V7610-I1

User Manual

Contents

1. Introduction....4

1.1 Specifications....4

2. Installation....5

2.1 Hardware installation....5

3. Connect to the router....6

3.1 Setup your local network....6

3.2 Connect to the router....9

4. Local Network....11

4.1 LAN IP Settings....11

4.2 WLAN Settings....11

4.2.1 Basic Setting....12

4.2.2 Advanced Setting....12

4.2.3 Security....13

4.2.4 Access Control....15

4.2.5 WPS....16

4.2.6 Status....16

5. Internet....17

5.1 WAN Mode....17

5.2 Ethernet WAN....17

5.3 PTM WAN....19

5.4 ATM WAN....20

5.5 ATM Settings....21

5.6 DSL Settings....21

5.7 3G Setting....22

6. VoIP....23

6.1 Port 1....23

6.2 Advanced....25

6.3 Tone....25

6.4 Others....26

6.5 Network....26

7. Advanced....27

7.1 ARP Table....27

7.2 LAN Device Table....27

7.3 Bridging....28

7.4 Routing....28

7.5 SNMP....29

7.6 IP QoS....30

7.6.1 Qos Poilcy....30

7.6.2 Qos Classification....30

7.7 Remote Access....30

7.8 Others....31

7.9 IPv6....32

7.9.1 IPv6 32

7.9.2 RADVD 32

7.9.3DHCPv6 32

7.9.4 MLD Proxy 34

7.9.5 MLD Snooping 35

7.7.6 IPv6 Routing 35

7.9.7 IPv6 IP/Port Filtering 35

8. Service 36

8.1 DHCP 36

8.1.1 None 36

8.1.2 DHCP Server 36

8.1.3 DHCP Relay 38

8.2 DNS 38

8.3 Firewall 39

8.3.1 Security settings 40

8.3.2 ALG 40

8.3.3 IP/Port filter 41

8.3.4 MAC filter 42

8.3.5 Port Forwarding 43

8.3.6 URL filter 43

8.3.7 Domain Blocking 44

8.3.8 DMZ 45

8.4 UPnP 45

8.5 RIP 46

8.6 Samba 47

9. Admin 48

9.1 Commit/Reboot 48

9.2 Backup/Restore 48

9.3 System Log 49

9.4 DoS 49

9.5 Password 50

9.6 Firmware Upgrade 51

9.7 Time Zone 51

9.8 TR-069 52

10. Diagnostics 53

10.1 Ping 53

10.2 Traceroute 54

10.3 ATM Loopback 56

10.4 DSL Tone 56

10.5 ADSL Connection 57

FAQ 58

11. Certification 61

FCC 61

1. Introduction

The router is a device with routing capability, wireless access point. It has Ethernet and ADSL/VDSL access capabilities. The Ethernet or ADSL/VDSL Router provides 10/100Base-T Ethernet interface and supports wireless 802.11/b/g/n/ and the following security protocols: WEP, WPA2 and 802.1x. Through the Ethernet or ADSL/VDSL access, the router can provides user with access to Internet.

This user manual is mainly used to guide the user to install and configure the Router from WEB UI.

1.1 Specifications

- Wireless AP, Router, 4 Port Switch and Firewall
- Support 802.11n, compatible with 802.11b and 802.11g
- Up to 54 Mbps wireless operation rate
- 64/128 bits WEP for security
- WPA2 support
- 4 10/100MBase-T Ethernet interface (LAN)
- RFC-1483/2684 LLC/VC-Mux bridge/route mode
- RFC-2516 PPPoE
- RFC-2364 PPPoA
- 802.1d Spanning-Tree Protocol
- DHCP Client/Server/Relay
- NAT
- RIP v1/v2
- DNS Relay Agent
- Support DMZ, virtual server, ALG
- IGMP Proxy/Snooping
- Protection against Denial of Service attack
- IP Packet filtering
- MAC filtering
- URL filtering
- IP QoS
- Dynamic DNS
- UPnP support
- System log support, can record the state of the router
- Remote management
- Firmware upgrade through FTP, TFTP and HTTP
- Configuration backup/restore
- Diagnostic tools
- Voip support

2. Installation

2.1 Hardware installation

To install the device correctly, you should prepare as follows:

- A RTL867x board
- 12V DC power
- RJ-45 Ethernet cable
- COM Port cable (Optional)

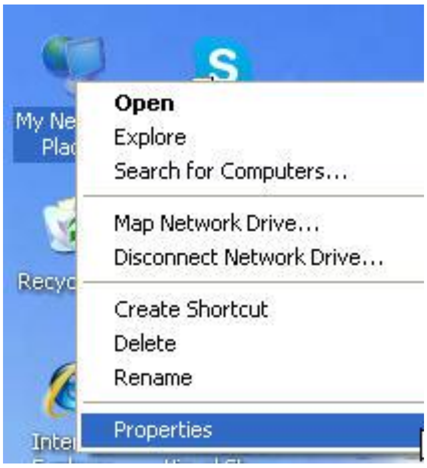
Then you can follow the procedures to setup the device:

1. Connect RJ-45 cable from your PC to RTL867x Ethernet Port
2. Connect PC’s COM port to RTL867x COM port if you have COM port cable. You can monitor the status of system and input control command from PC’s HyperTerminal.
3. Connect the 12V DC power

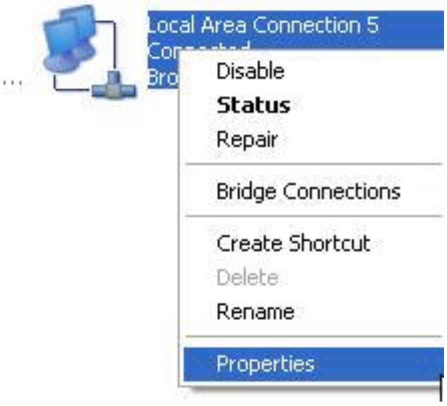
3. Connect to the router

3.1 Setup your local network

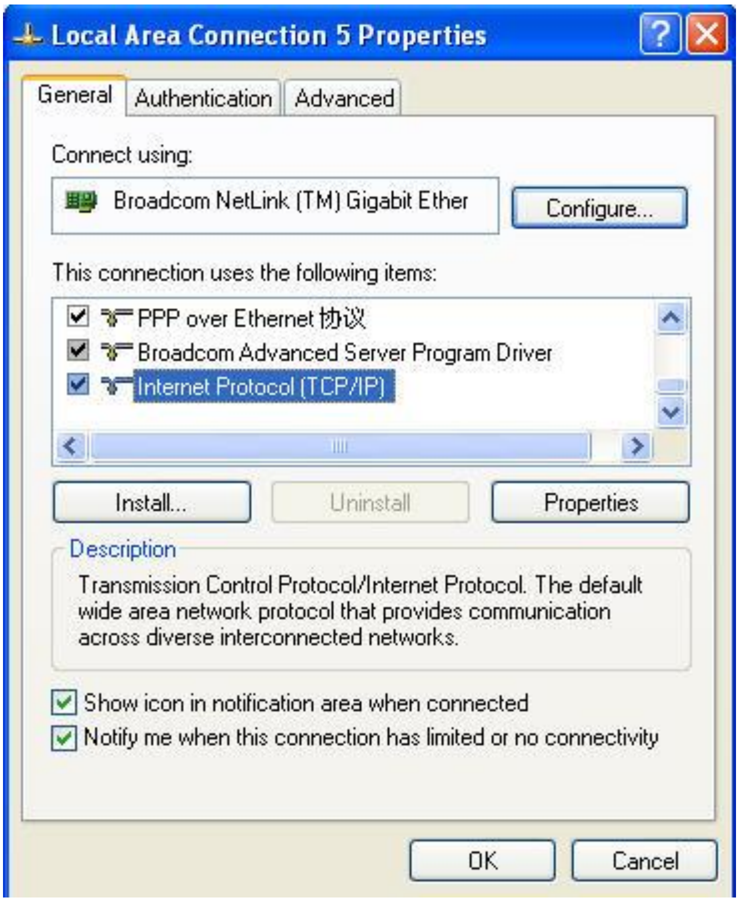
1. Right click the “Network” icon on you desktop, select “properties” in the pop-up menu



2. In the following window, right click on the “Local connection” and select “properties”



3. In the pop-up dialog box, select the “Internet Protocol (TCP/IP)”, and then click the “properties” button



Connect using:

Broadcom NetLink (TM) Gigabit Ether

This connection uses the following items:

- ☑ PPP over Ethernet 协议
- ☑ Broadcom Advanced Server Program Driver
- ☑ Internet Protocol (TCP/IP)

Description

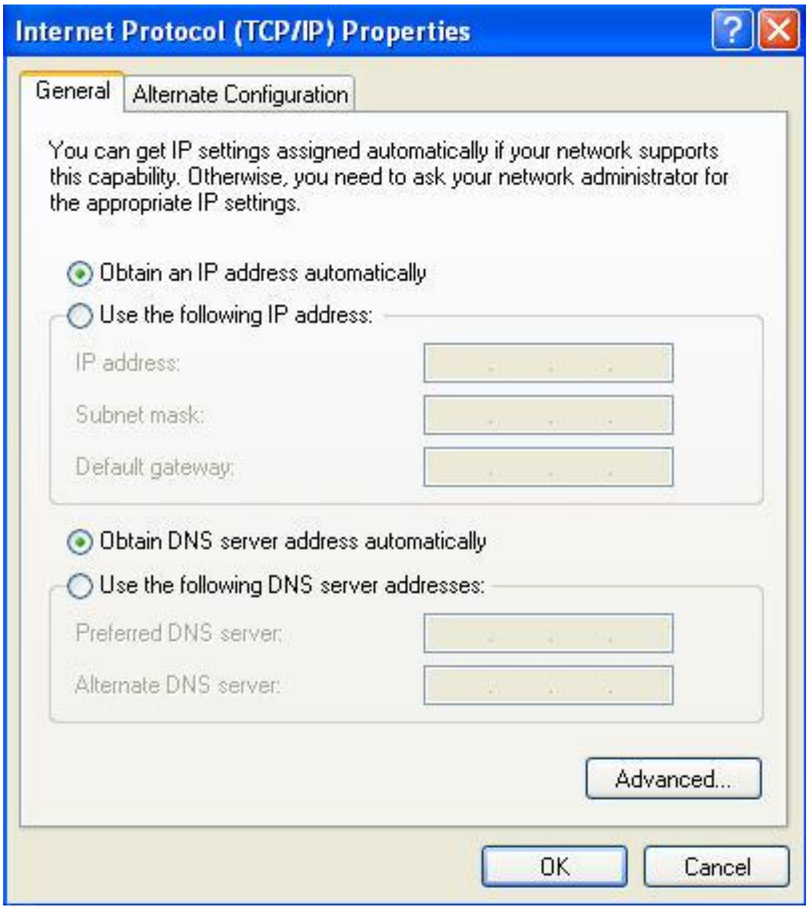
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

4. In the subsequent opening of the window, you can select "obtain IP address automatically (O) " or "Use the following IP address (S) "

   a) Obtain IP address automatically (O)



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

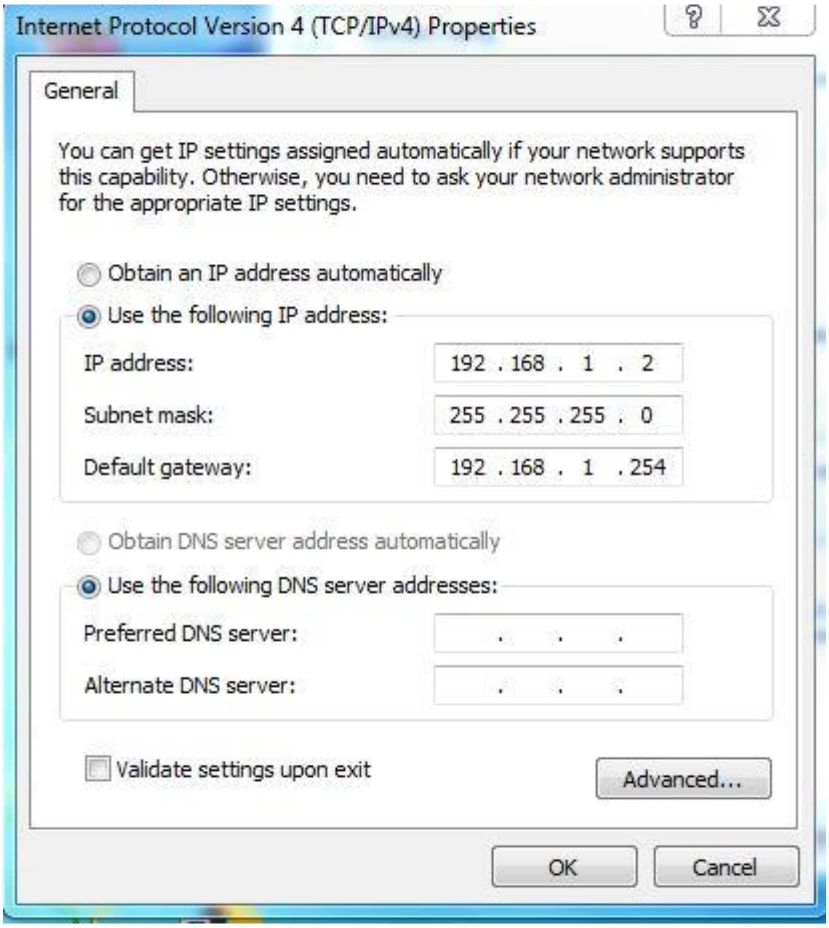
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

b) Use the following IP address (S)
IP address: 192.168.1.xx (xx is between 2 and 254)
Subnet mask: 255.255.255.0
Gateway: 192.168.1.254
DNS Server: You can fill out your local DNS server address (ask your ISP provider) can also be the router as a DNS proxy server.
Click “OK” to submit the current settings after setup is complete.


Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

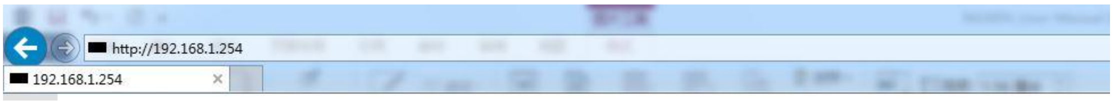
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

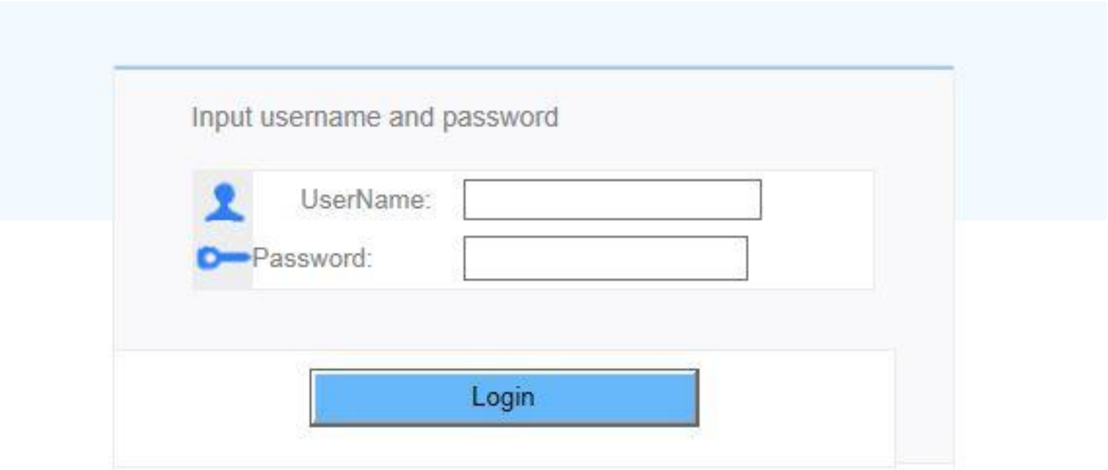
3.2 Connect to the router

1. Open IE browser, and input “http://192.168.1.254” in the address bar and press enter


http://192.168.1.254

192.168.1.254

2. Input username and password on the pop-up dialog to login the router



Input username and password

UserName:

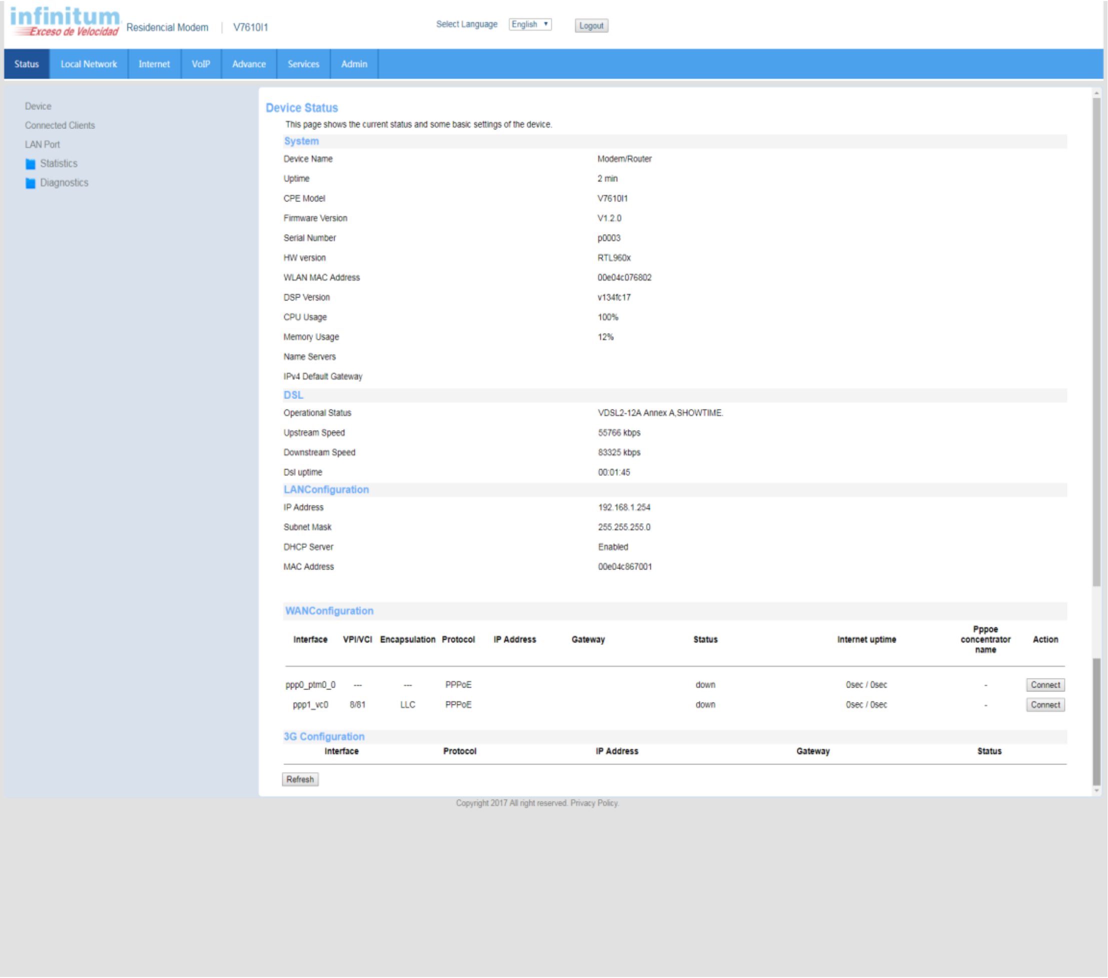
Password:

Login

User Name: TELMEX

Password :Generated by sequence number

3. If the username and password is correct, then you will see the web management pages.



Device Status

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

System

Device Name	Modem/Router
Uptime	2 min
CPE Model	V7610I1
Firmware Version	V1.2.0
Serial Number	p0003
HW version	RTL960x
WLAN MAC Address	00e04c076802
DSP Version	v134fc17
CPU Usage	100%
Memory Usage	12%
Name Servers	
IPv4 Default Gateway	

DSL

Operational Status	VDSL2-12A Annex A,SHOWTIME.
Upstream Speed	55766 kbps
Downstream Speed	83325 kbps
Dsl uptime	00:01:45

LANConfiguration

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00e04c867001

WANConfiguration

Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status	Internet uptime	Pppoe concentrator name	Action
ppp0_ptm0_0	---	---	PPPoE			down	0sec / 0sec	-	Connect
ppp1_vc0	8/81	LLC	PPPoE			down	0sec / 0sec	-	Connect

3G Configuration

Interface	Protocol	IP Address	Gateway	Status

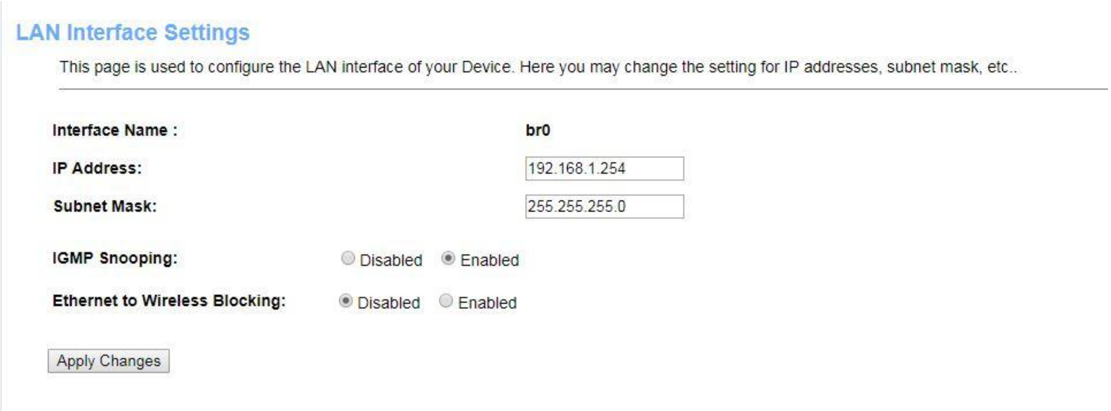
Refresh

Copyright 2017 All right reserved. Privacy Policy.

4. Local Network

4.1 LAN IP Settings

Go to the Local Network page, you can configure the LAN interface of your Router. You may change the setting for IP address, subnet mask, etc..



LAN Interface Settings

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

Interface Name :	br0
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
IGMP Snooping:	○ Disabled ● Enabled
Ethernet to Wireless Blocking:	● Disabled ○ Enabled

- IP address
  The IP address of the Ethernet router’s LAN interface, the default value is 192.168.1.1.
- Subnet mask
  The subnet mask of the Ethernet router’s LAN interface, the default value is 255.255.255.0.
- IGMP Snooping
  You can enable/disable the IGMP Snooping function by the select radio.

Note:
If you change the IP address of the LAN interface, you should use the new IP address to reconnect to the web server.

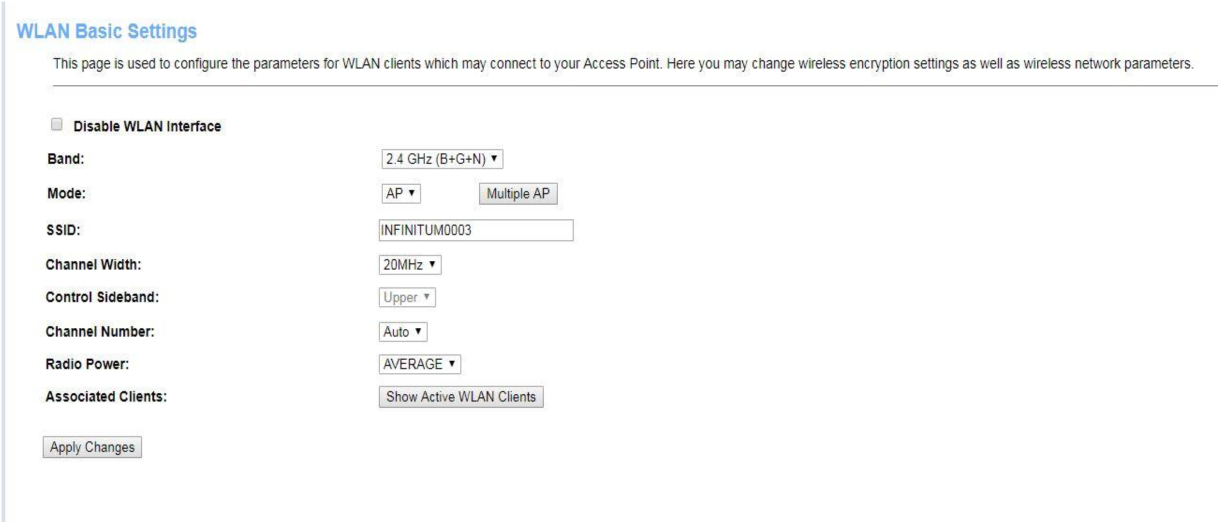
4.2 WLAN Settings

To connect to the Wireless AP, we should have the most basic configuration of the router at first.

