

---

**AirLive 2.5GE XPON ONU**  
**&**  
**AirLive XPON ONU-1GE**  
**USER MANUAL**

airlive®

---

## Contents

Chapter 1	Product Introduction .....	1
1.1	Product Description.....	1
1.2	Special features.....	1
1.3	Technical Parameter.....	2
1.4	Application chart.....	3
1.5	Panel description.....	3
Chapter 2	Quick Installation .....	6
2.1	Standard Packing Contents.....	6
2.2	Quick Installation .....	6
Chapter 3	Configuration .....	8
3.1	Login.....	8
3.2	Status .....	9
3.2.1	Device Information .....	9
3.2.2	Statistics.....	10
3.2.3	Logout.....	11
3.3	Setup.....	11
3.3.1	WAN.....	11
3.3.2	LAN .....	13
3.4	Advanced.....	16
3.4.1	Route .....	16
3.4.2	NAT .....	17
3.4.3	QoS .....	19
3.4.4	CWMP.....	20
3.4.5	VLAN Mapping.....	21
3.4.6	Others .....	21
3.5	Service .....	22
3.5.1	IGMP .....	22

---

3.5.2 UPnP .....	23
3.6 Firewall.....	23
3.6.1 MAC Filtering .....	23
3.6.2 IP/Port Filtering .....	24
3.6.3 URL Filter .....	25
3.6.4 ACL.....	26
3.6.5 DOS Setting.....	28
3.8 Maintenance .....	29
3.8.1 Update .....	29
3.8.2 Password.....	30
3.8.3 Reboot/Restore .....	30
3.8.4 Time .....	31
3.8.5 Log .....	32
3.8.6 Diagnostics.....	32

# Chapter 1 Product Introduction

## 1.1 Product Description

The AirLive 2.5GE XPON ONU (1\*2.5GE+1GE) is specially designed to meet the needs of telecom operators for FTTO (office), FTTD (desktop), FTTH (home), SOHO broadband access, video surveillance, etc. It is based on mature XPON technology, high reliability, easy maintenance, and can provide QoS guarantee for different services. The ONU's 2.5GE network port can fully meet the high access bandwidth requirements of WIFI 6 technology, AR/VR technology, 8K video and other technologies, and can bring fast Internet access experience and lower Internet latency for home users and enterprise users. The AirLive XPON ONU-1GE has the function only without the additional 2.5GE port. The XPON ONU-1GE comes with a single Gigabit RJ-45 port.



Figure 1-1: AirLive 2.5GE XPON ONU (left) & XPON ONU-1GE (right)

## 1.2 Special features

- Integrated auto detecting, auto configuration, and auto firmware upgrade technology.
- Support OAM/OMCI remote configuration and maintenance.
- Support rich VLAN, DHCP Server and IGMP snooping multicast feature.
- Fully compatibility with OLT based on Broadcom/PMC/Cortina chipset.
- Support NAT, Firewall function.
- Support bridge and router mode.

## 1.3 Technical Parameter

Technical items	Descriptions
PON interface	1 G/EPON port (EPON PX20+ and GPON Class B+) Receiving sensitivity: $\leq -28\text{dBm}$ Transmitting optical power: $0\sim+4\text{dBm}$ Transmission distance: 20KM
Wavelength	Tx1310nm, Rx 1490nm
Optical interface	SC/PC connector
Interface (2.5GE XPON ONU)	1* 10/100/1000Mbps and 1* 10/100/1000/2500Mbps auto adaptive Ethernet interfaces. Full /Half Duplex, RJ45 connectors.
Indicator (2.5GE XPON ONU)	5 indicators, SYS, PON, LOS, LAN1~2
Interface (XPON ONU-1GE)	1* 10/100/1000Mbps auto adaptive Ethernet interfaces. Full /Half Duplex, RJ45 connectors.
Indicator (XPON ONU-1GE)	3 indicators, SYS, LINK/ACT, REG.
Operating condition	$-5^{\circ}\text{C}\sim 55^{\circ}\text{C}$ , 10%~90% (non-condensing)
Storing condition	$-30^{\circ}\text{C}\sim 60^{\circ}\text{C}$ , 10%~90% (non-condensing)
Power supply	DC 12V, 0.5A
Power consumption	$\leq 4\text{W}$
Dimension (2.5GE XPON ONU)	100mm*92mm*29.5mm(L*W*H)
Net weight (2.5GE XPON ONU)	0.11Kg
Dimension (XPON ONU-1GE)	82mm*82mm*25mm (L*W*H)
Net weight (XPON ONU-1GE)	0.08Kg

