:	User ▼
Old Password:	
New Password:	
Confirm Password:	

User Account Table:

Select	User Name	Privilege
○	admin	root
○	user	user

5.5.3 Reboot

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

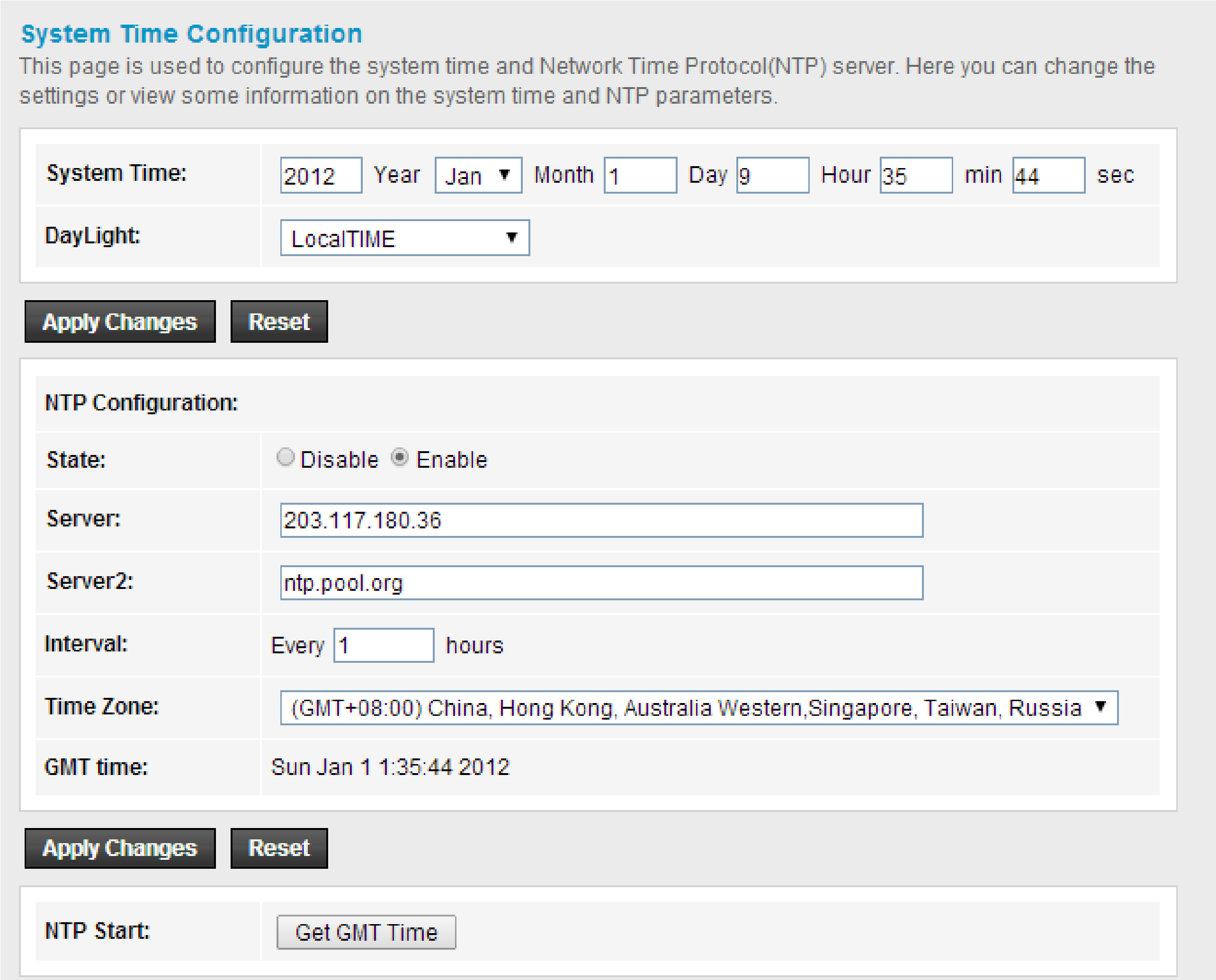


Reboot

This page is used to reboot your system or restore to default setting.

5.5.4 Time

You can set the time server and time zone for your wireless Router system time.