In this section, you can set the wireless network parameters required to access the AP of your WLAN interface.

4.2.1 Basic Setting

Go to Local Network ->WLAN->Basic Setting page, you can configure the wireless parameters.



WLAN Basic Settings

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

☐ Disable WLAN Interface

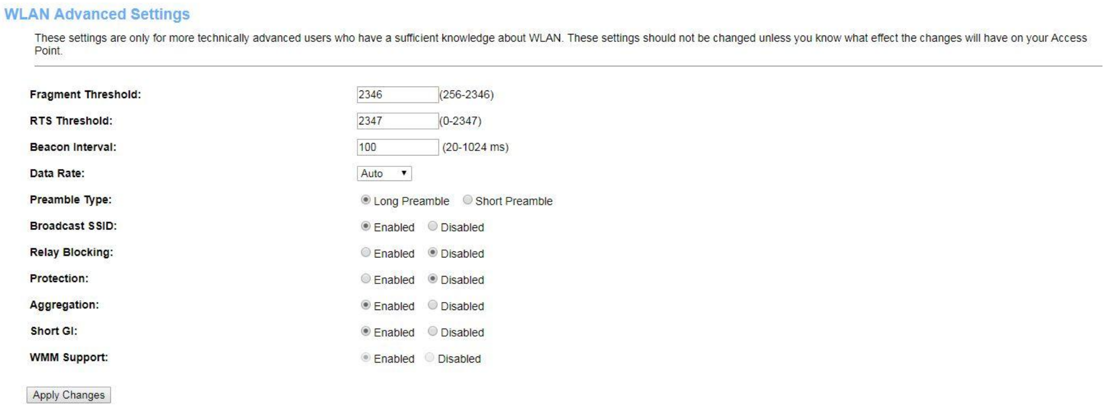
Band:	2.4 GHz (B+G+N) ▾
Mode:	AP ▾ [Multiple AP]
SSID:	INFINITUM0003
Channel Width:	20MHz ▾
Control Sideband:	Upper ▾
Channel Number:	Auto ▾
Radio Power:	AVERAGE ▾
Associated Clients:	[Show Active WLAN Clients]

[Apply Changes]

Here you may enable or disable the wireless function. You can also change the wireless parameters, such as Band, SSID, Channel Width, Control Sideband, Channel Number and Radio Power.

4.2.2 Advanced Setting

Go to Local Network ->WLAN->Advanced Setting page, you can configure the advanced parameters for your wireless LAN.



WLAN Advanced Settings

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

Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto ▾
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
Relay Blocking:	○ Enabled ● Disabled
Protection:	○ Enabled ● Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WMM Support:	● Enabled ○ Disabled

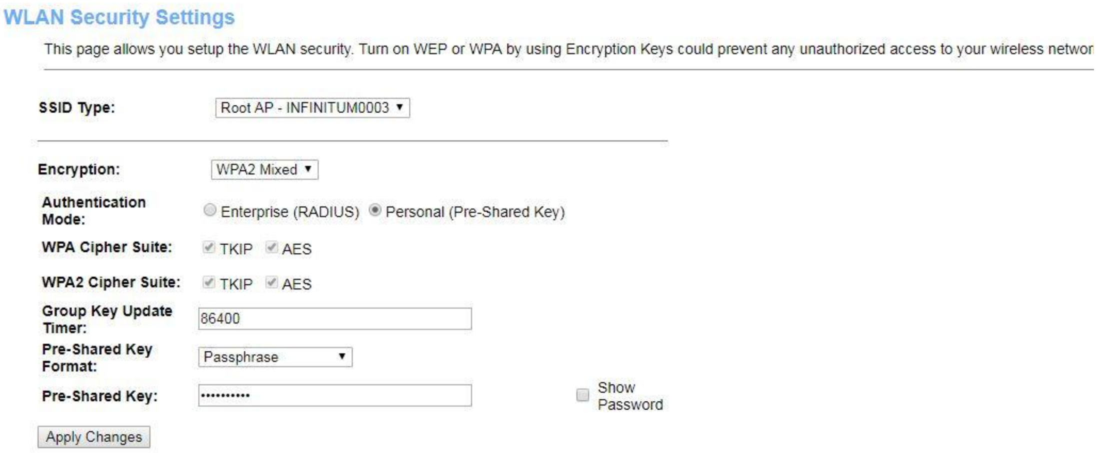
[Apply Changes]

Note:

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 exactly what will happen for the changes you made on your Access Point.

4.2.3 Security

Go to Local Network ->WLAN-> Security page, you can configure the wireless security parameters.



WLAN Security Settings

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

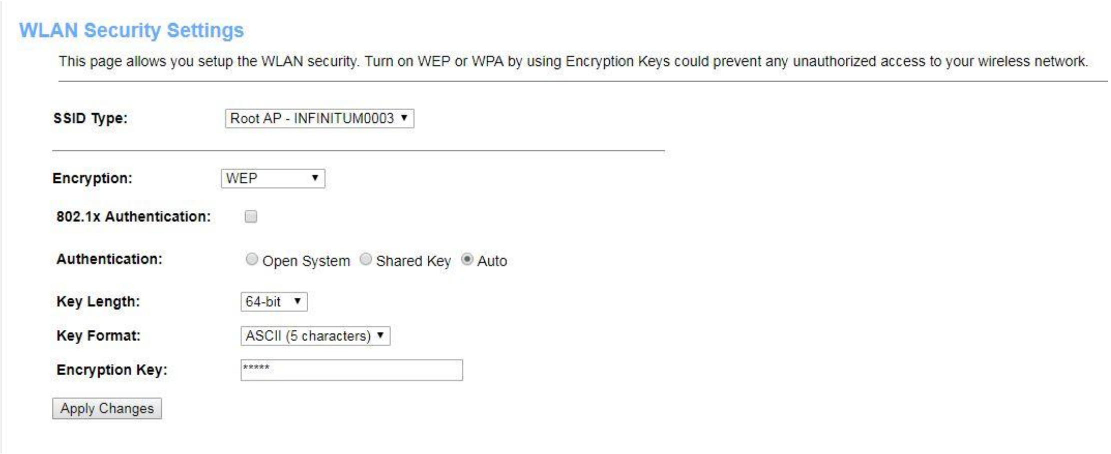
SSID Type:	Root AP - INFINITUM0003 ▾
Encryption:	WPA2 Mixed ▾
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	☑ TKIP ☑ AES
WPA2 Cipher Suite:	☑ TKIP ☑ AES
Group Key Update Timer:	86400
Pre-Shared Key Format:	Passphrase ▾
Pre-Shared Key:	•••••••••• □ Show Password

Here you can choose the encryption method to prevent any unauthorized access to your wireless network.

There are three most commonly used encryption method (a total of six encryption support), including the WEP encryption, WPA-Personal, WPA2-Personal, etc.

(1) WEP

If the encryption is WEP, you should click “Set WEP key” button to enter the WEP key setup page.



WLAN Security Settings

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

SSID Type: Root AP - INFINITUM0003

Encryption: WEP

802.1x Authentication: □

Authentication: ○ Open System ○ Shared Key ● Auto

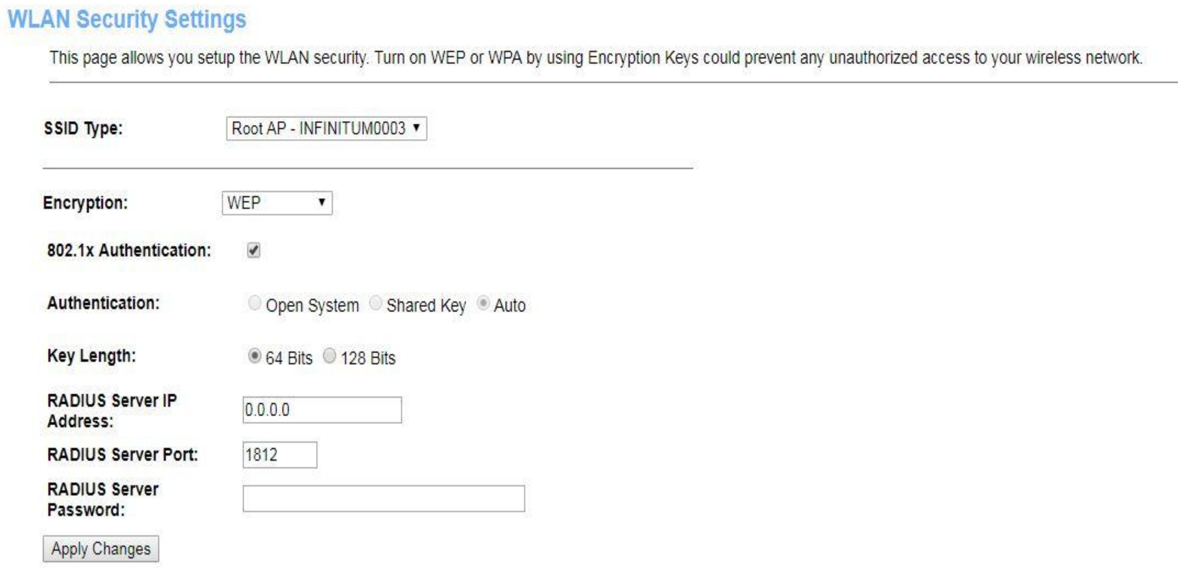
Key Length: 64-bit

Key Format: ASCII (5 characters)

Encryption Key: *****

- Key Length: the length of the WEP key, it can be 64 bits or 128 bits
- Key Format: the format of the WEP key, it can be ASCII or hex
- Encryption key: the WEP key
- Default Tx Key: you can select one key from the follow 4 Encryption key as the current key

If you want to use 802.1x authentication, you can enable this option on the checkbox. You should set the port, IP address and password for the authentication radius server.



WLAN Security Settings

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

SSID Type: Root AP - INFINITUM0003

Encryption: WEP

802.1x Authentication: ☑

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: ● 64 Bits ○ 128 Bits

RADIUS Server IP Address: 0.0.0.0

RADIUS Server Port: 1812

RADIUS Server Password:

(2) WPA/WPA2

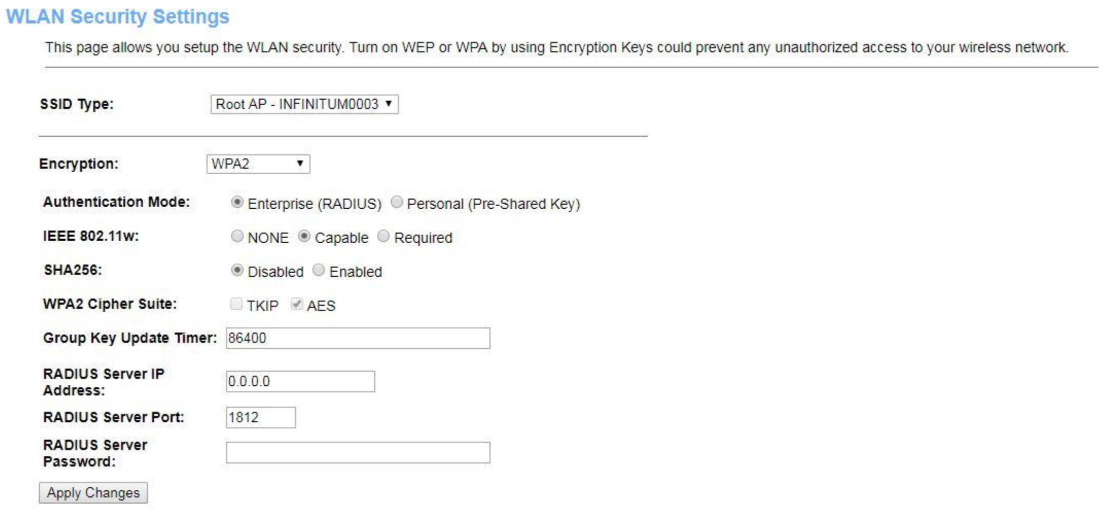
There are two WPA encryption rules: AES and TKIP, you can select anyone as the encryption. There are also two WPA Authentication mode, it can be either Enterprise (RADUIS) or Personal (Pre-Shared Key).

The most commonly used authentication mode is Pre-Shared Key. You should set the Pre-Shared Key Format and Pre-Shared Key value.

- Pre-Shared Key Format: it can be either Passphrase or Hex (64 characters)

- ➢ Pre-Shared Key: the value of the Pre-Shared Key

If the authentication mode is RADIUS, you should set the port, IP address and password for the authentication radius server.



WLAN Security Settings

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

SSID Type: Root AP - INFINITUM0003 ▾

Encryption: WPA2 ▾

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

IEEE 802.11w: ○ NONE ● Capable ○ Required

SHA256: ● Disabled ○ Enabled

WPA2 Cipher Suite: □ TKIP ☑ AES

Group Key Update Timer: 86400

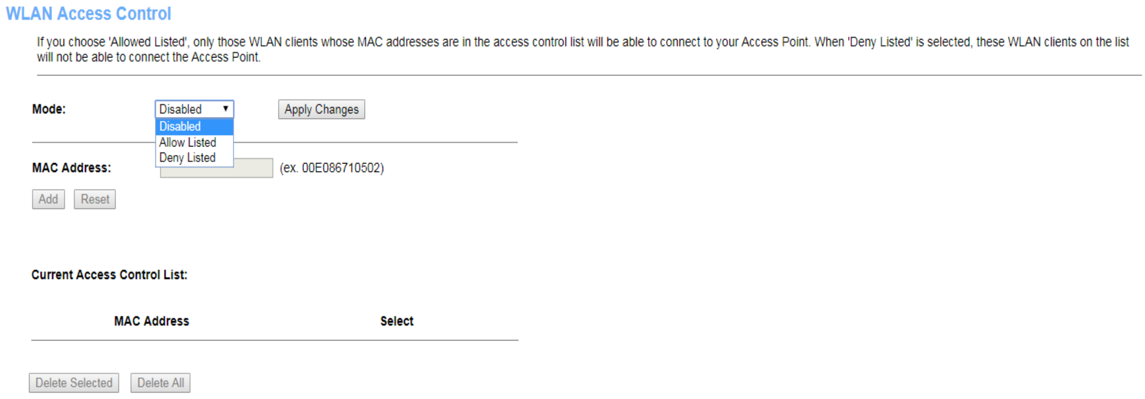
RADIUS Server IP Address: 0.0.0.0

RADIUS Server Port: 1812

RADIUS Server Password:

4.2.4 Access Control

Wireless access control function is used to allow or prohibit the client access to the wireless network by MAC address.



WLAN Access Control

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

Mode: Disabled ▾

MAC Address: (ex. 00E086710502)

Current Access Control List:

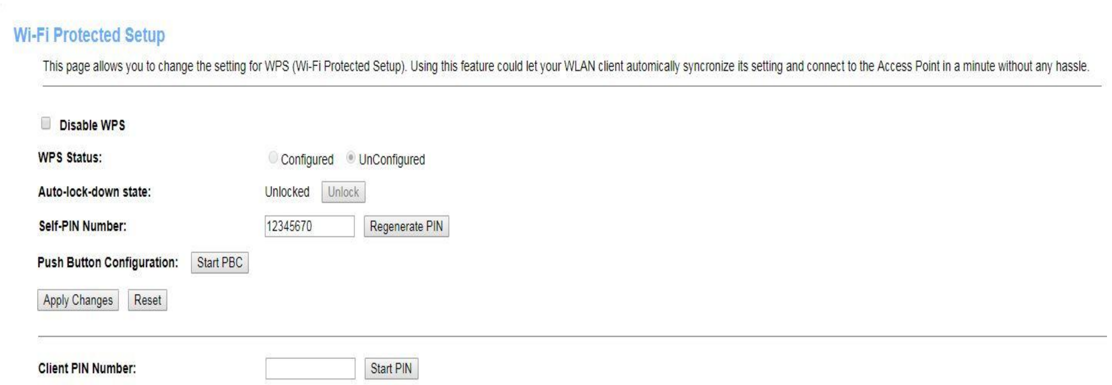
MAC Address	Select

- ➢ Wireless Access Control Mode: it can be “disable”, “Allow Listed” or “Deny Listed”. If the mode is “disable”, it means the wireless access control function is closed; if the mode is “Allow Listed”, only the client on the list will be able to connect to you access point; if the mode is “Deny Listed”, these wireless clients on the list will not be able to connect to you access point.
- ➢ MAC Address: the MAC address of the client you want to allow or prohibit

- Current Access Control List: it show the MAC address table you configured, you can delete it as you need.

4.2.5 WPS

Go to Local Network ->WLAN->WPS page, you can change the setting for WPS (Wi-Fi Protected Setup).



Wi-Fi Protected Setup

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

□ Disable WPS

WPS Status: ○ Configured ● UnConfigured

Auto-lock-down state: Unlocked Unlock

Self-PIN Number: 12345670 Regenerate PIN

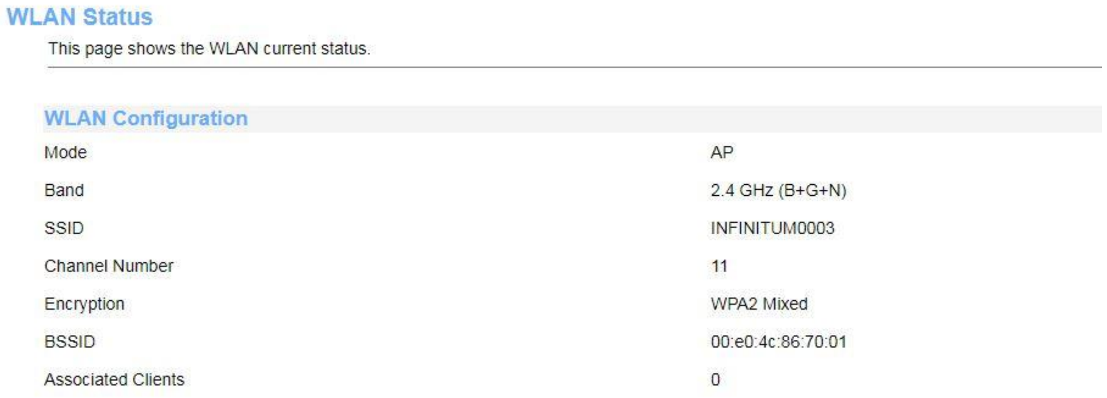
Push Button Configuration: Start PBC

Apply Changes Reset

Client PIN Number: Start PIN

4.2.6 Status

shows the WLAN current status.



WLAN Status

This page shows the WLAN current status.

WLAN Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	INFINITUM0003
Channel Number	11
Encryption	WPA2 Mixed
BSSID	00:e0:4c:86:70:01
Associated Clients	0

5. Internet

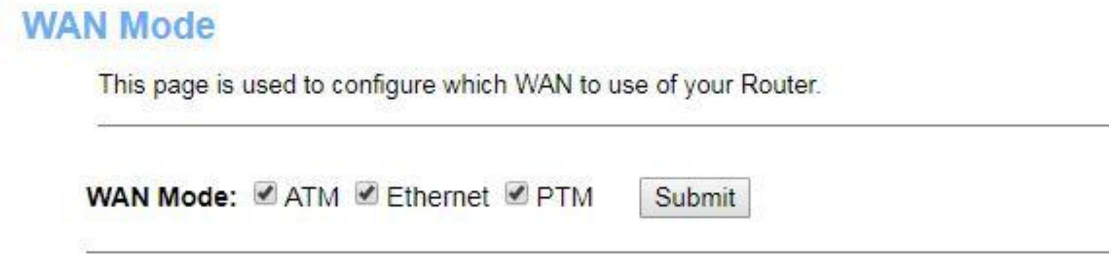
To enjoy the surfing, we should have the most basic configuration of the router at first. In this chapter, you can set the basic network parameters required to access the Internet.

The router supports the following three common means to access:

- Dynamic IP access: ISP (such as China Telecom) assigns IP address to users via DHCP.
- Static IP access: ISP provides a static IP address to users.
- PPPoE dial-up access(Ethernet): use PPPoE virtual dial-up connection to the Internet.

5.1 WAN Mode

Go to Internet ->WAN Mode page, you can configure the parameters for the channel modes of your Router.



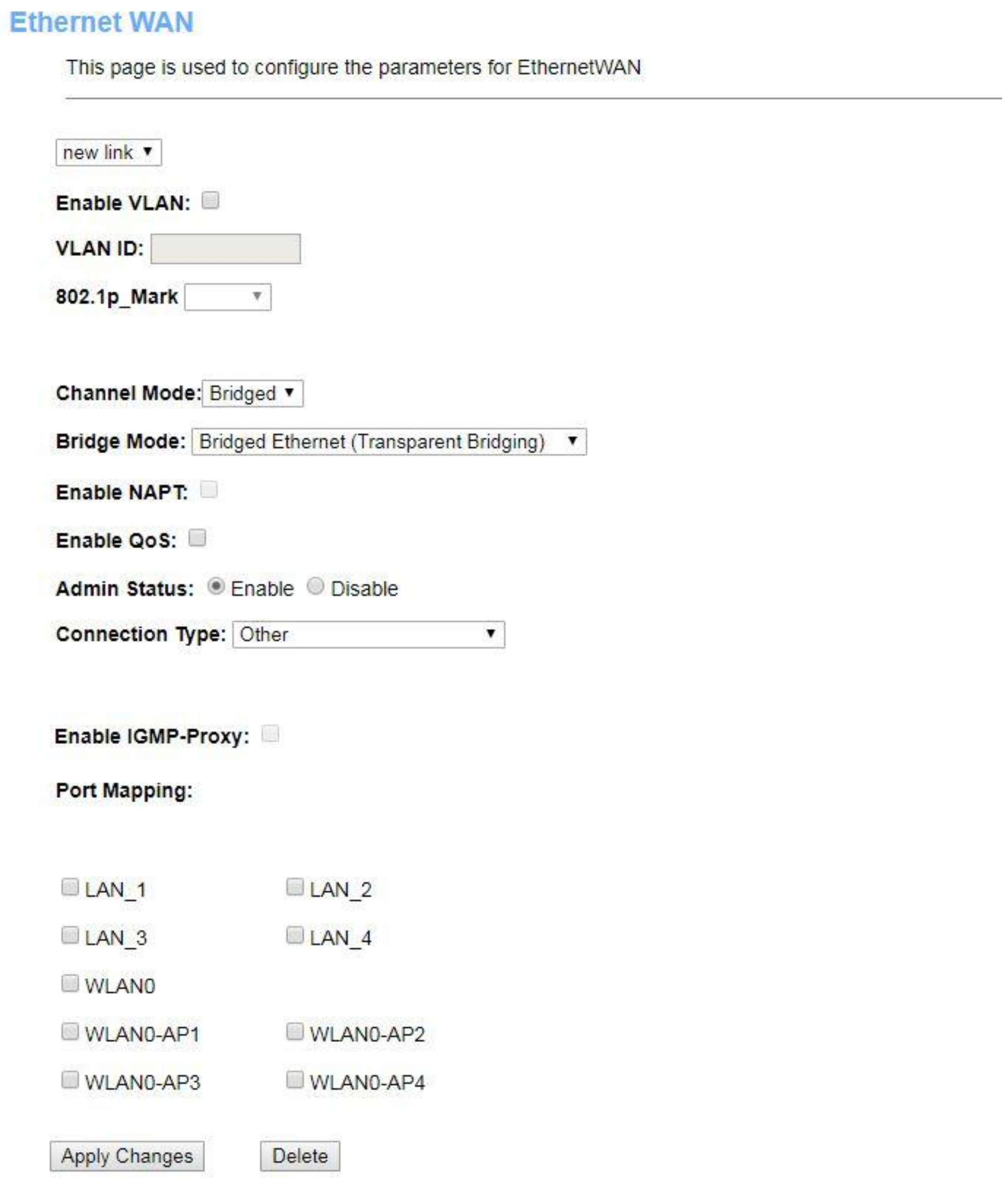
WAN Mode

This page is used to configure which WAN to use of your Router.