## 1.4 Application chart

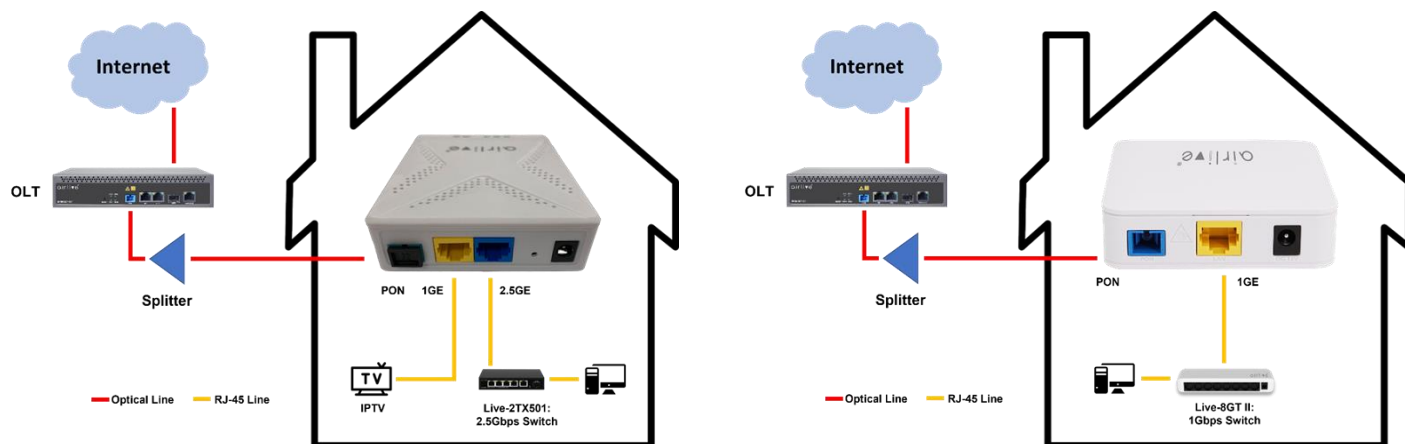


Figure 1-2: Application chart (left 2.5GE model, right 1GE model)

## 1.5 Panel description

### Interface/Button panel 2.5GE XPON ONU

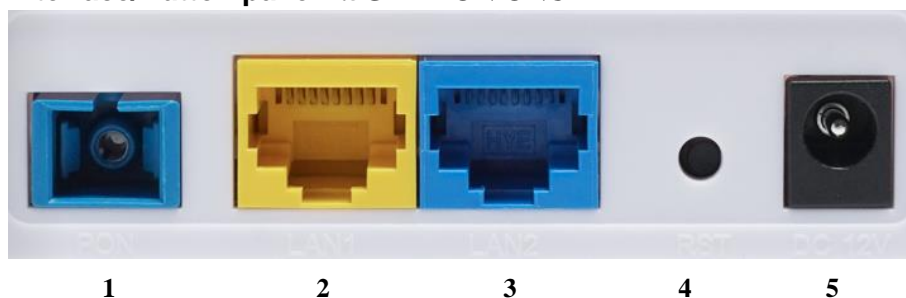


Figure 1-3: Interface/Button panel

Name	Function
1: PON	Connect to OLT by SC type fiber connector, single mode optical fiber cable.
2/3: LAN1/2	The blue LAN2 is a 2.5GbE port and the yellow LAN1 is a 1GE port. Connect to PC or other devices with Ethernet port by Cat5/Cat5E cable, RJ-45 connector.
4: RST	Press RST button over 10 seconds, ONU restores factory default and reboots.
5: DC 12V	Connect with power adapter. DC 12V, 0.5A.

## Indication Panel 2.5GE XPON ONU

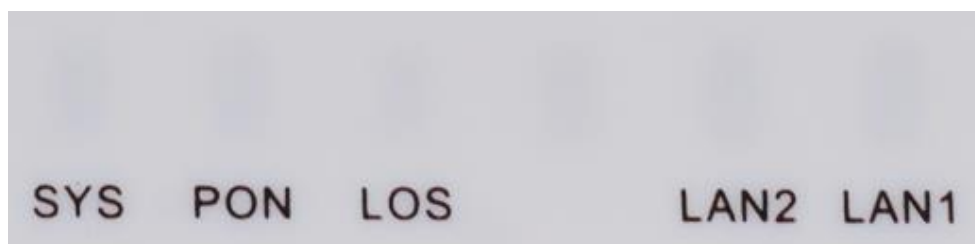


Figure 1-4: Indication panel

LED	Mark	Status	Description
System	SYS	On / Off	System is not running or fatal error.
		Blink	Normal running.
Registration	PON	On	The device is registered to the PON system.
		Off	The device is not registered to the PON system.
		Blink	The device is registering.
Optical signal loss	LOS	Blink	Device does not receive optical signal.
		Off	Device receives optical signal.
LAN	LAN1 LAN2	On	Port is connected properly.
		Off	Port connection exception or not connected.
		Blink	Port is sending or/and receiving data.

## Interface/Button panel XPON ONU-1GE



Figure 1-3: Interface/Button panel

Name	Function
1: PON	Connect to OLT by SC type fiber connector, single mode optical fiber cable.
2: LAN	Connect PC or other devices with Ethernet port by Cat5 cable, RJ-45 connector.
3: DC 12V	Connect with power adapter. DC 12V, 0.5A.
4: RST	Press RST button over 10 seconds, ONU restores factory default and reboot.

## Indication Panel XPON ONU-1GE

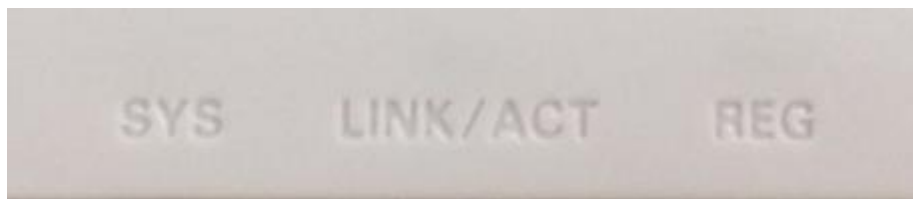


Figure 1-4: Indication panel

LED	Mark	Status	Description
Interface	LINK/ACT	ON	Port is connected properly (LINK).
		Off	Port connection exception or not connected.
		Blink	Port is sending or/and receiving data (ACT).
Registration	REG	ON	<b>Green:</b> The device is registered to PON system.
		OFF	Device has received optical signal and not registered to the PON system.
		Blink	<b>Red:</b> The Device does not receive optical signals.
System	SYS	On / Off	System is not running or fatal error
		Blink	Normal running



## Chapter 2 Quick Installation

### 2.1 Standard Packing Contents

When you receive your product, please check carefully to make sure that the product does not have any defects. If something is wrong with shipping, please contact carrier; other damage or lack of some parts, please contact with dealer.