System Time Configuration

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

System Time:	2012 Year Jan ▼ Month 1 Day 9 Hour 35 min 44 sec
DayLight:	LocalTIME ▼

NTP Configuration:	
State:	○ Disable ● Enable
Server:	203.117.180.36
Server2:	ntp.pool.org
Interval:	Every 1 hours
Time Zone:	(GMT+08:00) China, Hong Kong, Australia Western,Singapore, Taiwan, Russia ▼
GMT time:	Sun Jan 1 1:35:44 2012

NTP Start:	Get GMT Time

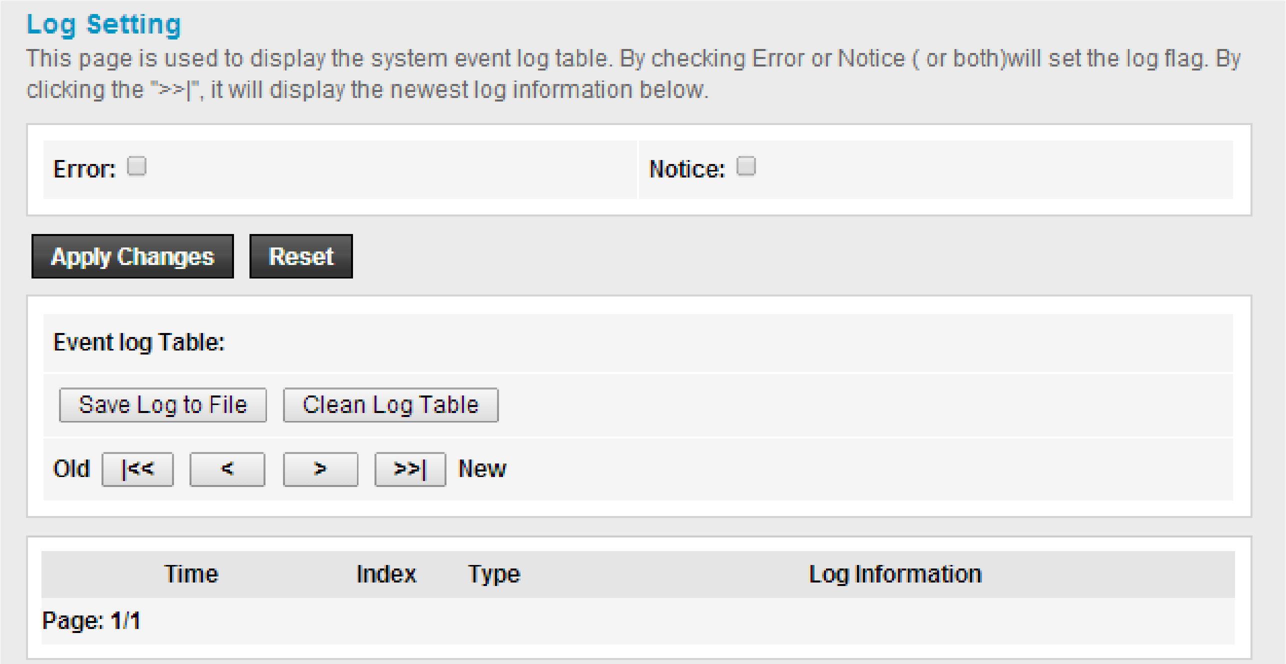
You can specify the device’s time zone according to GMT (Greenwich Mean Time) or copy computer time as the current time only by clicking the **Copy Computer Time** button.

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

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

5.5.5 Log

Log page shows the working status of the wireless router, user can check the running status information here:



Log Setting

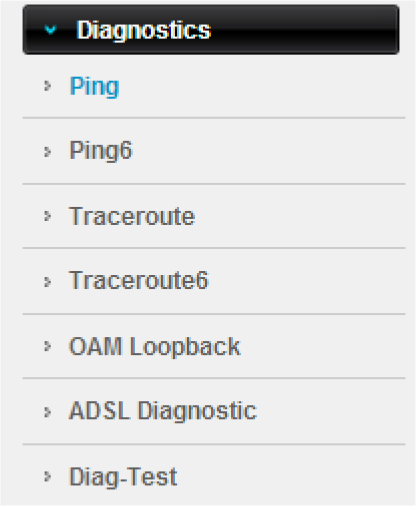
This page is used to display the system event log table. By checking Error or Notice (or both)will set the log flag. By clicking the ">>|", it will display the newest log information below.