WAN Mode: ☑ ATM ☑ Ethernet ☑ PTM

5.2 Ethernet WAN

Go to Internet -> Ethernet Mode page, you can configure the parameters for the channel modes of your Router.



Ethernet WAN

This page is used to configure the parameters for EthernetWAN

new link ▾

Enable VLAN: □

VLAN ID:

802.1p_Mark ▾

Channel Mode: Bridged ▾

Bridge Mode: Bridged Ethernet (Transparent Bridging) ▾

Enable NAPT: □

Enable QoS: □

Admin Status: ● Enable ○ Disable

Connection Type: Other ▾

Enable IGMP-Proxy: □

Port Mapping:

□ LAN_1 □ LAN_2

□ LAN_3 □ LAN_4

□ WLAN0

□ WLAN0-AP1 □ WLAN0-AP2

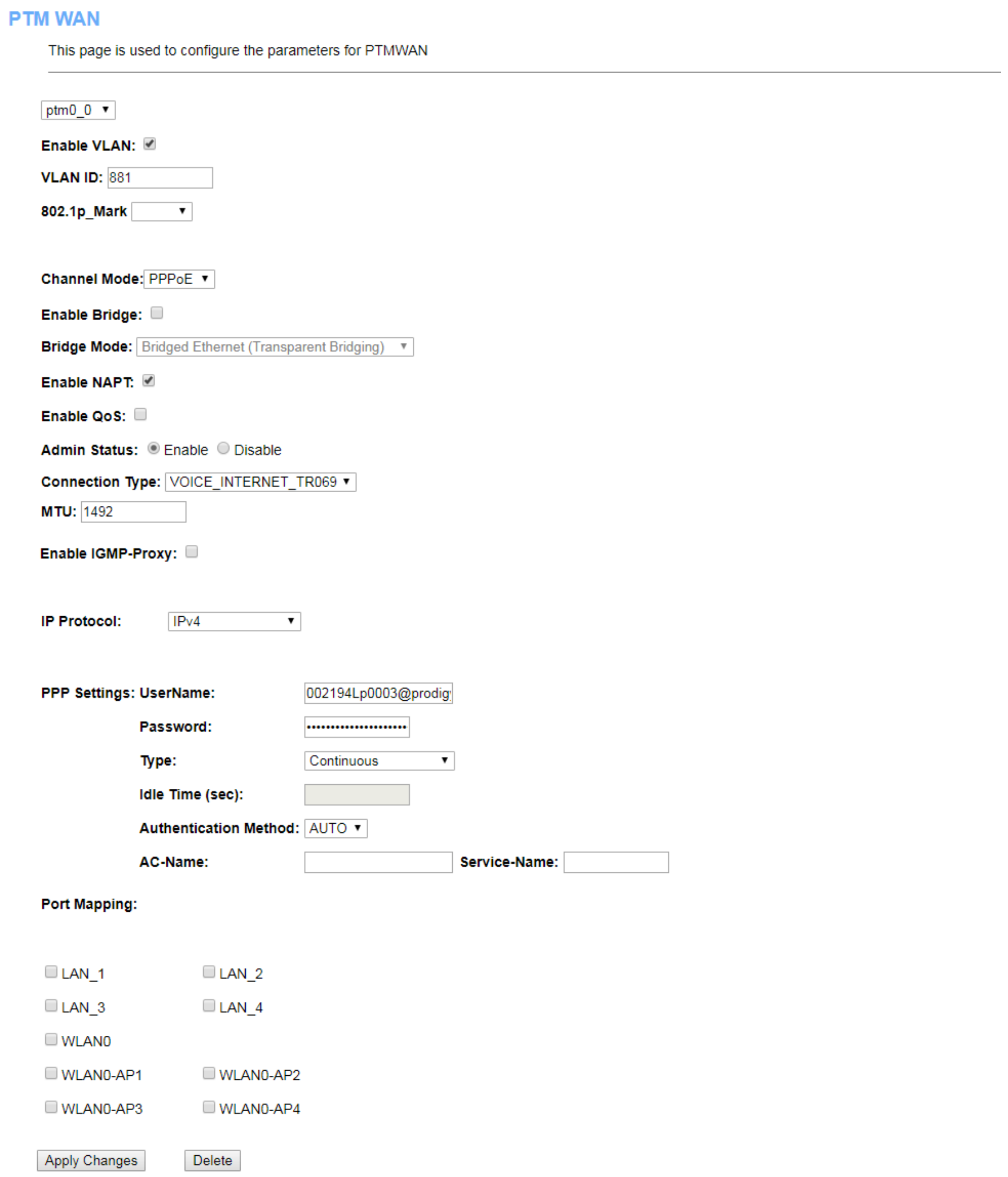
□ WLAN0-AP3 □ WLAN0-AP4

There are many parameters on the channel configuration:

- Channel mode
  operation of the Ethernet channel, it can be Bridge, IPOE, PPPoE
- Enable NAPT
  Enable or disable the NATP function of the Ethernet channel
- Enable IGMP-Proxy
  Enable or disable the IGMP function of the Ethernet channel
- Connection Type
  The type of other,INTERNET,TR069 and so on.

5.3 PTM WAN

Go to Internet ->PTM WAN page, you can configure the parameters for the channel modes of your Router



PTM WAN

This page is used to configure the parameters for PTMWAN

ptm0_0 ▾

Enable VLAN: ☑

VLAN ID: 881

802.1p_Mark ▾

Channel Mode: PPPoE ▾

Enable Bridge: □

Bridge Mode: Bridged Ethernet (Transparent Bridging) ▾

Enable NAPT: ☑

Enable QoS: □

Admin Status: ● Enable ○ Disable

Connection Type: VOICE_INTERNET_TR069 ▾

MTU: 1492

Enable IGMP-Proxy: □

IP Protocol: IPv4 ▾

PPP Settings: UserName: 002194Lp0003@prodig

Password: ••••••••••••••••••••

Type: Continuous ▾

Idle Time (sec):

Authentication Method: AUTO ▾

AC-Name: Service-Name:

Port Mapping:

□ LAN_1 □ LAN_2

□ LAN_3 □ LAN_4

□ WLAN0

□ WLAN0-AP1 □ WLAN0-AP2

□ WLAN0-AP3 □ WLAN0-AP4

There are many parameters on the channel configuration:

- Channel mode

  operation of the Ethernet channel, it can be Bridge, PPPoE,IPOE

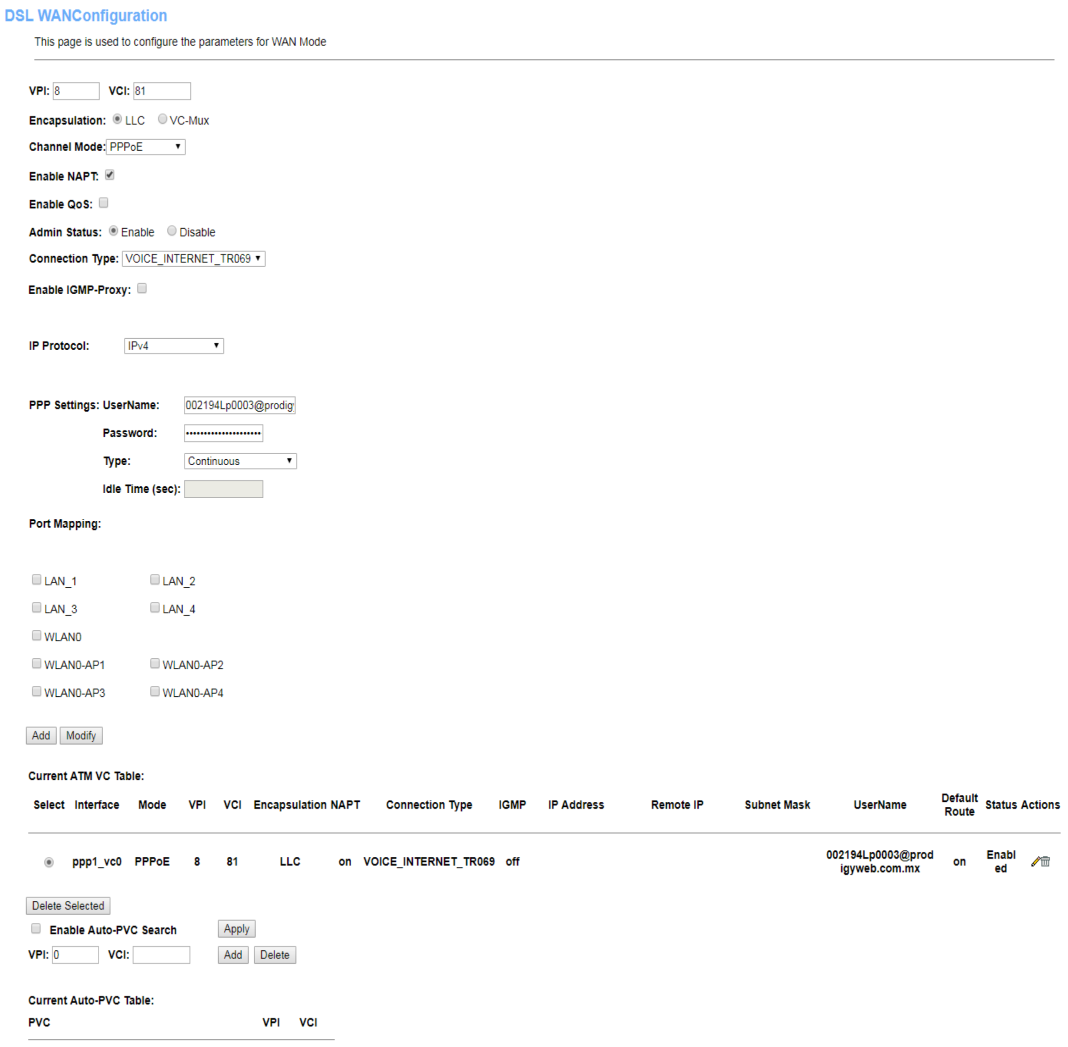
- Enable NAPT

  Enable or disable the NATP function of the Ethernet channel

- Enable IGMP-Proxy
  Enable or disable the IGMP function of the Ethernet channel
- Connection Type
  The type of other,INTERNET,TR069 and so on.

5.4 ATM WAN

Go to Internet ->ATM WAN page, you can configure the parameters for the channel modes of your Router



DSL WANConfiguration

This page is used to configure the parameters for WAN Mode

VPI: 8 VCI: 81

Encapsulation: ● LLC ○ VC-Mux

Channel Mode: PPPoE

Enable NAPT: ☑

Enable QoS: □

Admin Status: ● Enable ○ Disable

Connection Type: VOICE_INTERNET_TR069

Enable IGMP-Proxy: □

IP Protocol: IPv4

PPP Settings: UserName: 002194Lp0003@prodig

Password: ••••••••••••••••••••

Type: Continuous

Idle Time (sec):

Port Mapping:

□ LAN_1 □ LAN_2

□ LAN_3 □ LAN_4

□ WLAN0

□ WLAN0-AP1 □ WLAN0-AP2

□ WLAN0-AP3 □ WLAN0-AP4

Current ATM VC Table:

Select	Interface	Mode	VPI	VCI	Encapsulation	NAPT	Connection Type	IGMP	IP Address	Remote IP	Subnet Mask	UserName	Default Route	Status	Actions
●	ppp1_vc0	PPPoE	8	81	LLC	on	VOICE_INTERNET_TR069	off				002194Lp0003@prodigyweb.com.mx	on	Enabled	

□ Enable Auto-PVC Search

VPI: 0 VCI:

Current Auto-PVC Table:

PVC	VPI	VCI

There are many parameters on the channel configuration:

- VPI,VCI
  ISP provides
- Channel mode
  operation of the Ethernet channel, it can be Bridge, PPPoE,IPOE
- Enable NAPT

Enable or disable the NATP function of the Ethernet channel

- Enable IGMP-proxy

  Enable or disable the IGMP function of the Ethernet channel

- User name

  ISP provides

- Password

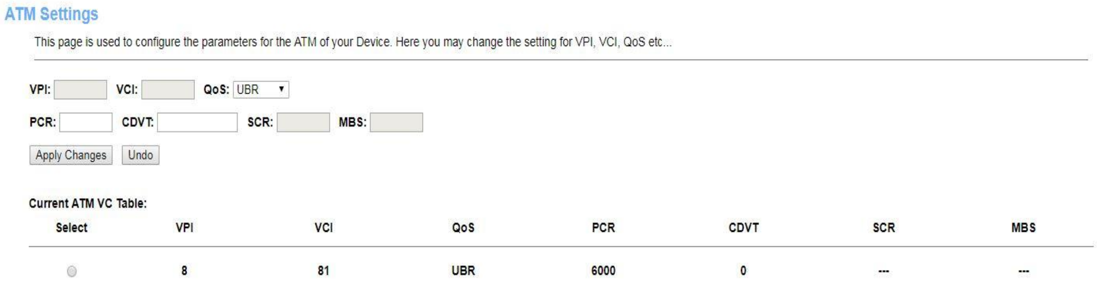
  ISP provides

- Connection Type

  The type of other,INTERNET,TR069 and so on.

5.5 ATM Settings

Go to Internet -->ATM Setting page, you can configure the parameter for the ATM of your Router.



ATM Settings

This page is used to configure the parameters for the ATM of your Device. Here you may change the setting for VPI, VCI, QoS etc...

VPI: VCI: QoS: UBR

PCR: CDVT: SCR: MBS:

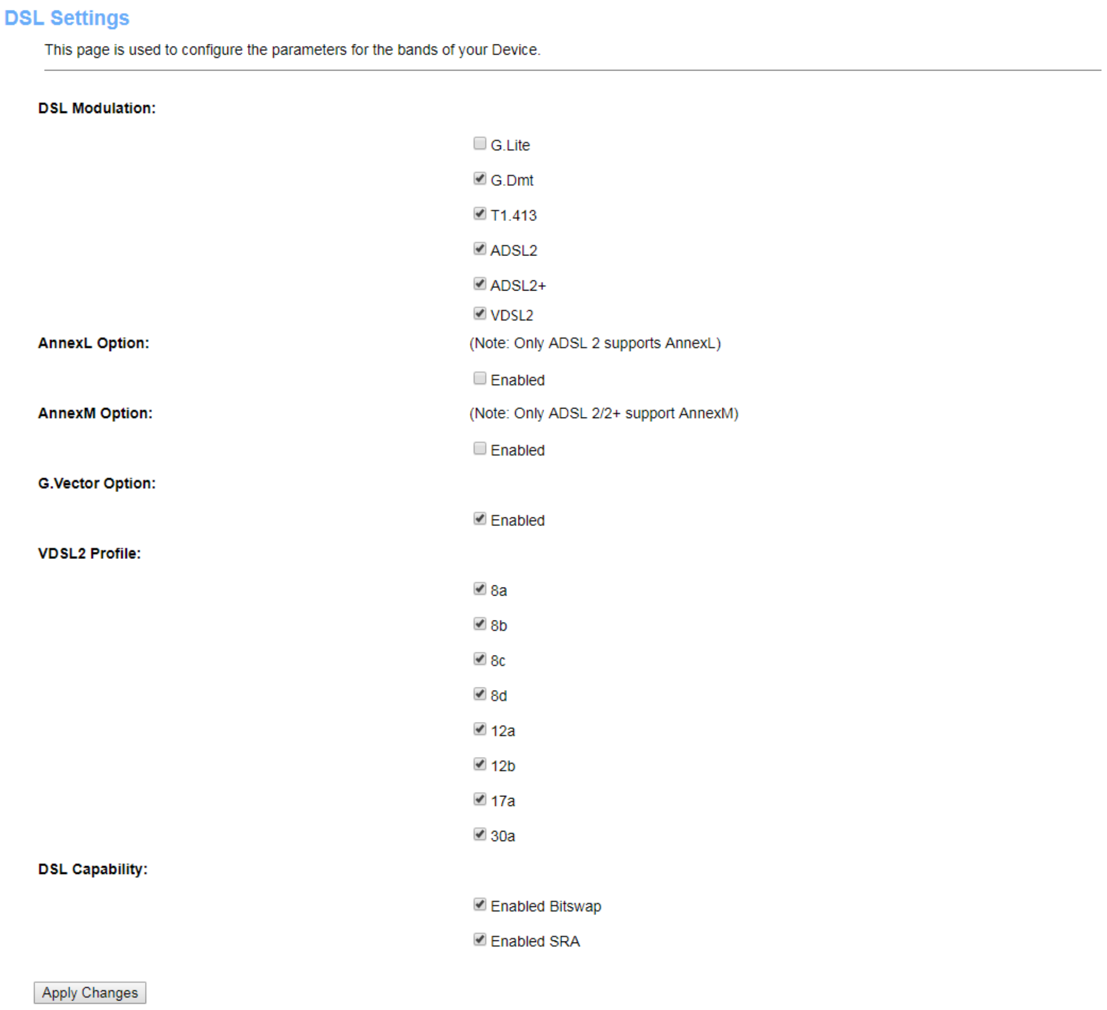
Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	8	81	UBR	6000	0	---	---

You can change the settings for QoS, PCR, CDVT, SCR and MBS.

5.6 DSL Settings

Go to Internet -> DSL Settings page, you can configure which DSL modulation of your modem will support.


DSL Settings

This page is used to configure the parameters for the bands of your Device.

DSL Modulation:

☐ G.Lite

☑ G.Dmt

☑ T1.413

☑ ADSL2

☑ ADSL2+

☑ VDSL2

AnnexL Option: (Note: Only ADSL 2 supports AnnexL)

☐ Enabled

AnnexM Option: (Note: Only ADSL 2/2+ support AnnexM)

☐ Enabled

G.Vector Option:

☑ Enabled

VDSL2 Profile:

☑ 8a

☑ 8b

☑ 8c

☑ 8d

☑ 12a

☑ 12b

☑ 17a

☑ 30a

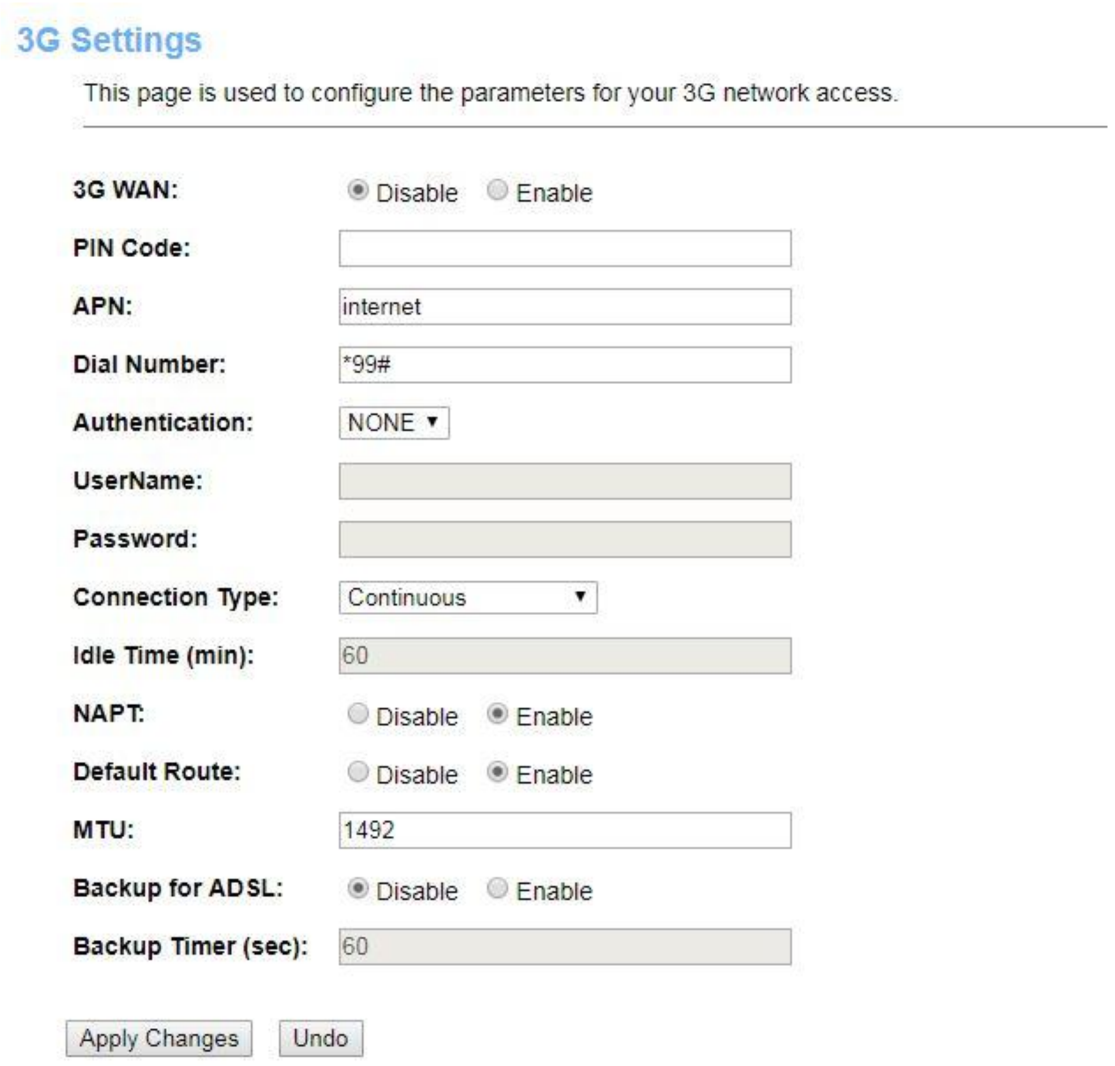
DSL Capability:

☑ Enabled Bitswap

☑ Enabled SRA

5.7 3G Setting

Go to Internet -> 3G Settings page, you can configure the parameter for the ATM of your Router.