Contents	Quantity
Dual Mode ONU	1 pcs
Power Adapter	1 pcs
Installation Guide	1 pcs

### 2.2 Quick Installation

1. Connecting the optical fiber cable to the unit.
  - a) Remove the protective cap of the optical fiber.
  - b) Clean the end of the optical fiber with an optical fiber end cleaner.
  - c) Remove the protective cap of the ONU optical interface (PON interface). Connect the fiber to the PON port on the unit.

Note: When measuring the optical power before connecting to the ONU, it is recommended to use a PON Inline Power Meter.

While connecting, please note:

- Keep the optical connector and the optical fiber clean.
  - Make sure there are no tight bends in the fiber and that the bending diameter is greater than 6cm. Otherwise, the optical signal loss may be increased, to the extent that signal may be unavailable.
  - Cover all optic ports and connectors with a protective cap to guard against dust and moisture when the fiber is not used.
2. Apply power to the unit. Push the power button.
  3. After the ONU is power ON, Indicators should light up as for normal operation. Check whether the PON interface status LED (PON) is on continuously. If it is, the connection is normal; otherwise, there is either a problem of the physical connection or the optical level at either end. This may be caused by either too much or too little attenuation over the

optical fiber. Please refer to the Layout Description section of this installation manual for normal LED activity.

4. Check all signal levels and services on all the ONU communication ports.

#### Unit Installation Adjustment

##### Installing the ONU on a horizontal surface (Bench top)

Put the ONU on a clean, flat, sturdy bench top. You must keep the clearance for all sides of the unit to more than 10cm for heat dissipation.

##### Installing the ONU on a vertical surface (Hanging on a wall)

You can install the ONU on a vertical surface by using the mounting holes on the bottom of the ONU chassis and two flat-head wood screws.

- a) Insert the screws into the wall. The screw positions must be in the same horizontal line and the distance between them must be 145mm. Reserved at least 6mm between the screw caps and the wall.
- b) Hang the ONU on the screws through the mounting holes.

## Chapter 3 Configuration

**\*\*Note\*\*** For this guide images of the 2.5GE XPON ONU WEBui were used.

After finishing the basic connection configuration, you can use its basic function. In order to satisfy individuation service requirements, this charter provides the user parameter modification and individuation configuration description.

This model of ONU is designed as SFU (single family unit, bridge mode). When it works on bridge mode, VLAN of LAN port can be configured by OLT. You can also use this model as HGU, you can configure router mode or bridge mode through its web management.

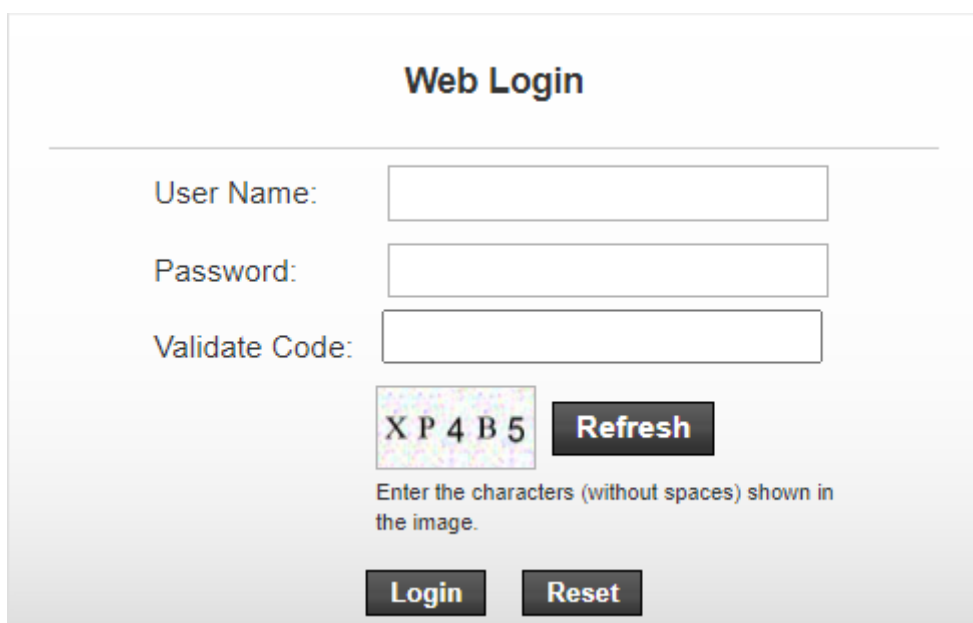
### 3.1 Login

The device is configured by the web interface. The following steps will enable you to login:

1. Conform “Quick Installation” to install.
2. The device default IP is 192.168.1.1.
3. Open your web browser, type the device IP in the address bar.
4. Entry of the username and password will be prompted. Enter the default login username and password.

*By default, Administration level username is "admin", password is "stdONU0i".*

*By default, User level username is "user", password is "user".*



The screenshot displays the 'Web Login' page. It features three input fields: 'User Name:', 'Password:', and 'Validate Code:'. Below the 'Validate Code' field is a CAPTCHA image showing the characters 'X P 4 B 5' and a 'Refresh' button. Below the CAPTCHA is the instruction 'Enter the characters (without spaces) shown in the image.' At the bottom of the form are 'Login' and 'Reset' buttons.

**Figure 3-1: Login**

For security, you will be asked to modify password after you logged in by default password. The new password must meet the requirements that are displayed on the web page. After submitting, it requires you to login by new password.

Please Modify Super User Password

Password must contain at least the following two types of characters:0-9,a-z,A-Z,special characters(.\_@!~#\$\$%^()+=?)

New Password:	<input style="width: 90%;" type="password" value="....."/>
Confirm Password:	<input style="width: 90%;" type="password" value="....."/>

**Figure 3-2: Change Password**

## 3.2 Status

This part shows the main information of the product.