Error: □ Notice: □

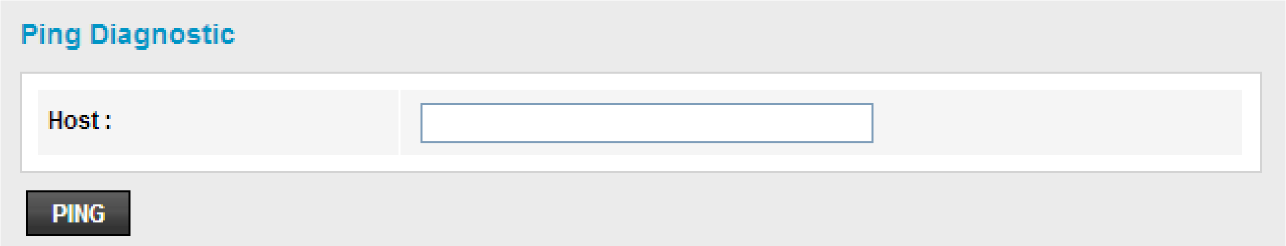
Time	Index	Type	Log Information
Page: 1/1			

5.5.6 Diagnostics

This section is useful for testing unless you know what effect the configuration will have on your wireless router.



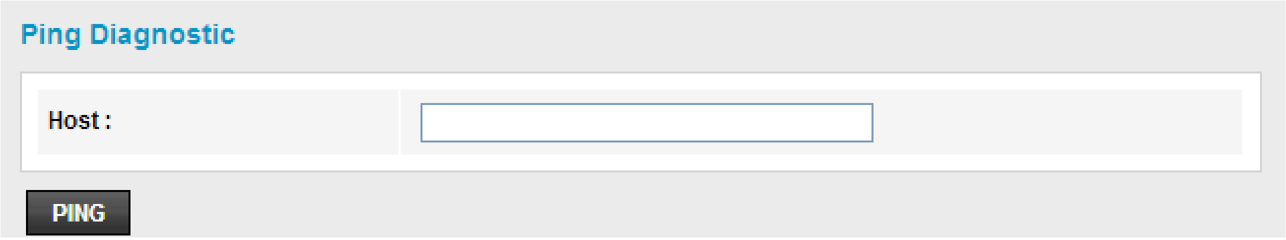
5.5.6.1 Ping



Ping Diagnostic

Host :

5.5.6.2 Ping6

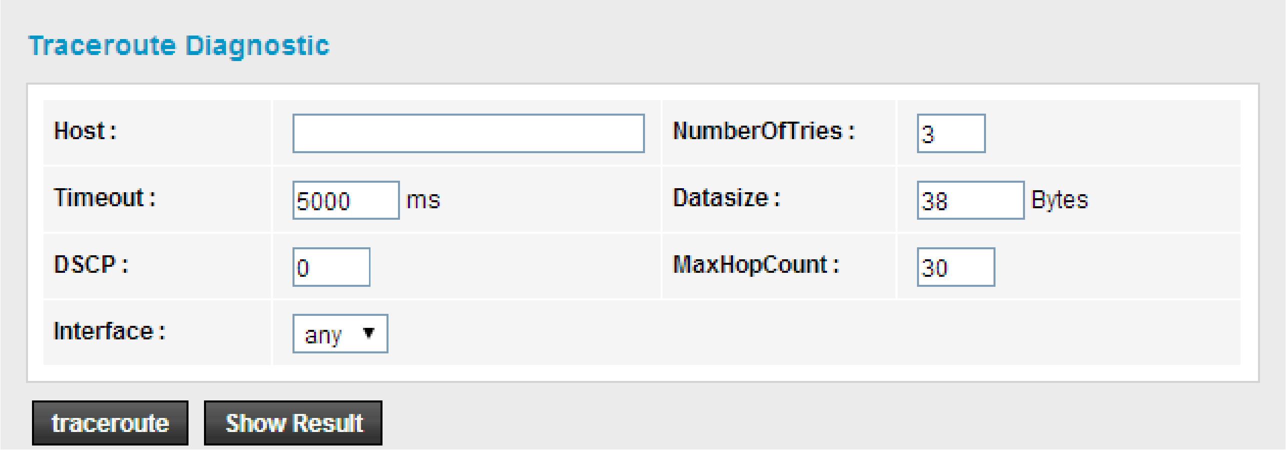


Ping Diagnostic

Host :	

5.5.6.3 Traceroute

Traceroute is a network debugging utility that attempts to trace the path a packet takes through the network.