3G Settings

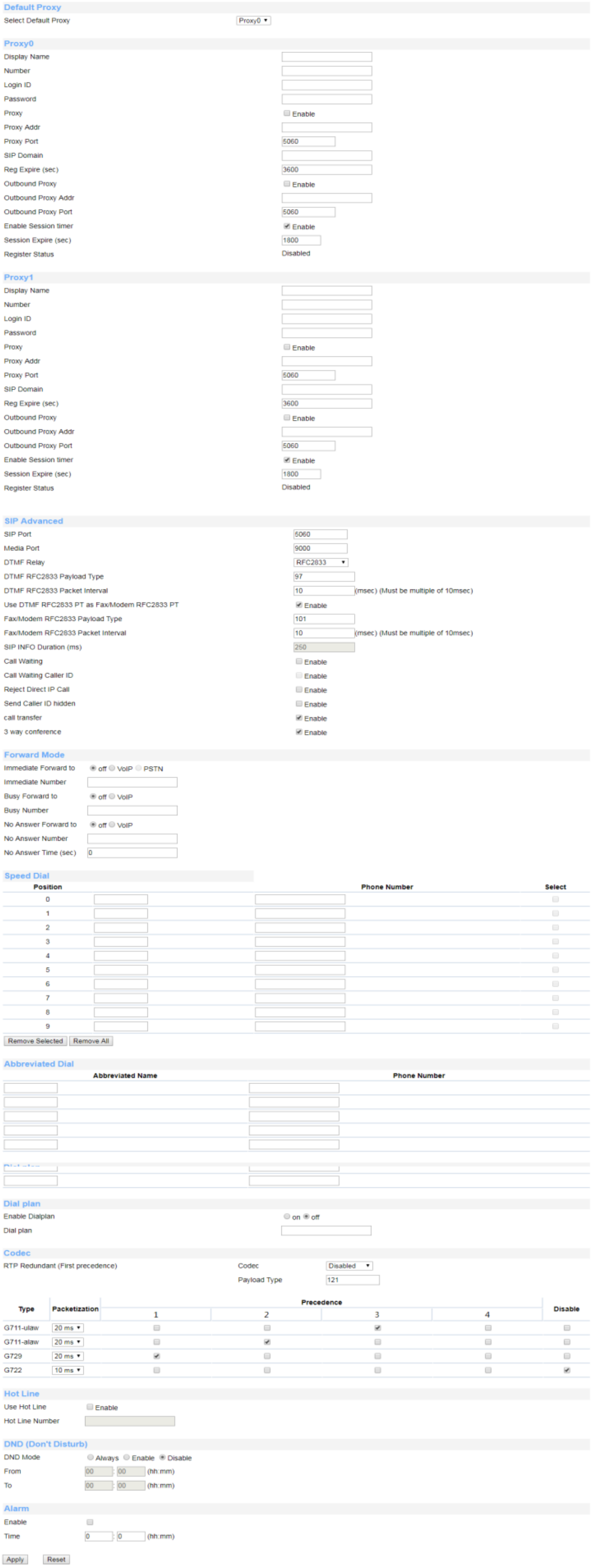
This page is used to configure the parameters for your 3G network access.

3G WAN:	● Disable ○ Enable
PIN Code:	
APN:	internet
Dial Number:	*99#
Authentication:	NONE ▾
UserName:	
Password:	
Connection Type:	Continuous ▾
Idle Time (min):	60
NAPT:	○ Disable ● Enable
Default Route:	○ Disable ● Enable
MTU:	1492
Backup for ADSL:	● Disable ○ Enable
Backup Timer (sec):	60

6. VoIP

6.1 Port 1

VoIP is real-time transmit the Voice in IP network, Go to VoIP ->Port 1 page ,This page let user to config Port 1



Default Proxy

Select Default Proxy	Proxy0 ▾

Proxy0

Display Name	
Number	
Login ID	
Password	
Proxy	☐ Enable
Proxy Addr	
Proxy Port	5060
SIP Domain	
Reg Expire (sec)	3600
Outbound Proxy	☐ Enable
Outbound Proxy Addr	
Outbound Proxy Port	5060
Enable Session timer	☑ Enable
Session Expire (sec)	1800
Register Status	Disabled

Proxy1

Display Name	
Number	
Login ID	
Password	
Proxy	☐ Enable
Proxy Addr	
Proxy Port	5060
SIP Domain	
Reg Expire (sec)	3600
Outbound Proxy	☐ Enable
Outbound Proxy Addr	
Outbound Proxy Port	5060
Enable Session timer	☑ Enable
Session Expire (sec)	1800
Register Status	Disabled

SIP Advanced

SIP Port	5060
Media Port	9000
DTMF Relay	RFC2833 ▾
DTMF RFC2833 Payload Type	97
DTMF RFC2833 Packet Interval	10 (msec) (Must be multiple of 10msec)
Use DTMF RFC2833 PT as Fax/Modem RFC2833 PT	☑ Enable
Fax/Modem RFC2833 Payload Type	101
Fax/Modem RFC2833 Packet Interval	10 (msec) (Must be multiple of 10msec)
SIP INFO Duration (ms)	250
Call Waiting	☐ Enable
Call Waiting Caller ID	☐ Enable
Reject Direct IP Call	☐ Enable
Send Caller ID hidden	☐ Enable
call transfer	☑ Enable
3 way conference	☑ Enable

Forward Mode

Immediate Forward to	● off ○ VoIP ○ PSTN
Immediate Number	
Busy Forward to	● off ○ VoIP
Busy Number	
No Answer Forward to	● off ○ VoIP
No Answer Number	
No Answer Time (sec)	0

Speed Dial

Position		Phone Number	Select
0			☐
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐

Remove Selected | Remove All

Abbreviated Dial

Abbreviated Name	Phone Number

Dial plan

Enable Dialplan	○ on ● off
Dial plan	

Codec

RTP Redundant (First precedence)	Codec	Disabled ▾
	Payload Type	121

Type	Packetization	Precedence				Disable
		1	2	3	4	
G711-ulaw	20 ms ▾	☐	☐	☑	☐	☐
G711-alaw	20 ms ▾	☐	☑	☐	☐	☐
G729	20 ms ▾	☑	☐	☐	☐	☐
G722	10 ms ▾	☐	☐	☐	☐	☑

Hot Line

Use Hot Line	☐ Enable
Hot Line Number	

DND (Don't Disturb)

DND Mode	○ Always ○ Enable ● Disable
From	00 : 00 (hh:mm)
To	00 : 00 (hh:mm)

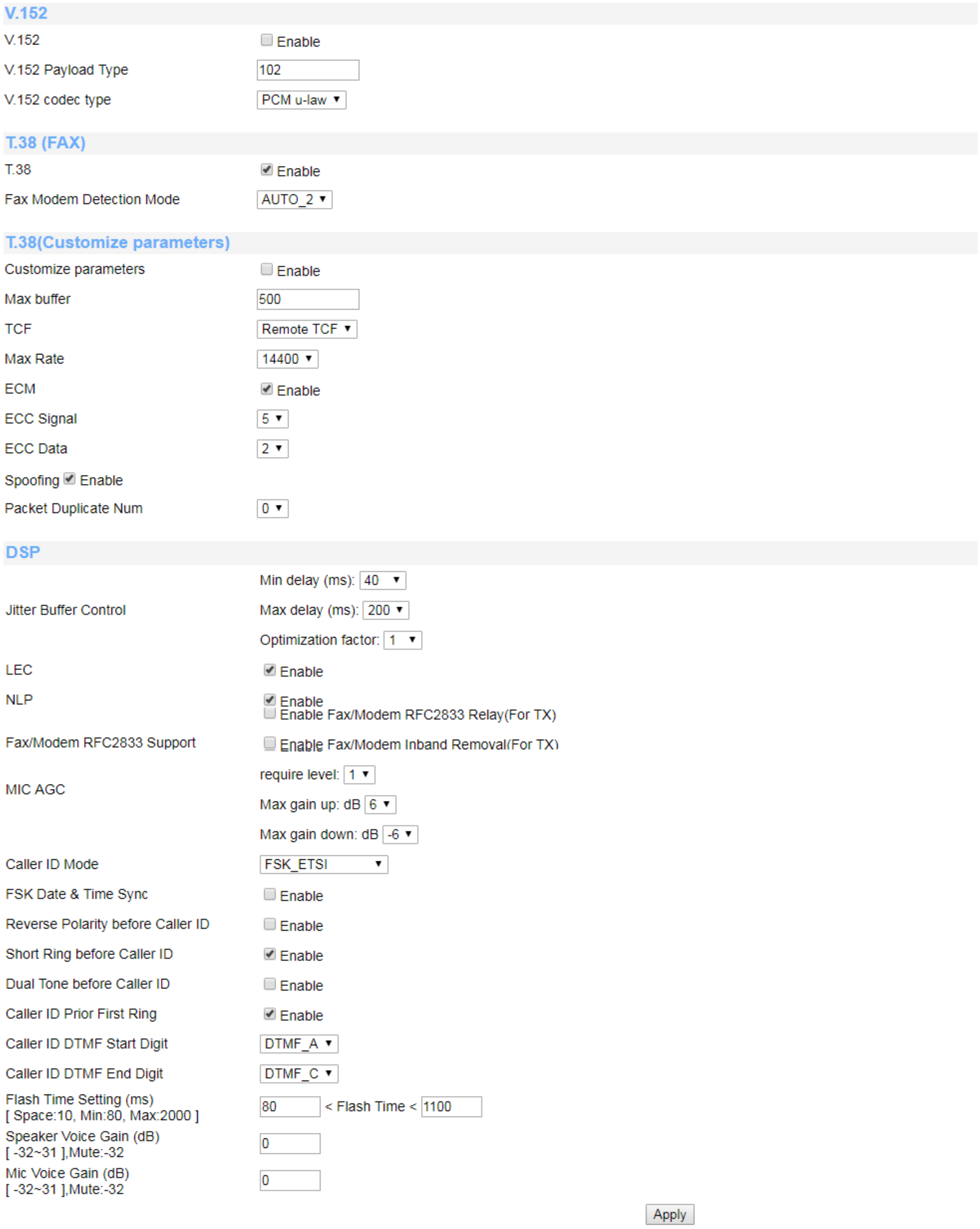
Alarm

Enable	☐
Time	0 : 0 (hh:mm)

Apply | Reset

6.2 Advanced

Go to VoIP ->Advanced page ,This page let user to config Advanced VoIP.



V.152

V.152	□ Enable
V.152 Payload Type	102
V.152 codec type	PCM u-law ▾

T.38 (FAX)

T.38	☑ Enable
Fax Modem Detection Mode	AUTO_2 ▾

T.38(Customize parameters)

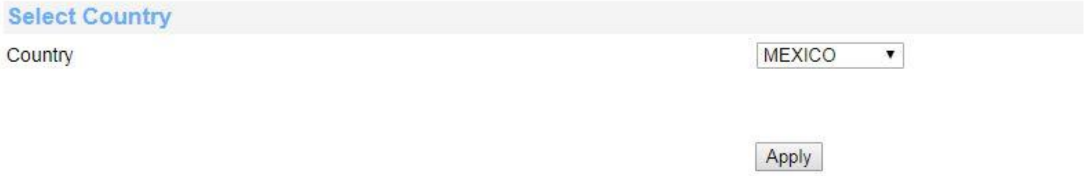
Customize parameters	□ Enable
Max buffer	500
TCF	Remote TCF ▾
Max Rate	14400 ▾
ECM	☑ Enable
ECC Signal	5 ▾
ECC Data	2 ▾
Spoofing ☑ Enable	
Packet Duplicate Num	0 ▾

DSP

Jitter Buffer Control	Min delay (ms): 40 ▾ Max delay (ms): 200 ▾ Optimization factor: 1 ▾
LEC	☑ Enable
NLP	☑ Enable
Fax/Modem RFC2833 Support	□ Enable Fax/Modem RFC2833 Relay(For TX) □ Enable Fax/Modem Inband Removal(For TX)
MIC AGC	require level: 1 ▾ Max gain up: dB 6 ▾ Max gain down: dB -6 ▾
Caller ID Mode	FSK_ETSI ▾
FSK Date & Time Sync	□ Enable
Reverse Polarity before Caller ID	□ Enable
Short Ring before Caller ID	☑ Enable
Dual Tone before Caller ID	□ Enable
Caller ID Prior First Ring	☑ Enable
Caller ID DTMF Start Digit	DTMF_A ▾
Caller ID DTMF End Digit	DTMF_C ▾
Flash Time Setting (ms) [Space:10, Min:80, Max:2000]	80 < Flash Time < 1100
Speaker Voice Gain (dB) [-32~31],Mute:-32	0
Mic Voice Gain (dB) [-32~31],Mute:-32	0

6.3 Tone

Go to VoIP ->Tone page .

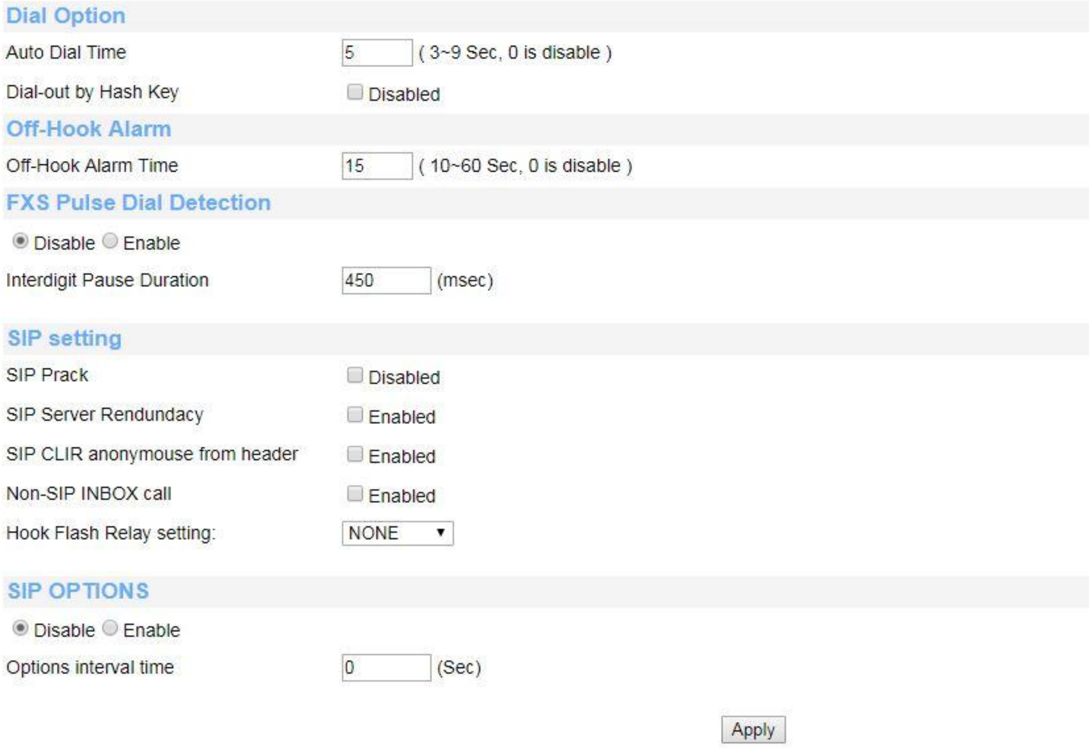


Select Country

Country	MEXICO ▾

6.4 Others

Go to VoIP ->Others page .



Dial Option

Auto Dial Time	5 (3~9 Sec, 0 is disable)
Dial-out by Hash Key	□ Disabled

Off-Hook Alarm

Off-Hook Alarm Time	15 (10~60 Sec, 0 is disable)

FXS Pulse Dial Detection

● Disable ○ Enable

Interdigit Pause Duration	450 (msec)

SIP setting

SIP Prack	□ Disabled
SIP Server Rendundacy	□ Enabled
SIP CLIR anonymouse from header	□ Enabled
Non-SIP INBOX call	□ Enabled
Hook Flash Relay setting:	NONE ▾

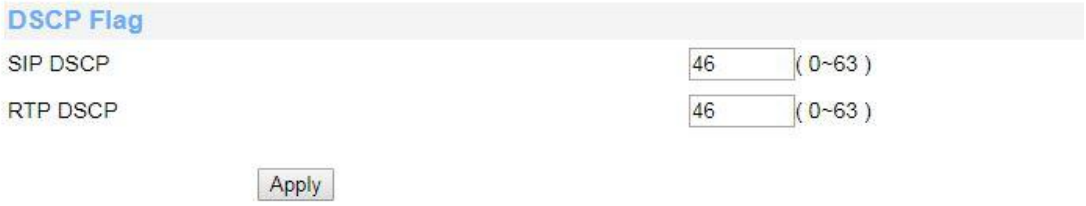
SIP OPTIONS

● Disable ○ Enable

Options interval time	0 (Sec)

6.5 Network

Go to VoIP ->Network page .

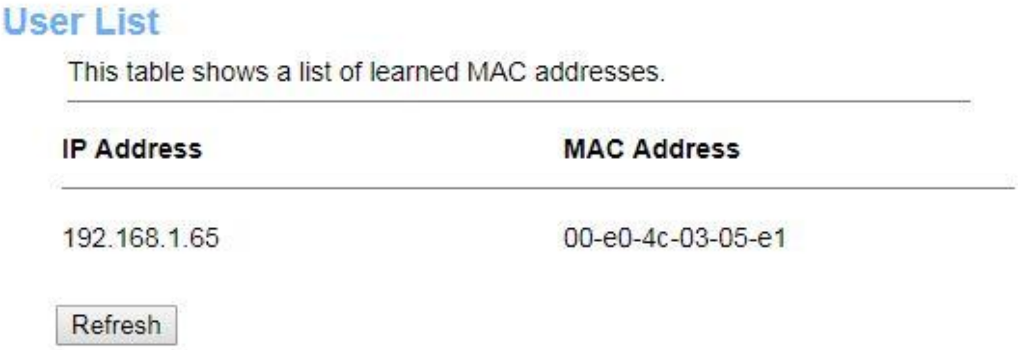

DSCP Flag

SIP DSCP	46	(0~63)
RTP DSCP	46	(0~63)

7. Advanced

7.1 ARP Table

This table shows a list of learned MAC addresses.

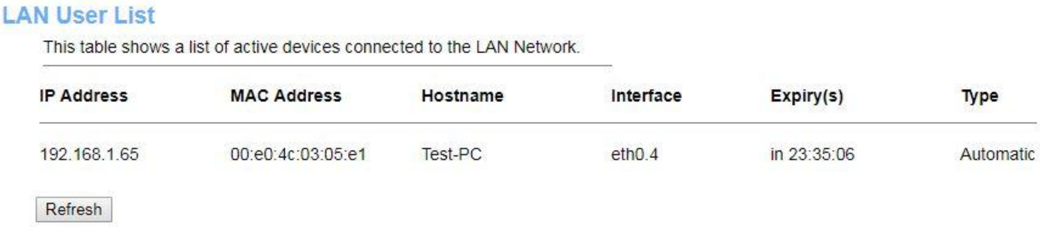

User List

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.65	00-e0-4c-03-05-e1

7.2 LAN Device Table

This table shows a list of active devices connected to the LAN Network.

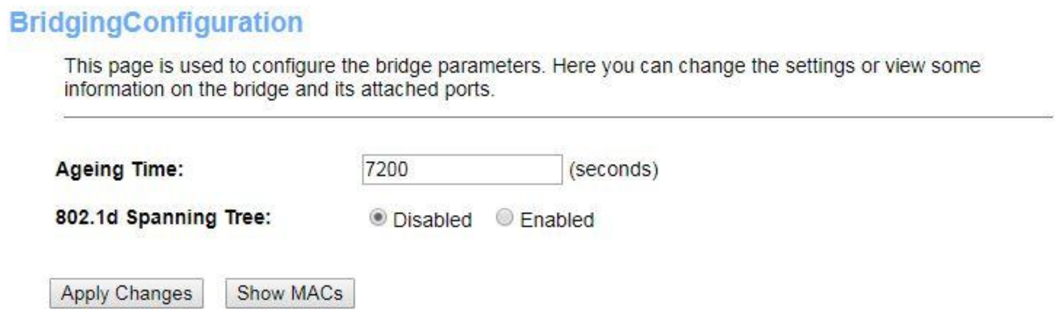

LAN User List

This table shows a list of active devices connected to the LAN Network.

IP Address	MAC Address	Hostname	Interface	Expiry(s)	Type
192.168.1.65	00:e0:4c:03:05:e1	Test-PC	eth0.4	in 23:35:06	Automatic

7.3 Bridging

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.



BridgingConfiguration

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.

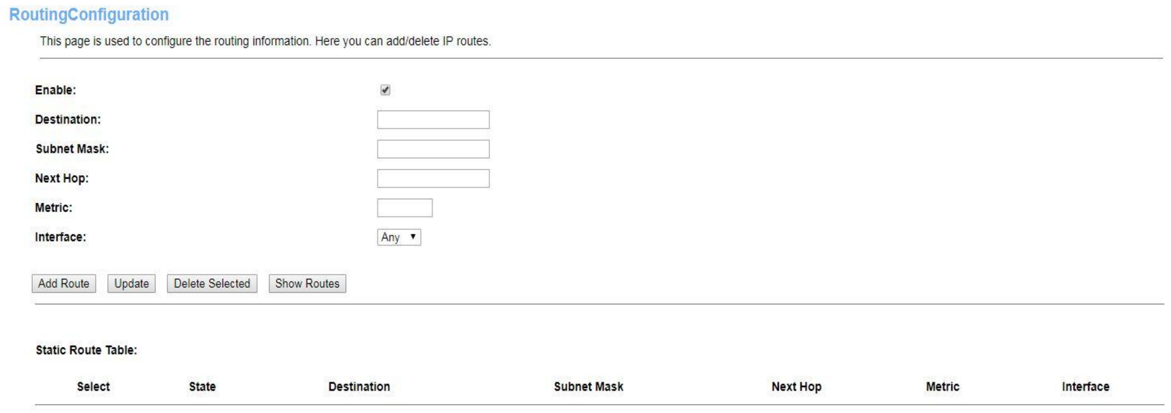
Ageing Time: 7200 (seconds)

802.1d Spanning Tree: ● Disabled ○ Enabled

7.4 Routing

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

Go to Advanced->Routeing page, you can configure the routing information. Here you can add or delete IP routes.



RoutingConfiguration

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

Enable: ☑

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface: Any

Static Route Table:

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface

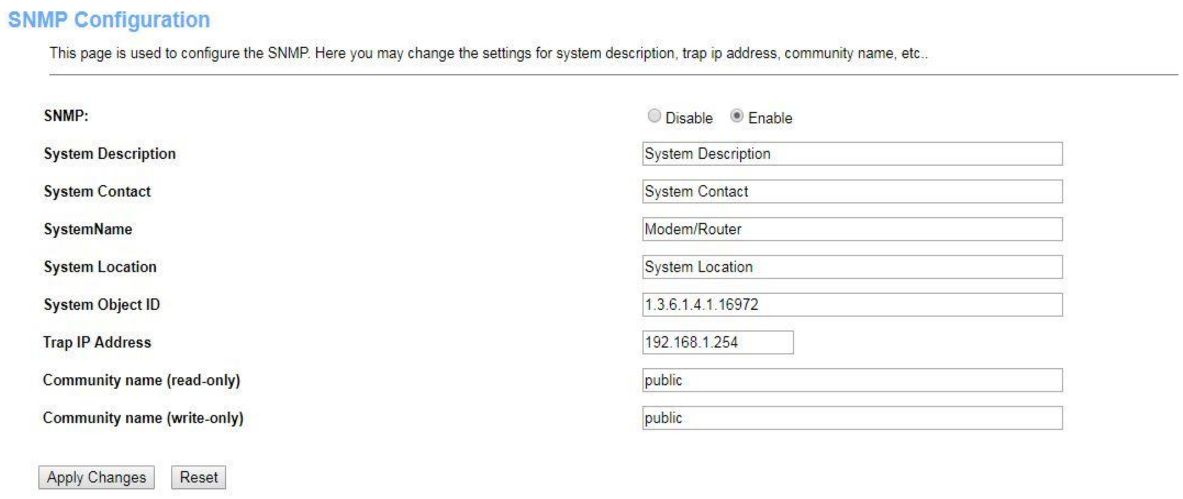
- ➢ Enable
  enable or disable the route entry you add
- ➢ Destination
  destination IP address. It can be a subnet IP or a host address. All zeros indicate that the route entry should be used for all destinations for which no other route is defined.
- ➢ Subnet Mask
  the network mask of the destination.
- ➢ Next Hop
  the IP address of the next hop through which traffic will forward the destination.

- Metric
  defines the number of hops between network nodes that data packets travel.
- Interface
  the WAN interface to which a static route is to be applied.

7.5 SNMP

Simple Network Management Protocol (SNMP) is a series of protocol and specification, they provide a kind of from the Internet to collect information about network management method in the system.SNMP also report to the network management workstation for device problems and provides a method.

Go to Advanced ->SNMP page, you can configure the SNMP Protocol.



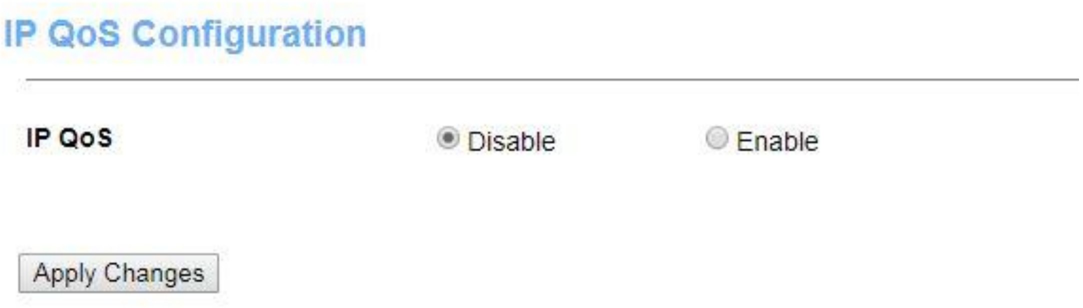
SNMP Configuration

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

SNMP:	○ Disable ● Enable
System Description	System Description
System Contact	System Contact
SystemName	Modem/Router
System Location	System Location
System Object ID	1.3.6.1.4.1.16972
Trap IP Address	192.168.1.254
Community name (read-only)	public
Community name (write-only)	public

7.6 IP QoS

7.6.1 Qos Poilcy

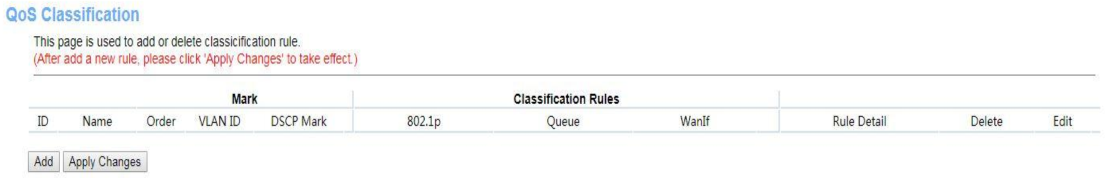


IP QoS Configuration

IP QoS ● Disable ○ Enable

7.6.2 Qos Classification

This page is used to add or delete classicification rule.



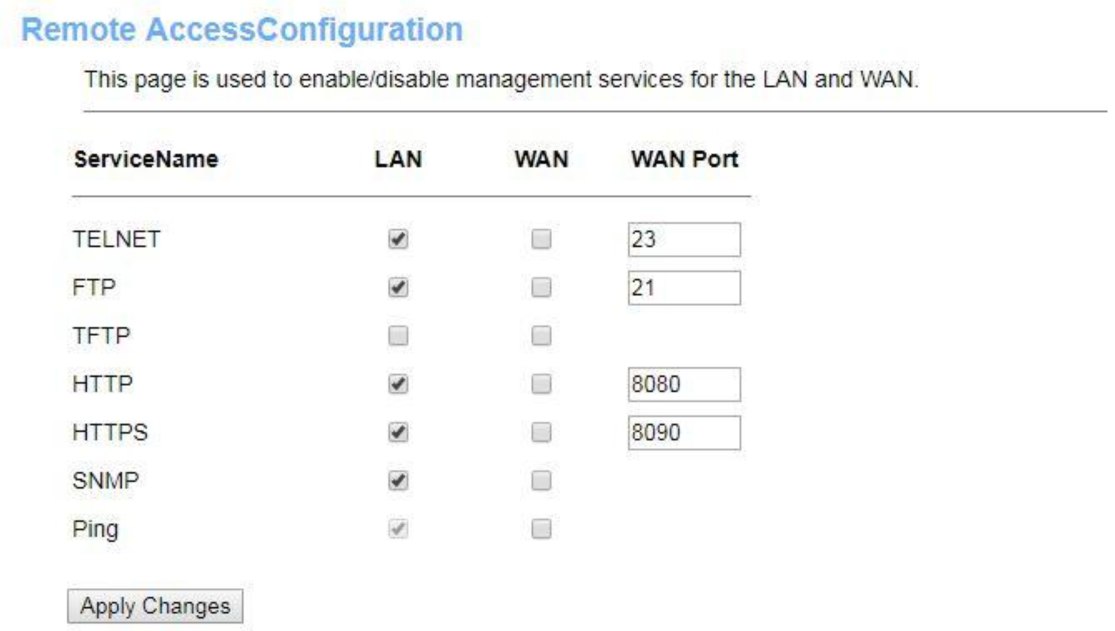
QoS Classification

This page is used to add or delete classicification rule.
(After add a new rule, please click 'Apply Changes' to take effect.)

		Mark			Classification Rules					
ID	Name	Order	VLAN ID	DSCP Mark	802.1p	Queue	WanIf	Rule Detail	Delete	Edit

7.7 Remote Access

This page is used to enable/disable management services for the LAN and WAN.



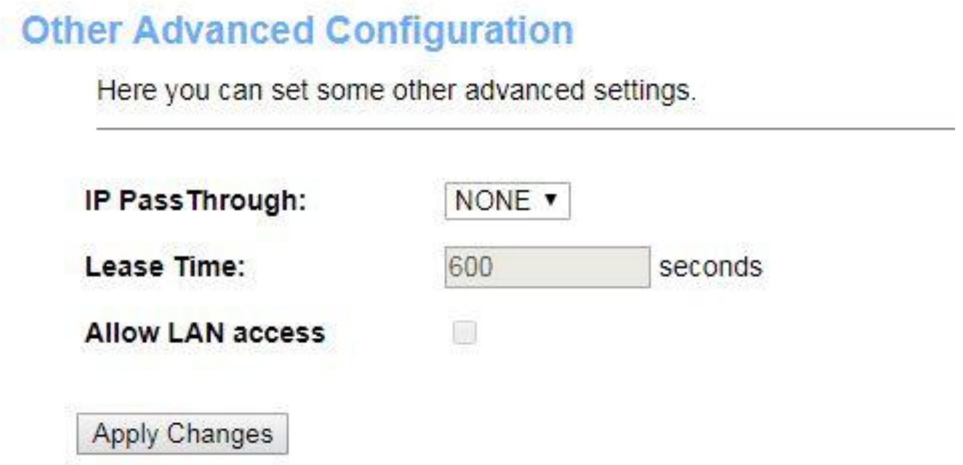
Remote AccessConfiguration

This page is used to enable/disable management services for the LAN and WAN.

ServiceName	LAN	WAN	WAN Port
TELNET	☑	□	23
FTP	☑	□	21
TFTP	□	□	
HTTP	☑	□	8080
HTTPS	☑	□	8090
SNMP	☑	□	
Ping	☑	□	

7.8 Others

Here you can set some other advanced settings.



Other Advanced Configuration

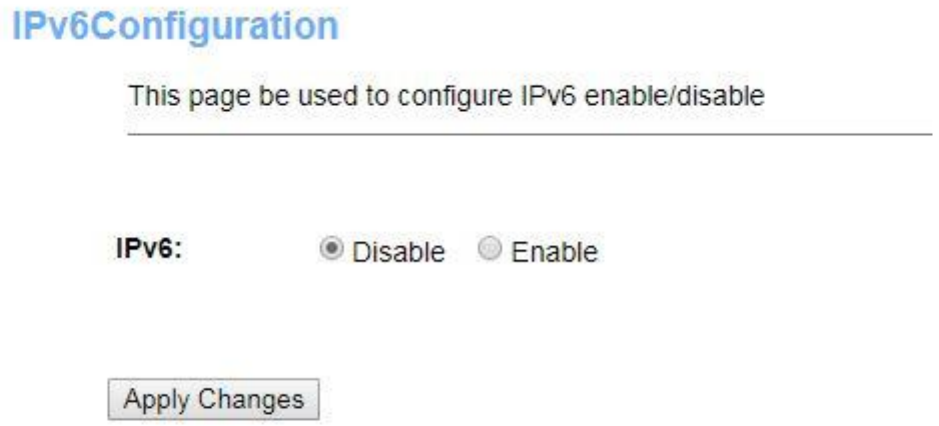
Here you can set some other advanced settings.

IP PassThrough:	NONE ▼
Lease Time:	600 seconds
Allow LAN access	□

7.9 IPv6

7.9.1 IPv6

This page be used to configure IPv6 enable/disable



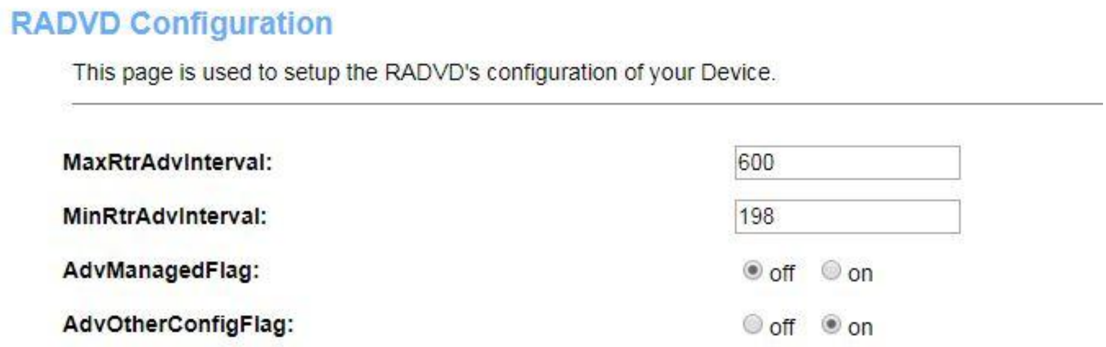
IPv6Configuration

This page be used to configure IPv6 enable/disable

IPv6: ● Disable ○ Enable

7.9.2 RADVD

This page is used to setup the RADVD's configuration of your Device.



RADVD Configuration

This page is used to setup the RADVD's configuration of your Device.

MaxRtrAdvInterval:	600
MinRtrAdvInterval:	198
AdvManagedFlag:	● off ○ on
AdvOtherConfigFlag:	○ off ● on

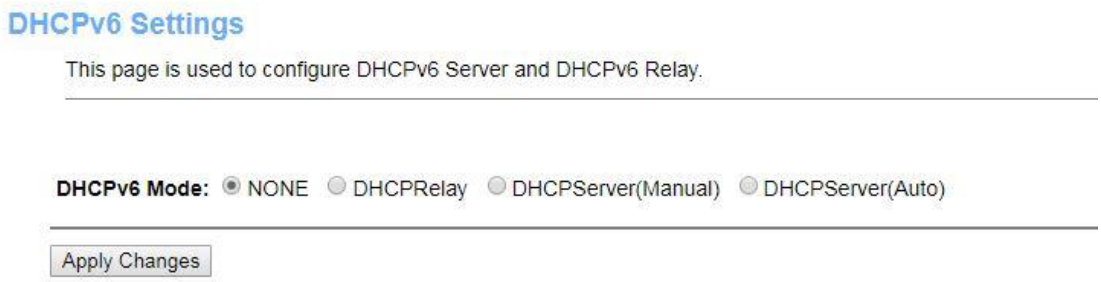
7.9.3DHCPv6

Go to the Advanced -->DHCPv6 page, you can configure the DHCPv6 mode of your Router as

None, DHCP Relay or DHCP Server.

7.9.3.1 None

If the DHCPv6 mode is “None”, the router will do nothing when the hosts request an IP address by DHCPv6 protocol.



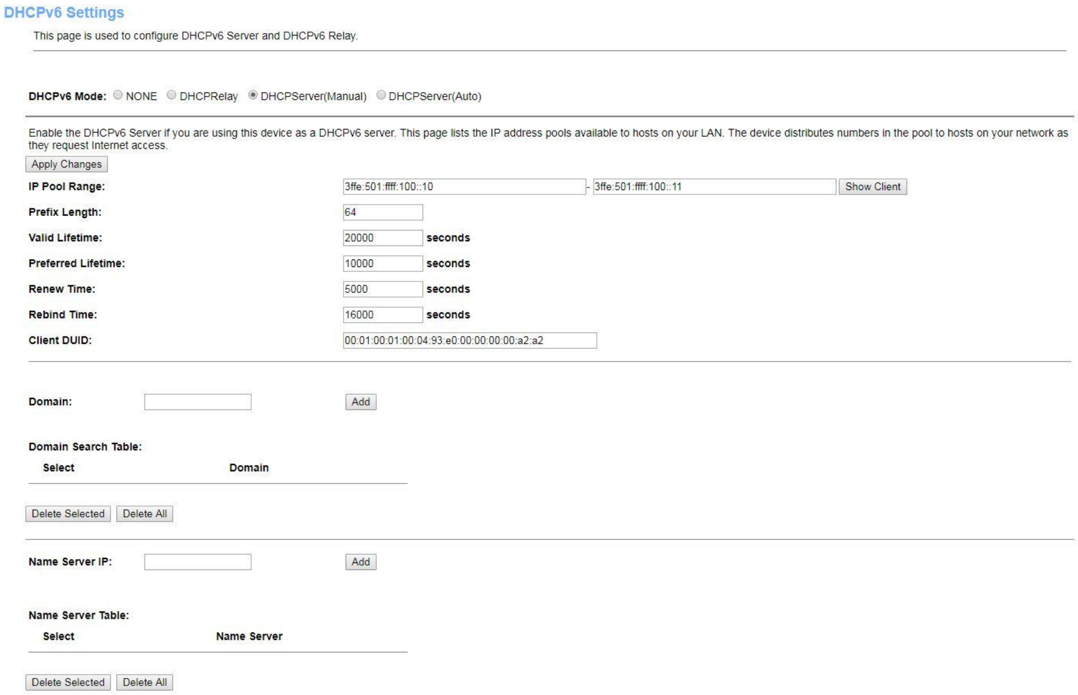
DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: ● NONE ○ DHCPRelay ○ DHCPServer(Manual) ○ DHCPServer(Auto)

7.9.3.2 DHCP Server

The DHCP Server is used to configure correct TCP/IP protocol related parameters for the computer on you local network. If you enable the DHCP Server function of the Ethernet router, you can make the DHCP Server automatically configure the TCP/IP protocol parameters (such as IP address, subnet mask, gate way and DNS servers) for the computer on you local network.



DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: ○ NONE ○ DHCPRelay ● DHCPServer(Manual) ○ DHCPServer(Auto)

Enable the DHCPv6 Server if you are using this device as a DHCPv6 server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

IP Pool Range:	3ffe:501:ffff:100::10 - 3ffe:501:ffff:100::11
Prefix Length:	64
Valid Lifetime:	20000 **seconds**
Preferred Lifetime:	10000 **seconds**
Renew Time:	5000 **seconds**
Rebind Time:	16000 **seconds**
Client DUID:	00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

Domain:

Domain Search Table:

Select	Domain

Name Server IP:

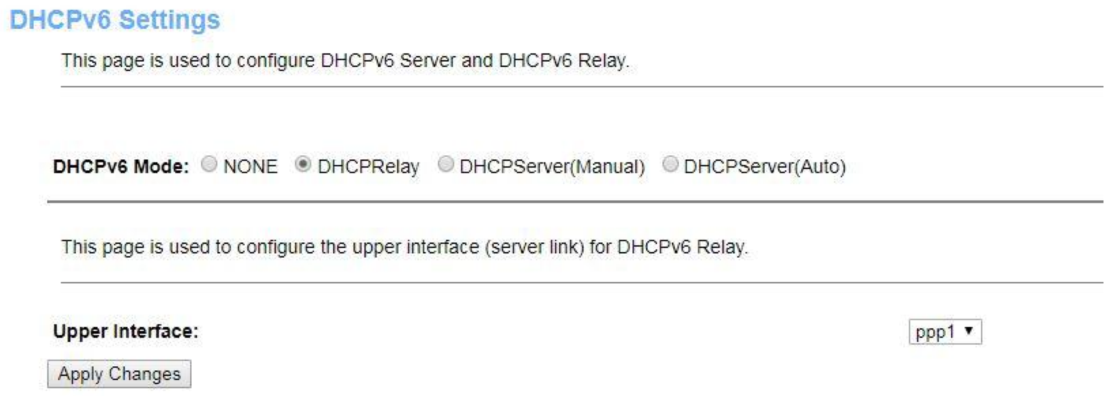
Name Server Table:

Select	Name Server

- DHCPv6 Mode
  the DHCP mode can be DHCP Server, DHCP Relay and None.
- IP Pool Range
  the DHCP IP pool address

7.9.3.3 DHCP Relay

If you are using the other DHCP Server to assign IP address to your hosts on the LAN, you can set the relay server’s IP address.



DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

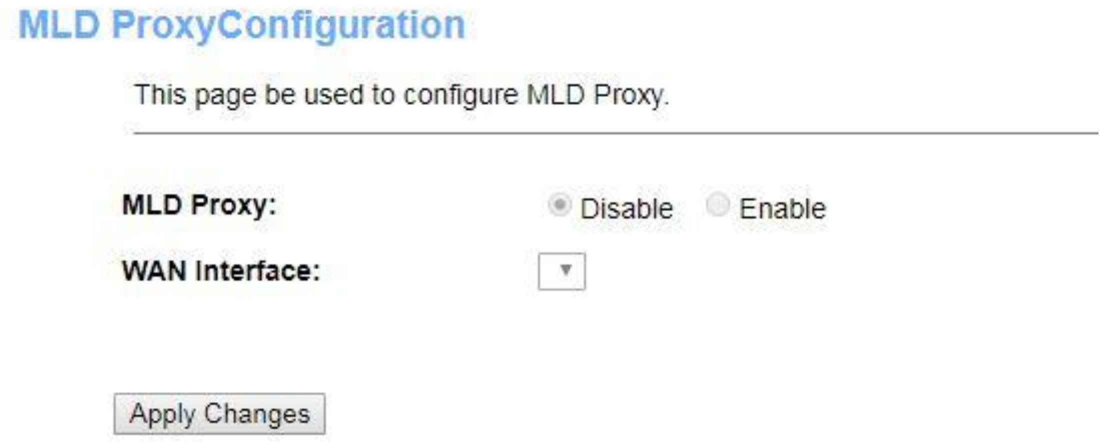
DHCPv6 Mode: ○ NONE ● DHCPRelay ○ DHCPServer(Manual) ○ DHCPServer(Auto)

This page is used to configure the upper interface (server link) for DHCPv6 Relay.

Upper Interface: ppp1

7.9.4 MLD Proxy

This page be used to configure MLD Proxy.



MLD ProxyConfiguration

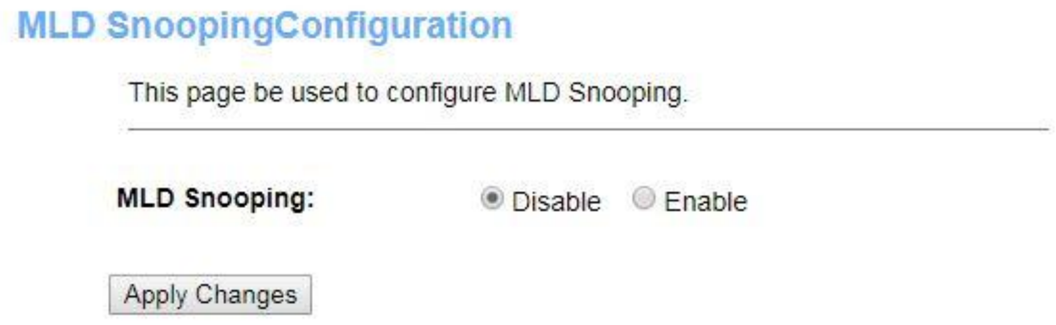
This page be used to configure MLD Proxy.

MLD Proxy: ● Disable ○ Enable

WAN Interface:

7.9.5 MLD Snooping

This page be used to configure MLD Snooping.



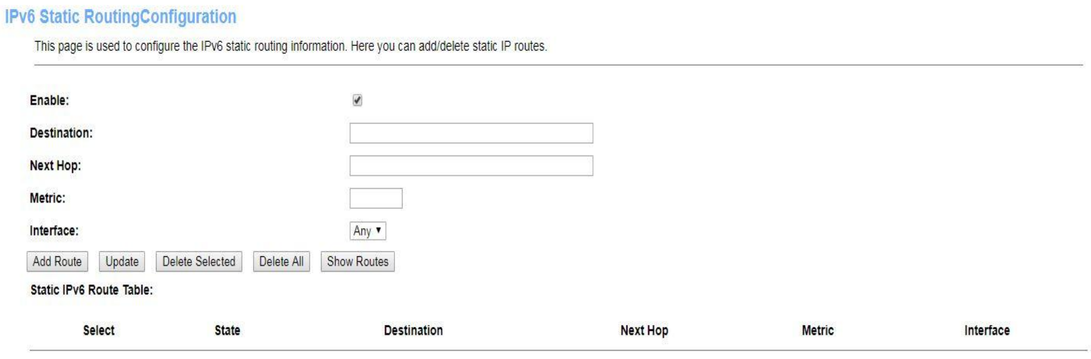
MLD SnoopingConfiguration

This page be used to configure MLD Snooping.

MLD Snooping: ● Disable ○ Enable

7.7.6 IPv6 Routing

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



IPv6 Static RoutingConfiguration

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

Enable: ☑

Destination:

Next Hop:

Metric:

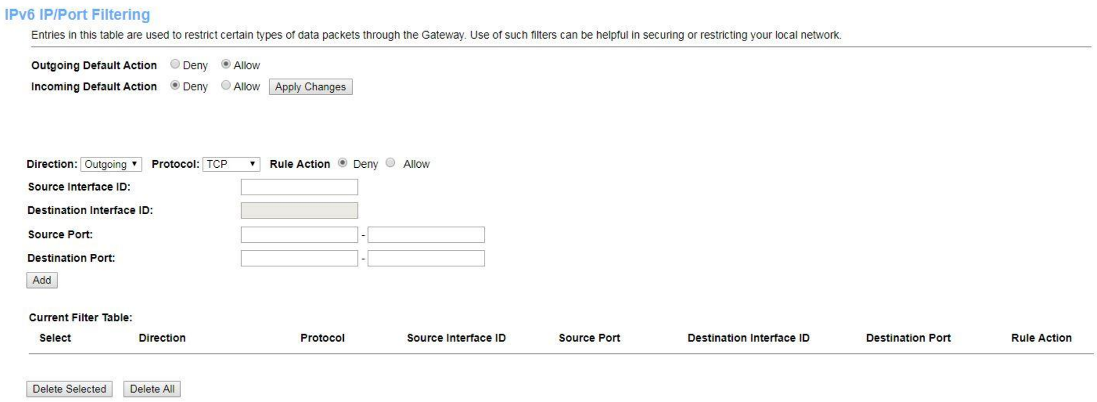
Interface: Any

Static IPv6 Route Table:

Select	State	Destination	Next Hop	Metric	Interface

7.9.7 IPv6 IP/Port Filtering

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



IPv6 IP/Port Filtering

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

Outgoing Default Action ○ Deny ● Allow

Incoming Default Action ● Deny ○ Allow

Direction: Outgoing Protocol: TCP Rule Action ● Deny ○ Allow

Source Interface ID:

Destination Interface ID:

Source Port: -

Destination Port: -

Current Filter Table:

Select	Direction	Protocol	Source Interface ID	Source Port	Destination Interface ID	Destination Port	Rule Action

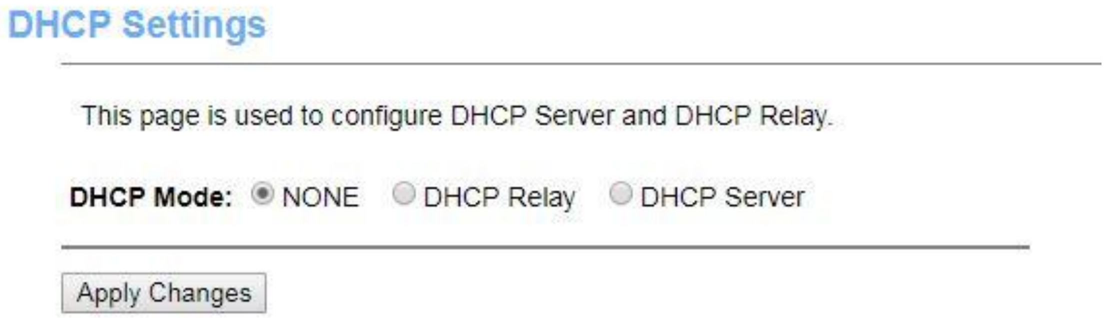
8. Service

8.1 DHCP

Go to the Service-->DHCP page, you can configure the DHCP mode of your Router as None, DHCP Relay or DHCP Server.

8.1.1 None

If the DHCP mode is "None", the router will do nothing when the hosts request an IP address by DHCP protocol.



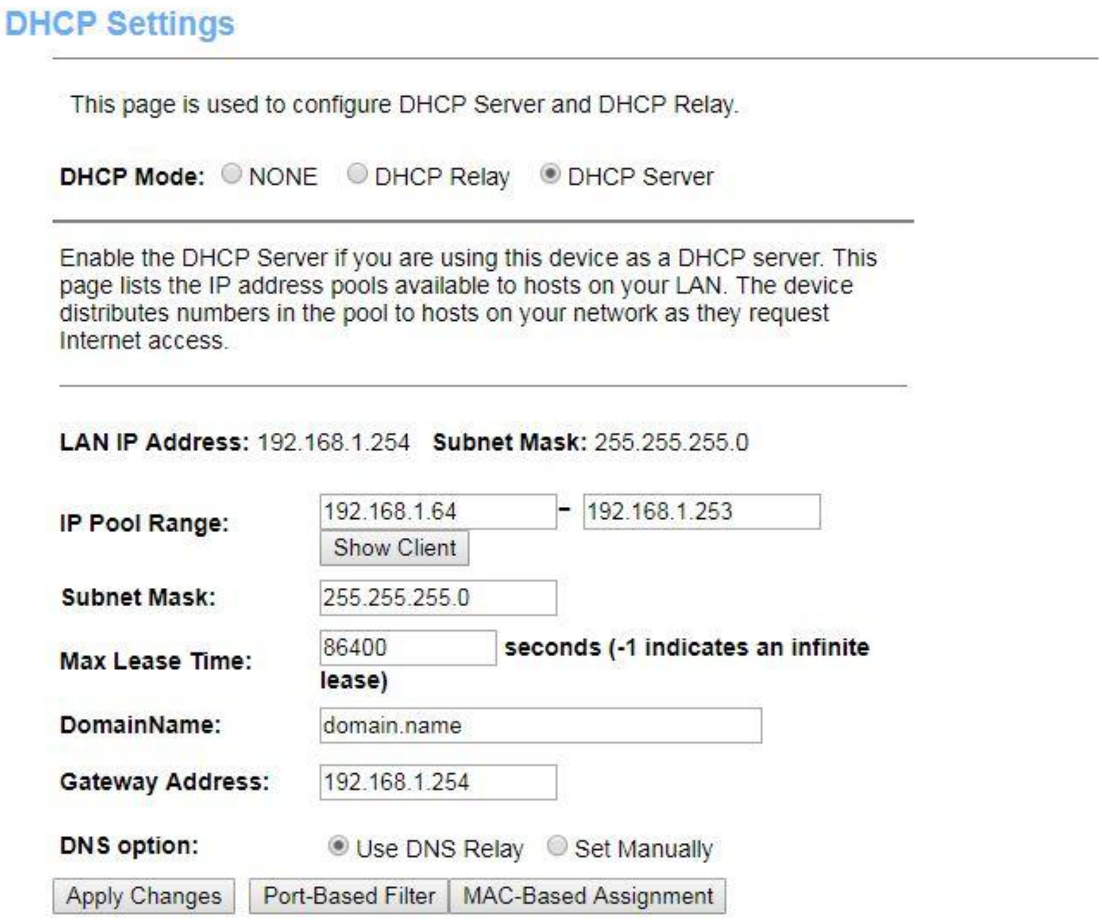
DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: ● NONE ○ DHCP Relay ○ DHCP Server

8.1.2 DHCP Server

The DHCP Server is used to configure correct TCP/IP protocol related parameters for the computer on you local network. If you enable the DHCP Server function of the Ethernet router, you can make the DHCP Server automatically configure the TCP/IP protocol parameters (such as IP address, subnet mask, gate way and DNS servers) for the computer on you local network.



DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: ○ NONE ○ DHCP Relay ● DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.254 Subnet Mask: 255.255.255.0

IP Pool Range: 192.168.1.64 - 192.168.1.253

Subnet Mask: 255.255.255.0

Max Lease Time: 86400 seconds (-1 indicates an infinite lease)

DomainName: domain.name

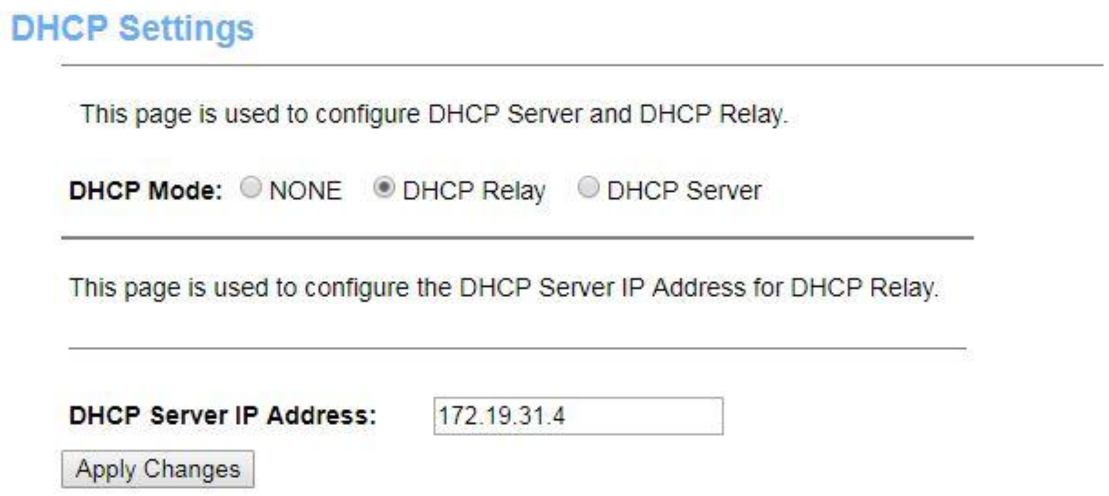
Gateway Address: 192.168.1.254

DNS option: ● Use DNS Relay ○ Set Manually

- DHCP Mode
  the DHCP mode can be DHCP Server, DHCP Relay and None.
- IP Pool Range
  the DHCP IP pool address
- Gateway Address
  the default gateway address
- Max Lease Time
  the time that the DHCP client is allowed to maintain a network connection.
- Domain Name
  a user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool
- DNS option
  Use DNS Relay and Set Manually

8.1.3 DHCP Relay

If you are using the other DHCP Server to assign IP address to your hosts on the LAN, you can set the relay server’s IP address.



DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: ○ NONE ● DHCP Relay ○ DHCP Server

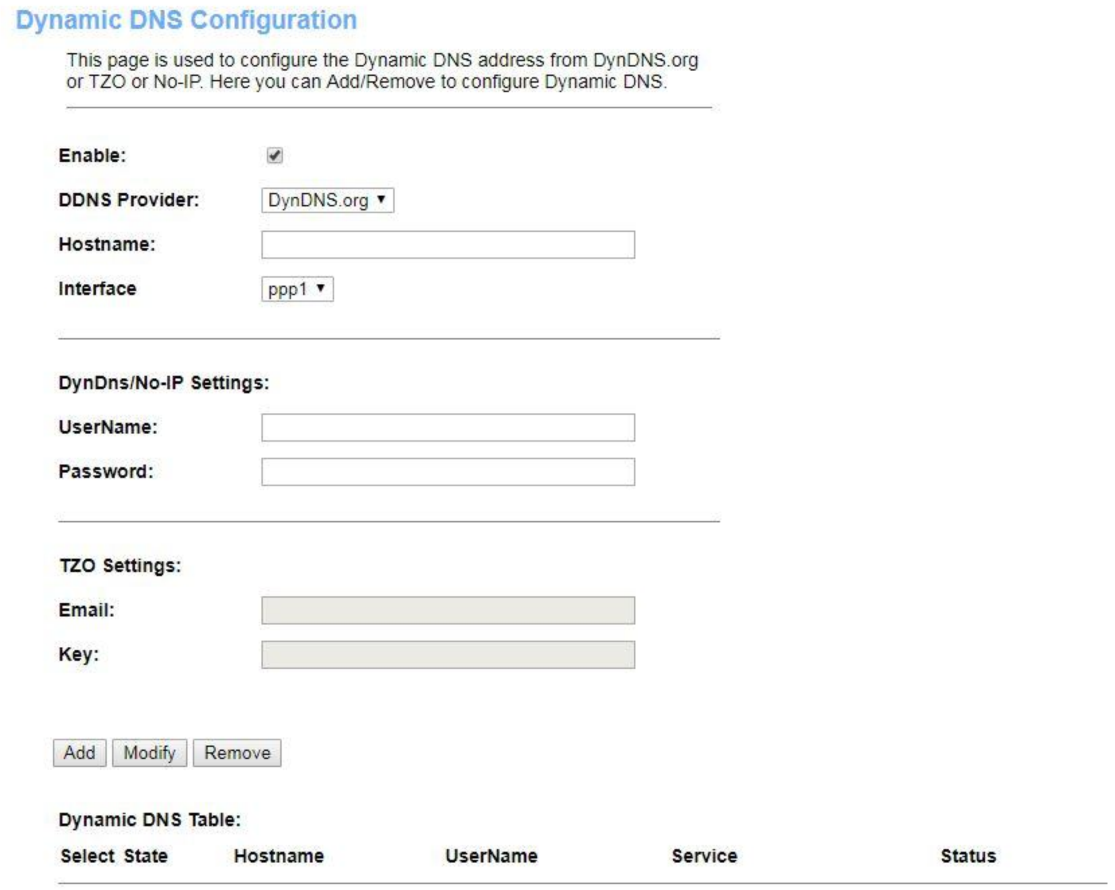
This page is used to configure the DHCP Server IP Address for DHCP Relay.

DHCP Server IP Address: 172.19.31.4

- Relay server
  the IP address of the DHCP Relay server.

8.2 DNS

Go to Service->DNS page, you can configure the IP address of DDNS server.



Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO or No-IP. Here you can Add/Remove to configure Dynamic DNS.

Enable: ☑

DDNS Provider: DynDNS.org

Hostname:

Interface: ppp1

DynDns/No-IP Settings:

UserName:

Password:

TZO Settings:

Email:

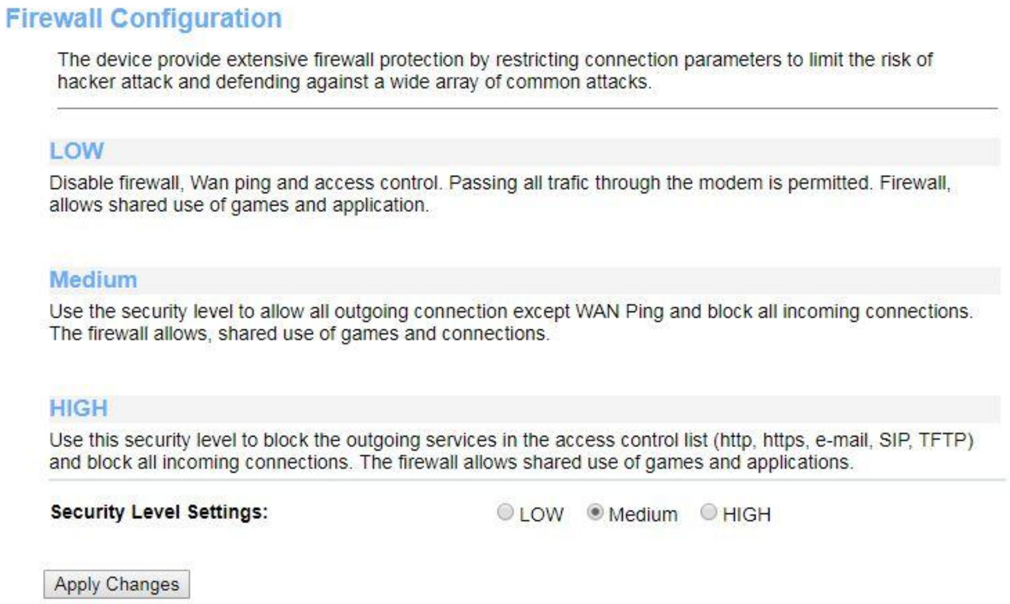
Key:

Dynamic DNS Table:

Select	State	Hostname	UserName	Service	Status

8.3 Firewall

8.3.1 Security settings



Firewall Configuration

The device provide extensive firewall protection by restricting connection parameters to limit the risk of hacker attack and defending against a wide array of common attacks.

LOW

Disable firewall, Wan ping and access control. Passing all trafic through the modem is permitted. Firewall, allows shared use of games and application.

Medium

Use the security level to allow all outgoing connection except WAN Ping and block all incoming connections. The firewall allows, shared use of games and connections.

HIGH

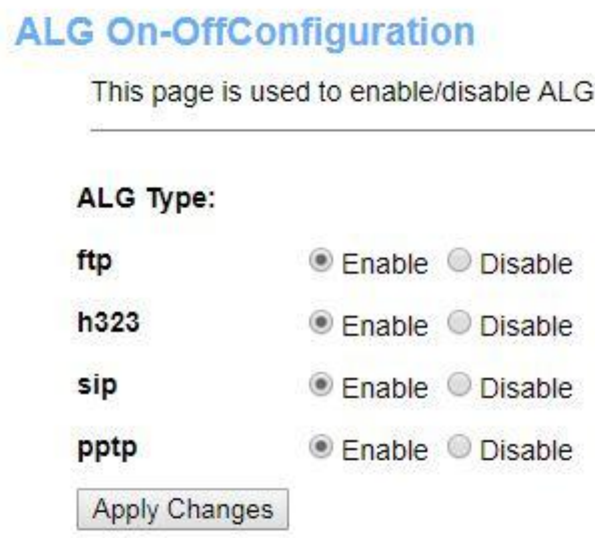
Use this security level to block the outgoing services in the access control list (http, https, e-mail, SIP, TFTP) and block all incoming connections. The firewall allows shared use of games and applications.

Security Level Settings: ○ LOW ● Medium ○ HIGH

8.3.2 ALG

The router supports several NAT ALG and pass-Through function.

Go to Service ->Firewall->ALG page, you can configure the ALG settings. Here you can enable or disable the ALG or pass-through function for each application.


ALG On-OffConfiguration

This page is used to enable/disable ALG services.

ALG Type:

ftp ● Enable ○ Disable

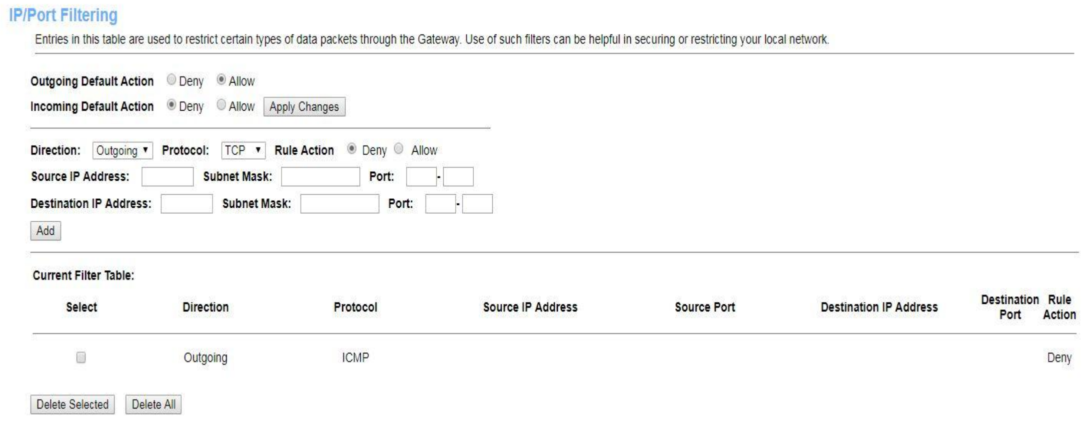
h323 ● Enable ○ Disable

sip ● Enable ○ Disable

pptp ● Enable ○ Disable

8.3.3 IP/Port filter

Go to Service ->Firewall->IP/Port Filter page, you can set the IP/Port filter rules to secure or restrict your local network.


IP/Port Filtering

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

Outgoing Default Action ○ Deny ● Allow

Incoming Default Action ● Deny ○ Allow

Direction: Outgoing Protocol: TCP Rule Action ● Deny ○ Allow

Source IP Address: Subnet Mask: Port: -

Destination IP Address: Subnet Mask: Port: -

Current Filter Table:

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action
□	Outgoing	ICMP					Deny

On the front of the page, you can see the default action of outgoing/incoming connection. If the IP connection doesn't match any filter rules, the router will handle the connection with the default action setting.

- Default Action

  the filter mode of this entry, it can be "Allow" and "Deny". If the mode is "Allow", the IP connection matches the rule will be permitted, if the mode is "Deny", the IP connection matches the rule will be denied.

- Protocol

  the protocol of this entry, it can be “IP”, “ICMP”, “TCP” and “UDP”.
- Direction

  the direction of this entry, it can be “upstream” and “Downstream”.
- Source IP Address/ Mask Address

  the source IP address and mask address of the entry.
- Dest IP Address/ Mask Address

  the destination IP address and mask address of the entry.
- Sport

  If the protocol is “TCP” or “UDP”, you should set the source port of the entry, it can be a single port or a port range.
- Dport

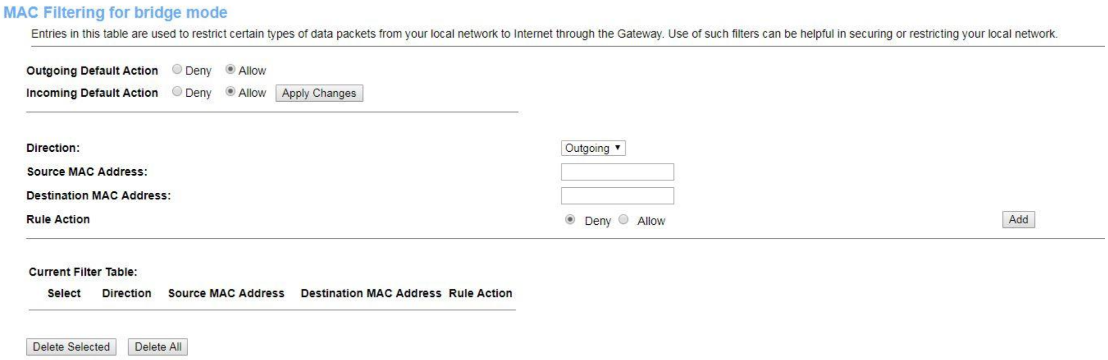
  If the protocol is “TCP” or “UDP”, you should set the destination port of the entry, it can be a single port or a port range.
- Deny or Allow

  enable or disable this filter entry.

8.3.4 MAC filter

In order to management your local network better, you can use the MAC address filter function to control the internet access.

Go to F Service ->Firewall->MAC Filter page, you can set the MAC filtering rules.



MAC Filtering for bridge mode

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 Action ○ Deny ● Allow

Incoming Default Action ○ Deny ● Allow [Apply Changes]

Direction: Outgoing ▾

Source MAC Address:

Destination MAC Address:

Rule Action ● Deny ○ Allow [Add]

Current Filter Table:

Select	Direction	Source MAC Address	Destination MAC Address	Rule Action

- Outgoing/Incoming Default Policy

  the default action of outgoing/incoming connection. It can be “Deny” or “Allow”. If the connection doesn’t match any MAC filtering rules, the router will handle the connection with the default action you have set.
- Direction

  the direction of the filter entry, it can be “Outgoing” or “Incoming”.

- ➢ Action

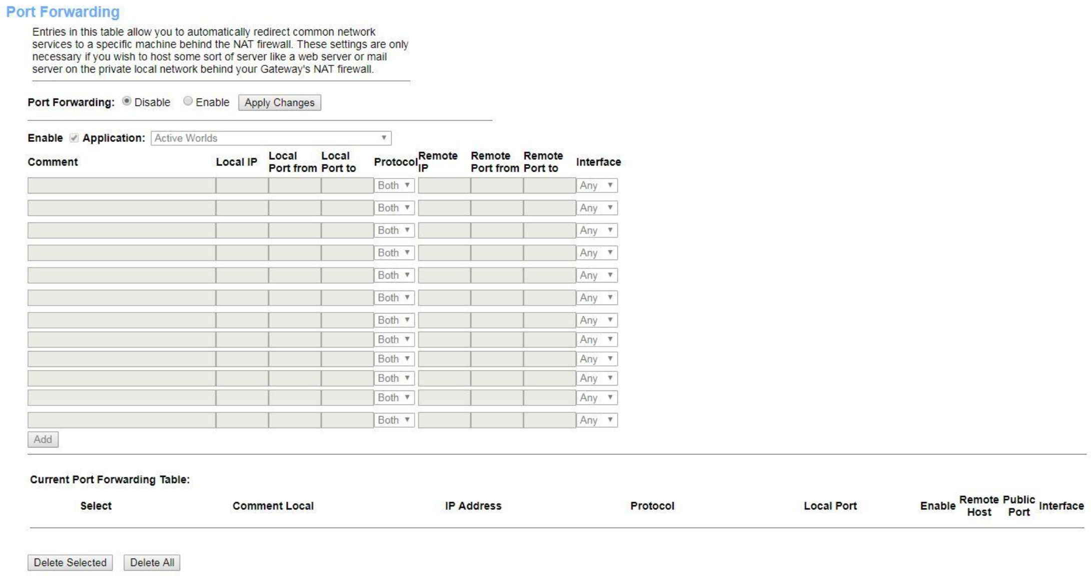
  the action of the filter entry, it can be “Deny” or “Allow”. If the action is “Deny”, the connection matches the filter rule will be denied, if the action is “Allow”, the connection matches the filter rule will be allowed.
- ➢ Source MAC

  the source MAC address of the filter entry, if empty means matches any source MAC address.
- ➢ Destination MAC

  the destination MAC address of the filter entry, if empty means matches any source MAC address.

8.3.5 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

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: ● Disable ○ Enable [Apply Changes]

Enable ☑ Application: Active Worlds ▼

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼
				Both ▼				Any ▼

[Add]

Current Port Forwarding Table:

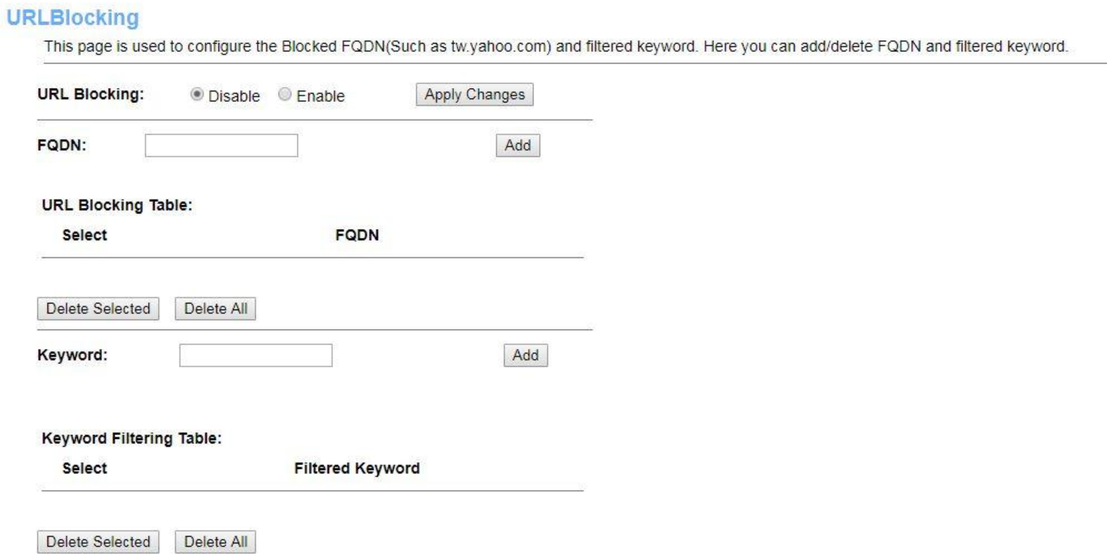
Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface

[Delete Selected] [Delete All]

8.3.6 URL filter

In order to manage the site control of your local LAN client, you can use URL filtering function to specify which site can’t be accessed.

Go to Service ->Firewall->URL Filter page, you can add and delete the filtered keyword.



URLBlocking

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: ● Disable ○ Enable

FQDN:

URL Blocking Table:

Select	FQDN

Keyword:

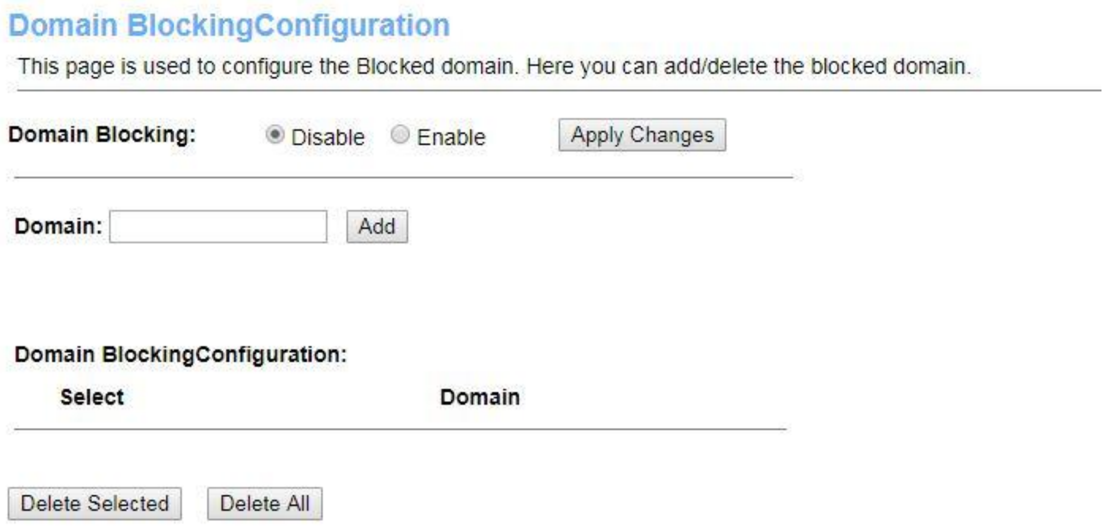
Keyword Filtering Table:

Select	Filtered Keyword

- URL Blocking Capability
  Enable or disable the URL filtering function. If it is enabled, the access to the site which matches the keyword will be blocked by the router, if it is disabled, nothing will be done.
- Keyword
  the keyword of the site you want to block.
- URL Blocking Table
  it shows the current URL filtering entry

8.3.7 Domain Blocking

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.
Go to Service ->Firewall -> Domain Blocking page



Domain BlockingConfiguration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: ● Disable ○ Enable

Domain:

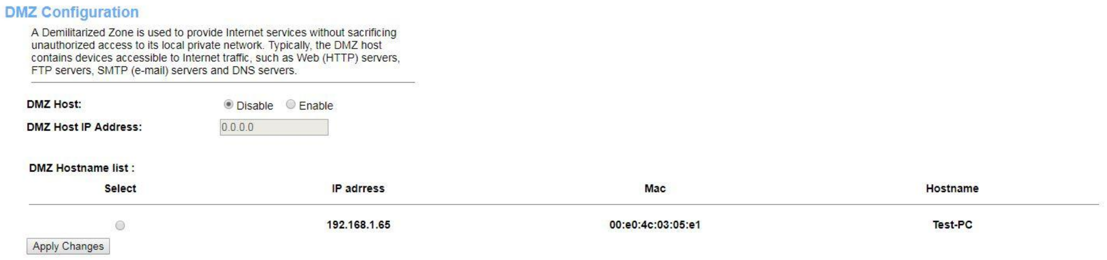
Domain BlockingConfiguration:

Select	Domain

8.3.8 DMZ

A Demilitarized Zone (DMZ) allows a single host on your LAN to expose ALL of its ports to the Internet.

Go to Service ->Firewall ->DMZ page, you can configure the DMZ settings.



DMZ Configuration

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 Host: ● Disable ○ Enable

DMZ Host IP Address: 0.0.0.0

DMZ Hostname list :

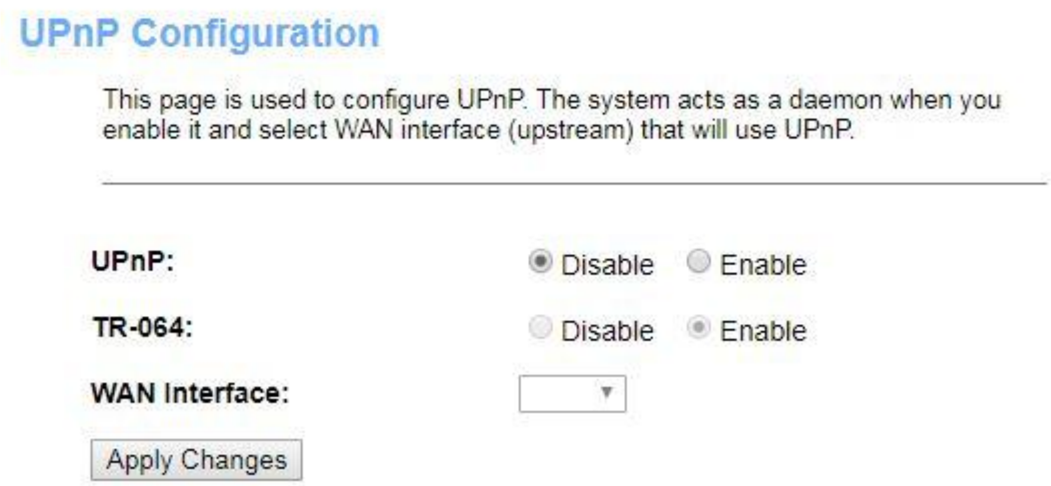
Select	IP adrress	Mac	Hostname
○	192.168.1.65	00:e0:4c:03:05:e1	Test-PC

- Enable DMZ
  enable or disable the DMZ function.
- DMZ Host IP Address
  the IP address of the DMZ host.

8.4 UPnP

UPnP (Universal Plug and Play networking protocol), this feature requires the operating system must support the UPnP application. LAN hosts can request a specific port translation on router by UPnP protocol, so the external hosts can access the resources on the internal hosts when needed.

Go to Service ->Firewall ->UPnP page, here you can configure UPnP.



UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: ● Disable ○ Enable

TR-064: ○ Disable ● Enable

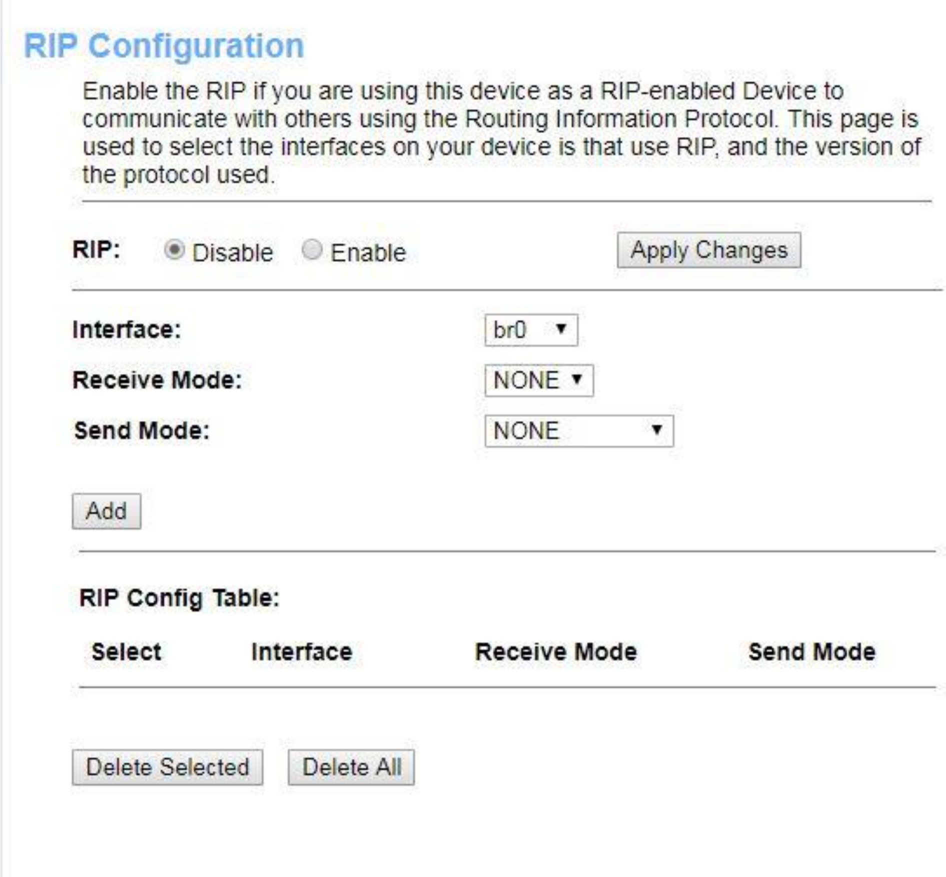
WAN Interface:

- UPnP
  enable or disable the UPnP function
- WAN interface
  which interface runs UPnP fucntion

8.5 RIP

RIP is an internet protocol you can setup to share routing table information with other routing devices.

Go to Service ->Firewall ->RIP page, you can configure the RIP settings. Here you can enable or disable the RIP function.



RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled Device to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device is that use RIP, and the version of the protocol used.

RIP: ● Disable ○ Enable

Interface: br0

Receive Mode: NONE

Send Mode: NONE

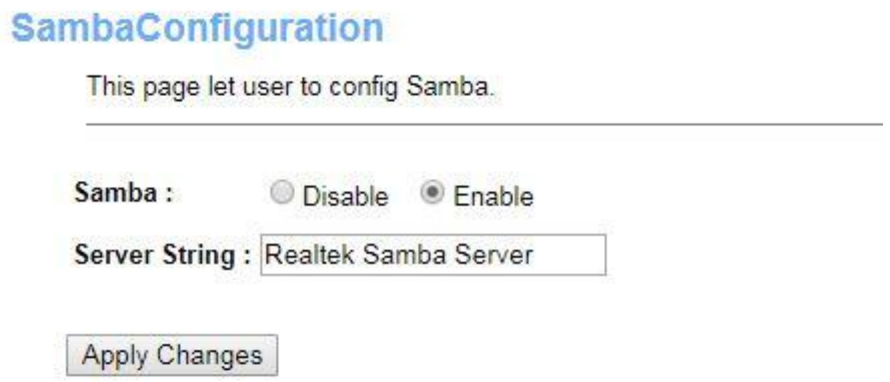
RIP Config Table:

Select	Interface	Receive Mode	Send Mode

- ➢ RIP
  enable or disable the RIP function of the router.
- ➢ Interface
  the interface on which you want to enable RIP
- ➢ Recv Version
  indicate the RIP version in which information must be passed to the device it can be accepted into its routing table
- ➢ Send Version
  indicate the RIP version this interface will use when it sends its route information to the other device

8.6 Samba

Go to Service ->Firewall ->Samba page ,This page let user to config Samba.



SambaConfiguration

This page let user to config Samba.

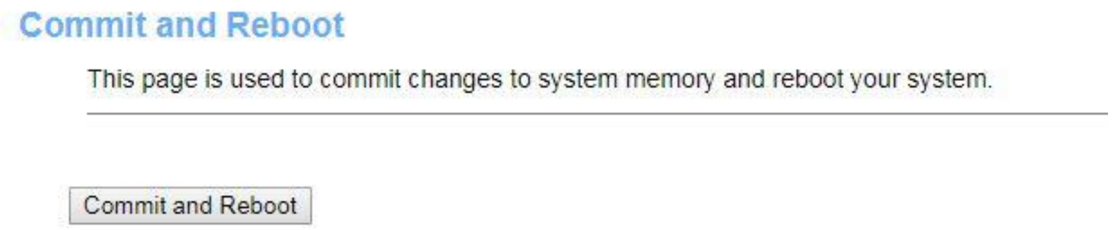
Samba : ○ Disable ● Enable

Server String : Realtek Samba Server

9. Admin

9.1 Commit/Reboot

Go to Admin ->Commit/Reboot page, you can commit changes to system memory and reboot your device with different configuration.

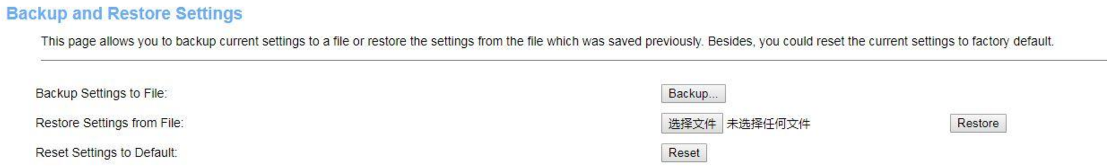


Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

9.2 Backup/Restore

Go to Admin ->Backup/Restore page, you can save the current configuration settings to a file, and you can also restore the settings from a configuration file.



Backup and Restore Settings

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

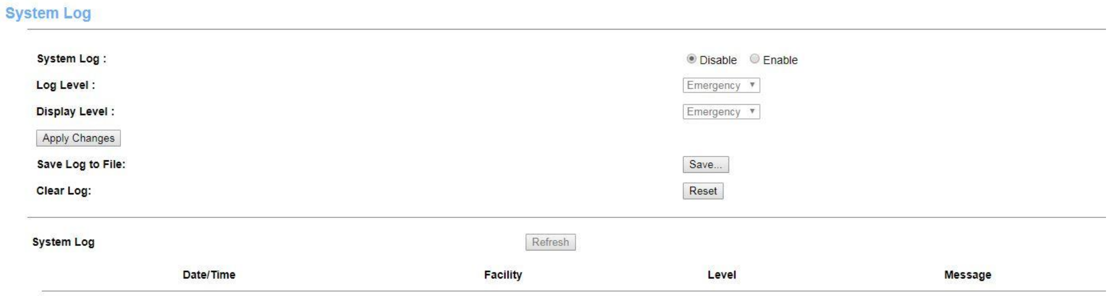
Backup Settings to File: Backup...

Restore Settings from File: 选择文件 未选择任何文件 Restore

Reset Settings to Default: Reset

9.3 System Log

Go to Admin ->System Log page, you can configure the parameters of the system log, and view the system log information.



System Log

System Log : ● Disable ○ Enable

Log Level : Emergency

Display Level : Emergency

Save Log to File:

Clear Log:

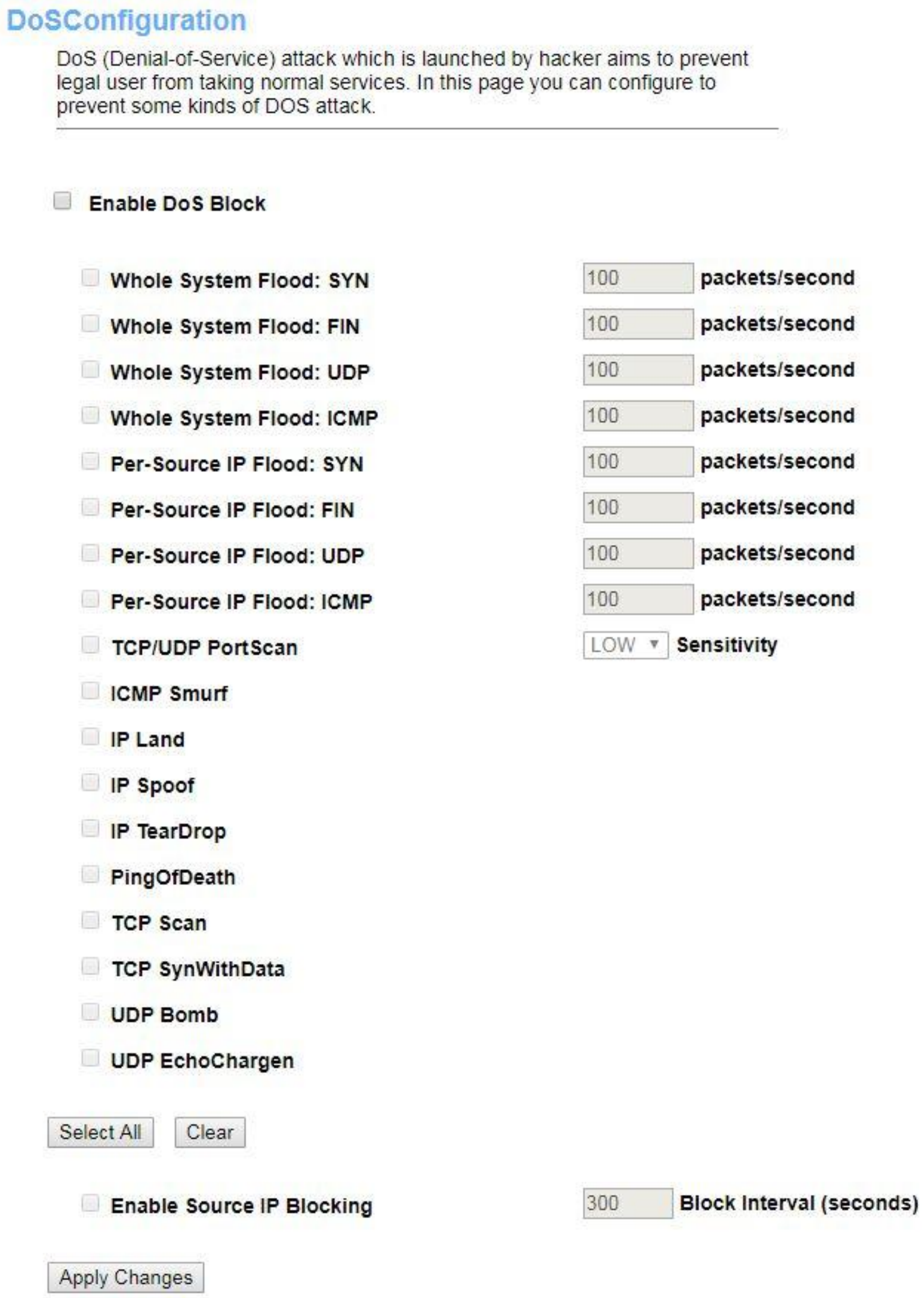
System Log

Date/Time	Facility	Level	Message

9.4 DoS

The router provides a protection of Denial of Service attack.

Go to Admin->DoS page, you can configure the dos parameters. You can enable or disable the DoS prevention, and you can also specify the hack item.



DoSConfiguration

DoS (Denial-of-Service) attack which is launched by hacker aims to prevent legal user from taking normal services. In this page you can configure to prevent some kinds of DOS attack.

□ Enable DoS Block

□ 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

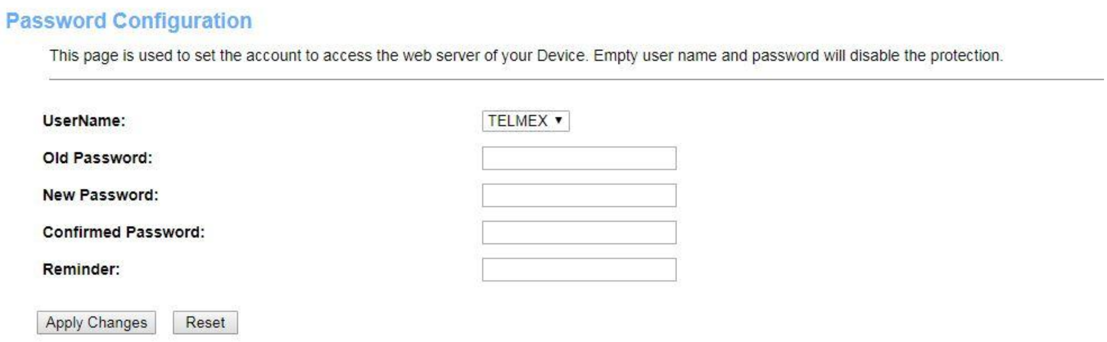
□ UDP Bomb

□ UDP EchoChargen

□ Enable Source IP Blocking 300 Block Interval (seconds)

9.5 Password

Go to Admin->Password page, you can configure the user account of the router. Here you can add user account to access the web server, and modify the password of the specified user.



Password Configuration

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

UserName: TELMEX ▾

Old Password:

New Password:

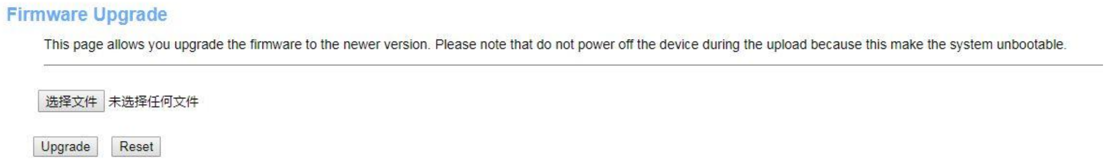
Confirmed Password:

Reminder:

9.6 Firmware Upgrade

The router supports the firmware upgrade from HTTP.

Go to Admin->Firmware Update page, you can upgrade the firmware to the new version.



Firmware Upgrade

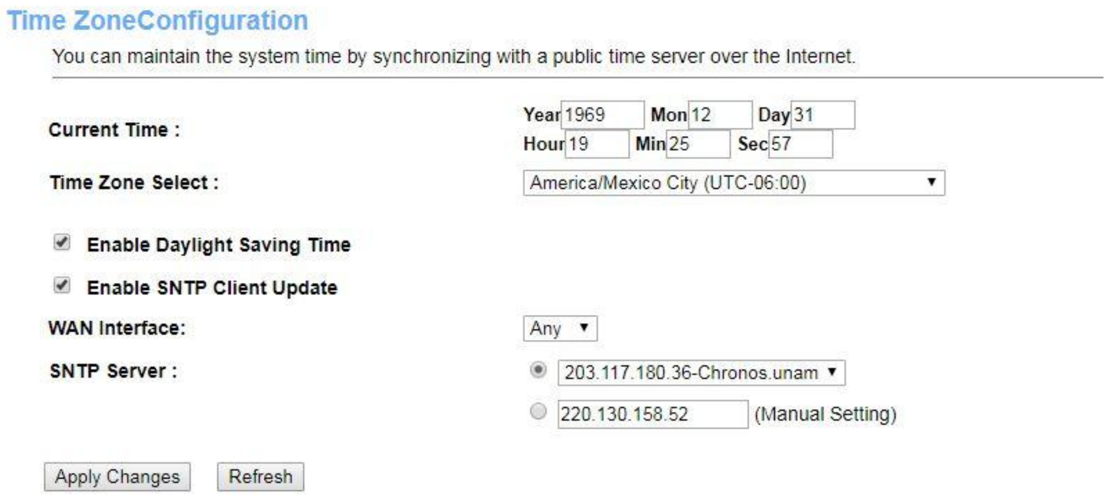
This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

You should select the correct firmware image first, and then apply the “Upload” button.

9.7 Time Zone

Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP server.

Go to Admin->Time Zone page, you can configure the system time.



Time ZoneConfiguration

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

Current Time :	Year 1969 Mon 12 Day 31 Hour 19 Min 25 Sec 57
Time Zone Select :	America/Mexico City (UTC-06:00) ▼

☑ Enable Daylight Saving Time

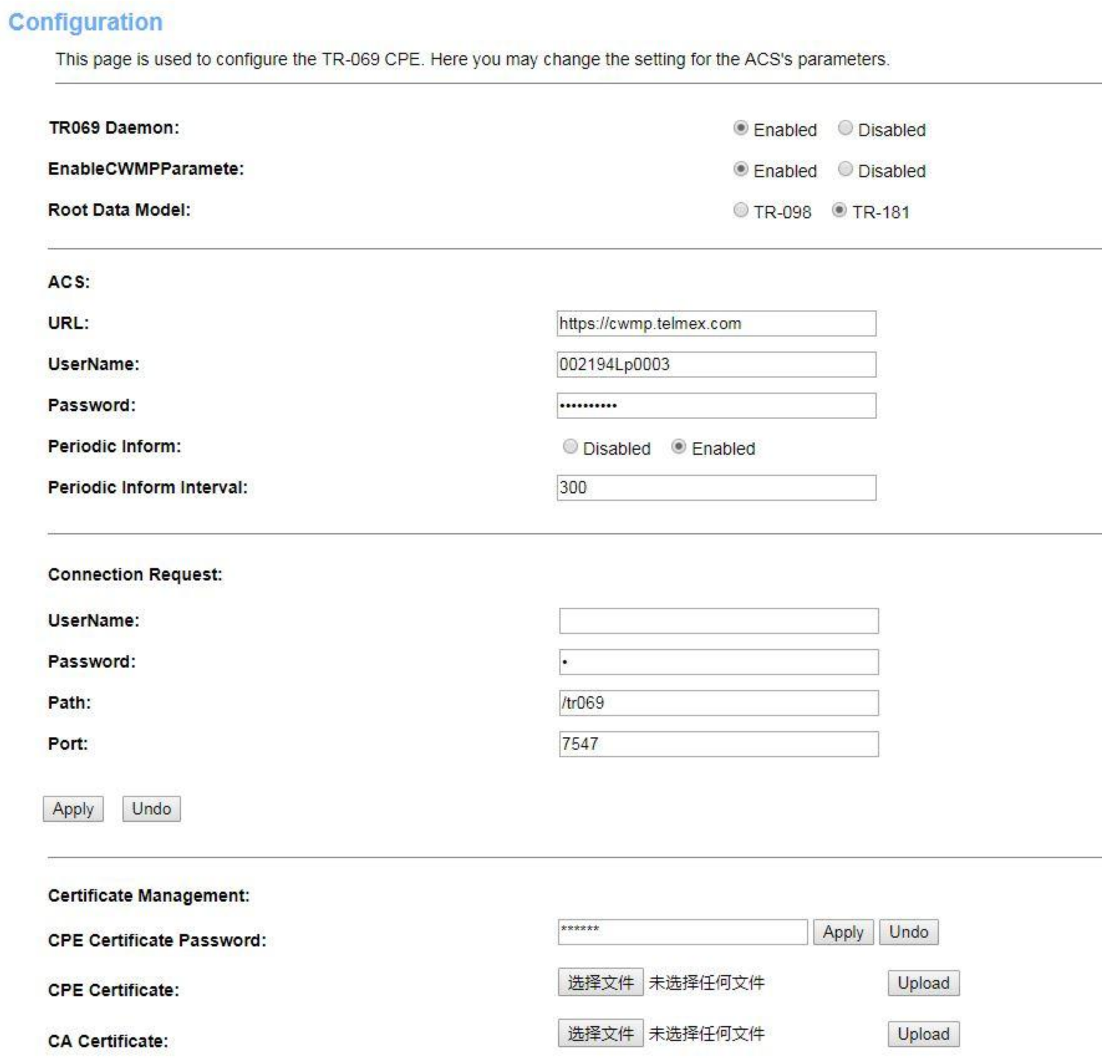
☑ Enable SNTP Client Update

WAN Interface:	Any ▼
SNTP Server :	● 203.117.180.36-Chronos.unam ▼ ○ 220.130.158.52 (Manual Setting)

9.8 TR-069

Tr069 is also called CWMP, CPE WAN Management Protocol (CWMP) is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The CPE TR-069 configuration should be well defined to be able to communicate with the remote ACS.

Go to Admin->Tr-069 page, you can configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.



Configuration

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

TR069 Daemon:	● Enabled ○ Disabled
EnableCWMPParamete:	● Enabled ○ Disabled
Root Data Model:	○ TR-098 ● TR-181
ACS:	
URL:	https://cwmp.telmex.com
UserName:	002194Lp0003
Password:	••••••••••
Periodic Inform:	○ Disabled ● Enabled
Periodic Inform Interval:	300
Connection Request:	
UserName:	
Password:	•
Path:	/tr069
Port:	7547

Certificate Management:	
CPE Certificate Password:	******
CPE Certificate:	未选择任何文件
CA Certificate:	未选择任何文件

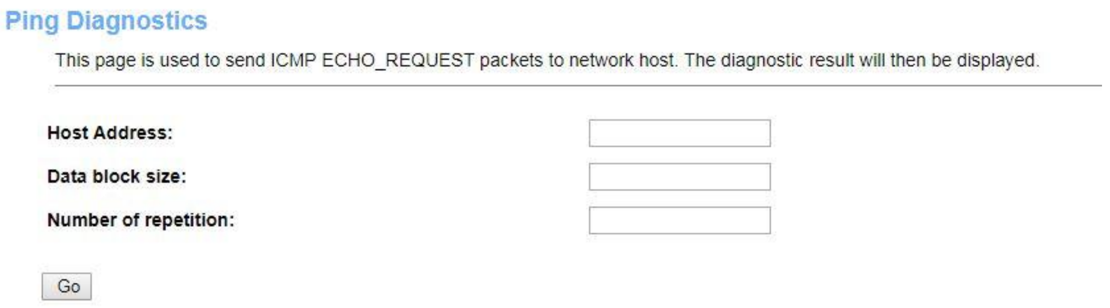
10. Diagnostics

The router provides several useful diagnostic tools.

10.1 Ping

The router provides a ping command to send a message to the host you specify.

Go to Status->Diagnostics->Ping page, you can ping a host you wanted.



Ping Diagnostics

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

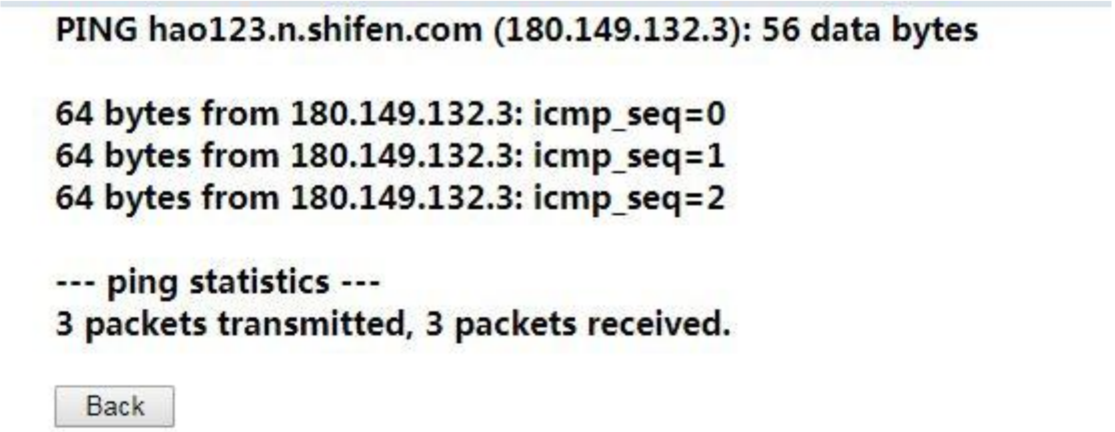
Host Address:

Data block size:

Number of repetition:

- Host
  an IP address or host name you want to ping.

When you set the host, click the “Go” button to start the ping process, then the ping result will be shown.

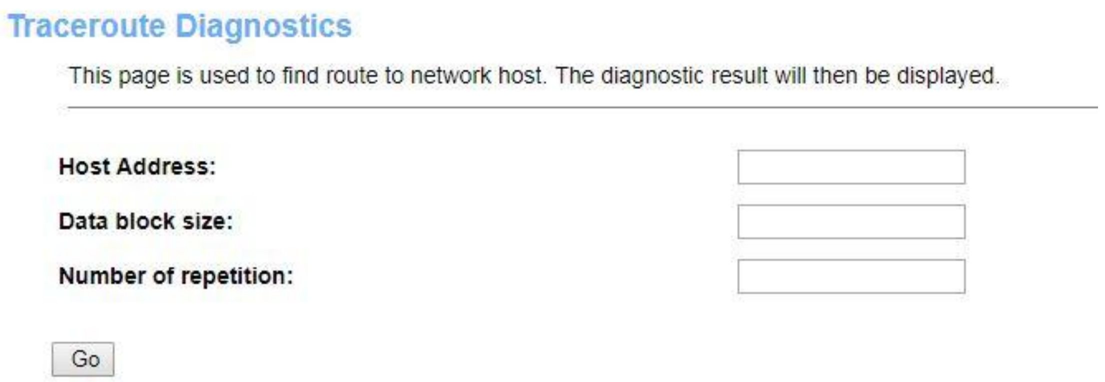


```
PING hao123.n.shifen.com (180.149.132.3): 56 data bytes

64 bytes from 180.149.132.3: icmp_seq=0
64 bytes from 180.149.132.3: icmp_seq=1
64 bytes from 180.149.132.3: icmp_seq=2

--- ping statistics ---
3 packets transmitted, 3 packets received.
```

10.2 Traceroute

The router provides a tracert command to measure the route path and transit times of packets across an Internet Protocol (IP) network.

Go to Status->Diagnostics->Traceroure page, you can tracert a host you wanted.



Traceroute Diagnostics

This page is used to find route to network host. The diagnostic result will then be displayed.

Host Address:

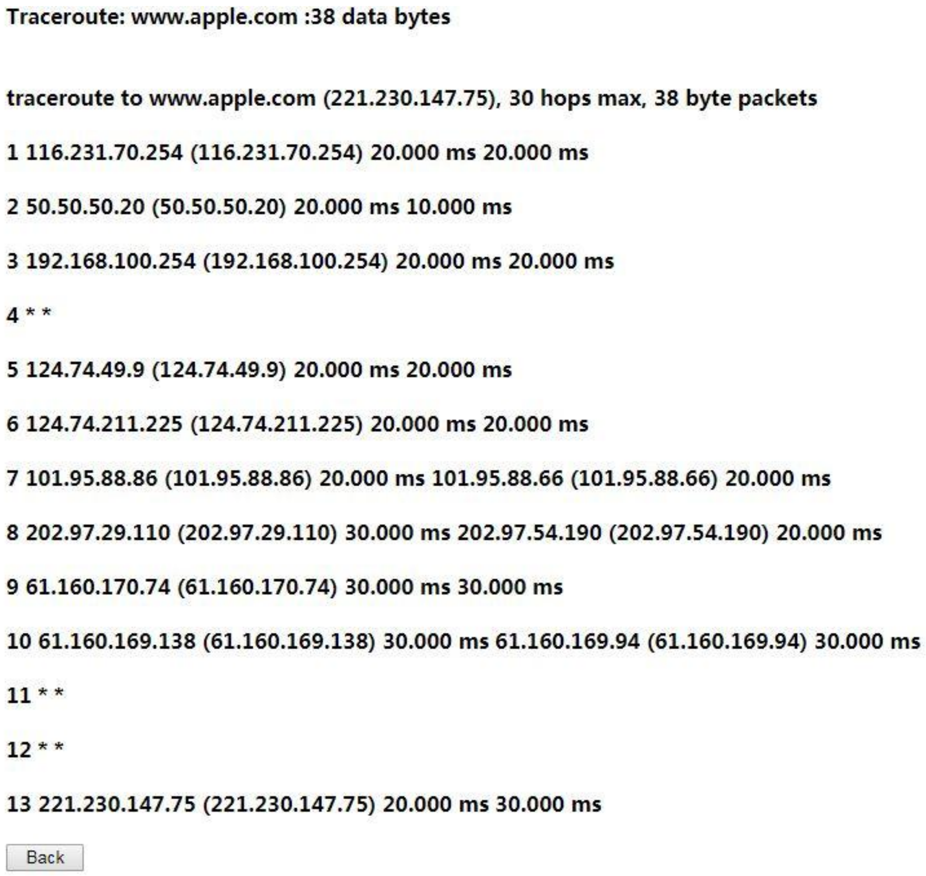
Data block size:

Number of repetition:

- Host

  an IP address or host name you want to run trace route command

For example, you can set the host to www.apple.com, and then click the "Go" button to start the trace route process. Several times later, you can see the trace route result.

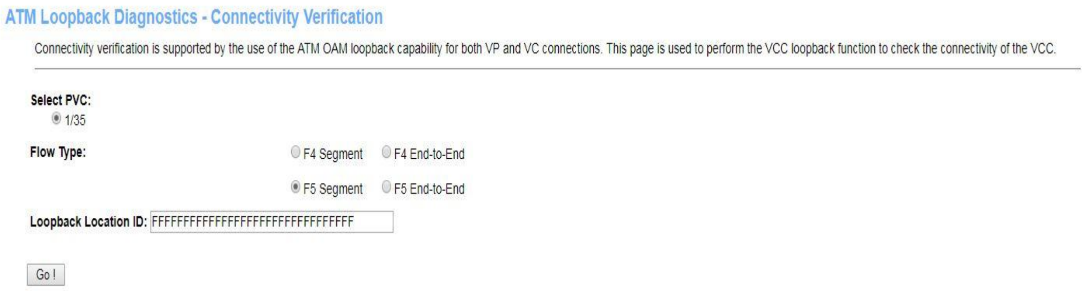


```
Traceroute: www.apple.com :38 data bytes

traceroute to www.apple.com (221.230.147.75), 30 hops max, 38 byte packets

1 116.231.70.254 (116.231.70.254) 20.000 ms 20.000 ms

2 50.50.50.20 (50.50.50.20) 20.000 ms 10.000 ms

3 192.168.100.254 (192.168.100.254) 20.000 ms 20.000 ms

4 * *

5 124.74.49.9 (124.74.49.9) 20.000 ms 20.000 ms

6 124.74.211.225 (124.74.211.225) 20.000 ms 20.000 ms

7 101.95.88.86 (101.95.88.86) 20.000 ms 101.95.88.66 (101.95.88.66) 20.000 ms

8 202.97.29.110 (202.97.29.110) 30.000 ms 202.97.54.190 (202.97.54.190) 20.000 ms

9 61.160.170.74 (61.160.170.74) 30.000 ms 30.000 ms

10 61.160.169.138 (61.160.169.138) 30.000 ms 61.160.169.94 (61.160.169.94) 30.000 ms

11 * *

12 * *

13 221.230.147.75 (221.230.147.75) 20.000 ms 30.000 ms
```

10.3 ATM Loopback

OAM Loopback allows you to verify the connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. ATM uses two cell flows: F4 used in VPs and F5 used in VCs.

Go to Status->Diagnostics->ATM Loopback page, you can perform the loopback function to check the connectivity of the VCC.



ATM Loopback Diagnostics - Connectivity Verification

Connectivity verification is supported by the use of the ATM 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.

Select PVC:
● 1/35

Flow Type: ○ F4 Segment ○ F4 End-to-End
● F5 Segment ○ F5 End-to-End

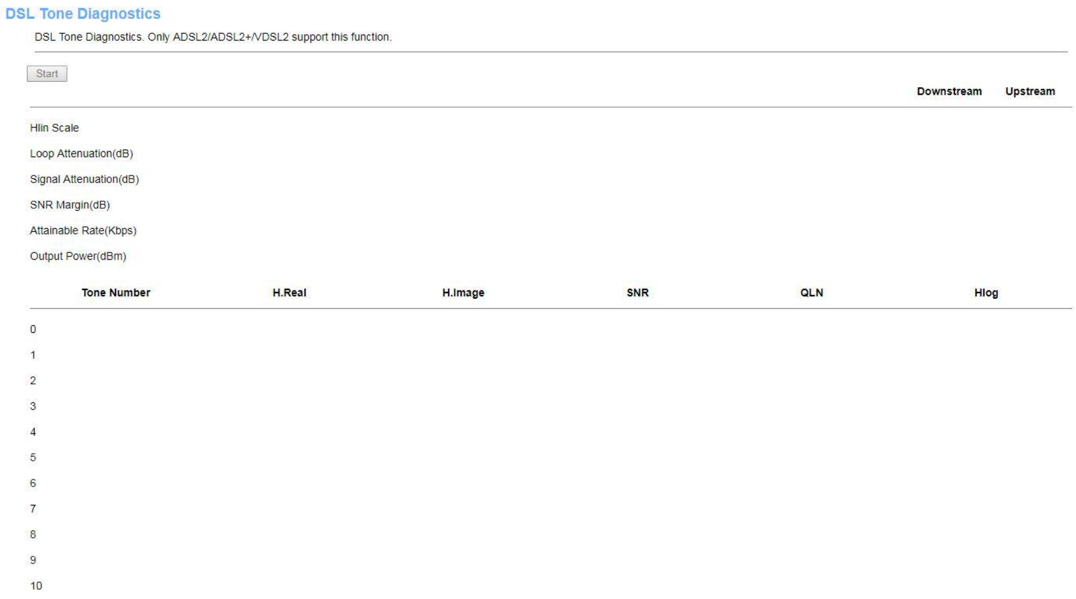
Loopback Location ID: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

- Flow type
  the ATM OAM flow type. The selection can be F5 Segment, F5 End-to-End, F4 Segment or F4 End-to-End.
- VPI
  the VPI number you want to do the loopback diagnostics
- VCI
  the VCI number you want to do the loopback diagnostics

10.4 DSL Tone

DSL diagnostics allows you to diagnostics the DSL tone.

Go to Status->Diagnostics->DSL Tone page, you can start the DSL tone diagnostic.



DSL Tone Diagnostics

DSL Tone Diagnostics. Only ADSL2/ADSL2+/VDSL2 support this function.

Start

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

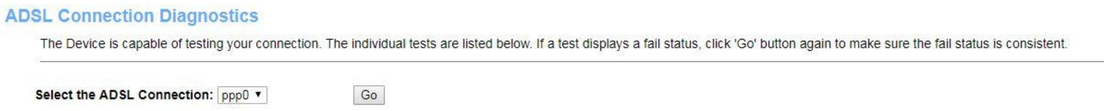
Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Click the “Start” button to start the diagnostic, and then wait several minutes later you will see the test result.

10.5 ADSL Connection

The Diagnostic Test allows you to test your DSL connection of the physical layer and protocol layer for both LAN and WAN sides.

Go to Status->Diagnostics-> ADSL Connection page, you can select a interface to run diagnostic.

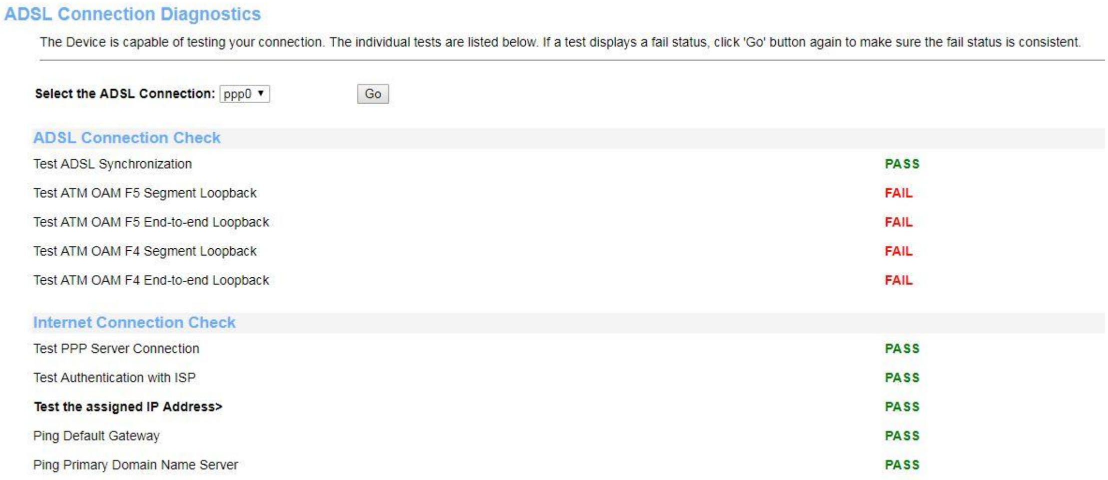


ADSL Connection Diagnostics

The Device is capable of testing your connection. The individual tests are listed below. If a test displays a fail status, click 'Go' button again to make sure the fail status is consistent.

Select the ADSL Connection: ppp0 ▼ Go

Click the “Run Diagnostic Test” button to start the test, and then wait several times later you can see the diagnostic result.



ADSL Connection Diagnostics

The Device is capable of testing your connection. The individual tests are listed below. If a test displays a fail status, click 'Go' button again to make sure the fail status is consistent.

Select the ADSL Connection: ppp0

ADSL Connection Check

Test ADSL Synchronization	PASS
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

Internet Connection Check

Test PPP Server Connection	PASS
Test Authentication with ISP	PASS
Test the assigned IP Address>	PASS
Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS

FAQ

Q: Power LED does not come on after power is switched on.

A:

- Check the outlet by plugging in another electronic device.
- Call the customer service number or return the DSL Router to the vendor.

Q: Internet LED is off.

A:

- Verify that your DSL Router is properly configured for TCP/IP.
- Ensure that the correct network adapter driver is installed for your operating system. If necessary, reinstall the driver.
- Check that the speed of the network adapter or duplex mode has not been configured manually. It is recommended that the adapter be set to auto-negotiation.
- Ensure that the network connection is established before launching the browser.
- In the network connection tab, verify that your username and password are correct.

Q: LAN LED does not come on after connection is established.

A:

- Verify that the power is switched on.
- Ensure that the cable is plugged into the DSL Router and a LAN computer.
- Check the network adapter or the cable connections for defects.

Q: The device cannot access the Internet

A: Run a health check on your device. Use the ping utility to check whether the device can communicate with the DSL Router LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.

If you statically assigned a private IP address to the computer, verify the following:

- Check that the DSL Router IP address on the device is your public IP address. If it is not, correct the address or configure the device to receive IP information automatically.
- Verify with your ISP that the DNS server specified for the computer is valid. Correct the address or configure the device to receive this information automatically.

Q: The LAN devices cannot display web pages on the Internet.

A: Verify that the DNS server IP address specified on the device is correct for your ISP. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the gateway is correct, and then you can use the ping utility to test connectivity with your ISP's DNS server.

Q: I forgot my user ID or password.

A: If you have not changed the password from the default, try using **`admin`** as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the back panel of the DSL Router three times. Then, type the default User ID and password shown above.

Note: Resetting the device removes any custom settings and returns all settings to their default values.

Q: I cannot access the web pages from my browser.

A:

- Use the ping utility to check whether the device can communicate with the xDSL Router LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.
- Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later.
- Verify that the device's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the gateway.

Q: I cannot login to the configuration pages.

A:

- Verify that the username and password are correct.
- Ensure the PC indicator is on and the TCP/IP configuration is correct.
- Ensure the data indicator is on when using Ping command.
- Try resetting the device.

Q: I'm having trouble accessing some web servers.

A:

- The MTU of the operating system might be at or near its maximum.
- The operating system might need to be patched.

Q: Changes to the web pages are not being retained.

A: Be sure to Apply/Save after any changes to the web pages.

11. Certification

FCC

FCC – North American EMI Verification
FCC – Verificación EMI de los estados unidos

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.

NOTE: 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

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

RF Exposure Warning Statements:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment shall be installed and operated with minimum distance 20cm between the radiator & body.