### 3.2.1 Device Information

#### 3.2.1.1 Device Info

This page shows the device basic information, such as Software Version, PON SN, LAN info, WAN info and so on.

Status
Setup
Advanced
Service
Firewall
Maintenance

▶ Device Info

▶ Device Info

▶ PON

▼ Statistics

▼ Logout

### Status

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

System

Alias Name	XPON+1GE+2.5GE
Uptime	7 2:30:58
Date/Time	Sun Jan 8 2:30:58 2012
Firmware Version	V1.1.0
Built Date	Jul 28 2023 19:42:53
Serial Number	004F58000120

CWMP Status

Inform Status	No Inform Send(No cwnp connection)
Connection Request Status	No connection request

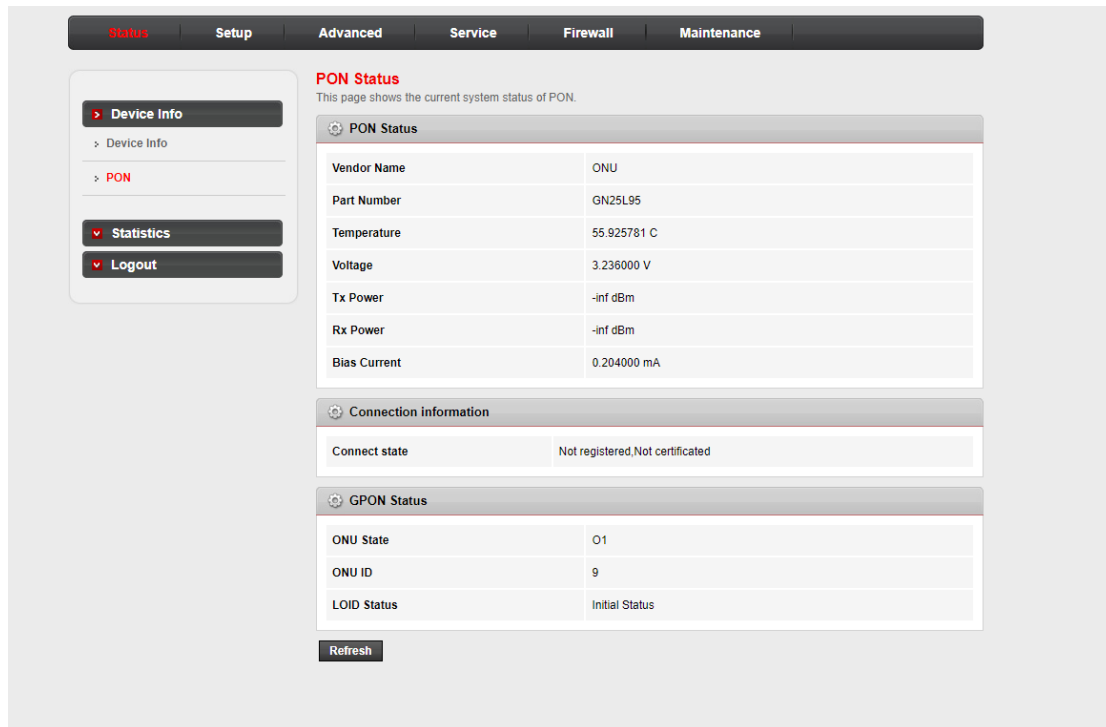
LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IPv6 Address	fe80::1eef:3ff:fe000120
DHCP Server	Enable
MAC Address	00:4F:5B:00:01:20

**Figure 3-3: Device Information**

### 3.2.1.2 PON Status

This page shows the current system status of PON.



**PON Status**  
This page shows the current system status of PON.

PON Status	
Vendor Name	ONU
Part Number	GN25L95
Temperature	55.925781 C
Voltage	3.236000 V
Tx Power	-inf dBm
Rx Power	-inf dBm
Bias Current	0.204000 mA

**Connection information**

Connect state	Not registered,Not certificated
---------------	---------------------------------

**GPON Status**

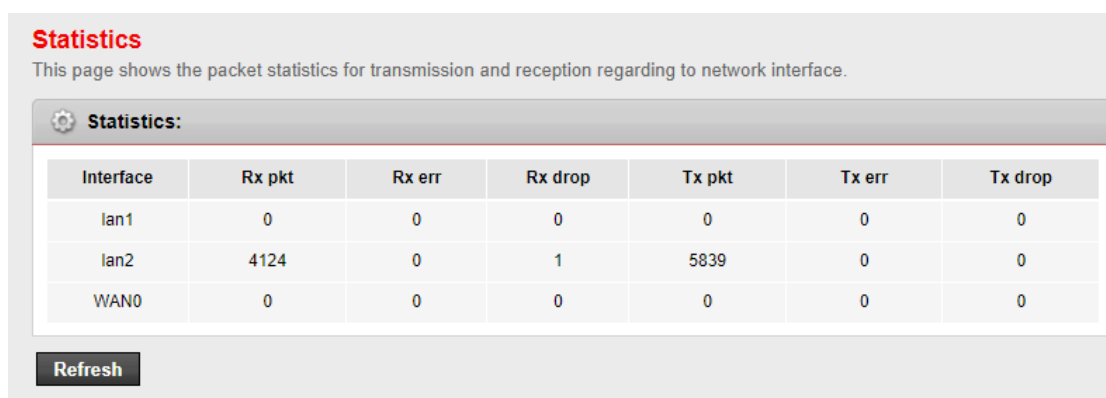
ONU State	O1
ONU ID	9
LOID Status	Initial Status

Refresh

Figure 3-4: PON Status

### 3.2.2 Statistics

This page shows the packet statistics for transmission and reception regarding the network interface.