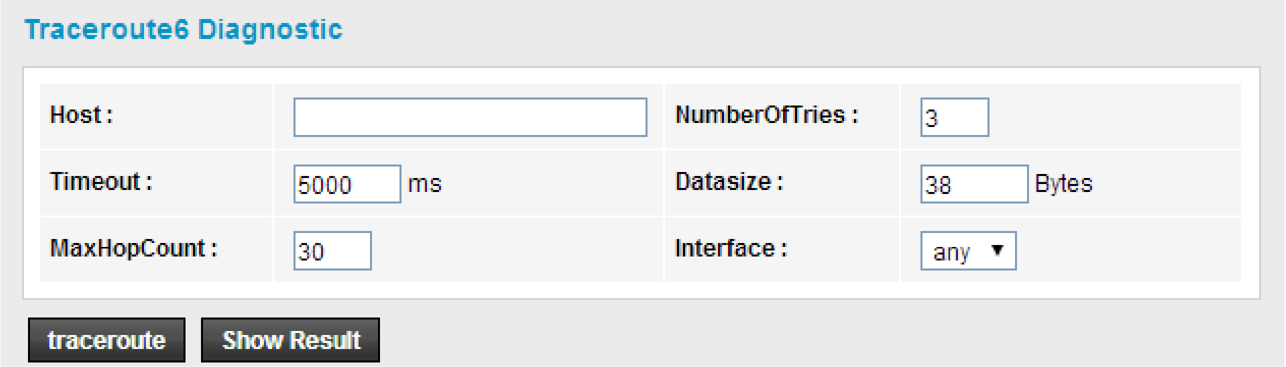


Traceroute Diagnostic

Host :		NumberOfTries :	3
Timeout :	5000 ms	Datasize :	38 Bytes
DSCP :	0	MaxHopCount :	30
Interface :	any ▼		

5.5.6.4 Traceroute6

Traceroute6 is an IPv6 varaint of the IPv4 traceroute tool, a computer network tool used to determine the route taken by packets across an IP network.

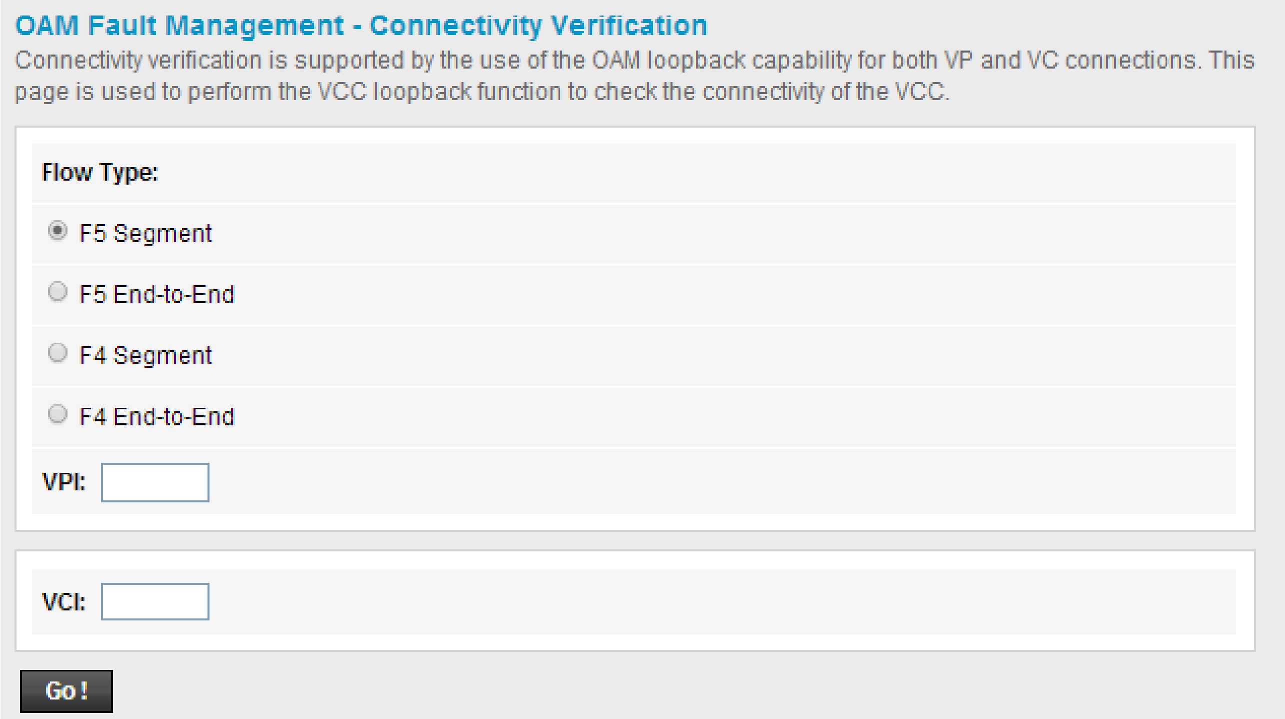


Traceroute6 Diagnostic

Host :		NumberOfTries :	3
Timeout :	5000 ms	Datasize :	38 Bytes
MaxHopCount :	30	Interface :	any ▼

5.5.6.5 OAM Loopback

OAM Loopback capability allows the router to automatically detect the connectivity of the VCC.



OAM Fault Management - Connectivity Verification

Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Flow Type:

● F5 Segment

○ F5 End-to-End

○ F4 Segment

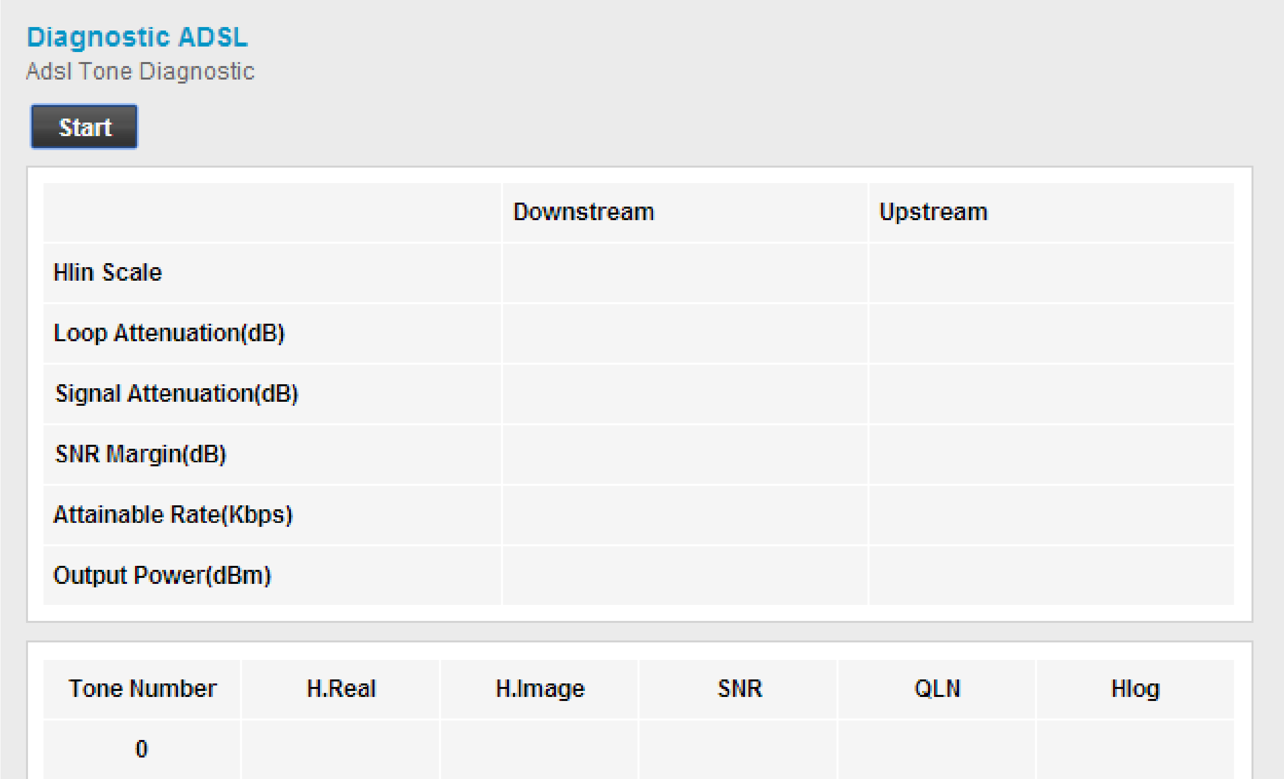
○ F4 End-to-End

VPI:

VCI:

5.5.6.6 ADSL Diagnostic

Click **Start** button to enable diagnose function and then you can see ADSL status in this page.