**Statistics**  
This page shows the packet statistics for transmission and reception regarding to network interface.

**Statistics:**

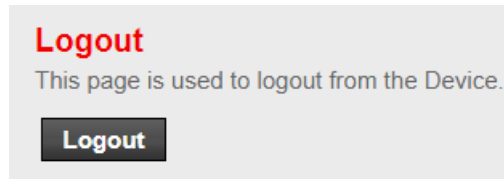
Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
lan1	0	0	0	0	0	0
lan2	4124	0	1	5839	0	0
WAN0	0	0	0	0	0	0

Refresh

Figure 3-4: WAN Connection

### 3.2.3 Logout

This page is used to logout from the Device.



**Figure 3-6: Logout**

## 3.3 Setup

### 3.3.1 WAN

#### 3.3.1.1 WAN Configuration

This page is used to configure the parameters for the WAN interface of the ONU.

Note: When connect type of PPPoE only is "Manual", the "Connect" and "Disconnect" button will be enabled.

### 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.

Default Route Selection:		<input checked="" type="radio"/> Auto	<input type="radio"/> Specified
Channel Mode:	<input type="text" value="Bridge"/>	Enable NAPT:	<input type="checkbox"/>
Enable IGMP:	<input type="checkbox"/>		
VLAN:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable	
VLAN ID(1-4095):	<input type="text"/>	VLAN Cos(0-7):	<input type="text"/>
Multicast VLAN ID(1-4095):	<input type="text"/>		
Application Mode:	<input type="text" value="INTERNET"/>		
PPP Settings:			
User Name:	<input type="text"/>	Password:	<input type="text"/>
Service Name:	<input type="text"/>		
Type:	<input type="text" value="Continuous"/>	Idle Time (min):	<input type="text"/>
WAN IP Settings:			
Type:	<input checked="" type="radio"/> Fixed IP	<input type="radio"/> DHCP	
Local IP Address:	<input type="text"/>	Gateway:	<input type="text"/>
NetMask:	<input type="text"/>		

Figure 3-7: WAN Connection

### 3.3.1.2 PON Settings

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

LOID:	<input type="text" value="123456789"/>
LOID Password:	<input type="text" value="123456"/>
<input type="button" value="Apply Changes"/>	

Figure 3-8: PON Settings

## 3.3.2 LAN

### 3.3.2.1 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...

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:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> Secondary IP	
Mac Based Tag Decision:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<input type="button" value="Apply Changes"/>	

Figure 3-9: LAN Interface Setup

### 3.3.2.2 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 host 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 requests an IP address.



LAN IP Address: 192.168.1.1	Subnet Mask: 255.255.255.0
DHCP Mode:	DHCP Server ▾
IP Pool Range:	192.168.1. 2 - 192.168.1. 254 <span>Show Client</span>
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
Max Lease Time:	1440 minutes
Domain Name:	
DNS Servers:	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
	192.168.1.1

Apply Changes Undo

Set VendorClass IP Range

Figure 3-10: DHCP Mode

### 3.3.2.3 DHCP Static

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.

**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)

Add Delete Selected Undo

⚙️ DHCP Static IP Table:

Select	IP Address	MAC Address
--------	------------	-------------

Figure 3-11: DHCP Static IP Configuration

### 3.3.2.4 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.

The screenshot shows the LAN IPv6 Setting configuration page, organized into three main sections:

- Lan Global Address Setting:** Contains a 'Global Address:' field with two input boxes separated by a slash (/). Below it is an 'Apply Changes' button.
- RA Setting:** Contains several options:
  - 'Enable:' with a checked checkbox.
  - 'M Flag:' with an unchecked checkbox.
  - 'O Flag:' with a checked checkbox.
  - 'Max Interval:' with an input box containing '600' and the unit 'Secs'.
  - 'Min Interval:' with an input box containing '200' and the unit 'Secs'.
  - 'Prefix Mode:' with a dropdown menu set to 'Auto'.
  - 'ULA Enable:' with an unchecked checkbox.
  - 'RA DNS Enable:' with an unchecked checkbox.Below this section is an 'Apply Changes' button.
- DHCPv6 Setting:** Contains:
  - 'DHCPv6 Mode:' with a dropdown menu set to 'Auto Mode'.
  - 'IPv6 Address Suffix Pool:' with two input boxes containing '::1' and '::ffff', separated by a hyphen (-), and a note '(ex. ::1:1:1:1 or ::1)'.
  - 'IPv6 DNS Mode:' with a dropdown menu set to 'Auto'.Below this section is an 'Apply Changes' button.

Figure 3-12: DHCP IPv6 Setting

## 3.4 Advanced

### 3.4.1 Route

#### 3.4.1.1 Static Route

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

**Routing Configuration**

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

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text" value="1"/>
Interface:	<input type="text" value="v"/>

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
--------	-------	-------------	-------------	---------	--------	-----

Figure 3-13: Routing Configuration

#### 3.4.1.2 IPv6 Static Route

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

**IPv6 Routing Configuration**

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

Destination:	<input type="text"/>
Prefix Length:	<input type="text"/>
Next Hop:	<input type="text"/>
Interface:	<input type="text" value="v"/>

IPv6 Static Route Table:

Select	Destination	NextHop	Interface
--------	-------------	---------	-----------

Figure 3-14: IPv6 Routing Configuration

## 3.4.2 NAT

### 3.4.2.1 DMZ

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

**DMZ**

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:	<input type="text"/>

**Apply Changes** **Reset**

⚙️ **Current DMZ Table:**

Select	WAN Interface	DMZ IP
--------	---------------	--------

**Delete Selected**

Figure 3-15: DMZ

### 3.4.2.2 Virtual Server

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

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

<b>Service Type:</b>	
<input checked="" type="radio"/> Usual Service Name:	AUTH ▾
<input type="radio"/> User-defined Service Name:	<input type="text"/>
<b>Protocol:</b>	TCP ▾
<b>WAN Setting:</b>	Interface ▾
<b>WAN Interface:</b>	any ▾
<b>WAN Port:</b>	113 (ex. 5001:5010)
<b>LAN Open Port:</b>	113
<b>LAN Setting:</b>	Ip Address ▾
<b>LAN IP Address:</b>	<input type="text"/>

**Apply Changes**

**Current Virtual Server Forwarding Table:**

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

Figure 3-16: Virtual Server

### 3.4.2.3 ALG

Setup NAT ALG and Pass-Through configuration

**NAT ALG and Pass-Through**  
Setup NAT ALG and Pass-Through configuration

<b>IPSec Pass-Through:</b>	<input checked="" type="checkbox"/> Enable
<b>L2TP Pass-Through:</b>	<input checked="" type="checkbox"/> Enable
<b>PPTP Pass-Through:</b>	<input checked="" type="checkbox"/> Enable
<b>FTP:</b>	<input checked="" type="checkbox"/> Enable
<b>H.323:</b>	<input checked="" type="checkbox"/> Enable
<b>SIP:</b>	<input checked="" type="checkbox"/> Enable
<b>RTSP:</b>	<input checked="" type="checkbox"/> Enable

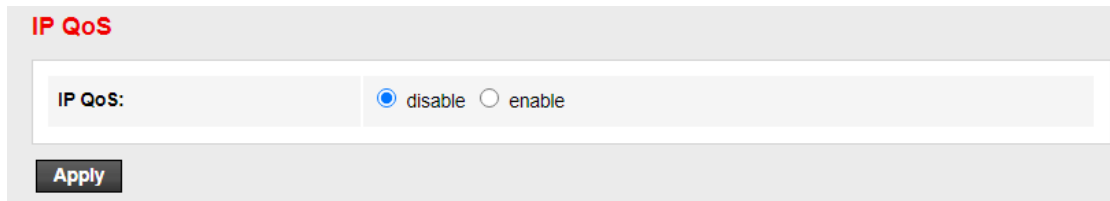
**Apply Changes** **Reset**

Figure 3-17: ALG

### 3.4.3 QoS

#### 3.4.3.1 QoS

This page allows user to set QoS rules.

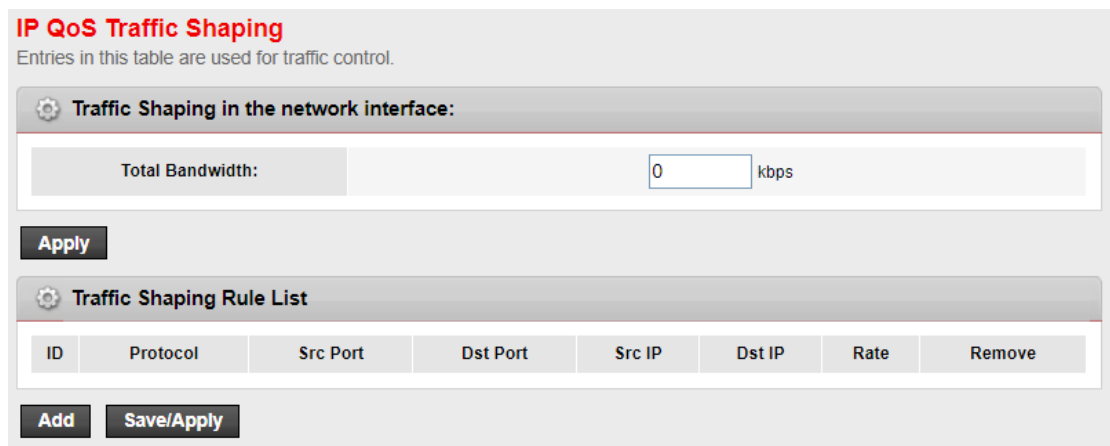


The screenshot shows the 'IP QoS' configuration page. It features a header 'IP QoS' in red. Below it is a form with a label 'IP QoS:' and two radio buttons: 'disable' (selected) and 'enable'. At the bottom of the form is an 'Apply' button.

Figure 3-18: QoS Configuration

#### 3.4.3.2 Traffic Shaping

Entries in this table are used for traffic control.



The screenshot shows the 'IP QoS Traffic Shaping' configuration page. It has a header 'IP QoS Traffic Shaping' in red and a sub-header 'Traffic Shaping in the network interface:'. Below this is a 'Total Bandwidth:' label and a text input field containing '0' followed by 'kbps'. An 'Apply' button is below. The next section is 'Traffic Shaping Rule List', which contains a table with the following columns: ID, Protocol, Src Port, Dst Port, Src IP, Dst IP, Rate, and Remove. At the bottom are 'Add' and 'Save/Apply' buttons.

ID	Protocol	Src Port	Dst Port	Src IP	Dst IP	Rate	Remove
----	----------	----------	----------	--------	--------	------	--------

Figure 3-19: IP QoS Traffic Shaping

### 3.4.4 CWMP

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

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

<b>ACS:</b>	
Enable:	<input checked="" type="checkbox"/>
URL:	<input type="text" value="http://172.21.70.44/cpe/?pd128"/>
User Name:	<input type="text" value="rtk"/>
Password:	<input type="text" value="rtk"/>
Periodic Inform Enable:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Periodic Inform Interval:	<input type="text" value="300"/> seconds

<b>Connection Request:</b>	
User Name:	<input type="text" value="rtk"/>
Password:	<input type="text" value="rtk"/>
Path:	<input type="text" value="/tr069"/>
Port:	<input type="text" value="7547"/>

<b>Debug:</b>	
ACS Certificates CPE:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Show Message:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
CPE Sends GetRPC:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Skip MReboot:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Delay:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Auto-Execution:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

<b>Certificate Management:</b>	
CPE Certificate Password:	<input type="text" value="client"/> <input type="button" value="Apply"/> <input type="button" value="Undo"/>
CPE Certificate:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/>
CA Certificate:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/>

Figure 3-20: TR-069 Configuration MAC Filter

### 3.4.5 VLAN Mapping


This page is used to configure VLAN binding for Lan ports.

**VLAN Binding Configuration**  
This page is used to configure vlan binding for lan ports.

Port Binding ▼

**Apply Changes**

**Vlan Binding Table:**

Port	Binding Mode	VLAN Binding	Modify
LAN1	Port Binding		

**Figure 3-21: VLAN Binding Configuration**

### 3.4.6 Others

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

**Tunnel Configuration**  
This page is used to configure v6inv4 tunnel or v4inv6 tunnel.

**DS-Lite Tunnel:**

Enable:

Interface: ▼ (Only support IPv6 Wan Interface)

Mode: Auto ▼

**Apply Changes**

**Figure 3-22: Tunnel Configuration**



## 3.5 Service

### 3.5.1 IGMP

#### 3.5.1.1 IGMP Proxy

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:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast Allowed:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Robust Count:	<input type="text" value="2"/>
Last Member Query Count:	<input type="text" value="2"/>
Query Interval:	<input type="text" value="60"/> (seconds)
Query Response Interval:	<input type="text" value="100"/> (*100ms)
Group Leave Delay:	<input type="text" value="2000"/> (ms)

**Apply Changes** **Undo**

Figure 3-23: IGMP Proxy

#### 3.5.1.2 MLD

MLD Proxy and Snooping can be configured here.

**MLD Configuration**  
MLD Proxy and Snooping can be configured here.

MLD proxy:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Robust Counter:	<input type="text" value="2"/>
Query Interval:	<input type="text" value="125"/> (Second)
Query Response Interval:	<input type="text" value="10000"/> (millisecond)
Response Interval of Last Group Member:	<input type="text" value="1"/> (Second)

**Apply Changes** **Cancel**

Figure 3-24: MLD Configuration

## 3.5.2 UPnP

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

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

UPnP:  Disable  Enable

WAN Interface:

Apply Changes

Figure 3-25: UPnP Configuration

## 3.6 Firewall

### 3.6.1 MAC Filtering

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

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

MAC Address:  (ex. 00E086710502)

Add

Current MAC Filter Table:

Select	MAC Address

Delete Delete All

Figure 3-26: MAC Filtering

## 3.6.2 IP/Port Filtering

### 3.6.2.1 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to the Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network. This page allows user to set web page login timeout. If don't operate the web page for the time out, the account will logout automatically.

**Default Policy**       Permit    Deny

<b>Rule Action:</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny		
<b>Protocol:</b>	ICMP ▾		
<b>Source IP Address:</b>	<input type="text"/>	<b>Mask Address:</b>	<input type="text" value="255.255.255.255"/>
<b>Dest IP Address:</b>	<input type="text"/>	<b>Mask Address:</b>	<input type="text" value="255.255.255.255"/>
<b>SPort:</b>	<input type="text"/> - <input type="text"/>	<b>DPort:</b>	<input type="text"/> - <input type="text"/>
<b>Enable:</b>	<input checked="" type="checkbox"/>		

**Current Filter Table:**

Rule	WanIf	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Action
------	-------	----------	----------------	-------	--------------	-------	-------	--------

**Figure 3-27: IP/Port Filtering**

### 3.6.2.2 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.

**Default Action**     Permit    Deny

**Apply Changes**    **Reset**

**Rule Action:**     Permit    Deny

**Protocol:**   

**Source IPv6 Address:**   

**Dest IPv6 Address:**   

**SPort:**     -     **DPort:**     -

**Enable:**

**Apply Changes**

**Current Filter Table:**

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

Figure 3-28: IPv6/Port Filtering

### 3.6.3 URL Filter

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

**URL Blocking Configuration**

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

**URL Blocking Capability:**     Disable    Enable

**Apply Changes**

**Keyword:**

**AddKeyword**    **Delete Selected Keyword**

**URL Blocking Table:**

Select	Filtered Keyword

Figure 3-29: URL Blocking Configuration

## 3.6.4 ACL

### 3.6.4.1 ACL

You can specify which services are accessible from 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.

Use of such access control can be helpful in securing or restricting the Gateway management.

**ACL Configuration**

You can specify which services are accessible 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 management.

**LAN ACL Mode:**  White List  Black List

**WAN ACL Mode:**  White List  Black List

**Direction Select:**  LAN  WAN

**LAN ACL Switch:**  Enable  Disable

**IP Address:**  -  (The IP 0.0.0.0 represent any IP )

**Services Allowed:**

Any

**Current ACL Table:**

Select	Direction	IP Address/Interface	Service	Port	Action
0	LAN	0.0.0.0	ping	--	<input type="button" value="Delete"/>
1	LAN	0.0.0.0	web	80	<input type="button" value="Delete"/>

**Figure 3-30: ACL**

### 3.6.4.2 IPv6 ACL

You can specify which services are accessible from 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.

Use of such access control can be helpful in securing or restricting the Gateway management. This page allows the user to set port mirror for troubleshooting. After configuring port mirror, the traffic of the WAN connection will be copied and sent to the LAN port.

**Direction Select:**      LAN     WAN

**LAN ACL Switch:**      Enable      Disable

**IP Address:**      /

**Services Allowed:**  
 Any

**Current IPv6 ACL Table:**

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	<input type="button" value="Delete"/>

**Figure 3-31: IPv6 ACL**

### 3.6.5 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.

<input checked="" type="checkbox"/> Enable DoS Prevention	
<input checked="" type="checkbox"/> Whole System Flood: SYN	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Whole System Flood: FIN	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Whole System Flood: UDP	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Whole System Flood: ICMP	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Per-Source IP Flood: SYN	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Per-Source IP Flood: FIN	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Per-Source IP Flood: UDP	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> Per-Source IP Flood: ICMP	<input type="text" value="100"/> Packets/Second
<input checked="" type="checkbox"/> TCP/UDP PortScan	<input type="text" value="Low"/> Sensitivity
<input checked="" type="checkbox"/> ICMP Smurf	
<input checked="" type="checkbox"/> IP Land	
<input checked="" type="checkbox"/> IP Spoof	
<input checked="" type="checkbox"/> IP TearDrop	
<input checked="" type="checkbox"/> PingOfDeath	
<input checked="" type="checkbox"/> TCP Scan	
<input checked="" type="checkbox"/> TCP SynWithData	
<input checked="" type="checkbox"/> UDP Bomb	
<input checked="" type="checkbox"/> UDP EchoChargen	
<input type="button" value="Select ALL"/>	<input type="button" value="Clear ALL"/>
<input type="checkbox"/> Enable Source IP Blocking	<input type="text" value="300"/> Block time (sec)
<input type="button" value="Apply Changes"/>	

Figure 3-32: DOS Setting

## 3.8 Maintenance

### 3.8.1 Update

#### 3.8.1.1 Upgrade Firmware

This page allows you to upgrade the Router firmware to a 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.

**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

Figure 3-33: Upgrade Firmware

#### 3.8.1.2 Backup/Upload 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.

**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

Figure 3-34: Backup/Upload Settings

#### 3.8.1.3 Upload Logo

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

**Upgrade Logo**

This page allows you upgrade logo. Please note, do not power off the device during the upload because it may crash the system.

Select File:  No file chosen

Figure 3-35: Upgrade Logo



## 3.8.2 Password

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

**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:	<input type="text"/>
Privilege:	User ▾
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

**Add** **Modify** **Delete** **Reset**

⚙️ User Account Table:

Select	User Name	Privilege
<input type="radio"/>	admin	root
<input type="radio"/>	user	user

Figure 3-36: User Account Configuration

## 3.8.3 Reboot/Restore

### 3.8.3.1 Reboot/Restore

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

**Reboot**

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

**Reboot** **Restore to Default Setting**

Figure 3-37: Reboot

### 3.8.3.2 Reset Button Configuration

This page is used to configure the reset button state.

**Reset Button Configuration**  
This page is used to configure reset button state.

<b>Reset Button Enable:</b>	<input checked="" type="checkbox"/>
-----------------------------	-------------------------------------

**Apply Changes**

**Figure 3-38: Reset Button Configuration**

### 3.8.4 Time

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 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.

<b>System Time:</b>	<input type="text" value="2012"/> Year <input type="text" value="Jan"/> Month <input type="text" value="2"/> Day <input type="text" value="16"/> Hour <input type="text" value="2"/> min <input type="text" value="23"/> sec
<b>DayLight:</b>	<input type="text" value="LocalTIME"/>

**Apply Changes**   **Reset**

**NTP Configuration:**

<b>State:</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Server:</b>	<input type="text"/>
<b>Server2:</b>	<input type="text"/>
<b>Interval:</b>	Every <input type="text" value="1"/> hours
<b>Time Zone:</b>	<input type="text" value="(GMT) Gambia, Liberia, Morocco, England"/>
<b>GMT time:</b>	Mon Jan 2 16:23 2012

**Apply Changes**   **Reset**

<b>NTP Start:</b>	<input type="button" value="Get GMT Time"/>
-------------------	---

**Figure 3-39: System Time Configuration**

### 3.8.5 Log

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.

**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:

Apply Changes
Reset

**Event log Table:**

Old




New

Time	Index	Type	Log Information
Page: 1/1			

Figure 3-40: Log Configuration

### 3.8.6 Diagnostics

#### 3.8.6.1 Ping Diagnostic

**Ping Diagnostic**

Host:

Interface:

PING

Figure 3-41: Ping Diagnostic

#### 3.8.6.2 IPv6 Ping Diagnostic

**Ping6 Diagnostic**

Host:

Interface:

PING

Figure 3-42: IPv6 Ping Diagnostic

### 3.8.6.3 TraceRoute Diagnostic

**Traceroute Diagnostic**

Host :	<input type="text"/>	NumberOfTries :	<input type="text" value="3"/>
Timeout :	<input type="text" value="5000"/> ms	Datasize :	<input type="text" value="38"/> Bytes
DSCP :	<input type="text" value="0"/>	MaxHopCount :	<input type="text" value="30"/>
Interface :	<input type="text" value="any"/> ▾		

Figure 3-43: TraceRoute Diagnostic

### 3.8.6.4 IPv6 TraceRoute Diagnostic

**Traceroute6 Diagnostic**

Host :	<input type="text"/>	NumberOfTries :	<input type="text" value="3"/>
Timeout :	<input type="text" value="5000"/> ms	Datasize :	<input type="text" value="38"/> Bytes
MaxHopCount :	<input type="text" value="30"/>	Interface :	<input type="text" value="any"/> ▾

Figure 3-44: IPv6 TraceRoute Diagnostic

### 3.8.6.5 Loop Detection

This page is used to configure loop detection parameters. Here you can change the settings or view loop detect status.

#### Loop Detection

This page is used to configure loop detection parameters. Here you can change the settings or view loop detect status.

Loop Detection Enable:	<input type="checkbox"/>
Detection Interval:	<input type="text" value="5"/> (1-60)seconds
Recovery Interval:	<input type="text" value="300"/> (10 ~ 1800)seconds
Ethernet Type:	0x <input type="text" value="FFFA"/>
VLAN ID:	<input type="text" value="0"/>

seperate by ",", 0 represents untagged, ex. 0,45,46

**Apply Changes**

#### Loop Detection Status:

Port	Status
LAN1	No Loop

Figure 3-45: Loop Detection