Diagnostic ADSL

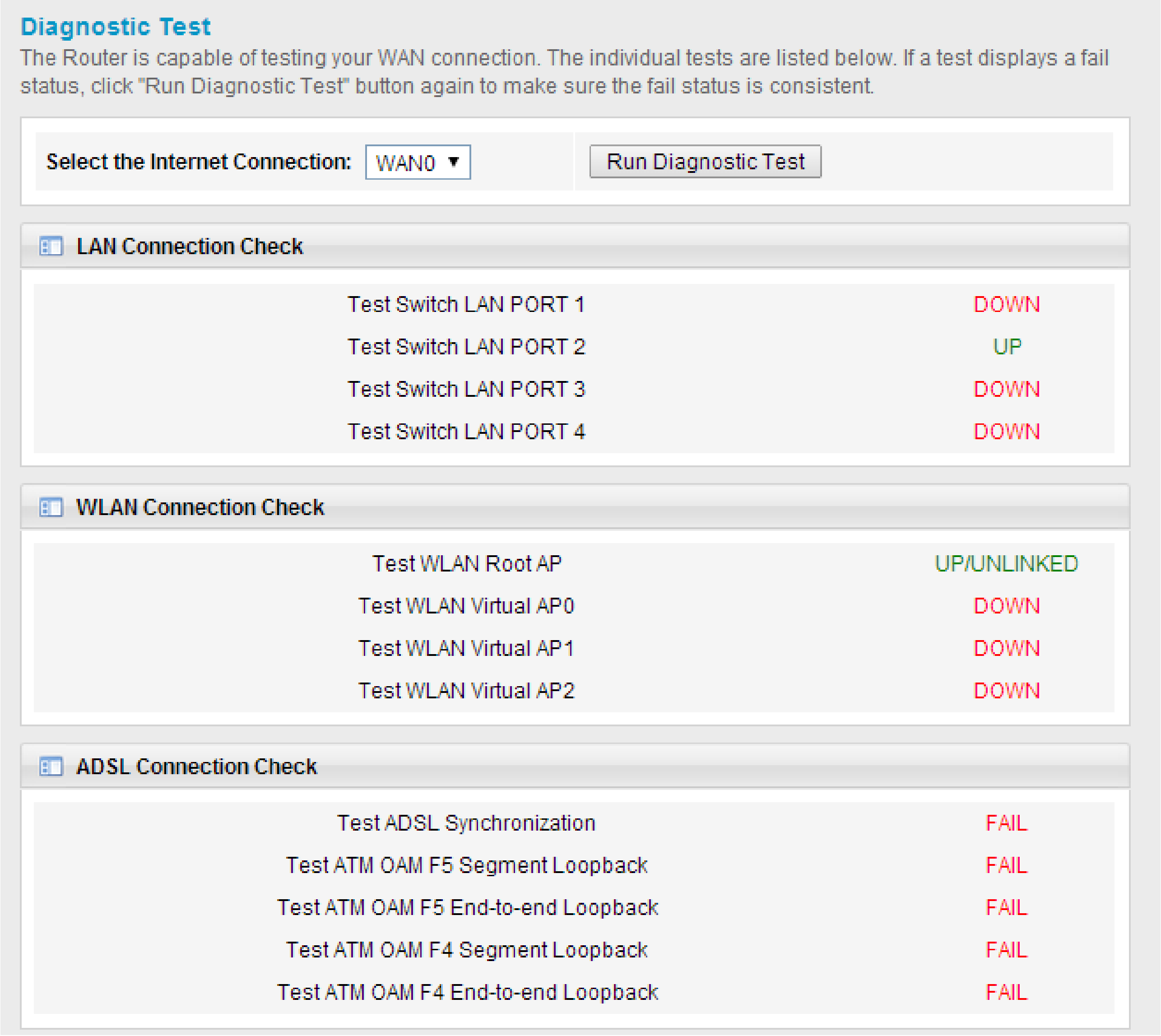
Adsl Tone Diagnostic

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					

5.5.6.7 Diagnostic Test

It is useful for checking connection status. Please press Run Diagnostic Test button.



Diagnostic Test

The Router is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

Select the Internet Connection: WAN0 ▼

LAN Connection Check

Test Switch LAN PORT 1	DOWN
Test Switch LAN PORT 2	UP
Test Switch LAN PORT 3	DOWN
Test Switch LAN PORT 4	DOWN

WLAN Connection Check

Test WLAN Root AP	UP/UNLINKED
Test WLAN Virtual AP0	DOWN
Test WLAN Virtual AP1	DOWN
Test WLAN Virtual AP2	DOWN

ADSL Connection Check

Test ADSL Synchronization	FAIL
Test ATM OAM F5 Segment Loopback	FAIL
Test ATM OAM F5 End-to-end Loopback	FAIL
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL