

TP-LINK®

User Guide

TX-VG1530

N300 Wireless VoIP GPON Router



COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **TP-LINK**[®] is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2014 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

<http://www.tp-link.com>

FCC STATEMENT



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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

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.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or tv interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning



This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux normes CNR exemptes de licence d'Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes:

(1) cet appareil ne doit pas provoquer d'interférences et

(2) cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Industry Canada Statement

Complies with the Canadian ICES-003 Class B specifications.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with RSS 210 of Industry Canada. This Class B device meets all the requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la Classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice& BSMI Notice

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

減少電磁波影響，請妥適使用。



Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.



Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.

This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA	US		

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **N300 Wireless VoIP GPON Router**

Model No.: **TX-VG1530**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

The above product is in conformity with the following standards or other normative documents

EN 300 328 V1.8.1

EN 301 489-1 V1.9.2 & EN 301 489-17 V2.2.1

EN 55022: 2010 + AC: 2011

EN 55024: 2010

EN 61000-3-2: 2006 + A1: 2009 + A2: 2009

EN 61000-3-3: 2013

EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011

EN 50385: 2002

The product carries the CE Mark:

CE 1588

Person responsible for marking this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue: 2014

TP-LINK TECHNOLOGIES CO., LTD

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park,
Shennan Rd, Nanshan, Shenzhen, China

CONTENTS

Package Contents	1
Chapter 1. Product Overview	2
1.1 Overview of the GPON router	2
1.2 Main Features	3
1.3 Panel Layout	4
1.3.1 The Front Panel	4
1.3.2 The Back Panel	5
Chapter 2. Connecting the GPON Router	7
2.1 System Requirements	7
2.2 Installation Environment Requirements	7
2.3 Connecting the GPON router	8
Chapter 3. Quick Installation Guide	10
3.1 TCP/IP Configuration	10
3.2 Quick Installation Guide	11
Chapter 4. Configuring the GPON Router	16
4.1 Login	16
4.2 Status	16
4.3 PON	17
4.3.1 Connect Status	18
4.3.2 Optical Status	18
4.3.3 Statistics	19
4.3.4 Advance	19
4.4 Network	20
4.4.1 WAN Settings	21
4.4.2 LAN Settings	29
4.4.3 IPv6 LAN Settings	30
4.4.4 MAC Clone	32
4.4.5 ALG Settings	32
4.4.6 Auto Vlan	33
4.4.7 GPON SN Settings	33
4.4.8 GPON CTC Settings	34

4.4.9	IPSec VPN	35
4.5	DHCP Server	38
4.5.1	DHCP Settings	38
4.5.2	Clients List.....	39
4.5.3	Address Reservation.....	40
4.5.4	Conditional Pool	41
4.6	Wireless.....	42
4.6.1	Basic Settings	42
4.6.2	WPS Settings	44
4.6.3	Wireless Security	46
4.6.4	Wireless Schedule	49
4.6.5	Wireless MAC Filtering	50
4.6.6	Wireless Advanced	51
4.6.7	Wireless Status	53
4.7	Guest Network	53
4.7.1	Basic Settings	53
4.7.2	Guest Network Status	55
4.8	Voice.....	55
4.8.1	SIP Account	55
4.8.2	Dial Map	57
4.8.3	Dial Plan.....	58
4.8.4	Phone Setup	61
4.8.5	Advanced Setup.....	63
4.8.6	Speed Dial.....	64
4.8.7	Call Log	65
4.8.8	Call Firewall.....	66
4.8.9	USB Voice Mail	68
4.9	USB Settings	70
4.9.1	USB Mass Storage	70
4.9.2	User Accounts.....	71
4.9.3	Storage Sharing	72
4.9.4	FTP Server.....	73
4.9.5	Media Server.....	75
4.9.6	Print Server	76
4.10	Route Settings	77
4.10.1	Default Gateway	77

4.10.2 Static Route	77
4.10.3 RIP Settings.....	78
4.11 IPv6 Route Settings	79
4.11.1 IPv6 Default Gateway.....	79
4.11.2 IPv6 Static Route.....	79
4.12 Forwarding.....	80
4.12.1 Virtual Servers	81
4.12.2 Port Triggering	82
4.12.3 DMZ	84
4.12.4 UPnP	85
4.13 Parental Control	85
4.14 Firewall	87
4.14.1 Rule	87
4.14.2 LAN Host	88
4.14.3 WAN Host.....	89
4.14.4 Schedule.....	90
4.15 IPv6 Firewall	91
4.15.1 IPv6 Rule	92
4.15.2 IPv6 LAN Host	93
4.15.3 IPv6 WAN Host.....	94
4.15.4 IPv6 Schedule.....	94
4.16 IPv6 Tunnel.....	95
4.17 Quality of Service	98
4.17.1 Basic Settings	98
4.17.2 SP/WRR Settings	99
4.17.3 Bandwidth Control	103
4.18 IP&MAC Binding	104
4.18.1 Binding Settings.....	104
4.18.2 ARP List.....	105
4.19 Dynamic DNS	105
4.20 Diagnostic.....	106
4.21 System Tools	107
4.21.1 System Log.....	107
4.21.2 Time Settings.....	108
4.21.3 Manage Control	109
4.21.4 CWMP Settings	110

4.21.5 SNMP Settings	110
4.21.6 Backup & Restore.....	111
4.21.7 Factory Defaults.....	112
4.21.8 Firmware Upgrade.....	112
4.21.9 Reboot	113
4.21.10 Statistics.....	114
4.22 Logout.....	115
Appendix A: Specifications	116
Appendix B: Troubleshooting	117
Appendix C: Telephony Features.....	120
Appendix D: Telephone Operation.....	122
Appendix E: Technical Support	125

Package Contents

The following contents should be found in your package:

- One TX-VG1530 N300 Wireless VoIP GPON Router
- One Power Adapter for TX-VG1530 N300 Wireless VoIP GPON Router
- Quick Installation Guide
- One RJ45 cable
- One Resource CD for TX-VG1530 N300 Wireless VoIP GPON Router, including:
 - This User Guide
 - Other Helpful Information

 Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1. Product Overview

Thank you for choosing the **TX-VG1530 N300 Wireless VoIP GPON Router**.

1.1 Overview of the GPON router

TP-LINK's N300 Wireless VoIP GPON Router TX-VG1530 is a next-generation Gigabit Passive Optical Network (GPON) integrated access device (IAD), ideal for Fiber to The Home solution. It's an incredibly robust all-in-one device allowing users to access high-speed internet connection via GPON port and share it wirelessly at 300Mbps wireless 802.11n speeds. Its two FXS ports for connecting to regular telephones, allow users to make economical VoIP calls. TX-VG1530 provides a perfect terminal solution and future-oriented service supporting capabilities for FTTH deployment.

1.2 Main Features

- All-in-One: High speed GPON ONT, NAT Router, 4-port Switch, Wireless N Access Point and VoIP Gateway in one device provides a one-stop networking solution.
- Complies with ITU G.984.1, ITU G.984.2, ITU G.984.3 and ITU G.984.4, providing you comprehensive GPON network compatibility.
- Extremely high access speed up to 2.488Gbps Downstream and 1.244Gbps Upstream.
- Wireless N speed up to 300Mbps makes it ideal for heavy bandwidth consuming or interruption sensitive applications like online gaming, Internet calls and even the HD video streaming.
- Full gigabit ports ensure ultimate transfer speeds.
- USB 2.0 port convenient for users sharing files over the network or the Internet through the router's FTP server.
- Built-in media server allows users to play music, video and view photos with Windows media player, PS3® or X-Box 360®.
- Built-in print server supports wireless printing from different computers by connecting a USB Printer to the router.
- Built-in Voice Mailbox ensures that you never miss a VoIP call.
- Two phone ports provide you cost-effective VoIP phone calls.
- Various call features such as caller ID, call waiting, call holding, call forwarding, 3-way conference calls and voicemail.
- Built-in IGMP snooping and proxy combined with 802.1Q VLAN(Virtual LAN) provide a smooth IPTV experience.
- Supports OMCI (ONT Management Control Interface) remote management.

1.3 Panel Layout

1.3.1 The Front Panel



Figure 1-1

The router's LEDs are located on the front panel (View from left to right). They indicate the device's working status. For details, please refer to LED Explanation.

LED Explanation:

Name	Colour	Status	Indication
 (Power)	Green	On	The GPON router is powered on.
		Off	The GPON router is off. Please ensure that the power adapter is connected correctly.
 (PON)	Green	On	The ONT GPON is registered and the link is activated.
		Flash	The ONT is trying to be registered or set up the connection.
		Off	The ONT is not discovered and registered.
 (LOS)	Red	On	The Tx power of the ONT is off.
		Flash	The ONU receives the optical power low. Please refer to Note for troubleshooting.
		Off	The ONU receives the optical power normally.
 (USB)	Green	On	A storage device or printer has connected to the USB port.
		Flash	The GPON router is sending or receiving data over this USB port.
		Off	No storage device or printer is plugged into the USB port.
 (LAN1-4)	Green	On	There is a device connected to this LAN port.
		Flash	The GPON router is sending or receiving data over this LAN port.
		Off	There is no device connected to this LAN port.
 (WLAN)	Green	Flash	Wireless is enabled.
		Off	Wireless is disabled.

🔒 (WPS)	Green	On	A wireless device has been successfully added to the network by WPS function.
		Flash	WPS handshaking is in process and will continue for about 2 minutes. Please press the WPS button on other wireless devices that you want to add to the network while the LED is flashing.
		Off	A wireless device has failed to be added to the network by WPS function. Please refer to 4.6.2 WPS Settings for more information.
☎ (Phone1-2)	Green	On	The phone connected is registered but not in use.
		Flash	The phone is in use.
		Off	There is no connection or the phone connected is not registered.

 Note:

If the LOS LED is flash, please check your Internet connection first. Refer to [2.3 Connecting the GPON Router](#) for more information about how to make Internet connection correctly. If you have already made a right connection, please contact your ISP to make sure if your Internet service is available now.

1.3.2 The Back Panel

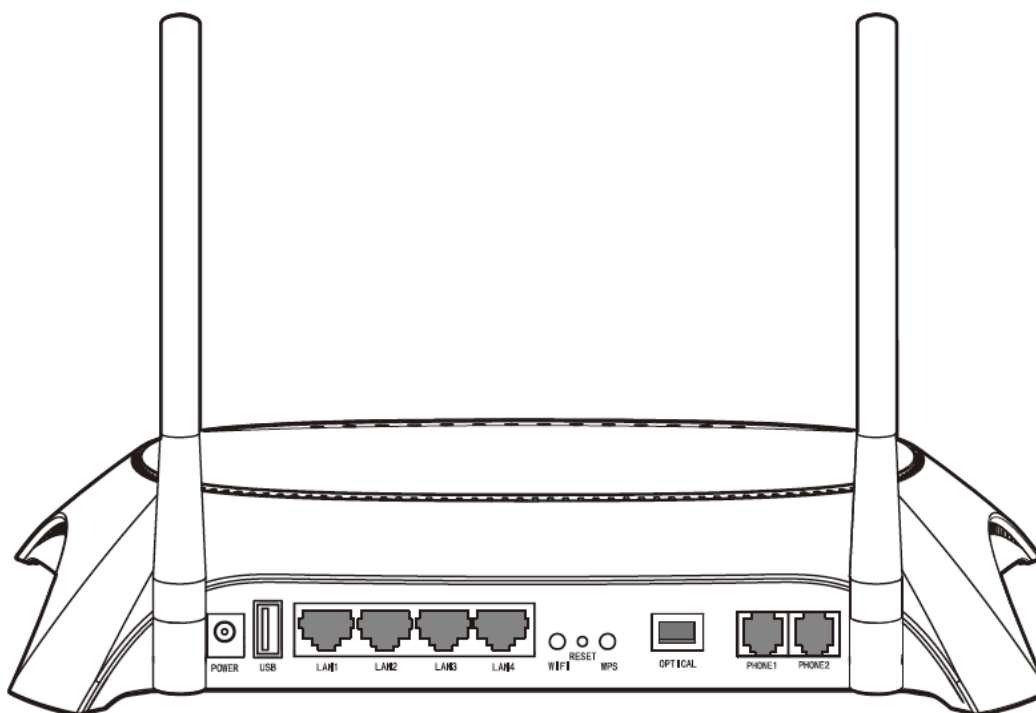


Figure 1-2

- **ON/OFF:** The switch for the power. (The ON/OFF Button is located on the side panel).
- **POWER:** The Power plug is where you will connect the power adapter.

- **USB:** The USB port connects to a USB storage device or a USB printer.
- **LAN1, LAN2, LAN3, LAN4:** Through these ports, you can connect the Router to your PC or the other Ethernet network devices.
- **WiFi:** The switch for the WiFi function.
- **RESET:** There are two ways to reset the Router's factory defaults.

Method one: With the Router powered on, use a pin to press and hold the Reset button for at least 6 seconds. And the Router will reboot to its factory default settings.

Method two: Restore the default setting from "Maintenance-SysRestart" of the Router's Web-based Utility.
- **WPS:** The switch for the WPS function. For details, please refer to [4.6.2 WPS Settings](#).
- **Optical:** Through the port, you can connect the GPON router with a fiber.
- **PHONE1/PHONE2:** The phone port connects to a phone set.
- **Antennas:** Used for wireless operation and data transmit.

Chapter 2. Connecting the GPON Router

2.1 System Requirements

- Broadband Internet Access Service (Fiber).
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

2.2 Installation Environment Requirements

- The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- The Router can be placed on a shelf or desktop.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

Generally, TX-VG1530 is placed on a horizontal surface. The device also can be mounted on the wall as shown in Figure 2-1.

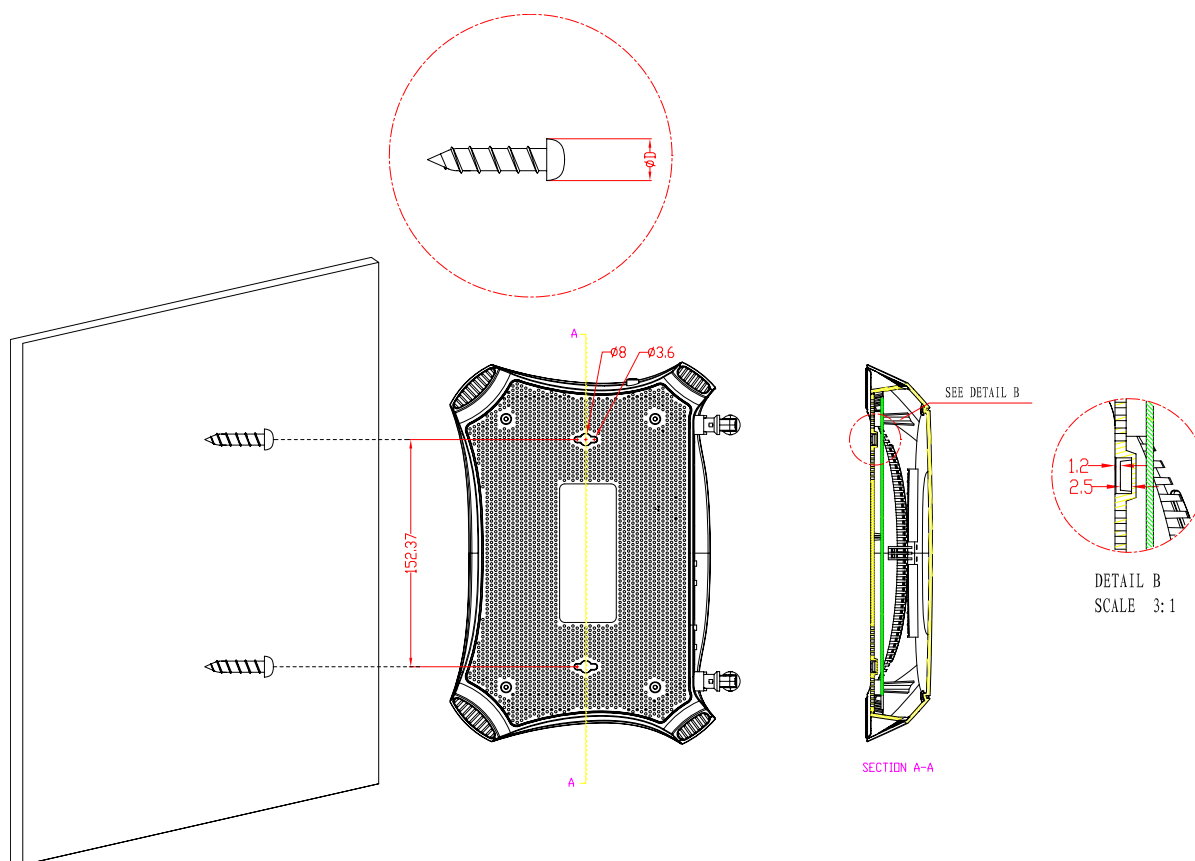


Figure 2-1 Wall-mount Install

 Note:

The diameter of the screw, 3.6mm<D<8mm, and the distance of two screws is 152.37mm. The screw that project from the wall need around 4mm based, and the length of the screw need to be at least 20mm to withstand the weight of the product.

2.3 Connecting the GPON router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.

Step 1: Connect the Fiber to the optical port of the GPON router TX-VG1530.

Step 2: Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the GPON router TX-VG1530.

Step 3: Connect your telephone to the Port labeled "PHONE 1/2" on the GPON router with a telephone line.

If you want to share files or use the USB Voice Mail function, please plug an external USB hard drive/USB flash disk into the USB port. To use the printer function, please connect a USB printer to the USB port.

To use USB Voice Mail function, please make sure the free space of the plugged external USB hard drive/USB flash disk is more than 4MB.

Step 4: Power on the computers and LAN devices.

Step 5: Attach the power adapter. Connect the power adapter to the power connector on the rear of the device and plug in the adapter to an electrical outlet or power extension. The electrical outlet shall be installed near the device and shall be easily accessible.

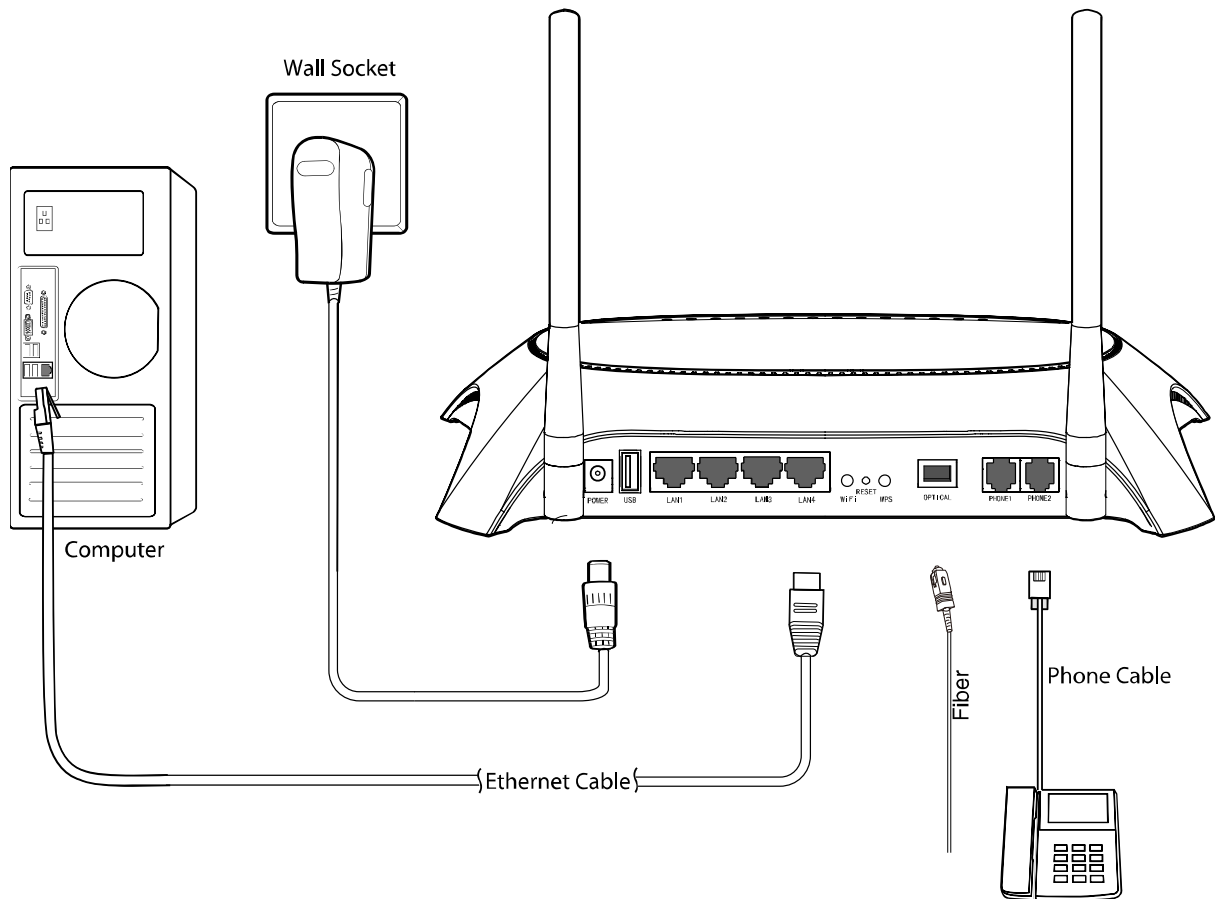


Figure 2-2

Note:

Only green SC/APC interface suits the OPTICAL port.

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TX-VG1530 N300 Wireless VoIP GPON Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the TX-VG1530 N300 Wireless VoIP GPON Router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the local PC to the LAN/WAN port of the GPON router. And then you can configure the IP address for your PC in the following way.

- Obtain an IP address automatically
 - 1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. If you need instructions as to how to do this, please refer to **T3** in [Appendix B: Troubleshooting](#).
 - 2) Then the built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd or command** in the field and press **Enter**. Type **ping 192.168.1.1** on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the router has been established.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

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

Figure 3-1

If the result displayed is similar to the screen shown below, it means that your PC has not connected to the router.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3-2

You can check it following the steps below:

1) Is the connection between your PC and the router correct?

The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

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

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

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TX-VG1530 N300 Wireless VoIP GPON Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type the default address `http://192.168.1.1` in the address field of the browser.



Figure 3-3

After a moment, a login window will appear, similar to the Figure 3-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **Login** button or press the **Enter** key.



Figure 3-4

Note:

If the above screen does not pop up, it means that your Web-browser has been set to a proxy. Go to **Tools** menu→**Internet Options**→**Connections**→**LAN Settings**, in the screen that appears, cancel the Using Proxy checkbox, and click **OK** to finish it.

2. After your successful login, you will see the Login screen as shown in Figure 3-5.

Status	Basic Status					
Pon						
Network						
DHCP Server						
Wireless						
Guest Network						
Voice						
USB Settings						
Route Settings						
IPv6 Route Settings						
Forwarding						
Parent Control						
Firewall						
IPv6 Firewall						
IPv6 Tunnel						
Quality of Service						
IP & MAC Binding						
Dynamic DNS						
Diagnostic						
System Tools						
Logout						

Device Information

Firmware Version: 0.9.1 1.0 v0029.0 Build 131125 Rel.60227n
Hardware Version: TX-VG1530 v1 00000000
System Up Time: 0 day(s) 00:58:34

WAN

Name	Connection Type	VLAN ID	IP/Mask	Gateway	DNS	Status
br_0_0_0	Bridge	0	N/A	N/A	N/A	PON Disconnected

IPv6 WAN

Name	Connection Type	VLAN ID	IPv6 Address/Prefix Length	Gateway	DNSv6	Status

LAN

MAC Address: 08:57:00:FA:6F:F0
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP: Enabled

IPv6 LAN

IPv6 Address: N/A
Prefix Length: 64
Autoconfiguration Type: RADVD

Wireless

Status: Enabled
SSID: TP-LINK_FA6FF0
Channel: Auto(Channel 6)
Channel Width: Auto
Mode: 11bgn mixed
Encryption: WPA-PSK/WPA2-PSK
MAC Address: 08:57:00:FA:6F:F0
Max Tx Rate: 300Mbps
WDS Status: Disabled

Voice

Profile Name	Registrar Address	Phone Number/User ID	Status

Figure 3-5

3. The GPON router supports SN authentication and CTC authentication, you can select one of them according to your ISP requirement.

If SN authentication is required, choose **Network→ GPON SN Settings** in the main menu, the GPON Configuration screen will appear, enter the **GPON Password** and **GPON SN** provided by your ISP and then click **Save**.

GPON Configuration	
GPON Password	
GPON Password:	length(0)
New Password:	
Save	
GPON SN	
GPON SN:	54505C4C9F045004
New SN:	
Save	

Figure 3-6

If CTC authentication is required, choose **Network→ GPON CTC Settings** in the main menu, the GPON Configuration screen will appear, enter the **GPON Username** and **GPON Password** provided by your ISP and then click **Save**.

GPON CTC Configuration	
This page is for setting GPON CTC authentication, including Username and Password.	
GPON Username:	tplink
GPON Password:	*****
Save	

Figure 3-7

- Choose **Pon→Connect Status** in the main menu, the GPON Status screen will appear. Click **Refresh** to update this page, then check whether the **ONU State** is registered.

System Information	
GPON Status	
Connection Type:	GPON
ONU ID:	1
ONU State:	Registered (05)
CTC Authentication:	--
Upstream FEC:	OFF
Downstream FEC:	OFF
Refresh	

Figure 3-8

 Note:

Once the ONU State is not registered, please check the GPON information and try again with the correct settings.

Choose **Network** → **WAN Settings** in the main menu, the WAN Interface screen will appear, then click **Add** to add a new entry. In the next screen you can configure the WAN Settings, then click **Save** to make your settings take effect.

WAN Settings

VLAN Configuration

Enable VLAN ☒

VLAN ID(1-4094):

802.1p(0-7):

WAN Service Setup

Connection Type:

PPP Username:

PPP Password:

Confirm password:

Connection Mode: ☒ Always on
☐ Connect on demand
☐ Connect manually
Max Idle Time: minutes (0 means remain active at all time)

Authentication Type:

Enable IPv4: ☒

Default Gateway:

Enable IPv6: ☐

Advance

Interface Bindings

☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4

☐ SSID1

Save **Back**

Figure 3-9

The basic settings for your GPON router are completed. Please try to log on to website to test your Internet connection.

Chapter 4. Configuring the GPON Router

This chapter will show each Web page's key function and the configuration way.

4.1 Login

After your successful login, you will see the twenty one main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

Status
Pon
Network
DHCP Server
Wireless
Guest Network
Voice
USB Settings
Route Settings
IPv6 Route Settings
Forwarding
Parent Control
Firewall
IPv6 Firewall
IPv6 Tunnel
Quality of Service
IP & MAC Binding
Dynamic DNS
Dagnostic
System Tools
Logout

The detailed explanations for each Web page's key function are listed below.

4.2 Status

Choose “**Status**”, you can see the corresponding information about **Device Information**, **WAN**, **IPv6 WAN**, **LAN**, **IPv6 WAN**, **Wireless** and **Voice**.

Basic Status						
Device Information						
Firmware Version:		0.9.1 1.0 v0029.0 Build 131125 Rel.60227n				
Hardware Version:		TX-VG1530 v1 00000000				
System Up Time:		0 day(s) 00:58:34				
WAN						
Name	Connection Type	VLAN ID	IP/Mask	Gateway	DNS	Status
br_0_0_0	Bridge	0	N/A	N/A	N/A	PON Disconnected
IPv6 WAN						
Name	Connection Type	VLAN ID	IPv6 Address/Prefix Length	Gateway	DNSv6	Status
LAN						
MAC Address:		08:57:00:FA:6F:F0				
IP Address:		192.168.1.1				
Subnet Mask:		255.255.255.0				
DHCP:		Enabled				
IPv6 LAN						
IPv6 Address:		N/A				
Prefix Length:		64				
Autoconfiguration Type:		RADVD				
Wireless						
Status:		Enabled				
SSID:		TP-LINK_FA6FF0				
Channel:		Auto(Channel 6)				
Channel Width:		Auto				
Mode:		11bgn mixed				
Encryption:		WPA-PSK/WPA2-PSK				
MAC Address:		08:57:00:FA:6F:F0				
Max Tx Rate:		300Mbps				
WDS Status:		Disabled				
Voice						
Profile Name	Registrar Address	Phone Number/User ID	Status			

Figure 4-1

4.3 PON

Choose “PON”, there are four submenus under the main menu: **Connect Status**, **Optical Status**, **Statistics** and **Advance**. The detailed explanations for each submenu are provided below.

Pon
Connect Status
Optical Status
Statistics
Advance

4.3.1 Connect Status

Choose “PON”→“**Connect Status**”, the GPON Status screen will appear, click **Refresh** to update this page, which shows you the current GPON Status. Here we use CTC authentication as an example (shown in Figure 4-2).

System Information	
GPON Status	
Connection Type:	GPON
ONU ID:	1
ONU State:	Registered (O5)
CTC Authentication:	--
Upstream FEC:	OFF
Downstream FEC:	OFF
Refresh	

Figure 4-2

- **Connection Type:** Here shows the type of the current connection.
- **ONU ID:** The ID of the ONU.
- **ONU Status:** The ONU is registered or not.
- **CTC Authentication:** The current status of CTC Authentication.
- **Upstream FEC:** Forward error correction (FEC) is used by the transport layer in communication systems, and is based on transmitting the data in an encoded format. By using the FEC technique, data transmission with a low error rate can be achieved, and retransmission are avoided.
This function enabled by OLT. If the status is on, which means the upstream transmit data via FEC. If the status is off, which means the upstream transmit data without FEC.
- **Downstream FEC:** This function enabled by OLT. If the status is on, which means the downstream transmit data via FEC. If the status is off, which means the downstream transmit data without FEC.

Click **Refresh** to update this page.

 Note:

Only when the downstream FEC enabled by OLT, the upstream FEC can be enabled as well.

4.3.2 Optical Status

Choose “PON”→“**Optical Status**”, the Optical link Status screen will appear, click **Refresh** to update this page, which shows you the current Optical link Status (shown in Figure 4-3).

GPON Infomation	
Optical link Status	
Transceiver Temperature:	44.13 °C
Supply Voltage:	3200 mV
Bias Current:	7.00 mA
TX Power:	1.43 dBm
RX Power:	-21.55 dBm
Refresh	

Figure 4-3

Click **Refresh** to update this page.

4.3.3 Statistics

Choose “PON”→“**Statistics**”, the traffic statistics screen will appear (shown in Figure 4-4), click **Refresh** to update this page, and then you can view the statistics of the GPON router, including GPON traffic and OMCI traffic of the current Packets Statistic.

Traffic Statistics	
GPON Statistics	
Bytes Sent:	0
Bytes Received:	0
Packets Sent:	0
Packets Received:	0
OMCI Statistics	
Packets Sent:	0
Packets Received:	0
Refresh	

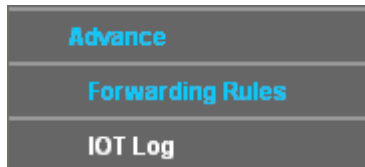
Figure 4-4

- **Bytes Sent:** The total number of bytes sent by the GPON router.
- **Bytes Received:** The total number of bytes received by the GPON router.
- **Packets Sent:** The total number of packets sent by the GPON router.
- **Packets Received:** The total number of packets received by the GPON router.

Click **Refresh** to update this page.

4.3.4 Advance

Choose “PON”→“**Advance**”, there are two submenus under the menu. The detailed explanations for each submenu are provided below.



4.3.4.1 Forwarding Rules

Choose “PON” → “Advance” → “Forwarding Rules”, and you will see the GPON Forwarding Rules Table in the screen similar to Figure 4-5.

 The screen shows the 'GPON Forwarding Rules' configuration page. It includes a header, a description, radio buttons for configuration source, a status message, and a table of forwarding rules.

Direction	Vid	Pbit	Change to Vid	Change to Pbit	GEM Port	T-Cont	Queue	Operation

Figure 4-5

4.3.4.2 IOT Log

Choose “PON” → “Advance” → “IOT Log”, and you will see the GPON OMCI Debug screen (shown in Figure 4-6).

 The screen shows the 'GPON OMCI Debug' configuration page. It includes a header, a description, and an 'Export' button.

This page exports the GPON OMCI config information.

Export

Figure 4-6

Click the **Export** button to save the GPON OMCI settings as a backup file in your local computer.

4.4 Network

Choose “Network”, there are many submenus under the main menu. Click any one of them, and you will be able to configure the corresponding function.

Network
WAN Settings
LAN Settings
IPv6 LAN Settings
MAC Clone
ALG Settings
Auto Vlan
GPON SN Settings
GPON CTC Settings
IPSec VPN

4.4.1 WAN Settings

Choose “**Network**”→“**WAN Settings**”, and you will see the WAN Port Information Table in the screen similar to Figure 4-7, which describes the WAN port settings and the relevant manipulation to each interface. There are four different configurations for the connection types, which are Static IP, Dynamic IP, PPPoE and Bridge. You can select the corresponding types according to your needs.

WAN Interface									
This page is for choosing the type of WAN interface. Choose Add, or Edit to configure a WAN interface.									
Name	Type	VLAN ID	IPvX	IP/Mask	Gateway	DNS	Status	Connect	Action
br_0_0_0	Bridge	0	N/A	N/A	N/A	N/A	Connected	Disconnect	Edit Delete
Add Refresh									

Figure 4-7

Click **Add** to add a new entry, you can configure the parameters for VLAN and WAN Service in the next screen (shown in Figure 4-8).

WAN Settings	
VLAN Configuration Enable VLAN: ☒ VLAN ID(1-4094): 1 802.1p(0-7): 0	
WAN Service Setup Connection Type: PPPoE PPP Username: PPP Password: Confirm password: Connection Mode: ☒ Always on ☐ Connect on demand ☐ Connect manually Max Idle Time: 15 minutes (0 means remain active at all time) Authentication Type: AUTO_AUTH Enable IPv4: ☒ Default Gateway: Current Connection Enable IPv6: ☐	
Hide ▲ Service Name: (do not change unless necessary) Server Name: (do not change unless necessary) MTU(Bytes): 1480 (1480 as default, do not change unless necessary) Enable Fullcone NAT: ☐ Enable SPI Firewall: ☐ Enable IGMP Proxy: ☒ Use IP address specified by ISP: ☐ Echo request interval: 30 (0-120 seconds, 0 means no request) Set DNS server manually: ☐	
Interface Bindings ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐ SSID1	
Save Back	

Figure 4-8

4.4.1.1 Static IP

Select this option if your ISP provides static IP information to you. You should set static IP address, IP subnet mask, and gateway address in the screen below.

WAN Settings	
VLAN Configuration Enable VLAN: ☒ VLAN ID(1-4094): 1 802.1p(0-7): 0	
WAN Service Setup Connection Type: Static IP Enable IPv4: ☒ IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Gateway: 0.0.0.0 (optional) DNS Server: 0.0.0.0 (optional) Secondary DNS Server: 0.0.0.0 (optional) Default Gateway: Current Connection Enable IPv6: ☒ IPv6 Address: :: Prefix Length: 64 IPv6 Gateway: :: (optional) IPv6 DNS Server: :: (optional) Secondary IPv6 DNS Server: :: (optional) IPv6 Default Gateway: Current Connection MTU(Bytes): 1500 (1500 as default, do not change unless necessary) Enable NAT: ☒ Enable Fullcone NAT: ☐ Enable SPI Firewall: ☐ Enable IGMP Proxy: ☒	
Interface Bindings ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐ SSID1	
Save Back	

Figure 4-9

VLAN Configuration:

- **Enable VLAN:** Enable or disable this function. Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same LAN, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. If you want to active this function, this function must be enabled.
- **VLAN ID (1~4094):** Identifies the virtual channel endpoints in a VLAN network. The valid range is from 1 to 4094. Please input the value provided by your ISP.

WAN Service Setup:

- **Enable IPv4:** Check the box to enable IPv4.
- **IP Address:** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask:** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Gateway:** Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **DNS Server/ Secondary DNS Server:** Here you can set DNS Server (at least one) manually. The Route will use this DNS Server for priority.

- **Default Gateway:** select a WAN Interface from the drop-down list as the IPv4 default gateway.
- **Enable IPv6:** Check the box to enable IPv6.
- **IPv6 Address:** Enter the IPv6 address in dotted-decimal notation provided by your ISP.
- **Prefix length:** Enter the length of the prefix
- **IPv6 Gateway:** Enter the gateway IPv6 address in dotted-decimal notation provided by your ISP.
- **IPv6 DNS Server/ Secondary DNS Server:** Here you can set DNS Server (at least one) manually. The Router will use this DNS Server for priority.
- **IPv6 Default Gateway:** select a WAN Interface from the drop-down list as the IPv6 default gateway.

 Note:

Each IP address entered in the fields must be in the appropriate IPv6 form, which is eight IP octets separated by a colon (x:x:x:x:x:x:x:x). The router will not accept the IP address if it is not in this format.

Click **Advanced**, advanced selections for WAN Service Setup can be shown.

- **MTU (bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default **MTU** value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this GPON router is hosting your network's connection to the Internet, please select the check box. If another Router exists in your network, you don't need to select the option.
- **Enable Fullcone NAT:** It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy:** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the GPON router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

Interface Bindings:

Here you can select specified LAN interfaces to the same object, then the specified LAN interfaces could connect to WAN only via specified connection type.

For example, if you select PPPoE as the connection type, at the same time bind LAN1, LAN2 and SSID1 together, then the three interfaces could only connect to WAN via the specified PPPoE link.

WAN Service Setup
Connection Type:
PPP Username:
PPP Password:
Confirm password:
Connection Mode: ☒ Always on
☐ Connect on demand
☐ Connect manually
Max Idle Time: minutes (0 means remain active at all time)
Authentication Type:
Enable IPv4: ☒
Default Gateway:
Enable IPv6: ☐
[Advance](#)

Interface Bindings
☒ LAN1 ☒ LAN2 ☐ LAN3 ☐ LAN4
☒ SSID1 ☐ SSID2 ☐ SSID3

[Save](#) [Back](#)

Figure 4-10

Click the **Save** button to save the settings.

4.4.1.2 Dynamic IP

Select this option, the GPON router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP.

WAN Settings	
VLAN Configuration Enable VLAN: ☒ VLAN ID(1-4094): 1 802.1p(0-7): 0	
WAN Service Setup Connection Type: Dynamic IP Enable IPv4: ☒ IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Gateway: 0.0.0.0 Default Gateway: Current Connection Enable IPv6: ☒ IPv6 Address: :: Prefix Length: 0 IPv6 Gateway: :: Addressing Type: DHCPv6 IPv6 Default Gateway: Current Connection	
MTU(Bytes): 1500 (1500 as default, do not change unless necessary) Hide	
Enable NAT: ☒ Enable Fullcone NAT: ☐ Enable SPI Firewall: ☐ Enable IGMP Proxy: ☒ Get IP with Unicast: ☐ (It is usually not required) Set DNS server manually: ☐ Set IPv6 DNS Server manually: ☐ Host Name: TX-VG1530	
Interface Bindings ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐ SSID1	
Save Back	

Figure 4-11

Click **Advanced**, advanced selections for WAN Service Setup can be shown.

- **MTU (bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default **MTU** value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this GPON router is hosting your network's connection to the Internet, please select the check box. If another Router exists in your network, you don't need to select the option.
- **Enable Fullcone NAT:** It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy:** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the GPON router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

- **Get IP Unicast:** This is disabled by default. The minority of DHCP Server of ISP will not support to enable this. When the route is connected right but IP cannot get, you can select this box.
- **Set DNS Server manually:** Choose “Set DNS Server manually”, you can set DNS Server manually here. The GPON router will use this DNS Server for priority.
- **Host Name:** Here displays model No. of your GPON router.

Click the **Save** button to save the settings.

4.4.1.3 PPPoE

If your ISP provides a **PPPoE** connection and you need to use an ATM Interface, choose **PPPoE** in the drop-down list, and then the screen will be displayed as below.

The screenshot displays the WAN Settings configuration page. It is divided into three main sections: VLAN Configuration, WAN Service Setup, and Interface Bindings.

VLAN Configuration:

- Enable VLAN: ☒
- VLAN ID(1-4094):
- 802.1p(0-7):

WAN Service Setup:

- Connection Type: **PPPoE** (dropdown menu)
- PPP Username:
- PPP Password:
- Confirm password:
- Connection Mode:
 - ☒ Always on
 - ☐ Connect on demand
 - ☐ Connect manually
- Max Idle Time: minutes (0 means remain active at all time)
- Authentication Type: **AUTO_AUTH** (dropdown menu)
- Enable IPv4: ☒
- Default Gateway: **Current Connection** (dropdown menu)
- Enable IPv6: ☐
- Service Name: (do not change unless necessary)
- Server Name: (do not change unless necessary)
- MTU(Bytes): (1480 as default, do not change unless necessary)
- Enable Fullcone NAT: ☐
- Enable SPI Firewall: ☐
- Enable IGMP Proxy: ☒
- Use IP address specified by ISP: ☐
- Echo request interval: (0-120 seconds, 0 means no request)
- Set DNS server manually: ☐

Interface Bindings:

- LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐
- SSID1 ☐ SSID2 ☐ SSID3 ☐

At the bottom right, there is a **Hide** button with a downward arrow. At the bottom center, there are **Save** and **Back** buttons.

Figure 4-12

- **PPP Username/Password/Confirm Password:** Enter the User Name, Password and Confirm Password provided by your ISP. These fields are case-sensitive.
- **Authentication Method:** Select the **Authentication Method** from the drop-down list, the default method is **AUTO_AUTH**, and you can leave it as a default setting.

- **Choose the right connection type according to your needs:** For PPPoE connection, you can select **Connect on demand** or **Connect automatically** or **Connect manually**. Connect on demand is dependent on the traffic. If there is no traffic (or **Idle** for a pre-specified period of time), the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.

Click **Advanced**, advanced selections for WAN Service Setup can be shown.

- **Service Name/Server Name:** Enter the Service Name and Server Name if it was provided by your ISP. You can leave them blank, if the ISP doesn't provide them.
- **MTU (bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default **MTU** value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable Fullcone NAT:** It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy:** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the GPON router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.
- **Use IP address specified by ISP:** Choose "Use IP address specified by ISP", you can enter the IP address provided by your ISP.
- **Echo request Interval:** This value determines the interval of the echo request. Here you can specify the value between 0-120 seconds, 0 means no request. The default value is 30.
- **Set DNS Server manually:** Choose "Set DNS Server manually", you can set DNS Server manually here. The GPON router will use this DNS Server for priority.

Click the **Save** button to save the settings.

4.4.1.4 Bridge

If you select this type of connection, the router can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

WAN Settings	
VLAN Configuration Enable VLAN ☒ VLAN ID(1-4094): 1 802.1p(0-7): 0	
WAN Service Setup Connection Type: Bridge	
Interface Bindings ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐ SSID1 ☐ SSID2 ☐ SSID3	
Save Back	

Figure 4-13

 Note:

After you finish the Internet configuration, please click **Save** to make the settings take effect.

4.4.2 LAN Settings

Choose “**Network**”→“**LAN Settings**” menu, and you will see the LAN screen (shown in Figure 4-14). Please configure the parameters for LAN ports according to the descriptions below.

LAN Settings	
Note: If the LAN IP address or subnet mask is changed, please make sure the DHCP Address Pool and the static IP assigned by DHCP Server are in the same subnet with the new LAN IP.	
Group:	Default
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Enable IGMP Snooping:	☐
Enable Second IP:	☐
DHCP Server:	☐ Disable ☒ Enable ☐ DHCP Relay
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.199
Leased Time:	1440 minutes (1~2880 minutes, the default value is 1440)
Gateway:	192.168.1.1 (optional)
Default Domain:	(optional)
DNS Server:	0.0.0.0 (optional)
Secondary DNS Server:	0.0.0.0 (optional)
Save Back	

Figure 4-14

- **IP Address:** You can configure the GPON router's IP Address and Subnet Mask for LAN Interface.
- **IP Address:** Enter the GPON router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.
 - **Subnet Mask:** Enter the GPON router's Subnet Mask, the default value is 255.255.255.0.

- **Enable IGMP Snooping:** If you select the option, please choose the IGMP Mode: Standard Mode or Blocking Mode.
- **Enable Second IP:** You can configure the GPON router's second IP Address and Subnet Mask for LAN Interface through which you can also access to the Web-based Utility as the default IP Address and Subnet Mask.
- **DHCP Server:** These settings allow you to configure the GPON router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the GPON router's Ethernet LAN interface. DHCP service will supply IP settings to computers which are configured to automatically obtain IP settings that are connected to the GPON router through the Ethernet port. When the GPON router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the GPON router, you must change the range of IP addresses in the pool used for DHCP on the LAN.
 - **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. The default Start IP Address is **192.168.1.100**.
 - **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The default End IP Address is **192.168.1.199**.
 - **Leased Time:** The Leased Time is the amount of time in which a network user will be allowed connection to the GPON router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **1440** minutes.

The detailed configuration about DHCP server, please refer to section [4.5 DHCP Server](#).

4.4.3 IPv6 LAN Settings

Choose menu "Network"→"IPv6 LAN Settings", you can configure LAN IPv6 interface for your GPON router.

Figure 4-15

- **Address Autoconfiguration Type:** Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided.
If RADVD is selected, it doesn't need to be configured.

If DHCPv6 Server is selected, please complete the following parameters.

Group:	Default
Address Autoconfiguration Type:	☐ RADVD ☒ DHCPv6 Server
Start IPv6 Address:	::1 (1~FFFE)
End IPv6 Address:	::FFFE (1~FFFE)
Leased Time:	86400 seconds (The default value is 86400)

Figure 4-16

- **Start IPv6 Address:** Enter a value for the DHCPv6 server to start with when issuing IPv6 addresses.
 - **End IPv6 Address:** Enter a value for the DHCPv6 server to end with when issuing IPv6 addresses.
 - **Leased Time:** The Leased Time is the amount of time in which a network user will be allowed connection to the GPON router with their current dynamic IPv6 address. Enter the amount of time, in hours, then the user will be “leased” this dynamic IPv6 address. After the dynamic IPv6 address has expired, the user will be automatically assigned a new dynamic IPv6 address. The default is 86400 seconds.
- **Site Prefix Configuration Type:** Select a type to assign prefix to IPv6 addresses. Delegated and Static are provided.
- 1) If Delegated is selected, please complete the following parameters.

Site Prefix Configuration Type:	☒ Delegated ☐ Static
Prefix Delegated WAN Connection:	No available interface. ▼

Figure 4-17

- **Prefix Delegated WAN Connection:** Select a WAN connection form the drop-down list to assign prefix.
- 2) If Static is selected, please complete the following parameters.

Site Prefix Configuration Type:	☐ Delegated ☒ Static
Site Prefix:	
Site Prefix Length:	64

Figure 4-18

- **Site Prefix:** Enter a value for the site prefix.
- **Site Prefix Length:** Enter a value for the site prefix length.

Click the **Save** button to save the settings.

4.4.4 MAC Clone

Choose menu “**Network**”→“**MAC Clone**”, you can configure the MAC address of the WAN Interface as shown below.

The WAN Interface List displays the WAN Interfaces you have configured on the section [4.4.1 WAN Settings](#), and its default MAC Address. You can select corresponding WAN Interface from the drop-down list and click **Clone MAC To** button to clone your current PC MAC, and then click **Save**.

MAC Clone		
WAN Connection	MAC Address	Operation
Current PC's MAC	6C:62:6D:F7:32:09	Clone MAC To v
Note: 1. MAC clone may cause reconnection. 2. After MAC Clone, the bridge connections sharing the same VLAN ID with other connections may not work.		
Save		

Figure 4-19

Note:

Only the WAN Ports can use MAC Address Clone function. All the clone MAC addresses must not be the same with each other.

4.4.5 ALG Settings

Choose menu “**Network**”→“**ALG Settings**”, and then you can configure the basic security in the screen as shown in Figure 4-20.

ALG Settings	
Virtual Private Network(VPN):	
PPTP Pass-through:	☒ Enable ☐ Disable
L2TP Pass-through:	☒ Enable ☐ Disable
IPSec Pass-through:	☒ Enable ☐ Disable
Application Layer Gateway(ALG):	
FTP ALG:	☒ Enable ☐ Disable
TFTP ALG:	☒ Enable ☐ Disable
H323 ALG:	☒ Enable ☐ Disable
SIP ALG:	☒ Enable ☐ Disable
Save	

Figure 4-20

➤ **Virtual Private Network (VPN):** VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the GPON router.

- **PPTP Passthrough:** Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the GPON router, click **Enable**.

- **L2TP Passthrough:** Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the GPON router, click **Enable**.
 - **IPSec Passthrough:** Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the GPON router, click **Enable**.
- **Application Layer Gateway (ALG):** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP etc.
- **FTP ALG:** To allow FTP clients and servers to transfer data across NAT, click **Enable**.
 - **TFTP ALG:** To allow TFTP clients and servers to transfer data across NAT, click **Enable**.

Click the **Save** button to save your settings.

4.4.6 Auto Vlan

Choose "**Network**"→"**Auto Vlan**", you can search for available VLAN Mode and VLAN Tag on the page as shown in Figure 4-21.

This page is used to search for available 【VLAN Mode】 and 【VLAN Tag】

Connection Type	VLAN Mode	VLAN Tag
Dynamic IP	Untag	-
Dynamic IP / PPPoE	Tag	100

Search

Figure 4-21

Click the **Search** button to search for available VLAN Mode and VLAN Tag.

4.4.7 GPON SN Settings

Choose "**Network**"→"**GPON SN Settings**", the GPON Configuration screen will appear on the page as shown in Figure 4-22.

GPON Configuration	
GPON Password	
GPON Password:	length(0)
New Password:	
Save	
GPON SN	
GPON SN:	54505C4C9F045004
New SN:	
Save	

Figure 4-22

GPON Password

- **GPON Password:** Displays the factory default password.
- **New Password:** Enter the password provided by your ISP.

Click **Save** to make the settings take effect.

GPON SN

- **GPON SN:** Displays the factory default SN.
- **New SN:** Enter the SN provided by your ISP.

Click **Save** to make the settings take effect.

4.4.8 GPON CTC Settings

Choose “**Network**”→“**GPON CTC Settings**”, the GPON Configuration screen will appear on the page as shown in Figure 4-23.

GPON CTC Configuration	
This page is for setting GPON CTC authentication, including Username and Password.	
GPON Username:	tplink
GPON Password:	
Save	

Figure 4-23

Enter the **GPON Password** and **GPON SN** provided by your ISP.

Click the **Save** button to save your settings.

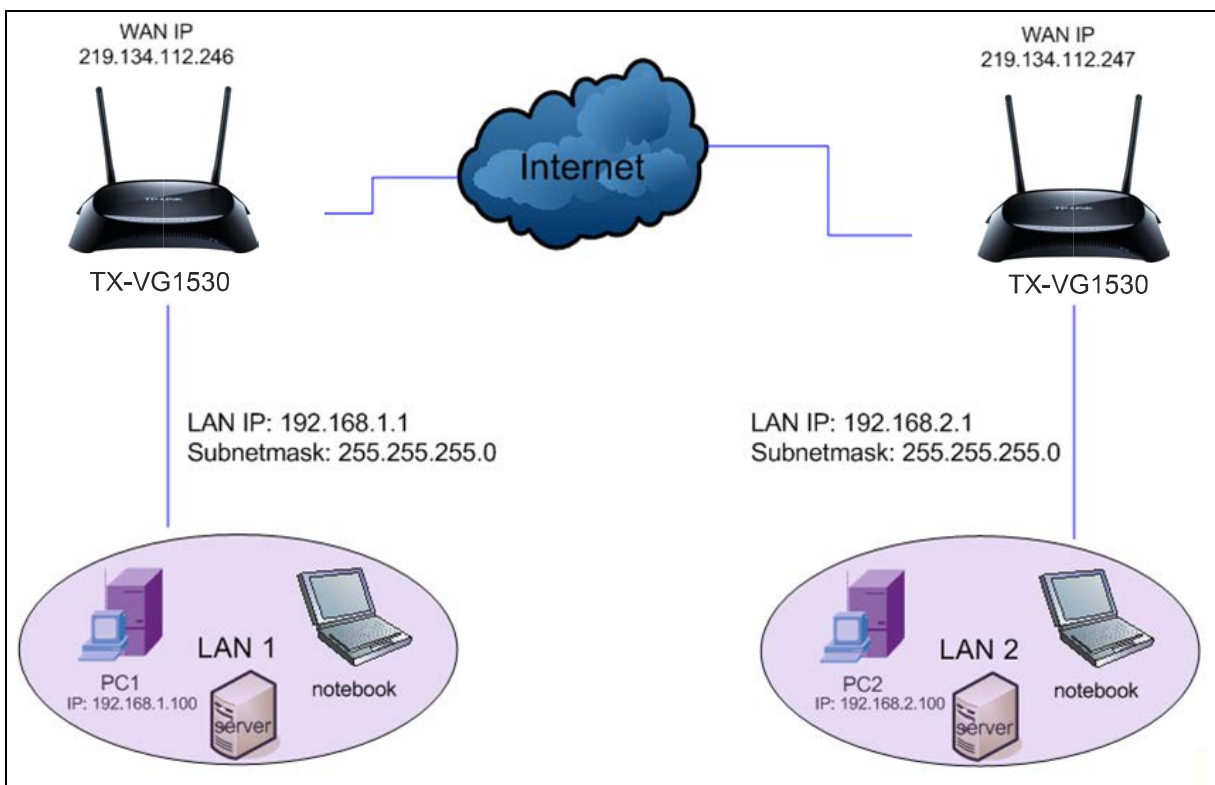
4.4.9 IPsec VPN

Choose “**Network**”→“**IPsec VPN**”, you can add/remove or enable/disable the IPsec tunnel connections on the screen as shown in Figure 4-24.

IPsec Tunnel Mode Connections						
☐ Dead Peer Detection (Caution: It may cause transmission unstable!)						
Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Option
Add New Connection						

Figure 4-24

This section will guide you to configure a VPN tunnel between two TX-VG1530s. The topology is as follows.



Note:

You could also use other VPN Routers to set VPN tunnels with TX-VG1530. TX-VG1530 supports up to 10 VPN tunnels simultaneously.

Click **Add New Connection** in Figure 4-24 and then you will enter the screen shown in Figure 4-25.

IPSec Settings	
IPSec Connection Name:	Connection name
Remote IPSec Gateway Address(URL):	0.0.0.0
Tunnel access from local IP addresses:	Subnet
IP Address for VPN:	0.0.0.0
IP Subnetmask:	255.255.255.0
Tunnel access from remote IP addresses:	Subnet
IP Address for VPN:	0.0.0.0
IP Subnetmask:	255.255.255.0
Key Exchange Method:	Auto(IKE)
Authentication Method:	Pre-Shared Key
Pre-Shared Key:	psk_key
Perfect Forward Secrecy:	Enable
Show Advanced Settings	
Save/Apply	

Figure 4-25

- **IPSec Connection Name:** Enter a name for your VPN.
- **Remote IPSec Gateway Address (URL):** Enter the destination gateway IP address in the box which is the public WAN IP or Domain Name of the remote VPN server endpoint. (For example: Input **219.134.112.247** in **Device1**, Input **219.134.112.246** in **Device 2**)
- **Tunnel access from local IP addresses:** Choose Subnet if you want the Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of your LAN. (For example: Input **192.168.1.1** in **Device1**, Input **192.168.2.1** in **Device2**)
- **IP Subnetmask:** Enter the Subnet mask of your LAN. (For example: Input **255.255.255.0** in both **Device1** and **Device2**)
- **Tunnel access from remote IP addresses:** Choose Subnet if you want the Remote Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of the Remote LAN. (For example: Input **192.168.2.1** in **Device1**, Input **192.168.1.1** in **Device2**)
- **IP Subnetmask:** Enter the subnetmask of the remote LAN. (For example: Input **255.255.255.0** in both **Device1** and **Device2**)
- **Key Exchange Method:** Select Auto (IKE) or Manual.
- **Authentication Method:** Select Pre-Shared Key (recommended).
- **Pre-Shared Key:** Input the Pre-Shared key for Authentication. (For example: Input 12345678)
- **Perfect Forward Secrecy:** PFS is an additional security protocol.

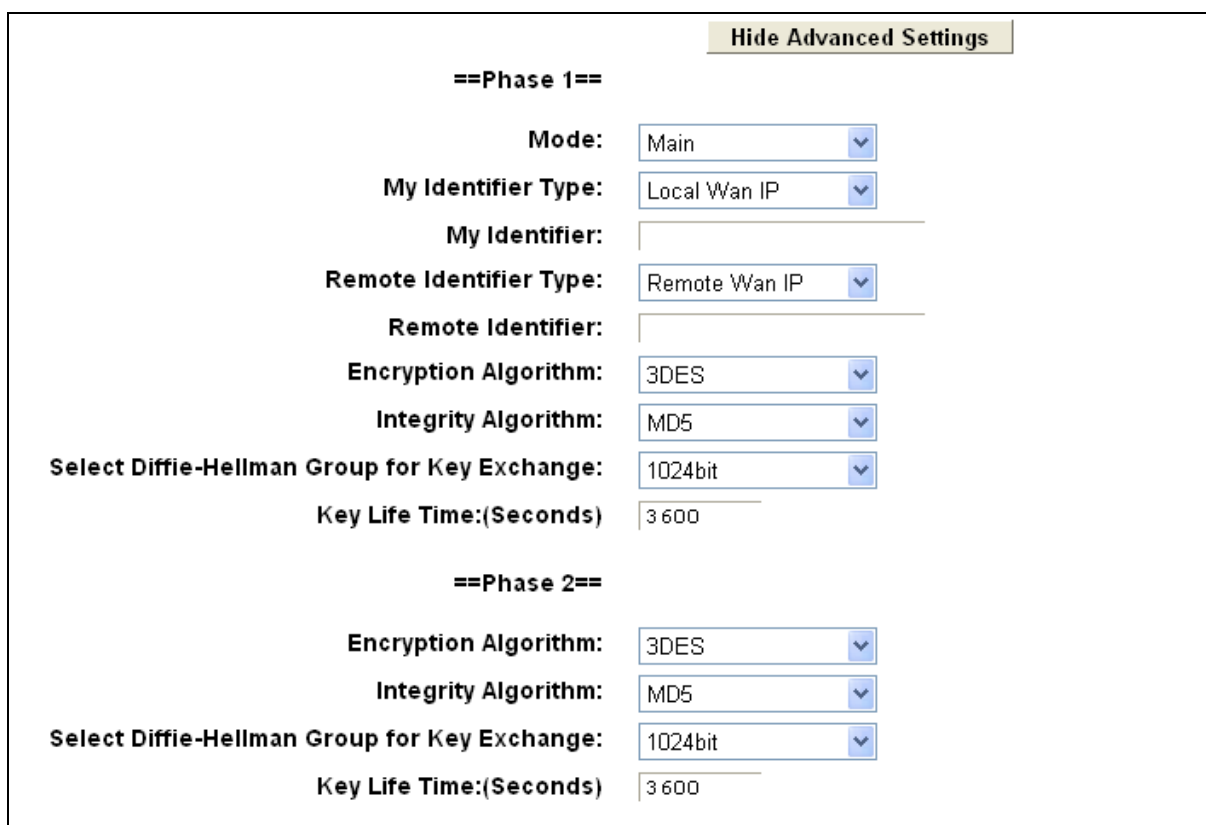
We recommend you leave the Advanced Settings as default value.

After complete the basic settings and click Save/Apply in both **Device1** and **Device2**, PCs in LAN1 could communicate with PCs in remote LAN2. (For example: You can ping the IP address of PC2 which is 192.168.2.100 in PC1)

 Note:

The VPN Servers Endpoint from both ends must use the same pre-shared keys and Perfect Forward Secrecy settings.

Click **Show Advanced Settings** and then you can configure the Advanced Settings.



Hide Advanced Settings

==Phase 1==

Mode: Main

My Identifier Type: Local Wan IP

My Identifier:

Remote Identifier Type: Remote Wan IP

Remote Identifier:

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time:(Seconds) 3600

==Phase 2==

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time:(Seconds) 3600

Figure 4-26

- **Mode:** Select Main Mode to configure the standard negotiation parameters for IKE phase1.
- **Aggressive Mode:** Select Aggressive Mode to configure IKE phase1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended-Less Secure)

 Note:

The difference between the two is that aggressive mode will pass more information in fewer packets, with the benefit of slightly faster connection establishment, at the cost of transmitting the identities of the security firewall in the clear. When using aggressive mode, some configuration parameters such as Diffie-Hellman groups, and PFS can not be negotiated, resulting in a greater importance of having "compatible" configuration on both ends.

- **Key Life Time:** Enter the number of seconds for the IPSec lifetime. It is the period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 3600.

Note:

If you want to change the default settings of **Advanced Settings**, please make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Life time in both **phase1** and **phase2**.

4.5 DHCP Server

Choose “**DHCP Server**”, you can see the next submenus:

DHCP Server
DHCP Settings
Clients List
Address Reservation
Conditional Pool

Click any of them, and you will be able to configure the corresponding function.

4.5.1 DHCP Settings

Choose menu “**DHCP Server**”→“**DHCP Settings**”, you can configure the DHCP Server on the page as shown in Figure 4-27. The GPON router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the GPON router on the LAN.

DHCP Settings	
This page allows you to set DHCP server which provides TCP/IP configuration for all the PCs connected to the Modem Router in the LAN.	
Group:	Default
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	☐ Disable ☒ Enable ☐ DHCP Relay
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.199
Lease Time:	1440 minutes (1~2880 minutes, the default value is 1440)
Default Gateway:	192.168.1.1 (optional)
Default Domain:	(optional)
DNS Server:	0.0.0.0 (optional)
Secondary DNS Server:	0.0.0.0 (optional)
Save	

Figure 4-27

- **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. The default Start IP Address is **192.168.1.100**.
- **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The default End IP Address is **192.168.1.199**.
- **Lease Time:** The Leased Time is the amount of time in which a network user will be allowed connection to the GPON router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be “leased” this dynamic IP address. After the dynamic IP

address has expired, the user will be automatically assigned a new dynamic IP address. The default is **24** hours.

- **Default Gateway - (Optional):** It is suggested to input the IP address of the LAN port of the GPON router. The default value is 192.168.1.1.
- **Default Domain - (Optional):** Input the domain name of your network.
- **DNS Server - (Optional):** Input the DNS IP address provided by your ISP or consult your ISP.
- **Secondary DNS Server - (Optional):** Input the IP address of another DNS server if your ISP provides two DNS servers.
- **DHCP Relay:** Select **Relay**, then you will see the next screen, and the GPON router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

Groups:	Default
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	☐ Disable ☐ Enable ☒ DHCP Relay
Remote Server's IP Address:	0.0.0.0
Note: You have to disable NAT of the WAN connections. Or the DHCP Relay may not take effect!	
Save	

 Note:

- 1) To use the DHCP server function of the GPON router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
- 2) You have to disable NAT of the WAN connections, or the DHCP Relay may not take effect.
- 3) If you select **Disabled**, the DHCP function will not take effect.

Click the **Save** button to save your settings.

4.5.2 Clients List

Choose menu **"DHCP Server"→"Clients List"**, you can view the information about the clients attached to the GPON router in the screen as shown in Figure 4-28.

DHCP Clients List				
This page displays the information of DHCP clients.				
ID	Client Name	MAC Address	IP Address	Valid Time
1	Unknown	24:AB:81:EE:EA:D8	192.168.1.101	23:47:06
2	qwe-PC	74:E5:0B:19:3B:BA	192.168.1.102	23:43:40
Refresh				

Figure 4-28

- **Client Name:** The name of the DHCP client
- **MAC Address:** The MAC address of the DHCP client
- **IP Address:** The IP address that the GPON router has allocated to the DHCP client

- **Valid Time:** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click the **Refresh** button.

4.5.3 Address Reservation

Choose menu “**DHCP Server**”→“**Address Reservation**”, you can view and add a reserved address for clients via the next screen (shown in Figure 4-29). When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

☐	MAC Address	IP Address	Groups	Status	Edit
☒	40:61:86:FC:6F:22	192.168.1.100	Default	Disabled	Edit

Figure 4-29

- **MAC Address:** The MAC address of the PC for which you want to reserve an IP address.
- **IP Address:** The IP address reserved for the PC by the GPON router.
- **Status:** The status of this entry either **Enabled** or **Disabled**.

To Reserve an IP address:

1. Click the **Add New** button. Then Figure 4-30 will pop up.
2. Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.

The static IP of DHCP Server can be set on this page.

MAC Address:
 IP Address:
 Groups:
 Status:

Figure 4-30

To modify or delete an existing entry:

1. Click the **Edit** in the entry you want to modify. If you want to delete the entry, click the **Delete**.

2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable Selected** button to make selected entries enabled/disabled.

Click the **Delete Selected** button to selected entries.

4.5.4 Conditional Pool

Choose menu “**DHCP Server**”→“**Conditional Pool**”, you can see the next screen (shown in Figure 4-31). This page displays vendor class settings and allows you to set parameters for vendor class by clicking corresponding buttons.

DHCP Conditional Pool						
This page displays vendor class settings and allows you to set parameters for vendor class by clicking corresponding buttons.						
☐	Vendor ID	Start IP Address/ End IP Address	Facility	Groups	Status	Edit
Add New Enable Selected Disable Selected Delete Selected						
Refresh						

Figure 4-31

To add a vendor class:

1. Click the **Add New** button. Then Figure 4-32 will pop up.
2. Enter parameters for the vendor class.

Click the **Save** button.

DHCP Conditional Pool

The vendor class IP range can be set on this page.

Facility:

Vendor ID:

Start IP Address:

End IP Address:

Default Gateway:

Device Type:

Add Option:

Option Value:

Groups:

Status:

Figure 4-32

To modify or delete an existing entry:

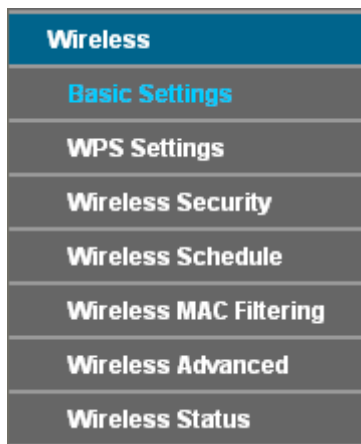
1. Click the **Edit** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable Selected** button to make selected entries enabled/disabled.

Click the **Delete Selected** button to selected entries.

4.6 Wireless

Choose “**Wireless**”, there are seven submenus to configure Wireless LAN settings. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



4.6.1 Basic Settings

Choose “**Wireless**”→”**Basic Settings**”, you will see the screen of **Wireless--Basic settings** shown as below. The basic settings for wireless networking are set on this screen.

A screenshot of the 'Wireless Basic Settings' configuration page. The page has a blue header with the title 'Wireless Basic Settings'. The main content area is white and contains several settings: 'Wireless' with radio buttons for 'Enable' (selected) and 'Disable'; 'SSID1', 'SSID2', and 'SSID3' each with a text input field and an 'Enable' checkbox; 'Region' with a dropdown menu set to 'United States'; a 'Warning' message; 'Mode' with a dropdown menu set to '11bgn mixed'; 'Channel' with a dropdown menu set to 'Auto'; 'Channel Width' with a dropdown menu set to 'Auto'; and two checkboxes at the bottom, 'Enable SSID Broadcast' (checked) and 'Enable WDS' (unchecked). A 'Save' button is located at the bottom right of the form.

Figure 4-33

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on Region requirements.

- **SSID (1-3):** Up to four SSIDs for each BSS (Basic Service Set) can be entered in the filed SSID1 ~ SSID3. The name can be up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. Check the Enable box to enable the desired

SSID. The wireless stations connected to different SSIDs can not communicate with each other.

- **Mode:** Select the desired mode.

11b only: Select if all of your wireless clients are 802.11b.

11g only: Select if all of your wireless clients are 802.11g.

11n only: Select only if all of your wireless clients are 802.11n.

11bg mixed: Select if you are using both 802.11b and 802.11g wireless clients.

11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

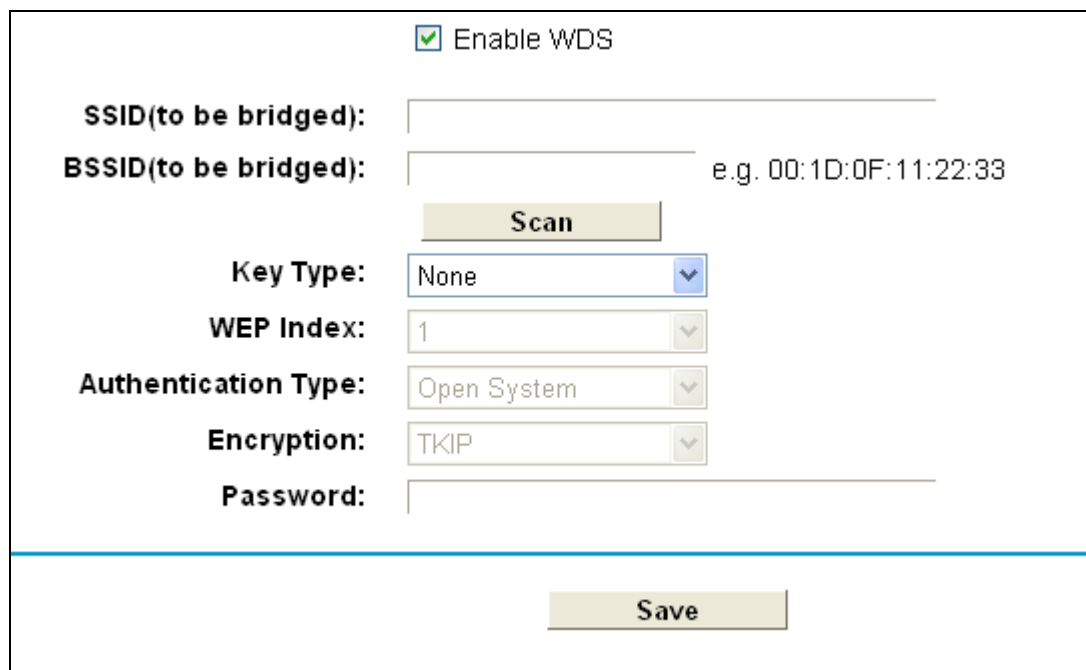
Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can be connected to the GPON router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the GPON router. It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the GPON router.

- **Channel:** Select the channel you want to use from the drop-down List of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width:** Select the channel width from the drop-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

 Note:

If **11b only**, **11g only**, or **11bg mixed** is selected in the **Mode** field, the **Channel Width** selecting field will turn grey and the value will become 20M, which is unable to be changed.

- **Enable SSID Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the GPON router. If you select the **Enable SSID Broadcast** checkbox, the Wireless Router will broadcast its name (SSID) on the air.
- **Enable WDS:** Check this box to enable WDS. With this function, the GPON router can bridge two or more Wlans. If this checkbox is selected, you will have to set the following parameters as shown in the figure below. Make sure the following settings are correct.



☒ Enable WDS

SSID(to be bridged):

BSSID(to be bridged): e.g. 00:1D:0F:11:22:33

Key Type:

WEP Index:

Authentication Type:

Encryption:

Password:

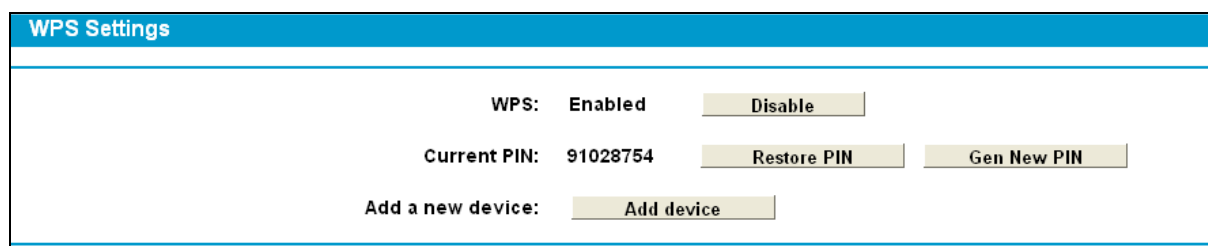
- **SSID (to be bridged):** The SSID of the AP your GPON router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID (to be bridged):** The BSSID of the AP your GPON router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Scan:** Click this button, you can search the AP which runs in the current channel.
- **Key type:** This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type
- **WEP Index:** This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the index of the WEP key.
- **Auth Type:** This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the authorization type of the Root AP.
- **Password:** If the AP your GPON router is going to connect needs password, you need to fill the password in this blank.

Click **Save** to save your settings.

4.6.2 WPS Settings

This section will guide you to add a new wireless device to an existing network quickly by **WPS** (also called **QSS**) function.

- a). Choose menu “**WPS Settings**”, and you will see the next screen (shown in Figure 4-34).



WPS Settings

WPS: Enabled

Current PIN: 91028754

Add a new device:

Figure 4-34

- **WPS:** Enable or disable the WPS function here.
- **Current PIN:** The current value of the GPON router's PIN is displayed here. The default PIN of the GPON router can be found in the label or User Guide.
- **Restore PIN:** Restore the PIN of the GPON router to its default.
- **Gen New PIN:** Click this button, and then you can get a new random value for the GPON router's PIN. You can ensure the network security by generating a new PIN.
- **Add device:** You can add a new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and GPON router using either Push Button Configuration (PBC) method or PIN method.

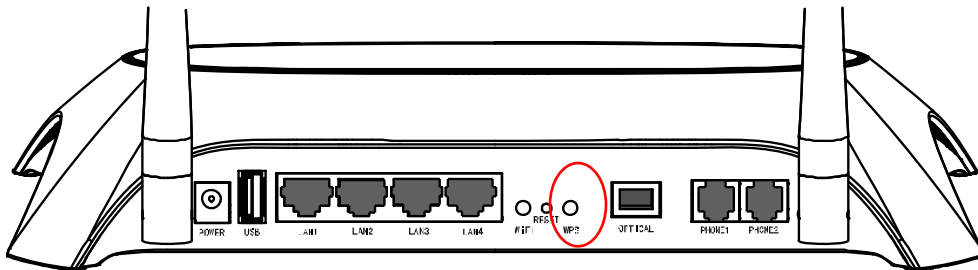
 **Note:**

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. Use the Wi-Fi Protected Setup Button

Use this method if your client device has a Wi-Fi Protected Setup button.

Step 1: Press the WPS button on the back panel of the GPON router, as shown in the following figure.



You can also keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-34, then Choose “**Press the button of the new device in two minutes**” and click **Connect**. (Shown in the following figure)

WPS Settings	
☐	Enter the new device's PIN. PIN:
☒	Press the button of the new device in two minutes.
Connect Back	

Figure 4-35

Step 2: Press and hold the WPS button of the client device directly.

Step 3: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: When the WPS LED is on, the client device has successfully connected to the GPON router.

Refer back to your client device or its documentation for further instructions.

II. Enter the client device's PIN on the GPON router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 1: Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-34, then the following screen will appear.

WPS Settings	
☒	Enter the new device's PIN. PIN:
☐	Press the button of the new device in two minutes.
Connect Back	

Figure 4-36

Step 2: Enter the PIN number from the client device in the field on the above WPS screen. Then click **Connect** button.

Step 3: “**Connect successfully**” will appear on the screen of Figure 4-36, which means the client device has successfully connected to the GPON router.

III. Enter the GPON router's PIN on your client device

Use this method if your client device asks for the GPON router's PIN number.

Step 1: On the client device, enter the PIN number listed on the GPON router's Wi-Fi Protected Setup screen. (It is also labeled on the bottom of the GPON router.)

Step 2: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 3: When the WPS LED is on, the client device has successfully connected to the GPON router.

Step 4: Refer back to your client device or its documentation for further instructions.

Note:

- 1) The WPS LED on the GPON router will light green for five minutes if the device has been successfully added to the network.
- 2) The WPS function cannot be configured if the Wireless Function of the GPON router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.6.3 Wireless Security

Choose menu “**Wireless**”→” **Wireless Security**”, you can configure the security settings of your wireless network.

There are three wireless security modes supported by the GPON router: WEP (Wired Equivalent Privacy), WPA-PSK (Pre-Shared Key), WPA2-PSK (Pre-Shared Key).

Wireless Security Settings

Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled.
 Note: WEP encryption are not supported with Multi SSID enabled.
 For network security, it is strongly recommended to enable wireless security and use WPA2-PSK AES encryption.

SSID: TP-LINK_045004

☐ Disable Wireless Security

☒ WPA/WPA2 - Personal (Recommended)

Authentication Type: WPA2-PSK

Encryption: AES

Wireless Password: 12345670
 (Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 (seconds, minimum is 30, 0 means no update)

☐ WPA/WPA2 - Enterprise

Authentication Type: Auto

Encryption: Auto

RADIUS Server IP:

RADIUS Server Port: 1812 (1-65535, 0 stands for default port 1812)

RADIUS Server Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

☐ WEP

Authentication Type: Open System

WEP Key Format: Hexadecimal

Selected Key:	WEP Key	Key Type
Key 1: ☒		Disabled
Key 2: ☐		Disabled
Key 3: ☐		Disabled
Key 4: ☐		Disabled

Save

Figure 4-37

- **SSID:** Select the SSID from the drop-down list.
- **Disable Wireless Security:** If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the following modes to enable security.
- **WPA/WPA2 – Personal (Recommended):** It's the WPA/WPA2 authentication type based on pre-shared passphrase.

☒ WPA/WPA2 - Personal (Recommended)

Authentication Type: WPA2-PSK

Encryption: AES

Wireless Password: 12345670
 (Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 (seconds, minimum is 30, 0 means no update)

Figure 4-38

- **Authentication Type** - You can choose the version of the WPA-Personal security on the drop-down list. The default setting is **Automatic**, which can select **WPA-Personal** (Pre-shared key of WPA) or **WPA2-Personal** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
- **Encryption** - You can select either **Auto**, or **TKIP** or **AES**.

- **Wireless Password** - You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

➤ **WPA/WPA2 – Enterprise:** It's based on Radius Server.

☒ WPA/WPA2 - Enterprise

Authentication Type:

Encryption:

RADIUS Server IP:

RADIUS Server Port:

RADIUS Server Password:

(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: (in second, minimum is 30, 0 means no update)

- **Authentication Type:** You can choose the version of the WPA security on the drop-down list. The default setting is **Auto**, which can select **WPA** (Wi-Fi Protected Access) or **WPA2** (WPA version 2) automatically based on the wireless station's capability and request.
- **Encryption:** You can select either **Auto**, or **TKIP** or **AES**.
- **RADIUS Server IP:** Enter the IP address of the Radius Server.
- **RADIUS Server Port:** Enter the port that radius service used.
- **RADIUS Server Password:** Enter the password for the Radius Server.
- **Group Key Update Period:** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

➤ **WEP:** It is based on the IEEE 802.11 standard.

☐ WEP

Authentication Type:

WEP Key Format:

Selected Key: **WEP Key** Key Type

Key 1: ☒		Disabled
Key 2: ☐		Disabled
Key 3: ☐		Disabled
Key 4: ☐		Disabled

- **Authentication Type:** You can choose the type for the WEP security on the drop-down list. The default setting is **Open System**. If you choose Auto, the GPON router can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format:** **Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **WEP Key:** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.

- **Key Type:** You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.
- **64-bit:** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.
- **128-bit:** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

Note:

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

Be sure to click the **Save** button to save your settings on this page.

4.6.4 Wireless Schedule

Choose menu "**Wireless**"→"**Wireless Schedule**", you can configure the Task Schedule as shown below.

Task Schedule

Schedule can be set on this page.

Click the schedule table or use the 'Add' button to choose the period on which you need the wireless off automatically!

Wireless Schedule:

☐ Enable
 ☒ Disable

Apply To:

Each Day

Start Time:

00:00

End Time:

24:00

Add

Time	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

<

>

Clear Schedule

Save

Figure 4-39

Note:

The time you set is the period you need the wireless off.

Before configure the wireless schedule, please set system time first which refer to [4.21.2 Time Settings](#), then you can enable or disable Wireless Schedule.

- **Apply To:** Select the day or days you need the wireless off.

- **Start Time, End Time:** You can select all day-24 hours or you may enter the **Start Time** and **End Time** in the corresponding field.

- **Add:** Click this button to add your selected time to the below table.

Click the **Clear Schedule** button to clear your settings in the table.

Click **Save** to complete the settings.

4.6.5 Wireless MAC Filtering

Choose menu “**Wireless**” → “**MAC Filtering**”, you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-40.

Wireless MAC Filtering settings

You can configure the Wireless MAC Filtering to control the wireless access on this page.

Wireless MAC Filtering: Enabled **Disable**

Filtering Rules

☒ **Deny** the stations specified by any enabled entries in the list to access.

☐ **Allow** the stations specified by any enabled entries in the list to access.

☐	MAC Address	Status	Description	Edit
☐	00:1D:0F:11:22:33	Enabled	Wireless station A	Edit

Add New **Enable Selected** **Disable Selected** **Delete Selected**

Figure 4-40

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disabled**.

- **MAC Address:** The wireless station's MAC address that you want to filter.
- **Status:** The status of this entry, either **Enabled** or **Disabled**.
- **Description:** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The following page will appear, shown in Figure 4-41:

Wireless MAC Filtering settings

You can configure the Wireless MAC Filtering to control the wireless access on this page.

MAC Address: e.g. 00:1D:0F:11:22:33

Description:

Status:

Host:

Save **Back**

Figure 4-41

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.

2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click the **Save** button to save this entry.

To edit or delete an existing entry:

1. Click the **Edit** in the entry you want to modify.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/ Disabled Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to selected entries.

For example: If you desire that the wireless station A with MAC address 00:1D:0F:11:22:33 and the wireless station B with MAC address 00:0A:EB:00:07:5F are able to access the GPON router, but all the other wireless stations cannot access the GPON router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button “**Allow the stations specified by any enabled entries in the list to access**” for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New** button.
 - 1) Enter the MAC address 00:1D:0F:11:22:33/00:0A:EB:00:07:5F in the **MAC Address** field.
 - 2) Enter wireless station A/B in the **Description** field.
 - 3) Select **Enabled** in the **Status** drop-down list.
 - 4) Click the **Save** button.
 - 5) Click the **Back** button.

The filtering rules that configured should be similar to the following list:

Filtering Rules
☐ Deny the stations specified by any enabled entries in the list to access.
☒ Allow the stations specified by any enabled entries in the list to access.

☐	MAC Address	Status	Description	Edit
☐	00:1D:0F:11:22:33	Enabled	Wireless station A	Edit
☐	00:0A:EB:00:07:5F	Enabled	Wireless station B	Edit

Add New
Enable Selected
Disable Selected
Delete Selected

4.6.6 Wireless Advanced

Choose menu “**Wireless**”→“**Wireless Advanced**”, you can configure the advanced settings of your wireless network.

Wireless Lan Advanced Settings	
Notice: Wireless mode included 11n, Fragmentation Threshold will be set to default value.	
Transmit Power:	100% ▼
Beacon Interval:	100 (25-1000)
RTS Threshold:	2346 (1-2346)
Fragmentation Threshold:	2346 (256-2346)
DTIM Interval:	1 (1-255)
	☒ Enable Short GI
	☐ Enable Client isolation
	☒ Enable WMM
Save	

Figure 4-42

- **Transmit Power:** Here you can specify the transmit power of GPON router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval:** Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the GPON router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the GPON router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval:** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the GPON router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI:** This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enabled Client isolation:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the GPON router but not with each other. To use this function, check this box. Client isolation is disabled by default.
- **Enable WMM:** WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.

 Note:

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

4.6.7 Wireless Status

Choose menu “**Wireless**”→“**Wireless Status**”, you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Wireless Stations Status				
This page displays the basic information of all stations in this wireless network.				
Current Connected Wireless Stations numbers: 0 Refresh				
ID	MAC Address	Current Status	Received Packets	Sent Packets

Figure 4-43

- **MAC Address:** The connected wireless station's MAC address.
- **Current Status:** The connected wireless station's running status, one of **STA-AUTH/ STA-ASSOC/ STA-JOINED/ WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ AP-UP/ AP-DOWN/ Disconnected**.
- **Received Packets:** Packets received by the station.
- **Sent Packets:** Packets sent by the station.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

4.7 Guest Network

Guest Network
Basic Settings
Guest Network Status

There are two submenus under the Guest Network menu: **Basic Settings** and **Guest Network Status**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.7.1 Basic Settings

Choose menu “**Guest Network**”→“**Basic Settings**”, and you will see the screen as shown in Figure 4-44. This feature allows you to create a separate network for your guests without allowing them to access your main network and the computers connected to it.

Figure 4-44

You can enable or disable Guest Network. When you enable this function, you could set wireless parameters for Guest Network.

- **SSID:** The guest network name. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network. The default name is TP-LINK_Guest_xxxxxx (xxxxxx is the last six numbers of MAC address).
- **Security:** The default value is disabled, but it's strongly recommended to enable WPA/WPA2-Personal. WPA/WPA2-Personal is the WPA/WPA2 authentication type based on pre-shared passphrase.
- **Authentication Type:** Select the Authentication Type from the drop-down list, the default method is **Auto**, and you can leave it as a default setting.
- **Encryption:** You can select either **Auto**, or **TKIP** or **AES**.
- **Wireless Password:** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- **Group Key Update Period:** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **Allow Guests to access my Local Network:** The guests have access to your Local Network, but can not login the GPON router's web management interface.
- **Allow Guests to access my USB Storage Sharing:** The guests can access the specified files on the USB storage device via the function of USB Storage Sharing, but the function of FTP Server, Media Server and Print Server are not available in Guest Network. For more details please refer to [4.9.3 Storage Sharing](#).
- **Guest Network Isolation:** This function can isolate wireless clients on your guest network from each other. Client isolation is disabled by default.
- **Guest Network Bandwidth Control:** With this function, you can configure the Upstream Bandwidth and Downstream Bandwidth for guest network.

Click **Save** to save your settings.

4.7.2 Guest Network Status

Choose menu “**Guest Network**”→“**Guest Network Status**”, you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Guest Network Status					
This page displays the basic information of guests in this wireless network.					
Current Connected Guest Network numbers: 0 Refresh					
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID

Figure 4-45

- **MAC Address:** The connected wireless station's MAC address.
- **Current Status:** The connected wireless station's running status.
- **Received Packets:** Packets received by the station.
- **Sent Packets:** Packets sent by the station.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

4.8 Voice

Choose “**Voice**”, there are nine submenus under the main menu. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

Voice
SIP Account
Digit Map
Dial Plan
Phone Setup
Advanced Setup
Speed Dial
Call Log
Call Firewall
USB Voice Mail

4.8.1 SIP Account

Choose “**Voice**”→“**SIP Account**”, you will see the screen similar to Figure 4-46. SIP accounts are necessary for making VoIP calls. This section introduces how to setup the SIP(Session Initiation Protocol) account for your GPON router.

SIP Account List					
Maximum 8 entries can be configured.					
Profile Name	Registrar Address	Phone Number	Status	Remove	Edit
test1	0.0.0.0	888888888	down	☐	Edit
Add Select All Deselect All Remove					

Figure 4-46

- **Profile Name:** Displays the profile name of the account.
- **Registrar Address:** Displays the IP address or domain name of the SIP Registrar server.
- **Phone Number:** Displays the phone number of the account.
- **Status:** Displays the status of the account. "Down" means that the account has not been registered.
- **Remove:** Check the box and then click the **Remove** button below so that the very account will be deleted.
- **Edit:** Click the **Edit** button to modify the very account.

To set up an SIP account, click the **Add** button in Figure 4-46. Configure the following parameters in Figure 4-47 and then click the **Save** button. Then an account is added. Please note that the blanks with red asterisk behind are required to be entered.

Voice - SIP Account	
SIP Account Basic Settings	
Phone Number/User ID *	Registrar Address 0.0.0.0 *
Authentication ID	Password
Hide	
SIP Account Advanced Settings	
Profile Name Account 1	Registrar Port 5060
Display Name	Priority 4
Preferred Receive Ptime 20	MWI Disable
Incoming Call Route ALL	SIP Proxy Port 5060
SIP Proxy 0.0.0.0	Outbound Proxy Port 5060
Outbound Proxy 0.0.0.0	
☒ Register via Outbound Proxy	
Preferred Codec	
Preferred Codec 1 G.711MuLaw	Preferred Codec 2 G.711ALaw
Preferred Codec 3 G.729a/b	Preferred Codec 4 G.726_32
Save Back	

Figure 4-47

SIP Account Basic

- **Phone Number/User ID:** Enter the phone number or the User ID of the account you applied.
- **Registrar Address:** Set the IP address of the SIP Registrar server, which is provided by your service provider.
- **Authentication ID:** Enter the name or number used for SIP Authorization with SIP Registrar. This value is provided by your service provider. If it's not provided, keep the default value.
- **Password:** This parameter, given by your service provider, holds the password used for authentication within VoIP SIP registrar.

SIP Account Advanced

- **Profile Name:** Assign a name to identify the profile. Please note that special characters are not allowed.
- **Display Name:** Assign a name for your account. This name is the Caller-ID you want to be displayed on your friend's display panel, which can let your friend easily know who is calling. Please note that special characters are not allowed.
- **Registrar Port:** Specify the port of the VoIP SIP registrar on which it will listen for register requests from VoIP device.
- **Preferred Receive Ptime:** Ptime, short for packet time, refers to the time interval for a voice packet to be sent by the remote caller. The unit is ms (millisecond). Usually the default value 20ms is OK.
- **Priority:** Select a priority for this account. This priority is useful when more than one account is added in this GPON router.
- **Incoming Call Route:** Select which line the incoming VoIP call will be routed to.
 - **None:** All incoming VoIP calls will be denied.
 - **Phone 1/Phone 2:** The incoming call will be routed to either Phone1 or Phone 2 randomly.
 - **Idle:** The incoming call will be routed to idle phone in priority.
 - **All:** The incoming call will be routed to both Phone1 and Phone 2 synchronously.
- **MWI:** MWI is short for Message Waiting Indicator. Enable this option, so there will be indications when voice message are received.
- **SIP Proxy:** Enter the SIP proxy if it's provided, or keep the default value.
- **SIP Proxy Port:** Enter the SIP proxy port if it's provided, or keep the default value.
- **Outbound Proxy:** Indicate the VoIP SIP outbound proxy server IP address. This parameter is very useful when VoIP device is behind a NAT, say the GPON router you use connects to Internet by other device. Keep the default if it's not provided by your service provider.
- **Outbound Proxy Port:** Specify the port of the VoIP SIP outbound proxy on which it will listen for messages. Keep the default value if it's not provided by your service provider.

Preferred Codec

- **Preferred Codec (1~4):** Codec is known as Coder-Decoder which is used for data signal conversion. Each codec uses a different bandwidth and hence provides different levels of voice quality. The default codec settings are shown in the corresponding field for your reference. Preferred Codec1 owns the top priority. You can change the value if you are provided with this parameter; otherwise leave it default.

Click **Save** to save your configurations.

Click **Back** to go back to the previous page.

4.8.2 Dial Map

Choose "**Voice**"→"**Dial Map**", you will see the screen as shown in Figure 4-48.

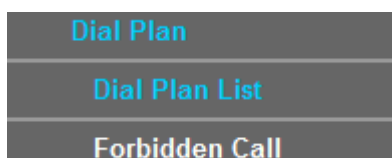
DigitMap																					
Current DigitMap	112 19 [2-5] 1x . t [2-8] x . t 9x . t 0xx . t (256 char max.)*																				
Example: digitmap settings <table border="1"> <thead> <tr> <th>Digitmap Rule</th> <th>Means</th> </tr> </thead> <tbody> <tr> <td>[2-5]</td> <td>match one digit between 2 and 5</td> </tr> <tr> <td>x</td> <td>match one digit between 0 and 9</td> </tr> <tr> <td>[57]</td> <td>5 or 7</td> </tr> <tr> <td>.</td> <td>repeat the previous digit 0 or more times</td> </tr> <tr> <td>t</td> <td>timeout</td> </tr> <tr> <td>3xxxx</td> <td>a digit string has 5 digits which begins with 3</td> </tr> <tr> <td>0x.t</td> <td>a digit string begins with 0 will be sent out after timeout</td> </tr> <tr> <td>0x.#</td> <td>a digit string begins with 0 will be sent out after # is dialed</td> </tr> <tr> <td>0x.</td> <td>a digit string begins with 0 will be sent out after timeout or # is dialed</td> </tr> </tbody> </table>		Digitmap Rule	Means	[2-5]	match one digit between 2 and 5	x	match one digit between 0 and 9	[57]	5 or 7	.	repeat the previous digit 0 or more times	t	timeout	3xxxx	a digit string has 5 digits which begins with 3	0x.t	a digit string begins with 0 will be sent out after timeout	0x.#	a digit string begins with 0 will be sent out after # is dialed	0x.	a digit string begins with 0 will be sent out after timeout or # is dialed
Digitmap Rule	Means																				
[2-5]	match one digit between 2 and 5																				
x	match one digit between 0 and 9																				
[57]	5 or 7																				
.	repeat the previous digit 0 or more times																				
t	timeout																				
3xxxx	a digit string has 5 digits which begins with 3																				
0x.t	a digit string begins with 0 will be sent out after timeout																				
0x.#	a digit string begins with 0 will be sent out after # is dialed																				
0x.	a digit string begins with 0 will be sent out after timeout or # is dialed																				
Save																					

Figure 4-48

Configure the current DigitMap settings, and click the **Save** button to make the configuration take effect.

4.8.3 Dial Plan

Choose “**Voice**”→“**Dial Plan**”, you can see the next submenus:



This section includes Dial Plan List and Forbidden Call. The function allows users to set rules for outgoing calls.

4.8.3.1 Dial Plan List

Choose “**Voice**”→“**Dial Plan**” →“**Dial Plan List**”, you will see the screen similar to Figure 4-49. Dial plan List allows the GPON router to use specific defined account or network to make outgoing calls. If actual numbers dialed match prefix number defined in the dial plan, the dialed number will be routed to the specified network according to this plan. Besides, operation of stripping prefix, replacing prefix or adding prefix, is helpful for users to make a quick and easy call.

Dial Plan					
Maximum 50 entries can be configured.					
Prefix	Op	Destination	Enable	Remove	Edit
Add Select All Deselect All Remove					

Figure 4-49

- **Prefix:** Displays the prefix of your plan. This prefix refers to the initial digit(s) of the numbers you dial.
- **Op:** Displays the operation of this plan.
- **Destination:** Displays the account or network used for this plan.

- **Enable:** Displays the interface(s) enabled in this plan.
- **Remove:** Check the box and then click the **Remove** button below so that the very plan will be deleted.
- **Edit:** Click the **Edit** button to modify the very plan.

To add a dial plan, click the **Add** button in Figure 4-49. Fill in the following parameters and click the **Save** button in Figure 4-50.

Dial Plan																								
Prefix	(16 char max.)*		Destination	None																				
Max Length	(3~32)*		Dial End With	#TimeOut																				
Operate	Strip Prefix		Strip Length	0																				
Interface Enable	☒ Phone 1 ☒ Phone 2																							
Example: 3 typical settings <table border="1"> <thead> <tr> <th>Prefix</th> <th>Operate</th> <th>Destination</th> <th>Dial number</th> <th>Dial out number</th> </tr> </thead> <tbody> <tr> <td>1234</td> <td>Strip Prefix: Strip length 3</td> <td>SIP Account 1</td> <td>1234000</td> <td>4000</td> </tr> <tr> <td>18</td> <td>Replace Prefix: Replace with 1865555</td> <td>SIP Account 1</td> <td>186666</td> <td>18655556666</td> </tr> <tr> <td>0</td> <td>Add Number: Add Number 17951</td> <td>SIP Account 2</td> <td>018655556666</td> <td>17951018655556666</td> </tr> </tbody> </table>					Prefix	Operate	Destination	Dial number	Dial out number	1234	Strip Prefix: Strip length 3	SIP Account 1	1234000	4000	18	Replace Prefix: Replace with 1865555	SIP Account 1	186666	18655556666	0	Add Number: Add Number 17951	SIP Account 2	018655556666	17951018655556666
Prefix	Operate	Destination	Dial number	Dial out number																				
1234	Strip Prefix: Strip length 3	SIP Account 1	1234000	4000																				
18	Replace Prefix: Replace with 1865555	SIP Account 1	186666	18655556666																				
0	Add Number: Add Number 17951	SIP Account 2	018655556666	17951018655556666																				
Save Back																								

Figure 4-50

- **Prefix:** Set number(s) as the prefix. Up to 16 characters can be entered.
- **Destination:** SIP account can be selected here. As to which one will be finally used, it depends on not only Destination selected here but also Dial Plan Priority configured on [Phone Setup](#) page. Please note that if you want to select a SIP account, you should first add one on [SIP Account](#) page; otherwise only NONE is available.
- **Max Length:** Specify the max length of numbers you wish to dial out. The length of the actual dialed number can not exceed the length set here. For example, if the length is set to “6”, when you dial “7654321”, only “765432” will be sent out.
- **Dial End With:** Ways of indicating when the dialing is finished.
 - If “TimeOut” is selected, the dialing will be sent out when timeout starts. The timeout activates when no more digits are dialed in a specific duration;
 - If “#” is selected, the dialing will not be sent until “#” is dialed;
 - If “#/TimeOut” is selected, the dialing will be sent out when timeout starts or “#” is dialed;
 - If “None” is selected, the dialing will not be sent out unless the length of number you dial meets the Max Length.
- **Operate:** Specify a dialing method to make call(s).
 - **Strip Prefix:** If it is selected, the original phone number will be sent out with the prefix deleted; you can limit the strip length by entering digits in “Strip Length” field.
Take the 1st dial plan in Figure 4-50 as an example. If you dial 12340000, number 40000 will be dialed out to make a call.
 - **Replace Prefix:** If it is selected, the original phone number will be sent out with the prefix replaced by what you set in the “Replace With” field.
Take the 2nd dial plan in Figure 4-50 as an example. If you dial 186666, number 18655556666 will be dialed out to make a call.

- **Add Number:** If it is selected, the original phone number will be sent out with what you set in “Add Number” field added ahead.

Take the 3rd dial plan in Figure 4-50 as an example. If you dial 018655556666, number 1795101865556666 will be dialed out to make a call.

- **Interface Enable:** You can check any box to enable interface(s). Numbers matching prefix in Dial Plan List can only be dialed out through the selected interface(s).

Click **Save** to save your configurations.

Click **Back** to go back to the previous page.

4.8.3.2 Forbidden Call

Choose “**Voice**”→“**Dial Plan**”→“**Forbidden Call**”, you will see the screen similar to Figure 4-51. Forbidden Call makes it possible for administrators to control user's access to the voice service.

Forbidden Call			
Maximum 20 entries can be configured.			
Prefix	Forbidden	Remove	Edit
020	Line2 / Line1	☐	Edit
Add Select All Deselect All Remove			

Figure 4-51

- **Prefix:** Displays the prefix of your plan. This prefix refers to the initial digit(s) of the numbers you dial.
- **Forbidden:** Displays the interface(s) disabled in this plan.
- **Remove:** Check the box and then click the **Remove** button below so that the very plan will be deleted.
- **Edit:** Click the **Edit** button to modify the very plan.

To add a dial plan, click the **Add** button in Figure 4-51. Fill in the following parameters and click the **Save** button in Figure 4-52.

Forbidden Call			
Prefix	020 (16 char max.)*	Interface Barring	☒ Phone 1 ☐ Phone 2
Save Back			

Figure 4-52

- **Prefix:** Set number(s) as the prefix. Up to 16 characters can be entered.
- **Interface Barring:** You can check any box to disable interface(s). Numbers matching prefix in Forbidden Call list are not allowed to be dialed out through the selected interface(s).

For example, if you set a dial plan list in the screen as shown in Figure 4-52, phone numbers starts with ‘020’ can only be dialed out through Phone1.

4.8.4 Phone Setup

Choose “Voice”→“Phone Setup”, you will see the screen similar to Figure 4-53. This section allows you to configure phone settings for phone 1 and phone 2.

Phone Setup

Phone1 **Phone2**

Phone Enable: ☒

Dial Settings

Dial Plan Priority: VoIP @ Auto ☒ FallBack to PSTN

End With '#': ☒

Anonymous Calling: ☐

Dial Restriction: According to Forbidden Call

WarmLine Enable: ☐

WarmLine Time: 3s

Warmline Number: [View/Set](#)

Answer Settings

MWI Mode: VMWI

Anonymous Call Blocking: ☐

DND(Do not disturb): ☐

Call Waiting: ☐

Forward Unconditionally: ☐ @ test1

Forward On "busy": ☐ @ test1

Forward On "no answer": ☐ @ test1

"No answer" time: 18 Seconds (5~60)

Telephony Settings

VAD Support: ☒

Speaker Gain: 0dB

Mic Gain: 0dB

[Save](#)

Figure 4-53

- **Phone Enable:** Check the box behind to enable the function.

Dial Settings

- **Dial Plan Priority:** The parameters configured in the 2nd field determine which SIP account to use when making outgoing calls. The following are different options:
 - **VOIP & Auto:** The SIP account specified in the matched dial plan will be chosen first. Otherwise, the account with top priority will be selected. To view the priority, please go to the screen as shown in Figure 4-47.
 - **VOIP & Account X (a certain account):** The Router will always use Account X to make calls.
- **End With '#':** Choose whether to use “#” as the end signal of your dialing or not.
- **Anonymous Calling:** Hide the own phone number for each call and it will not be displayed on the remote site. This feature is only available for VoIP calls and disabled by default.

- **Dial Restriction:** Choose the pull-down menu to set restriction for outgoing calls.
 - **None:** Allow all numbers to be dialed out.
 - **All:** Forbid all numbers to be dialed out.
 - **According to Forbidden Call:** Numbers will be dialed out according to settings in [Forbidden Call](#).
- **WarmLine Enable:** Check the box to enable WarmLine function. So if there is no dialing action after you pick up the phone set, after the warmline time the phone will dial out automatically with the numbers set in Warmline Number.
- **WarmLine Time:** Choose WarmLine Time from the drop-down list to specify an interval before the phone dials out automatically.
- **Warmline Number:** Click “**View/Set**” button to view or set Warmline Number.

Answer Settings

- **MWI Mode:** Options available are VMWI and CLID. If you don't know, please consult your service provider.
- **Anonymous Call Blocking:** Check the box to deny anonymous incoming calls.
- **DND(Do not disturb):** Check the box to deny all incoming calls.
- **Call Waiting:** Check the box to enable this function. When the line is busy, the incoming call will be indicated to wait.
- **Forward Unconditionally:** If the box behind is checked, all the incoming calls will be forwarded to the number set in the 1st field through selected account in the 2nd field. Please note that account available here varies with that in Dial Plan Priority field. If **IP** is selected, only IP address can be set in the 1st field.
- **Forward On "busy":** Check the box to enable this function. When the line is busy, all the incoming calls will be forwarded to the number set in the 1st field through selected account in the 2nd field. Please note that account available here varies with that in Dial Plan Priority field. If **IP** is selected, only IP address can be set in the 1st field.
- **Forward On "no answer"& "No answer" time:** Check the box to enable this function. When there is no answer, all the incoming calls will be forwarded to the number set before “@” through selected account when "No answer" time is out. Please note that account available here varies with that in Dial Plan Priority field. If **IP** is selected, only IP address can be set in the 1st field.

Telephony Settings

- **VAD Support:** VAD(Voice Activation Detection) prevents transmitting the silence packets to consume the bandwidth. It is also known as Silence Suppression which is a software application that ensures the bandwidth is reserved only when voice activity is activated. It is enabled by default.
- **Speaker Gain:** Sound Volume control of speaker.
- **Mic Gain:** Sound Volume control of microphone.

4.8.5 Advanced Setup

Choose “Voice”→“Advanced Setup”, you will see the next screen in Figure 4-54.

Figure 4-54

SIP Advanced Setup:

- **Bound Interface Name:** Bound Interface decides where to send/receive the VOIP traffic. Easy way to select the interface is to check the location of the SIP server. If it locates some where in the Internet then select **Any_WAN**. If it is on the local network then select **LAN**.
- **Locale Selection:** Select a country where you are located. The Router is embedded with some default parameters according to different countries such as ring tones.
- **DSCP for SIP/RTP:** DSCP(Differentiated Services Code Point) is the first 6 bits in the ToS byte. DSCP marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value. Select DSCP for the SIP(Session Initiation Protocol) and RTP(Real-time Transport Protocol) respectively. If you are unsure, please always keep the default value.
- **Dtmf Relay setting:** DTMF is Dual Tone Multi Frequency. Options available are SIPInfo, RFC2833, and InBand. If you are unsure which one to choose, please always keep the default value.
 - **SIPInfo:** If it is selected, the Router will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.
 - **RFC2833:** If it is selected, the Router will capture the keypad number you pressed and transfer it into digital form then send to the other side; the receiver will generate the tone according to the digital form it receives. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.
 - **InBand:** If it is selected, the Router will send the DTMF tone as audio directly when you press the keypad on the phone.
- **Registration Expire Timeout(s):** Expire time for the registration message sending.

- **Registration Retry Interval(s):** Set the time duration for your SIP Registrar server to keep your registration record. Before the time expires, the GPON router will send another register request to SIP Registrar again. If you are unsure of it, please always keep the default value.
- **Enable T38 support:** T38 specifies a protocol for transmitting a fax across IP network in real time. It allows the transfer of fax documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. It will only function when both sites support this feature and are enabled.

4.8.6 Speed Dial

Choose **"Voice"→"Speed Dial"**, you will see the screen as shown in Figure 4-55. This section introduces how to configure Speed Dial for your account.

Speed Dial function can help to store frequently used telephone numbers and make your dial more convenient. It allows you to make a call by pressing a short number and the pound sign # on the phone keypad instead of the original number.

Speed Dial	Number	Remove
------------	--------	--------

Buttons: Add, Select All, Deselect All, Remove

Figure 4-55

To add a Speed Dial entry, click the **Add** button and you will see the screen as shown in Figure 4-56. Fill in the following parameters and then click the Save button.

Enter the original number Eg. "26520001" in the Number space and the desired short number Eg. "1" in the Speed Dial space. Once complete, when dialing "26520001", you need simply press 1 followed by the pound"#" key.

Number: 26520001
Speed Dial: 1

Buttons: Save, Back

Figure 4-56

- **Number:** Enter a phone number.
- **Speed Dial:** Enter a number from 0~99.

Click the **Save** button, you will go back to the previous page and see the following list as shown in Figure 4-57.

Speed Dial	Number	Remove
1	26520001	☐

Buttons: Add, Select All, Deselect All, Remove

Figure 4-57

Click the **Save** button to make the configuration take effect. If you want to delete the entry, check the **Remove** box first, and then click the **Remove** button.

4.8.7 Call Log

Choose “**Voice**”→“**Call Log**”, you will see the screen as shown in Figure 4-58. This function allows you to view call logs and configure call log options.

The table below shows the latest 100 call logs. Click "Config" to choose which type of logs to display on the call log view.

Call Log: ☐ Disable ☒ Enable

No.	Start	Source	Dest	Type	Process	Time
-----	-------	--------	------	------	---------	------

Figure 4-58

- **Call Log:** Check the Enable if you want to make this function take effect; otherwise check the Disable.
- **Start:** Beginning time of the call.
- **Source:** Caller ID, either phone number or IP address.
- **Dest:** Caller ID, either phone number or IP address.
- **Type:** Call types, including Incoming (VoIP) and Outgoing (VoIP).
- **Process:** Process types, including Connected, Local forward, Remote forward, Local transfer, Remote transfer, Conference and Unconnected.
- **Time:** Total call time.

To configure the view of call log, click the **Config** button and you will see the screen as shown in Figure 4-59. This page displays all the call types and process types. You can choose some of them or all of them. Check the boxes before the corresponding options which you desire to view and click the **Save** button to make the configuration take effect.

This page allows you to choose which type of logs to display on Call Log view.

Call Type:

- ☒ Incoming(VoIP)
- ☒ Outgoing(VoIP)
- ☒ Incoming(PSTN)
- ☒ Outgoing(PSTN)

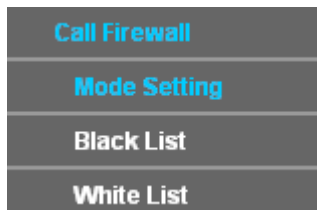
Process Type:

- ☒ Connected
- ☒ Local forward
- ☒ Remote forward
- ☒ Local transfer
- ☒ Remote transfer
- ☒ Conference
- ☒ Unconnected

Figure 4-59

4.8.8 Call Firewall

Choose “Voice”→“Call Firewall”, you can see the next submenus:



Call Firewall can be used to control incoming calls. This section introduces how to configure the Call Firewall. Choose “Voice”→“Call Firewall”→“Mode Setting”, you will see the screen as shown in Figure 4-60.

Call Firewall

Call Firewall Enable: ☐

Call Firewall Mode: ☒ Black
☐ White
☐ RejectAll

Attention!
 In Black List Mode, calls from numbers placed on the Black List will be denied;
 In White List Mode, only calls from numbers placed on the White List will be allowed;
 In Reject All Mode, all calls will be denied.

Save Black List White List

Figure 4-60

- **Call Firewall Enable:** Check the box if you want to make the Call Firewall take effect.
- **Black:** Check the **Black** box to enable Black List mode. Calls from numbers placed in the Black List will be denied.
- **White:** Check the **White** box to enable White List mode. Only calls from numbers placed in the White List will be allowed.
- **RejectAll:** Check the **RejectAll** box to enable Reject All mode. All incoming calls will be denied.

To configure the Black List, choose “Voice”→ “Call Firewall”→“Black List” on the main menu or click the **Black List** button on screen as shown in Figure 4-60, you will see the screen as shown in Figure 4-61.

Black List

Choose Add, or Remove to configure Black List.
 Maximum 30 entries can be configured.

ID	number	remove
1	555	☐

Add Select All Deselect All Remove

Figure 4-61

To add a new entry, click the **Add** button and you will see the screen as shown in Figure 4-62.

Figure 4-62

Enter a number with the length in the range of [3, 16] in the field of **Black List Number** and Click the **Save** button to make the configuration take effect, then you will go back to the previous page and see the following list as shown in Figure 4-61. If you want to delete the entry, check the **Remove** box first and then click the **Remove** button.

To configure the White List, choose “**Voice**” → “**Call Firewall**” → “**White List**” on the main menu or click the **White List** button on the screen as shown in Figure 4-60, then you will see the screen as shown in Figure 4-63.

ID	number	remove
1	5552510	☐

Figure 4-63

To add a new entry, click the **Add** button and you will see the screen as shown in Figure 4-64.

Figure 4-64

Enter a number with the length in the range of [3, 16] in the field of **White List Number** and click the **Save** button to make the configuration take effect, then you will go back to the previous page and see the following list as shown in Figure 4-63. If you want to delete the entry, check the **Remove** box first and then click the **Remove** button.

Note:

1. Partial matching rule is applied here, so this function works for all the incoming call numbers that start with the number you have configured in the Black List or the White List. For example, if the number you have configured in the Black List is 555, with Black List mode enabled the incoming call number 5554510 will be denied.
2. If the incoming call numbers match the rules set in both Black List and White list, longest matching rule will function in this situation. For example, if you set 222 in Black List and 2224 in White List, with Black List mode enabled, incoming call number 2224510 will be allowed.

4.8.9 USB Voice Mail

Choose “Voice”→“USB Voice Mail”, you will see the screen as shown in Figure 4-65. USB Voice mail is used to record voice messages when the call is not answered. To use this function, please make sure an external USB hard drive/USB flash disk with configure files has been plugged into the USB port on the GPON router.

USB Voice Mail

NOTE: Please wait for a few seconds when you click "Play" for the first time!

☒ Phone 1
 ☒ Phone 2

Item per Page 10

Phone	Source	Dest	Start Time	Length	Audition	Read Flag	Selected
1	888	111	2000-01-01 00:03:43	3s	Play	YES	☐
1	888	111	2000-01-01 00:15:27	2s	Play	YES	☐
1	888	111	2000-01-01 00:28:58	4s	Play	YES	☐
1	888	111	2000-01-01 00:02:29	2s	Play	YES	☐
1	888	111	2000-01-01 00:04:45	3s	Play	YES	☐
1	888	111	2000-01-01 00:05:20	2s	Play	YES	☐
2	888	111	2038-01-01 00:01:53	1s	Play	YES	☐
2	888	222	2038-01-01 00:02:53	6s	Play	NO	☐
2	4000	222	2038-01-01 00:08:54	7s	Play	NO	☐
2	888	222	2000-01-01 01:06:33	4s	Play	NO	☐

Last 1 2 3 Next

Refresh

Select All

Deselect All

Remove

Config

Figure 4-65

- **Phone:** Displays the phone that has voice message.
- **Source:** Displays the source of the voice message, i.e. the remote caller account.
- **Dest:** Displays the destination of the voice message, i.e. the local account.
- **Start Time:** Displays when the voice message starts.
- **Length:** Displays how long the voice message is.
- **Audition:** Click **Play** to listen to the voice message.
- **Read Flag:** Displays whether the voice message has been read or not.
- **Selected:** Check the box to select the corresponding voice message.

To refresh the web page, click **Refresh** button.

To delete a voice message, check the **Selected** box and then click **Remove** button.

To configure the USB Voice Mail, click **Config** button to enter the web page as shown in Figure 4-66.

USB Voice Mail Configuration

NOTE: Please fresh this page when USB hotplug happened!

☒ Enable Local Play Operation Notify
☐ Enable Global Wav Format
☒ Enable Remove Expired Voice

Expired Days(7~15):
 Voice Duration Limit(20~120s):
 USB MailBox Capacity(0~1149M):

Phone1
Phone2

Phone Enabled ☐

Phone Mode:

Customize Voice Notify For Record ☒

Voice Notify For Record:

Remote Access PIN:

Figure 4-66

- **Enable Local Play Operation Notify:** Check this box so there will be sound indication for operation when you listen to the voice messages. This is enabled by default. If you are very familiar with the operations, you can disable it.
- **Enable Global Wav Format:** Check this box and all the voice message will be saved as wav files in your USB device. It is convenient for users to listen to the voice messages on the computer. Considering the capacity of your USB device, it is disabled by default.
- **Enable Remove Expired Voice:** Check this box and then the expired voice messages will be deleted automatically. Considering the capacity of USB device, it is enabled by default.
- **Expired Days(7~15):** Configure the days that you want the voice messages to be kept.
- **Voice Duration Limit(20~120s):** This option is used to limit the duration of a voice message.
- **USB MailBox Capacity:** Set the capacity for the USB mailbox. Please note that the capacity set should be less than that of the USB device.
- **Phone Enable:** Check the box to enable this function.
- **Phone Mode:** If **no answer** is selected, voice notification will be played when there is no answer. If **unconditionally** is selected, all incoming calls will be directed to voice mail.
- **Customize Voice Notify For Record:** Check the box to enable voice notification customization. To record your own voice notification, press “*30” after picking up your phone set.
- **Voice Notify For Record:** Select to use the default or customized voice notification.
- **Remote Access PIN:** This PIN code is used to listen to the voice messages in a remote place. Operations are as follows.
 - 1) Call the local phone and wait for the voice notification.
 - 2) Press “*” before the notification is over.

- 3) Input the PIN code according to the notification.
- 4) You can listen to all the new messages after the PIN code is validated.

Click **Save** to save your configurations.

Click **Back** to go back to the previous page, i.e. Figure 4-65.

4.9 USB Settings

USB Settings
USB Mass Storage
User Accounts
Storage Sharing
FTP Server
Media Server
Print Server

There are six submenus under the USB Settings menu, **USB Mass Storage**, **User Accounts**, **Storage Sharing**, **FTP Server**, **Media Server** and **Print Server**. Click any of them, and you will be able to configure the corresponding function.

4.9.1 USB Mass Storage

Choose menu “**USB Settings**” → “**USB Mass Storage**”, you can configure a USB disk drive attached to the GPON router and view volume and share properties such as share name, capacity, status, and action, etc on this page as shown below.

USB Mass Storage

This page provides the basic information about the connected USB mass storage, to configure Storage Sharing/FTP/Media Server, please click the corresponding menu on the left side.

- Click the refresh button to detect your USB device. The Modem Router will automatically activate the first two USB storage devices or up to eight volumes;
- If you want to use other volumes in your storage device(s), please "Deactivate" some unused volumes and "Activate" the other desired volumes;
- Click "Disconnect" button before unplugging your USB device to avoid data loss or damage to the device.

Note:

Supported USB Mass Storage: hard disk, flash disk or memory card reader;

Supported File Type: FAT32 and NTFS;

Supported Volumes: Only two USB storage devices with up to eight volumes could be activated simultaneously, up to four USB storage devices with about eighteen volumes could be recognized.

USB Mass storage List:

Disk1: Teclast (CoolFlash) Rev: 0.00 Connected [Disconnect](#)

Volume	File System	Capacity	Status	Action
sda1	FAT32	1.1 GB	Active	Deactivate

[Refresh](#)

Figure 4-67

- **Volume:** The volume name of the USB drive the users have access to.
- **File System:** The system of the USB drive.

- **Capacity:** The storage capacity of the USB driver.
- **Status:** Indicates the shared or non-shared status of the volume. **Active** means volume can be shared, while **Inactive** means volume can not be shared. If **Deactivate** in Action field is enabled, **Inactive** will be displayed in the Status field, which means volume can not be shared.
- **Action:** When the volume is shared, you can click the **Deactivate** to stop sharing the volume; when volume is non-shared, you can click the **Activate** button to share the volume.

Click **Disconnect** to safely remove the USB storage device that is connected to USB port.

 Note:

Before removing the USB storage device, you should click "Disconnect" to make sure that all your data have been saved completely. Removing device directly may cause your USB storage device crashed.

4.9.2 User Accounts

You can specify the user name and password for Storage Sharing and FTP Server users on this page. Storage Sharing users can access the folders by entering the following URL into the address field of your browser or Windows Explorer, such as "\\192.168.1.1". FTP Server users can log into the FTP Server via FTP Client.

There are five users here, which provide means to control the access to the USB mass storage by Storage Sharing or FTP. The Super User has the right to read and write to Storage Sharing and FTP Server.

User Accounts			
This page allows you to control the user account for FTP/Samba Server. The "Super User" could access all active volumes and shared folders with full-access permission (Read & Write). Please click "Apply" button to apply your configuration.			
Index	User Name	Status	Action
1	admin*	Enabled	☒ Enable ☐ Disable
2			
3			
4			
5			
*: "Super User", It has full-access permission to all activated volume(s) and share folder(s).			
Choose Index: 1 New User Name: New Password: Confirm Password: Set (It will not take effect until you Apply it.)			
Refresh Apply			

Figure 4-68

To add a new user account, please follow the steps below:

1. Choose the index from the drop-down list of **Choose Index**.
2. Self-define a **New User Name**.
3. Enter the password in the **New Password** field.

4. Re-enter the password in the **Confirm Password** field.
5. Click the **Set** button, and then a new entry will be added in the table.
6. Click the **Apply** button to apply your settings.

Click the **Refresh** button to refresh this page immediately.

4.9.3 Storage Sharing

Choose menu “**USB Settings**” → “**Storage Sharing**”, you can configure a USB disk drive attached to the GPON router and view volume and share properties on this page as shown below.

Storage Sharing Settings

Storage Sharing allows you to share the files on the USB storage device with other computers locally. It is based on NetBIOS/SMB protocol which is supported by most Windows operating system or any other operating system.

Once you have configured the shared folders and then enabled the Storage Sharing function, you will be able to access the folders with the following methods:

For Windows OS: Open "Run" window in the Start menu and enter \\(IP Address) or \\(IP Address)\(Share Name), eg. \\192.168.1.1 or \\192.168.1.1\photo;

For Mac OS: Open "Connect to Server" window in the Go menu and enter smb://(IP Address) or smb://(IP Address)/(Share Name), eg. smb://192.168.1.1 or smb://192.168.1.1/photo.

anonymous: All active volume(s) will be shared and authentication is not **required**.

Server Status: Enabled Disable

☒ Anonymous access to all the volumes

Folder Table: (Any changes of this table will not take effect until you Apply it.)

	Share Name	Directory	User Access (F:Full-Access, R:Read-Only, N:No-Access)					Status	Edit
			1*	2	3	4	5		
☐	volume	/	F	-	-	-	-	Enabled	Edit

* : "Super User", It has full-access permission to all activated volume(s) and share folder(s).

Add New Folder
Enable Selected
Disable Selected
Delete Selected

Apply

Figure 4-69

- **Server Status:** Indicates the Storage Sharing's current status.
- **Anonymous access to all the volumes:** If this function is enabled, users can access all activated volumes of Storage Sharing without accounts.
- **Share Name:** This folder's display name.
- **Directory:** The real full path of the specified folder.
- **User Access:** The authorization of the user is displayed. * users mean Super Users who have the full-access permission to all activated volumes and share folders. Grey users mean the users who have no right to use this function. Others are common users.
- **Status:** The status of the entry is enabled or disabled.
- **Edit:** Click **Edit** in the table, and then you can modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-69.

Folder Browse

This page allow you to set a shared folder and access authorization for Storage Sharing service! It will not take effect when Anonymous access been enabled.

Share Name:

Directory:

User Access Control Table:

Index	User Name	Access Authorization
1*	admin	☒ Full-Access ☐ Read-Only ☐ No-Access
2		
3		
4		
5		

*: "Super User", It has full-access permission to all actived volume(s) and share folder(s).

Figure 4-70

2. Click the **Browse** button, and then select the **Select Volume** from the drop-down list.
3. Enter display name of the share folder in **Share Name** filed.
4. Click the **Apply** button to apply the settings.

You can click the **upper** button to go to the upper folder

Click the **Enable/Disable Selected** button to enable or disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

 Note:

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the Storage Sharing settings, you can click the Apply button to make the changes take effect.

4.9.4 FTP Server

Choose menu **"USB Settings"→"FTP Server"**, you can create an FTP server that can be accessed from the Internet or your local network.

FTP Server Setting

FTP (File Transfer Protocol) server allows you to share the files on the USB storage device to the local or public network. You will need to define the shared folders, then assign the user's authorization for the different folders.

Once you have configured the folders and enabled the FTP Server, you will be able to access the folders by entering the following URL on Windows Explorer or other FTP software:

ftp://(IP Address) eg. ftp://192.168.1.1

Server Status: **Enabled** **Disable**

Internet Access: ☐ Enable ☒ Disable

Internet Address: 0.0.0.0

Service Port: 21 (The default is 21. Do not change unless necessary.)

Folder Table: (Any changes of this table will not take effect until you Apply it.)

	Share name	Directory	User Index (F:Full-Access, R:Read-Only, N:No-Access)					Status	Edit
			1*	2	3	4	5		
☐	volume	/	F	-	-	-	-	Enabled	Edit

*: "Super User", It has full-access permission to all actived volume(s) and share folder(s).

Figure 4-71

- **Server Status:** Indicates the FTP Server's current status.
- **Internet Access:** Enable or disable this function.
- **Internet Address:** If **Internet Access** is enabled, WAN IP will be displayed here.
- **Service Port:** Enter the FTP Port number to use. The default is 21.
- **Share Name:** This folder's display name.
- **Directory:** The real full path of the specified folder.
- **User Index:** The authorization of the user is displayed.
- **Status:** The status of the entry is enabled or disabled.
- **Edit:** Click **Edit** in the table, and then you can modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-88.

Folder Browse

This page allow you to set a shared folder and access authorization for Ftp services!

Share Name:

Directory:

User Access Control Table:

Index	User Name	Access Authorization
1*	admin	☒ Full-Access ☐ Read-Only ☐ No-Access
2		
3		
4		
5		

*: "Super User", It has full-access permission to all actived volume(s) and share folder(s).

Figure 4-72

- Click the **Browse** button, and then select the **Select Volume** from the drop-down list.
- Enter display name of the share folder in **Share Name** filed.
- Click the **Apply** button to apply the settings.

You can click the **upper** button to go to the upper folder.

Click the **Enable/Disable Selected** button to enable or disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

 Note:

- The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
- If you want to change the FTP settings, you can click the Apply button to make the changes take effect.

4.9.5 Media Server

Choose menu “**USB Settings**”→“**Media Server**”, you can create media server that allows you to share stored content with other computers and devices on your home network and on the Internet.

Media Server Settings

You can set Media Server to share your media.

Server Enable: ☐

Server Name:

Content Scan: Manual Scan

Auto Scan ☐ every hour

Figure 4-73

- **Server Enable:** Select this box to enable this function.
- **Server Name:** The name of this Media Server.

To add a new share folder for your media server, please follow the instructions below:

- a) Click **Add New Folder** button, and you will see the screen as shown in Figure 4-91.
- b) Enter the name of the share folder in **Share Name** field.
- c) Click the **Apply** button to apply the configuration.

Folder Browse	
This page allow you to set a scan folder for DLNA media service!	
Share Name:	
Directory:	/
	Browse
Apply	

Figure 4-74

- b) Click the **Scan now** to scan all the share folders immediately. You can also select the **Auto-scan**, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

 Note:

The max share folders number is 6. If you want share a new folder when the numbers has been reached to be 6, you can delete a share folder and then add a new one.

4.9.6 Print Server

Choose menu **"USB Settings"→"Print Server"**, you can configure print server on this page as shown below.

Print Server Setting	
Server Status:	Online Stop

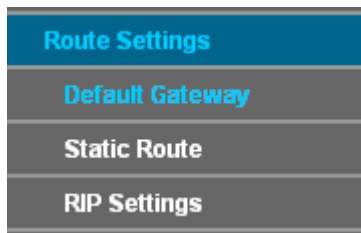
Figure 4-75

There are three states of the print server, they are as follows:

- **Online:** Indicates the print service has been turned on, and no user is using the print services at present. You can click the **"Stop"** button to stop the print service.
- **Offline:** Indicates the print service feature is disabled. You can click **"Start"** button to start the print service.
- **Busy:** Indicates the print service has been turned on, but at this moment other users are using print services.

4.10 Route Settings

Choose “**Route Settings**”, it includes three menus: **Default Gateway**, **Static Route** and **RIP Settings**. The detailed descriptions are provided below.



4.10.1 Default Gateway

Choose “**Route Settings**”→“**Default Gateway**”, you can see the Default Gateway screen. You can select a WAN Interface from the drop-down list as the system default gateway.

Default Gateway Settings

Note1: Select a preferred WAN interface as the system default gateway.

Select WAN Interface: No available interface. ▾ Add Interface

Save

Figure 4-76

Click the **Add Interface** button, you can add WAN Interfaces.

Click the **Save** button to save your settings.

4.10.2 Static Route

Choose “**Route Settings**”→ “**Static Route**”. You can see the Static Route screen, this screen allows you to configure the static routes (shown in Figure 4-77). A static route is a pre-determined path that network information must travel to reach a specific host or network.

Static Route

This page displays static route table. Click relevant button to configure it.

☐	Destination IP Address	Subnet Mask	Gateway	Status	Edit
☐	202.96.134.210	255.255.255.0	172.30.74.1	Enabled	Edit

Add New Enable Selected Disable Selected Delete Selected

Refresh

Figure 4-77

To add static routing entries:

1. Click the **Add New** button in Figure 4-77, and you will see the screen as shown in Figure 4-78.

Static Route	
Static Route information can be set on this page.	
Destination IP Address:	202.96.134.210
Subnet Mask:	255.255.255.0
Gateway:	172.30.74.1
Interface:	LAN
Status:	Enabled
Save Back	

Figure 4-78

2. Enter the following data:

- **Destination IP Address:** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Subnet Mask:** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway:** Here you should type the Gateway address correctly, and the option for **Interface** will adopt the default Gateway address for the Static Route.
- Interface:** Select the Interface name in the text box, or else, the default Use Interface will be adopted for the Static Route.
- **Status:** Select **Enabled** or **disabled** from the drop-down list.

3. Click **Save** to save your settings as shown in Figure 4-78.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

4.10.3 RIP Settings

Choose “**Route Settings**”→“**RIP Settings**”, you can see the RIP (Routing Information Protocol) screen which allows you to configure the RIP.

RIP Settings			
To activate RIP for the WAN interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save/Apply' button to start/stop RIP and save the configuration.			
NOTE: RIP cannot be configured on the WAN interface which has NAT enabled.			
Interface	Version	Operation	Enabled
Save			

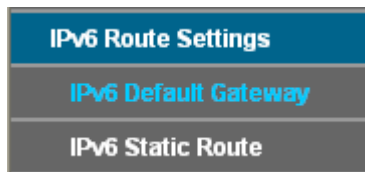
Figure 4-79

Note:

RIP cannot be configured on the WAN Interface which has NAT enabled (such as PPPoE).

4.11 IPv6 Route Settings

Choose “**IPv6 Route Settings**”, it includes three menus: **IPv6 Default Gateway**, **IPv6 Static Route**. The detailed descriptions are provided below.



4.11.1 IPv6 Default Gateway

Choose “**IPv6 Route Settings**”→“**IPv6 Default Gateway**”, you can see the IPv6 Default Gateway screen. You can select a WAN Interface from the drop-down list as the system default gateway.

The screenshot shows the 'IPv6 Default Gateway Settings' page. It has a blue header. Below the header, there is a text prompt: 'Select a preferred WAN interface as the system IPv6 default gateway.' Underneath, there is a label 'Select WAN Interface:' followed by a dropdown menu currently showing 'No available interface.' and a blue arrow icon. To the right of the dropdown is a yellow button labeled 'Add Interface'. At the bottom right of the page is a yellow button labeled 'Save'.

Figure 4-80

Click the **Add Interface** button, you can add WAN Interfaces.

Click the **Save** button to save your settings.

4.11.2 IPv6 Static Route

Choose “**IPv6 Route Settings**”→ “**IPv6 Static Route**”. You can see the IPv6 Static Route screen, this screen allows you to configure the static routes (shown in Figure 4-81). A static route is a pre-determined path that network information must travel to reach a specific host or network.

The screenshot shows the 'IPv6 Static Route' page. It has a blue header. Below the header, there is a text prompt: 'This page displays IPv6 static route table. Click relevant button to configure it.' Below this is a table with four columns: 'Destination IPv6 Address/Prefix Length', 'Gateway', 'Status', and 'Edit'. There is a checkbox in the first column. Below the table are four yellow buttons: 'Add New', 'Enable Selected', 'Disable Selected', and 'Delete Selected'. At the bottom center is a yellow button labeled 'Refresh'.

Figure 4-81

To add IPv6 static routing entries:

1. Click the **Add New** button in Figure 4-81, and you will see the screen as shown in Figure 4-82.

Static Route	
Static Route information can be set on this page.	
Destination IP Address:	202.96.134.210
Subnet Mask:	255.255.255.0
Gateway:	172.30.74.1
Interface:	LAN
Status:	Enabled
Save Back	

Figure 4-82

2. Enter the following data:
 - **Destination IP Address:** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
 - **Subnet Mask:** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
 - **Gateway:** Here you should type the Gateway address correctly, and the option for **Interface** will adopt the default Gateway address for the Static Route.
Interface: Select the Interface name in the text box, or else, the default Use Interface will be adopted for the Static Route.
 - **Status:** Select **Enabled** or **disabled** from the drop-down list.
3. Click **Save** to save your settings as shown in Figure 4-82.

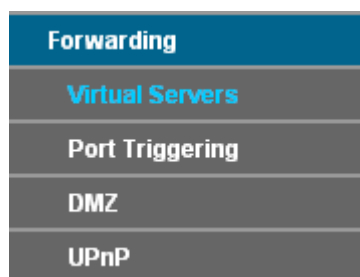
To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

4.12 Forwarding



There are four submenus under the Forwarding menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.12.1 Virtual Servers

Choose menu “**Forwarding**” → “**Virtual Servers**”, and then you can view and add virtual servers in the next screen (shown in Figure 4-83). Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

☐	Service Port	IP Address	Protocol	Status	WAN	Edit
☐	21	192.168.1.100	TCP or UDP	Enabled	pppoe_8_35_2	Edit

Figure 4-83

- **Service Port:** The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX – YYY; XXX is the Start port and YYY is the End port).
- **IP Address:** The IP address of the PC running the service application.
- **Protocol:** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the GPON router).
- **Status:** The status of this entry, "Enabled" means the virtual server entry is enabled.
- **Edit:** To modify or delete an existing entry.

To setup a virtual server entry:

1. Click the **Add New** button. (pop-up Figure 4-84)
2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** field.
3. Select the service you want to use from the **Use Interface** list.
4. Enter the IP address of the computer running the service application in the **IP Address** field.
5. Select the protocol used for this application in the **Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
6. Select the **Enabled** option in the **Status** drop-down list.

Click the **Save** button.

Virtual Server	
Virtual server defines the mapping from WAN service port to LAN server. All requests from the Internet to this service port will be redirected to the computer specified by the server IP. Note: Virtual Server setup is supported only when there is available interface.	
Use Interface:	pppoe_8_35_2
Service Port:	(XX-XX or XX)
IP Address:	
Protocol:	ALL
Status:	Enabled
Common Service Port:	---Please Select---
Save Back	

Figure 4-84

 Note:

It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and type the same IP address for that computer or server.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

 Note:

If you set the service port of the virtual server as 80, you must set the Web management port on **System Tools → Remote Management** page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.12.2 Port Triggering

Choose menu “**Forwarding**”→“**Port Triggering**”, you can view and add port triggering in the next screen (shown in Figure 4-85). Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. Port Triggering is used for some of these applications that cannot work with a pure NAT GPON router.

Port Trigger						
Some applications require multiple connections, such as Internet games, video conferences, Internet callings and so on. Due to firewall, these applications cannot work with a pure NAT Router. Port Triggering can help some of these applications deal with this problem.						
☐	Trigger Port	Trigger Protocol	Open Port	Open Protocol	Status	Edit
☐	6112	TCP or UDP	6112	TCP or UDP	Enable	Edit
Add New Enable Selected Disable Selected Delete Selected						
Refresh						

Figure 4-85

To add a new rule, follow the steps below.

1. Click the **Add New** button, the next screen will pop-up as shown in Figure 4-86.
2. Select a common application from the **Common Service Port** drop-down list, then the **Trigger Port** field and the **Open Ports** field will be automatically filled. If the **Common Service Port** do not have the application you need, enter the **Trigger Port** and the **Open Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All**.
5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.

Some applications require multiple connections, such as Internet games, video conferences, Internet callings and so on. Due to firewall, these applications cannot work with a pure NAT Router. Port Triggering can help some of these applications deal with this problem.

Note: Port Triggering is supported only when there is available interface.

Use Interface:

Trigger Port:

Trigger Protocol:

Open Port:

Open Protocol:

Status:

Common Service Port:

Figure 4-86

- **Trigger Port:** The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Trigger Protocol:** The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the GPON router).
- **Open Port:** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",", for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Open Protocol:** The protocol used for **Incoming Port**, either **TCP**, **UDP**, or **ALL** (all protocols supported by the GPON router).
- **Status:** The status of this entry, Enabled means the Port Triggering entry is enabled.
- **Modify:** To modify or delete an existing entry.
- **Common Service Port:** Some popular applications already listed in the drop-down list of **Open Protocol**.

To modify or delete an existing entry:

1. Find the desired entry in the table.

2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

Once the GPON router is configured, the operation is as follows:

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field.
2. The GPON router records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host.
3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

 Note:

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Open Ports** ranges cannot overlap each other.

4.12.3 DMZ

Choose menu “**Forwarding→DMZ**”, and then you can view and configure DMZ host in the screen (shown in Figure 4-87). The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. The GPON router forwards packets of all services to the DMZ host. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

DMZ
The DMZ host feature allows one local host to be exposed to the Internet for bidirectional communication. DMZ Status: ☐ Enable ☒ Disable DMZ Host IP Address: 0.0.0.0 Save

Figure 4-87

To assign a computer or server to be a DMZ server:

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

4.12.4 UPnP

Choose menu “**Forwarding→UPnP**”, and then you can view the information about **UPnP** in the screen (shown in Figure 4-88). The **Universal Plug and Play (UPnP)** feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

The screenshot shows the 'UPnP config' page. At the top, it says 'This page displays UPnP status and settings.' Below this, the 'Current UPnP Status' is shown as 'Disabled' with an 'Enable' button next to it. Underneath is the 'Current UPnP Settings List' which is a table with 7 columns: ID, App Description, External Port, Protocol, Internal Port, IP Address, and Status. At the bottom of the page is a 'Refresh' button.

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
Refresh						

Figure 4-88

- **Current UPnP Status:** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
- **Current UPnP Settings List:** This table displays the current UPnP information.
 - **App Description:** The description about the application which initiates the UPnP request.
 - **External Port:** The port which the GPON router opened for the application.
 - **Protocol:** The type of protocol which is opened.
 - **Internal Port:** The port which the GPON router opened for local host.
 - **IP Address:** The IP address of the local host which initiates the UPnP request.
 - **Status:** Either Enabled or Disabled. "Enabled" means that the port is still active; otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.

Click the **Disable** button to disable UPnP.

Click the **Refresh** button to update the Current UPnP Settings List.

4.13 Parental Control

Choose menu “**Parental Control**”, and you can configure the parental control in the screen as shown in Figure 4-89. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

Parent Control

Parental Control function can be used to control the Internet activities of the child, limit the child to access specified websites in specified time.

☐ Enable Parental Control

MAC Address Of Parental PC:

MAC Address of Current PC:

40:61:86:E5:B2:DC

Copy to Above

Save

MAC Address - 1:

MAC Address - 2:

MAC Address - 3:

MAC Address - 4:

MAC Address in current LAN:

40:61:86:E5:B2:DC

Fill In

--Please--

Apply To:

Each Day

Start Time:

00:00

End Time:

24:00

Add

Time	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

Clear Schedule

Add URL:

Add

☐ Details

Delete Selected

(It will not take effect until you save it.)

Save

Figure 4-89

- **Enable Parental Control:** Check the box if you want this function to take effect. This function is disabled by default.
- **MAC Address of Parental PC:** In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.
- **MAC Address of Current PC:** This field displays the MAC address of the PC that is managing this GPON router. If the MAC Address of your adapter is registered, you can click the Copy to Above button to fill this address to the MAC Address of Parental PC field above.
- **Add URL:** Here you can input the net addresses which the child is allowed to access.

Click the **Save** button to save your settings.

86

4.14 Firewall

Firewall
Rule
LAN Host
WAN Host
Schedule

There are four submenus under the Firewall menu: **Rule**, **LAN Host**, **WAN Host** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.14.1 Rule

Choose menu “**Firewall**” → “**Rule**”, and then you can view and set Access Control rules in the screen as shown in Figure 4-90.

The router can restrict the internet behavior of lan host. You can enable or disable this function on this page, and set default rules. Furthermore, you can set flexible combination rules by selecting proper "Lan Host", "Wan Host" and "Schedule" to construct the integrated and powerful internet control rules.

☐ Enable Firewall

Default Filtering Rules:

☒ **Allow** the packets not specified by any filtering rules to pass through the device

☐ **Deny** the packets not specified by any filtering rules to pass through the device

Note: The modern router will first try to match the packet with the enabled filtering rules one by one in the list and apply the first matching rule. If the packet is not specified by any filtering rules in the list, then the Default Filtering Rule will take effect.

	Description	Lan Host	Target	Schedule	Pass	Status	Edit
☐							

Figure 4-90

- **Enable Firewall:** Select the check box to enable the Firewall function, so the default filtering rules can take effect.
- **Description:** Here displays the description of the rule and this name is unique.
- **LAN Host:** Here displays the host selected in the corresponding rule.
- **Target:** Here displays the target selected in the corresponding rule.
- **Schedule:** Here displays the schedule selected in the corresponding rule.
- **Status:** Here displays the status of the rule, enabled or not.
- **Edit:** Here you can edit or delete an existing rule.
- **Add New:** Click the **Add New** button to add a new rule entry.
- **Enable Selected:** Click the **Enable Selected** button to enable the selected rules in the list.
- **Disable Selected:** Click the **Disable Selected** button to disable the selected rules in the list.
- **Delete Selected:** Click the **Delete Selected** button to delete the selected entries in the table.

The methods to add a new rule:

1. Click the **Add New** button and the next screen will pop up as shown in Figure 4-91.
2. Give a name (e.g. Rule_1) for the rule in the **Description** field.
3. Select a host from the **LAN Host** drop-down list or choose “**Add LAN Host**”.
4. Select a target from the **WAN Host** drop-down list or choose “**Add WAN Host**”.
5. Select a schedule from the **Schedule** drop-down list or choose “**Add Schedule**”.
6. In the **Action** field, select **Deny** or **Allow** to deny or allow your entry.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. In the **Direction** field, select **IN** or **OUT** from the drop-down list for the direction.
9. In the **Protocol** field, here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
10. Click the **Save** button.

Firewall Rules

An internet control rule can be set on this page.

Description:

LAN Host: [Add LAN Host](#)

WAN Host: [Add WAN Host](#)

Schedule: [Add Schedule](#)

Action:

Status:

Direction:

Protocol:

Figure 4-91

4.14.2 LAN Host

Choose menu “**Firewall**” → “**LAN Host**”, and then you can view and set a Host list in the screen as shown in Figure 4-92.

LAN HOST

	Description	Address Info	Edit
☐	Host_1	192.168.1.88	Edit

Figure 4-92

- **Description:** Here displays the description of the host and this description is unique.
- **Address Info:** Here displays the information about the host. It can be IP or MAC.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In the **Mode** field, select IP Address or MAC Address.
 - If you select IP Address, please follow the steps below:
 - 1) In **Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In **IP Address** field, enter the IP address.
 - If you select MAC Address, please follow the steps below:
 - 1) In **Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

Click the **Delete Selected** button to delete the selected entries in the table.

4.14.3 WAN Host

Choose menu “**Firewall**” → “**WAN Host**”, and then you can view and set a Host list in the screen as shown in Figure 4-93.

WAN HOST			
☐	Description	Details	Edit
☐	Host_1	202.114.71.2	Edit
Add New		Delete Selected	

Figure 4-93

- **Description:** Here displays the description about the WAN and this description is unique.
- **Details:** The details can be IP address, port, or domain name.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In Mode field, select **IP Address**, **MAC Address** or **URL Address**.

If you select **IP Address**, the screen shown is Figure 4-94.

WAN HOST	
Mode:	IP Address
Description:	
IP Address:	
Port:	
Save Back	

Figure 4-94

- 1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) In **IP Address** field, enter the IP address.

If you select **MAC Address**, the screen shown is Figure 4-95.

The screenshot shows the 'WAN HOST' configuration page. At the top, there's a blue header bar with the text 'WAN HOST'. Below it, the 'Mode' is set to 'MAC Address' in a dropdown menu. There are two text input fields: 'Description:' and 'MAC Address:'. At the bottom, there are two buttons: 'Save' and 'Back'.

Figure 4-95

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) In **MAC Address** field, enter the MAC address.

If you select **URL Address**, the screen shown is Figure 4-96.

The screenshot shows the 'WAN HOST' configuration page with 'Mode' set to 'URL Address'. It includes a 'Description:' field and an 'Add URL Address:' field with an 'Add' button. Below these is a table with one row containing a checkbox, a 'Detail' label, and a 'Delete' button. A note says '(It won't take effect until you save it)'. At the bottom are 'Save' and 'Back' buttons.

Figure 4-96

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) Enter the URL address in the **Add URL Address** field, and then click the **Add** button. The URL address will be shown in the **Detail** table. If you click the **Delete** button, the existing URL address in the **Detail** table can be deleted.

3. Click the **Save** button to complete the settings.

4.14.4 Schedule

Choose menu **"Firewall" → "Schedule"**, and then you can view and set a Schedule list in the next screen as shown in Figure 4-97.

The screenshot shows the 'Task Schedule' page. It has a blue header bar with 'Task Schedule'. Below is a table with two rows. The first row has a checkbox, a 'Description' header, and an 'Edit' button. The second row has a checkbox, the text 'Schedule_1', and an 'Edit' button. At the bottom, there are two buttons: 'Add New' and 'Delete Selected'.

Figure 4-97

➤ **Description:** Here displays the description of the schedule and this description is unique.

➤ **Edit:** Here you can modify an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Add New** button and the next screen will pop-up as shown in Figure 4-98.
2. In **Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Apply To** field, select the day or days you need.
4. In time field, you can select all day-24 hours or you may enter the **Start Time** and **Stop Time** in the corresponding field.
5. Click **Save** to complete the settings.

Click the **Clear Schedule** button to clear your settings in the table.

Schedule can be set on this page.

Description:

Apply To:

Start Time:

End Time:

Time	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

Figure 4-98

Click the **Delete Selected** button to delete the selected entries in the table.

4.15 IPv6 Firewall

IPv6 Firewall
IPv6 Rule
IPv6 LAN Host
IPv6 WAN Host
IPv6 Schedule

There are four submenus under the IPv6 Firewall menu: **IPv6 Rule**, **IPv6 LAN Host**, **IPv6 WAN Host** and **IPv6 Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.15.1 IPv6 Rule

Choose menu “**IPv6 Firewall**” → “**IPv6 Rule**”, and then you can view and set Access Control rules in the screen as shown in Figure 4-99.

IPv6 Firewall Rules

This device can restrict the internet behavior of certain IPv6 LAN hosts. You can set flexible combined rules by selecting proper "IPv6 LAN Host", "IPv6 WAN Host" and "IPv6 Schedule" to conduct powerful internet access control management.

☐ Enable IPv6 Firewall

Default Filtering Rules

☒ **Allow** the packets not specified by any filtering rules to pass through the device

☐ **Deny** the packets not specified by any filtering rules to pass through the device

Note: The modern router will first try to match the packet with the enabled filtering rules one by one in the list and apply the first matching rule. If the packet is not specified by any filtering rules in the list, then the Default Filtering Rule will take effect.

☐	Description	IPv6 LAN Host	Target	Schedule	Rule	Status	Edit
Add New Enable Selected Disable Selected Delete Selected							

Figure 4-99

- **Enable IPv6 Firewall:** Select the check box to enable the IPv6 Firewall function, so the Default Filtering Rules can take effect.
- **Description:** Here displays the description of the IPv6 rule and this name is unique.
- **IPv6 LAN Host:** Here displays the LAN host selected in the corresponding rule.
- **Target:** Here displays the target selected in the corresponding rule.
- **Schedule:** Here displays the schedule selected in the corresponding rule.
- **Status:** Here displays the status of the rule either enabled or disabled.
- **Edit:** Here you can edit or delete an existing rule.

To add a new IPv6 rule:

1. Click the **Add New** button, and you will see the screen as shown in Figure 4-100.

IPv6 Firewall Rules

An IPv6 internet control rule can be set on this page.

Description:

IPv6 LAN Host: [Add IPv6 LAN Host](#)

IPv6 WAN Host: [Add IPv6 WAN Host](#)

IPv6 Schedule: [Add IPv6 Schedule](#)

Action:

Status:

Direction:

Protocol:

Figure 4-100

2. Give a name (e.g. Rule_1) for the rule in the **Description** field.

3. Select a host from the **IPv6 LAN Host** drop-down list or choose “**Add IPv6 LAN Host**”.
4. Select a target from the **IPv6 WAN Host** drop-down list or choose “**Add IPv6 WAN Host**”.
5. Select a schedule from the **IPv6 Schedule** drop-down list or choose “**Add IPv6 Schedule**”.
6. In the **Action** field, select **Deny** or **Allow** to deny or allow your entry.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. In the **Direction** field, select **IN** or **OUT** from the drop-down list for the direction.
9. In the **Protocol** field, here are four options, All, TCP, UDP, and ICMPv6. Select one of them from the drop-down list for the target.
10. Click the **Save** button to save the settings.

Click the **Enable/ Disable Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete selected entries.

4.15.2 IPv6 LAN Host

Choose menu “**IPv6 Firewall**” → “**IPv6 LAN Host**”, and then you can view and set a Host list in the screen as shown in Figure 4-101.

IPv6 LAN HOST			
☐	Description	IPv6 Address Info	Edit
☐	IPv6 LAN1	2000::/64 /888-999	Edit
Add New		Delete Selected	

Figure 4-101

- **Description:** Here displays the description of the host and this description is unique.
- **IPv6 Address Info:** Here displays the information about the host.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button, and you will see the screen as shown in Figure 4-102.

IPv6 LAN Host	
Description: IPv6 LAN1 IPv6 Address: 2000:: Prefix Length: 64 Port: 888 - 999	
Save Back	

Figure 4-102

2. Create a unique name for the host (e.g. Host_1) in the **Description** field.
3. Enter an IPv6 address in the **IPv6 Address** field.

4. Enter the prefix length of the IPv6 address in the **Prefix Length** field.
5. Click the **Save** button to save the settings.

Click the **Delete Selected** button to delete selected entries.

4.15.3 IPv6 WAN Host

Choose menu “**IPv6 Firewall**” → “**IPv6 WAN Host**”, and then you can view and set a Host list in the screen as shown in Figure 4-103.

IPv6 WAN Host			
☐	Description	Details	Edit
☐	IPv6 WAN1	3333::/64 /888-999	Edit
Add New		Delete Selected	

Figure 4-103

- **Description:** Here displays the description about the WAN and this description is unique.
- **Details:** The details can be IPv6 address, prefix length or port.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button, and you will see the screen as shown in Figure 4-104.

IPv6 WAN Host	
Description: IPv6 WAN1 IPv6 Address: 3333:: Prefix Length: 64 Port: 888 - 999	
Save Back	

Figure 4-104

2. Create a unique description for the host (e.g. Host_1) in the **Description** field.
3. Enter an IPv6 address in the **IPv6 Address** field.
4. Enter the prefix length of the IPv6 address in the **Prefix Length** field.
5. Click the **Save** button to save the settings.

Click the **Delete Selected** button to delete selected entries.

4.15.4 IPv6 Schedule

Choose menu “**IPv6 Firewall**” → “**IPv6 Schedule**”, and then you can view and set a Schedule list in the next screen as shown in Figure 4-105.

IPv6 Task Schedule		
☐	Description	Edit
☐	IPv6 Sche1	Edit

Figure 4-105

- **Description:** Here displays the description of the schedule and this description is unique.
- **Edit:** Here you can modify an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Add New** button and you will see the screen as shown in Figure 4-106.

Schedule can be set on this page.

Description: IPv6 Sche1

Apply To: Each Day

Start Time: 00:00

End Time: 24:00

Time	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

Figure 4-106

2. Create a unique description for the schedule (e.g. Schedule_1) in **Description** field.
3. Select the day or days you need in **Apply To** field.
4. In time field, you can select all day-24 hours or you may enter the **Start Time** and **Stop Time** in the corresponding field.
5. Click **Save** to save the settings.

Click the **Clear Schedule** button to clear your settings in the table.

Click the **Delete Selected** button to delete selected entries.

4.16 IPv6 Tunnel

IPv6 tunnel is a kind of transition mechanism to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each-other over IPv4-only infrastructure before

IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

Choose menu “**IPv6 Tunnel**”, and you will see the screen as shown in Figure 4-107.

Figure 4-107

- **Enable:** Check the box to enable IPv6 Tunnel function. It is disabled by default.
- **Mechanism:** Select a type for IPv6 tunnel from the drop-down list. DS-Lite, 6RD and 6to4 are supported.

1) DS-Lite

This type is used in the situation that your WAN connection is IPv6 while LAN connection is IPv4. Select DS-Lite, and you will see the screen as shown in Figure 4-108.

Figure 4-108

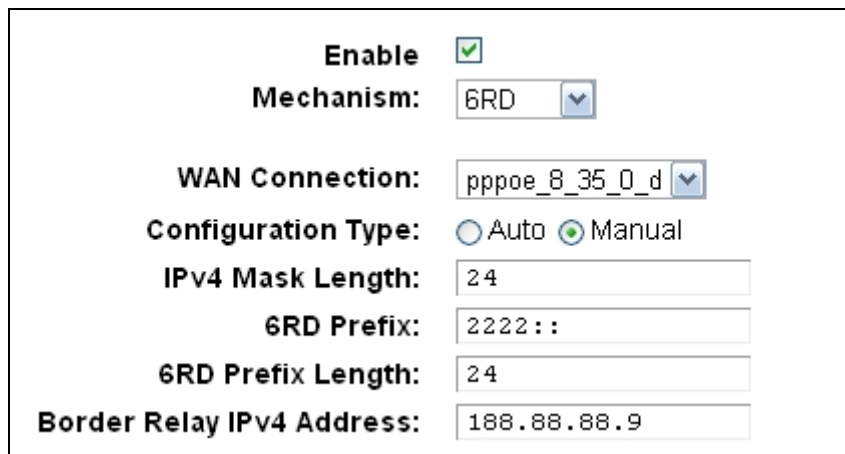
- **WAN Connection:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.
- **Configuration Type:** Select a configuration type for this tunnel. Auto means to obtain the Remote IPv6 Address automatically while Manual means you set it manually.
- **Remote IPv6 Address:** Enter the IPv6 address of the remote node.

Note:

In this type, there should not have any IPv4 WAN connections. If there are IPv4 WAN connections, the page will prompt you to delete all the IPv4 WAN connections.

2) 6RD

This type is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6. Select 6RD, and you will see the screen as shown in Figure 4-109.



Enable ☒
 Mechanism: 6RD
 WAN Connection: pppoe_8_35_0_d
 Configuration Type: ☐ Auto ☒ Manual
 IPv4 Mask Length: 24
 6RD Prefix: 2222::
 6RD Prefix Length: 24
 Border Relay IPv4 Address: 188.88.88.9

Figure 4-109

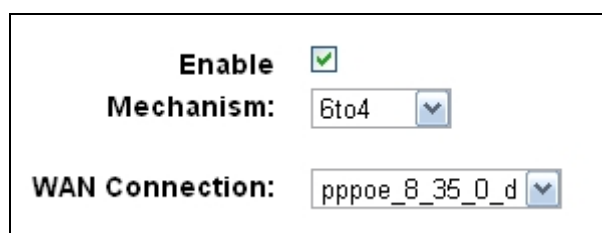
- **WAN Connection:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.
- **Configuration Type:** Select a configuration type for this tunnel. Auto means to obtain the following parameters automatically while Manual means you set them manually. If Auto is selected, only Dynamic IP connection can be selected from the drop-down list.
- **IPv4 Mask Length:** The length of the selected WAN connection's IPv4 mask.
- **6RD Prefix:** The prefix of the 6RD tunnel.
- **6RD Prefix Length:** The length of the 6RD prefix.
- **Border Relay IPv4 Address:** The IPv4 address of the border relay router of 6RD tunnel.

 Note:

In this type, there should not have any IPv6 WAN connections. If there are IPv6 WAN connections, the page will prompt you to delete all the IPv6 WAN connections.

3) 6to4

This type is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6. Select 6to4, and you will see the screen as shown in Figure 4-110.



Enable ☒
 Mechanism: 6to4
 WAN Connection: pppoe_8_35_0_d

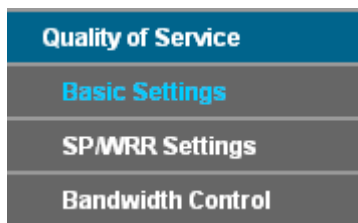
Figure 4-110

- **WAN Connection:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.

 Note:

In this type, there should not have any IPv6 WAN connections. If there are IPv6 WAN connections, the page will prompt you to delete all the IPv6 WAN connections.

4.17 Quality of Service



QoS (Quality of Service) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.

Choose menu “**Quality of Service**”, and you can see the submenus under the main menu: **Basic Settings**, **SP/WRR Settings** and **Bandwidth Control**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.17.1 Basic Settings

Choose menu “**Quality of Service**” → “**Basic Settings**”, and then you can configure the Upstream Bandwidth and Downstream Bandwidth in the next screen.

Quality of Service

This page allows you to enable or disable Quality of Service for upstream or downstream, set the Scheduler Algorithm and Total Bandwidth.

Note: For optimal control of Quality of Service, please configure the right Line Type and bandwidth. If you are not sure about these information, please ask your ISP for help.

Enable QoS of Upstream: ☐

Scheduler Algorithm: ☒ SP ☐ WRR ☐ Traffic Control

Total Bandwidth: 512 Kbps

Enable DSCP Mark ☐

Enable 802.1P Mark ☐

Enable QoS of Downstream: ☐

Scheduler Algorithm: ☐ SP ☒ WRR ☐ Traffic Control

Total Bandwidth: 1024 Kbps

Enable DSCP Mark ☐

Enable 802.1P Mark ☐

Save

Figure 4-111

- **Enable QoS of Upstream:** Check this box so that the QoS of Upstream can take effect.
- **Scheduler Algorithm:** When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The router provides three schedule modes: SP, WRR and Traffic Control.

- **SP-Mode:** Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved to death” because they are not served.
 - **WRR-Mode:** Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue and every queue can be assured of a certain service time. The weight value indicates the occupied proportion of the resource. WRR queue overcomes the disadvantage of SP queue that the packets in the queues with lower priority cannot get service for a long time. In WRR mode, though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of.
 - **Traffic Control:** In this mode you can set the total bandwidth through the WAN port, which can control the traffic rate and broadcast flow on each port to ensure network in working order, for more information please refer to [4.17.3 Bandwidth Control](#).
- **Total Bandwidth:** Enter your desired value for the upstream bandwidth through the WAN port, the default is 512Kbps.
- **Enable DSCP Mark:** In SP or WRR mode you can enable DSCP Mark, then you can set the DSCP value in Figure 4-112.
- **Enable 802.1P Mark:** In SP or WRR mode you can enable 802.1P Mark, then you can set the 802.1P priority in Figure 4-112.
- **Enable QoS of Downstream:** Check this box so that the QoS of Downstream can take effect.
- **Total Bandwidth:** Enter your desired value for the downstream bandwidth through the WAN port, the default is 1024Kbps.

4.17.2 SP/WRR Settings

Choose menu “**Quality of Service**” → “**SP/WRR Settings**”, and then you can view and configure the SP/WRR Settings in the screen.

SP/WRR Settings										
Queue Add, remove SP/WRR queues. Only when the Quality of Service is enabled and Scheduler Algorithm of upstream/downstream is SP/WRR can the queues take effect.										
☐	Queue Name	Direction	Scheduler Algorithm	Precedence	Weight (%)	Force Weight	Status	Edit		
Add New		Delete Selected								
Flow Classification Add, remove flow classification rules which related to one SP or WRR queue.										
☐	Class Name	Order	Classification Criteria		Classification Result				Status	Edit
			Ingress interface	Criteria	Direction	Queue	DSCP Mark	802.1P Mark		
Add New		Delete Selected								
Business Classification Add, remove business classification rules.										
☐	Classification Criteria		Classification Result					Status	Edit	
	Business Name		Direction	Queue	DSCP Mark	802.1P Mark				
Add New		Delete Selected								
Refresh										

Figure 4-112

Queue: Click **Add New** button shown in queue part in Figure 4-112, you can add a new queue in Figure 4-113.

Queue Configuration	
Direction:	downStream
Scheduler Algorithm:	WRR
Queue Name:	
Status:	Disable
Weight:	%
Enable Force Weight	☒
Save Back	

Figure 4-113

- **Direction:** Select the direction.
- **Scheduler Algorithm:** Displays the Scheduler Algorithm you have chosen in Figure 4-111
- **Queue Name:** Enter a name for the queue.
- **Status:** Select the status of the queue is enabled or disabled.
- **Precedence:** Set a priority for your queue, the range is 1~8, '1' stands for the highest priority while '8' stands for the lowest priority.
- **Weight:** In WRR mode you need set the weight for you queue, choose a integer from 1~100.
- **Enable Force Weight:** In WRR mode you could enable this function.

 Note:

- 1) Only enable the QoS function of the relevant direction, the queue configuration in SP or WRR mode could take effect.
- 2) At most you could establish 8 upstream queues and 8 upstream queues.

Click the **Save** button to save your settings.

Click **Back** to go back to the previous page

Flow classification: Flow classification function identifies packets conforming to certain characters according to certain rules. Click **Add New** button shown in flow classification in Figure 4-112, you can add a new classification in Figure 4-114.

Flow Classification Configuration	
Class Name:	
Status:	Disable
Order:	Last
Specify Classification Criteria (A blank criteria indicates it is not used for classification.)	
Ingress Interface:	All LAN
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Specify Classification Results (A blank criteria indicates no operation.)	
Direction:	Upstream
Queue:	
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1P Priority:	
Save Back	

Figure 4-114

- **Class Name:** Enter a name for your classification.
- **Status:** Select the status of the classification is enabled or disabled.
- **Order:** Set a priority for classification, “Last” means the lowest priority.
- **Ingress Interface:** Select your desired Interface.
- **Ether type:** Select your ether type from the dropdown list.

- **Mark Differentiated Service Code Point (DSCP):** Enter the number to remark the DSCP priority. To make this function take effect, make sure you have enabled DSCP mark in Figure 4-111.
- **Mark 802.1P Priority:** Select the type to remark the 802.1p priority. To make this function take effect, make sure you have enabled 802.1P mark in Figure 4-111.

Click the **Save** button to save your settings.

Click **Back** to go back to the previous page

Business Classification: The QoS of this GPON router supports VoIP, TR069 and Other business packets. Click **Add New** button shown in Business Classification part in Figure 4-112, you can add a new Classification in Figure 4-115.

Business Classification Configuration

Business Name: VoIP

Status: Disable

Specify Classification Results (A blank criteria indicates no operation.)

Direction: Upstream

Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1P Priority:

Save **Back**

Figure 4-115

- **Business Name:** Select your desired type from the dropdown list.
- **Status:** Select the status of the classification is enabled or disabled..
- **Direction:** Displays the current business direction.
- **Queue:** Select your desired queue you have set from the dropdown list.
- **Mark Differentiated Service Code Point (DSCP):** Enter the number to remark the DSCP priority. To make this function take effect, make sure you have enabled DSCP mark in Figure 4-111.
- **Mark 802.1P Priority:** Select the type to remark the 802.1p priority. To make this function take effect, make sure you have enabled 802.1P mark in Figure 4-111.

Click the **Save** button to save your settings.

Click **Back** to go back to the previous page

4.17.3 Bandwidth Control

Choose menu “**Quality of Service**” → “**Bandwidth Control**”, and then you can view and configure the Bandwidth Control rules in the screen below.

This page allows you to set Traffic Control Rules. Only when the Quality of Service is enabled and Scheduler Algorithm of upstream/downstream is Traffic Control can the rules take effect.

☐ Enable VoIP Bandwidth Guarantee

Bandwidth Control Rules

☐	Description	Priority	Upstream Bandwidth		Downstream Bandwidth		Status	Edit
			Min	Max	Min	Max		
Add New Enable Selected Disable Selected Delete Selected								

Figure 4-116

- **Description:** This is the information about the rules such as address range.
- **Upstream Bandwidth:** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Downstream Bandwidth:** This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Edit:** Click **Edit** to modify the rule.

To add/modify a Bandwidth Control rule, follow the steps below.

1. Click **Add New** shown in Figure 4-116, you will see a new screen shown in Figure 4-117.
2. Enter the information like the screen shown below.

☒ Enable

IP Range: --

Port Range: --

Protocol: ▼

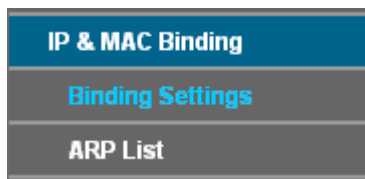
Priority: ▼ (1 means highest priority)

	Min Rate(Kbps)	Max Rate(Kbps)
Upstream:		
Downstream:		

Figure 4-117

3. Click the **Save** button.

4.18 IP&MAC Binding



There are two submenus under the IP & MAC Binding menu: **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.18.1 Binding Settings

This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire (shown in Figure 4-118).

The screenshot shows the 'Binding Settings' page. At the top, there's a section for 'ARP Binding' with radio buttons for 'Enable' and 'Disable' (currently selected), and a 'Save' button. Below this is a table with columns: 'MAC Address', 'IP Address', 'Binding Status', and 'Edit'. There's a checkbox in the first row. Below the table are four buttons: 'Add New', 'Enable Selected', 'Disable Selected', and 'Delete Selected'. At the bottom center is a 'Refresh' button.

Figure 4-118

- **MAC Address:** The MAC address of the controlled computer in the LAN.
- **IP Address:** The assigned IP address of the controlled computer in the LAN.
- **Bound:** Check this option to enable ARP binding for a specific device.
- **Edit:** To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Edit** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-119).

The screenshot shows the 'Binding Settings' page for adding or modifying an entry. It contains a text box with the message 'This page allows you to set IP-MAC Binding entries.' Below this are three input fields: 'MAC Address:', 'IP Address:', and 'Bind' (with a checked checkbox). At the bottom right are 'Save' and 'Back' buttons.

Figure 4-119

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New** button as shown in Figure 4-118.

2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disable Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete selected entries.

4.18.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 4-120).

ARP List

☐	MAC Address	IP Address	Status
☐	40:61:86:E5:B2:DC	192.168.1.100	Loaded

Load Selected

Delete Selected

Refresh

Figure 4-120

- **MAC Address:** The MAC address of the controlled computer in the LAN.
- **IP Address:** The assigned IP address of the controlled computer in the LAN.
- **Status:** Indicates whether or not the MAC and IP addresses are bound.
- **Load:** Load the item to the IP & MAC Binding list.

Click the **Load Selected** button to load selected items to the IP & MAC Binding list.

Click the **Refresh** button to refresh all items.

4.19 Dynamic DNS

Choose menu “**Dynamic DNS**”, and you can configure the Dynamic DNS function.

The GPON router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

Parameters of dynDns can be set on this page.

Service Provider: [Go to register...](#)

Domain Name:

User Name:

Password:

Enable DDNS ☐

Connection Status: Disconnected

Figure 4-121

- **Service Provider:** This field displays the service provider of DDNS.
- **Domain Name:** Enter the Domain name you received from dynamic DNS service provider.
- **Username & Password:** Type the “User Name” and “Password” for your DDNS account.
- **Enable DDNS:** Activate the DDNS function or not.
- **Login/ Logout:** Login to or logout of the DDNS service.

4.20 Diagnostic

Choose “**Diagnostic**”, you can view the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides in the screen. Select the desired type and click the start button.

The router's internet connection status can be tested on this page. Please select the desired type and click the start button.

Diagnostics Type

Test internet surfing

Test WAN interface connection

Figure 4-122

4.21 System Tools

System Tools
System Log
Time Settings
Manage Control
CWMP Settings
SNMP Settings
Backup & Restore
Factory Defaults
Firmware Upgrade
Reboot
Statistics

Choose menu “**System Tools**”, and you can see the submenus under the main menu: **System Log**, **Time Settings**, **Manage Control**, **CWMP Settings**, **SNMP Settings**, **Backup & Restore**, **Factory Defaults**, **Firmware Upgrade**, **Reboot** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

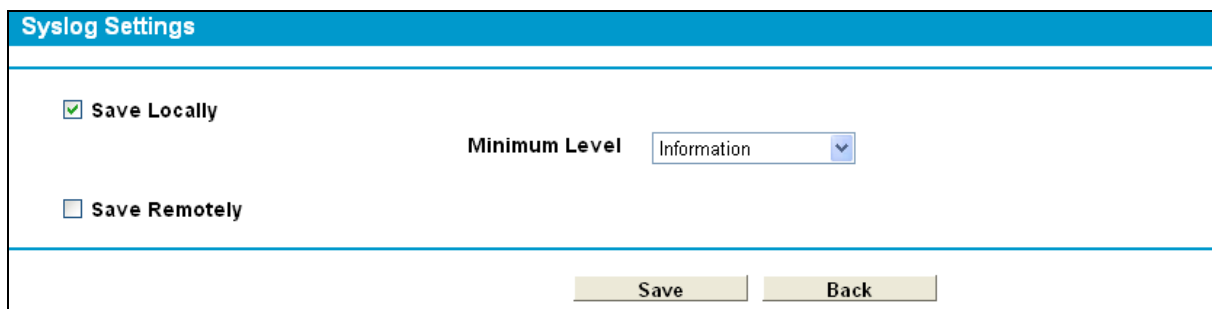
4.21.1 System Log

Choose menu “**System Tools**” → “**System Log**”, and then you can view the logs of the GPON router.

System Log					
Log Type: ALL		Log Level: Debug			
Index	Time	Type	Level	Content	
Refresh Clear Log Save Log Log Settings					

Figure 4-123

- **Log Type:** By selecting the log type, only logs of this type will be shown.
- **Log Level:** By selecting the log level, only logs of this level will be shown.
- **Refresh:** Refresh the page to show the latest log list.
- **Clear Log:** All the logs will be deleted from the GPON router permanently, not just from the page.
- **Save Log:** Click to save all the logs in a txt file.
- **Log Settings:** Click to set the logs in the screen (shown in Figure 4-124).



Syslog Settings

☒ **Save Locally**

Minimum Level Information

☐ **Save Remotely**

Save **Back**

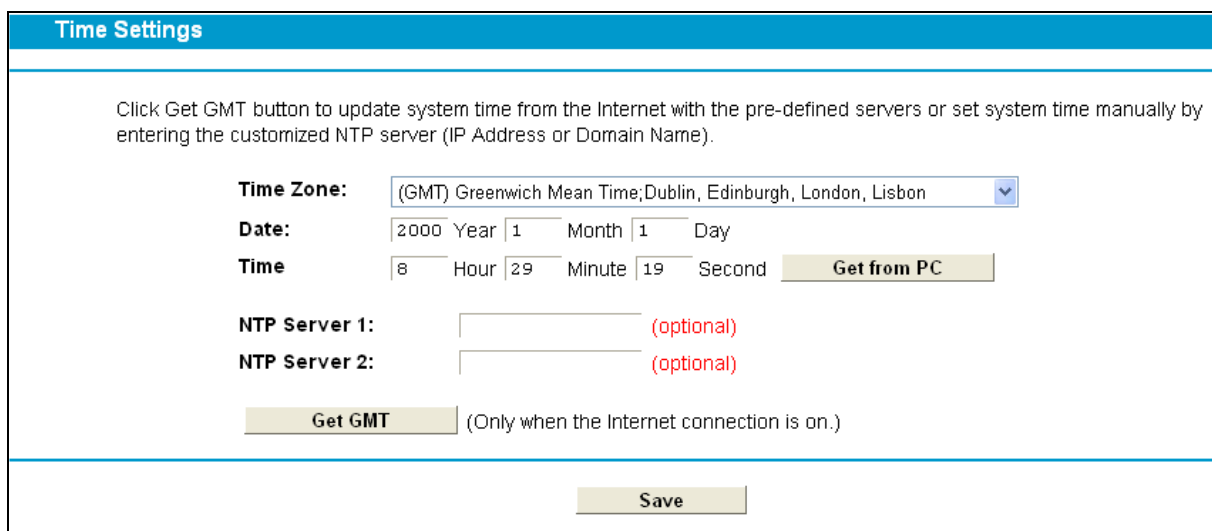
Figure 4-124

- **Save Locally:** If **Save Locally** is selected, events will be recorded in the local memory.
- **Minimum Level:** Select the Minimum level in the drop-down list, for the Minimum Level, all logged events above or equal to the selected level will be displayed.
- **Save Remotely:** If **Save Remotely** is selected, events will be sent to the specified IP address and UDP port of the remote system log server.

Click the **Save** button to save your settings.

4.21.2 Time Settings

Choose menu “**System Tools**” → “**Time Settings**”, and then you can configure the time on the following screen.



Time Settings

Click Get GMT button to update system time from the Internet with the pre-defined servers or set system time manually by entering the customized NTP server (IP Address or Domain Name).

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

Date: 2000 Year 1 Month 1 Day

Time 8 Hour 29 Minute 19 Second **Get from PC**

NTP Server 1: (optional)

NTP Server 2: (optional)

Get GMT (Only when the Internet connection is on.)

Save

Figure 4-125

- **Time Zone:** Select your local time zone from this pull down list.
- **Date:** Enter your local date in MM/DD/YY into the right blanks.
- **Time:** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server 1 / NTP Server 2:** Enter the address or domain of the **NTP Server 1** or **NTP Server 2**, and then the GPON router will get the time from the NTP Server preferentially. In addition, the GPON router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

To set time manually:

1. Select your local time zone.

2. Enter the **Date** in Year/Month/Day format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

4.21.3 Manage Control

Choose “**System Tools**” → “**Manage Control**”, you can see the screen (shown in Figure 4-124)

Manage Control											
Current User Status User Type: Admin Username: admin Host IP Address: 192.168.1.100 Host MAC Address: 6C:62:6D:F7:32:09											
Account Management Old Password: New User Name: New Password: Confirm password:											
Service Configuration <table border="1"> <thead> <tr> <th></th> <th>HTTP Service</th> <th>Available Host (IP/MAC)</th> </tr> </thead> <tbody> <tr> <td>Local Management</td> <td>Port 80 </td> <td> </td> </tr> <tr> <td>Remote Management</td> <td>Enable ☐ Port 80 </td> <td> </td> </tr> </tbody> </table>				HTTP Service	Available Host (IP/MAC)	Local Management	Port 80		Remote Management	Enable ☐ Port 80	
	HTTP Service	Available Host (IP/MAC)									
Local Management	Port 80										
Remote Management	Enable ☐ Port 80										
Save											

Figure 4-126

- **Current User Status:** This box displays the information about **User Type**, **User Name**, **Host IP Address** and **Host MAC Address**.
- **Account Management:** Here you can set the account user information about **Old Password**, **New User Name**, **New Password** and **Confirm Password**.
- **Service Configuration:** Here you can modify the port of the GPON router's web management interface and limit the hosts which can login this GPON router's web management interface.

4.21.4 CWMP Settings

Choose “**System Tools**” → “**CWMP Settings**”, you can configure the CWMP function in the screen.

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

CWMP Settings

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select the desired values and click "Save/Apply" to configure the TR-069 client options.

CWMP: ☐ Enable ☒ Disable

Inform: ☐ Enable ☒ Disable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Interface used by TR-069 client:

Display SOAP messages on serial console: ☐ Enable ☒ Disable

☒ Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request Path:

Connection Request Port:

Connection Request URL:

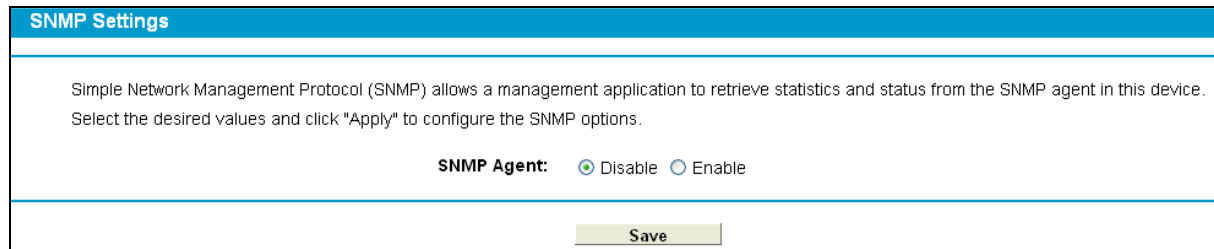
Figure 4-127

- **CWMP:** Select enable the CWMP function.
- **Inform:** Enable or disable the function. If enabled, the information will be informed to ACS server periodically.
- **Inform Interval:** Enter the interval time here.
- **ACS URL:** Enter the website of ACS which is provided by your ISP.
- **ACS User Name/Password:** Enter the User Name and password to login the ACS server.
- **Interface used by TR-069 client:** Select the interface used by TR-069 client.
- **Display SOAP messages on serial console:** Enable or disable this function.
- **Connection Request User Name/Password:** Enter the User Name and Password that provided the ACS server to login the GPON router.
- **Connection Request Path:** Enter the path that connects to the ACS server.
- **Connection Request Port:** Enter the port that connects to the ACS server.
- **Connection Request URL:** Enter the URL that connects to the ACS server.

4.21.5 SNMP Settings

Choose “**Management**” → “**SNMP Agent**”, you can see the SNMP-Configuration screen as shown below.

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.



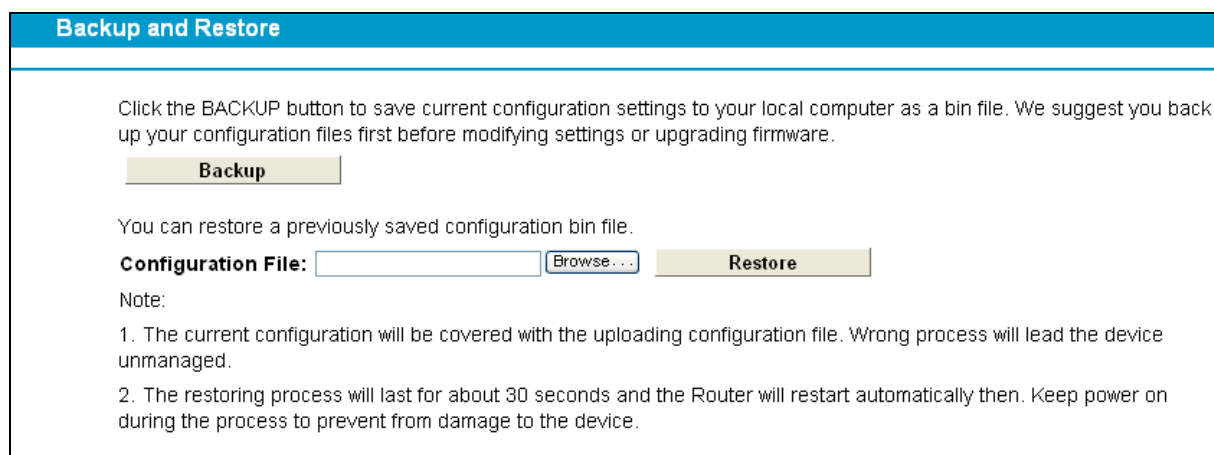
The image shows the 'SNMP Settings' page in a web interface. It has a blue header with the title 'SNMP Settings'. Below the header, there is a text block explaining that SNMP allows a management application to retrieve statistics and status from the SNMP agent in this device, and instructs the user to select desired values and click 'Apply' to configure the options. Below this text, there is a label 'SNMP Agent:' followed by two radio buttons: 'Disable' (which is selected) and 'Enable'. At the bottom of the page, there is a 'Save' button.

Figure 4-128

An **SNMP Agent** is an application running on the GPON router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

4.21.6 Backup & Restore

Choose menu "**System Tools**" → "**Backup & Restore**", and then you can save the current configuration of the GPON router as a backup file and restore the configuration via a backup file as shown in Figure 4-129.



The image shows the 'Backup and Restore' page in a web interface. It has a blue header with the title 'Backup and Restore'. Below the header, there is a text block explaining that clicking the BACKUP button will save current configuration settings to the local computer as a bin file, and suggests backing up configuration files before modifying settings or upgrading firmware. Below this text, there is a 'Backup' button. Further down, there is a text block stating that a previously saved configuration bin file can be restored. Below this, there is a 'Configuration File:' label, a text input field, a 'Browse...' button, and a 'Restore' button. At the bottom, there is a 'Note:' section with two numbered points: 1. The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. 2. The restoring process will last for about 30 seconds and the Router will restart automatically then. Keep power on during the process to prevent from damage to the device.

Figure 4-129

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the GPON router 's configuration, follow these instructions.
 - Click the **Browse** button to find the configuration file which you want to restore.
 - Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

 Note:

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the GPON router will

restart automatically then. Keep the power of the GPON router on during the process, in case of any damage.

4.21.7 Factory Defaults

Choose menu “**System Tools** → **Factory Defaults**”, and then and you can restore the configurations of the GPON router to factory defaults on the following screen

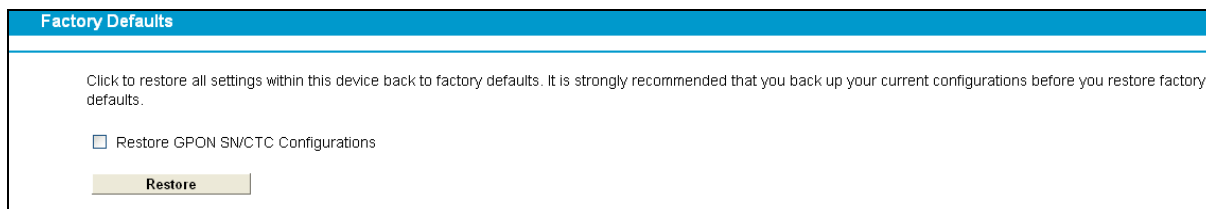


Figure 4-130

- **Restore GPON SN/CTC Configurations:** Check this box, the current GPON SN/CTC settings will be deleted when you restore the configurations of the ONT to its factory defaults.

Click the **Restore** button to reset all configuration settings to their default values.

- The default **User Name**: admin
- The default **Password**: admin
- The default **Subnet Mask**: 255.255.255.0

 **Note:**

All changed settings will be lost when defaults are restored.

4.21.8 Firmware Upgrade

Choose menu “**System Tools** → **Firmware Upgrade**”, and then you can update the latest version of firmware for the GPON router on the following screen.

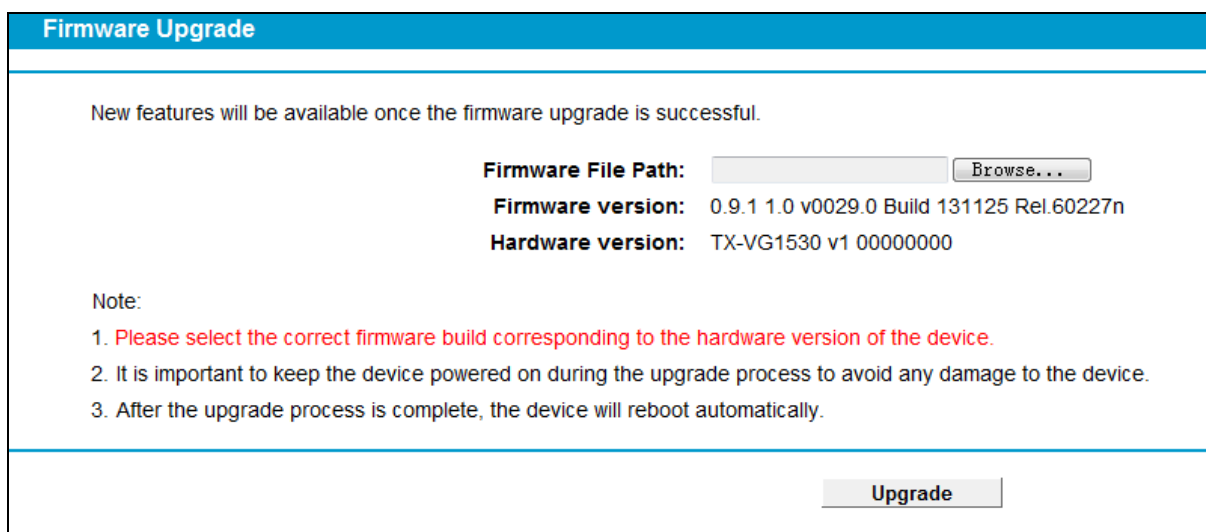


Figure 4-131

- **Firmware Version:** Displays the current firmware version.

- **Hardware Version:** Displays the current hardware version. The hardware version of the upgrade file must accord with the GPON router's current hardware version.

To upgrade the GPON router's firmware, follow these instructions below:

1. Download a most recent firmware upgrade file from our website (www.tp-link.com).
2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
3. Click the **Upgrade** button.
4. The GPON router will reboot while the upgrading has been finished.

 Note:

- 1) New firmware versions are posted at <http://www.tp-link.com> and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the GPON router rather than the configuration, you can try to upgrade the firmware.
- 2) When you upgrade the GPON router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
- 3) Do not turn off the GPON router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the GPON router.
- 4) The firmware version must correspond to the hardware.
- 5) The upgrade process takes a few moments and the GPON router restarts automatically when the upgrade is complete.

4.21.9 Reboot

Choose menu **"System Tools"** → **"Reboot"**, and then you can click the **Reboot** button to reboot the GPON router via the next screen.

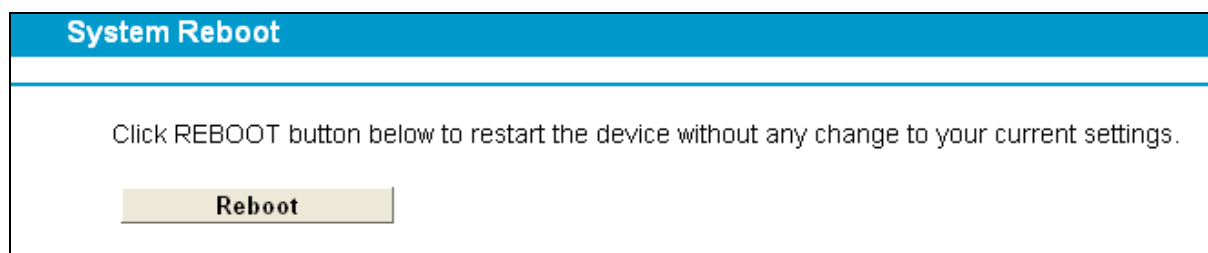


Figure 4-132

Some settings of the GPON router will take effect only after rebooting, which include

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the GPON router (system will reboot automatically).
- Restore the GPON router's settings to factory defaults (system will reboot automatically).

- Update the configuration with the file (system will reboot automatically).

4.21.10 Statistics

Choose menu “**System Tools**” → “**Statistics**”, and then you can view the statistics of the GPON router, including total traffic and current traffic of the last Packets Statistic Interval.

Traffic Statistics

Traffic Statistics--LAN

Traffic Statistics: ☐ Enable ☒ Disable

Statistics Interval: Sec

Statistics List:

IP Address MAC Address	Total		Current					Operation
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
Current list is blank								

Figure 4-133

- **Statistics Status:** Enable or Disable. The default value is disabled. To enable it, click the **Enable**. If it is disabled, the function of DoS protection in Security settings will be disabled.
- **Statistics Interval (5-60):** The default value is 10. Select a value between 5 and 60 seconds in the drop-down list. The Packets Statistic interval indicates the time section of the packets statistic.

Click **Reset All** to reset the values of all the entries to zero.

Click **Delete All** to delete all entries in the table.

Click the **Refresh** button to refresh immediately.

Statistics Table:

IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	Packets	The total number of packets received and transmitted by the GPON router.
	Bytes	The total number of bytes received and transmitted by the GPON router.
Current	Packets	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
Operation	Reset	Reset the value of the entry to zero.
	Delete	Delete the existing entry in the table.

4.22 Logout

Choose “**Logout**”, and you will back to the login screen as shown in Figure 4-134.

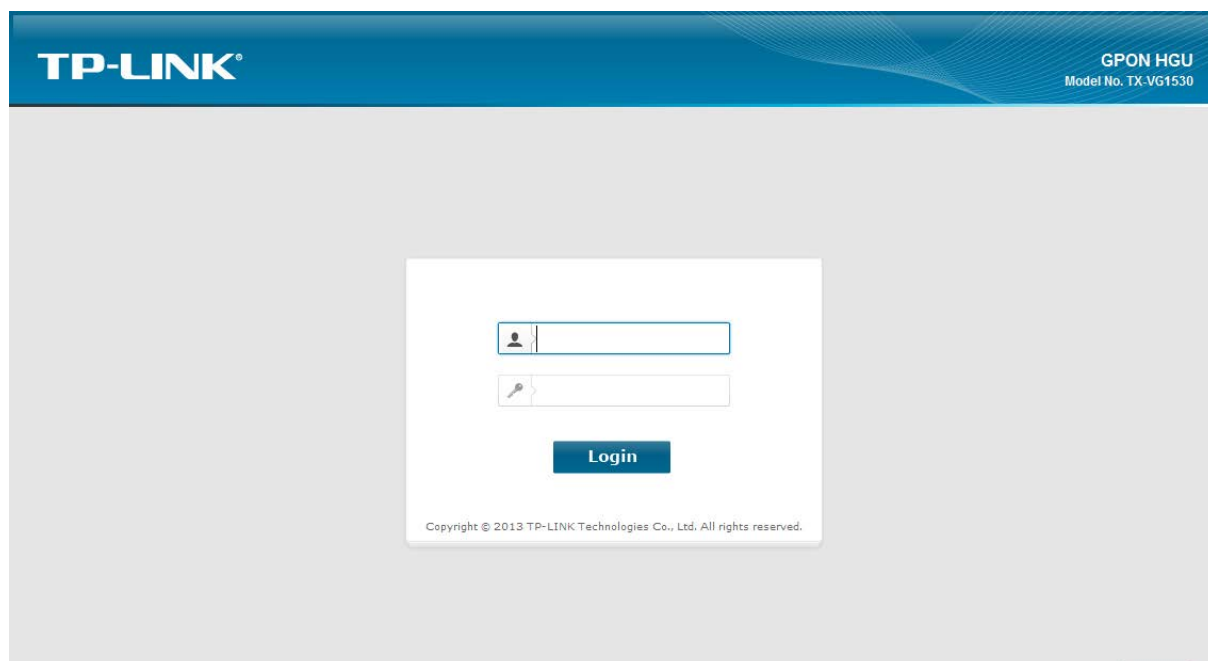


Figure 4-134

Appendix A: Specifications

General	
Standards and Protocols	ITU 984.1, ITU 984.2, ITU 984.3, ITU 984.4, IEEE802.1p, IEEE 802.11b, IEEE802.11e, IEEE 802.11g, IEEE 802.11n, IEEE 802.3, IEEE 802.3u, TCP/IP, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Safety & Emission	FCC, CE
Ports	Four 10/100/1000M Auto-Negotiation RJ45 ports (Auto MDI/MDIX) One optical port, Two RJ11 ports, One USB 2.0 port
LEDs	Power, PON, LOS, USB, LAN1-4, WLAN, WPS, Phone1-2
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5 1000Base-TX: UTP category 5, 5e, 6G.652 SMF Max line length: 20Km
Data Rates	Downstream: Up to 2.488Gbps Upstream: Up to 1.244Gbps
System Requirement	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™, Windows 7, Windows 8, MAC® OS, NetWare®, UNIX® or Linux.
Physical and Environment	
Working Temperature	0 °C ~ 40 °C
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40 °C ~ 70 °C
Storage Humidity	5% ~ 90% RH (non-condensing)

Appendix B: Troubleshooting

T1. How do I restore my GPON router's configuration to its factory default settings?

With the GPON router powered on, press and hold the **RESET** button on the front panel for at least 6 seconds before releasing it.

 Note:

Once the GPON router is reset, the current configuration settings will be lost and you will need to re-configure the router.

T2. What can I do if I don't know or forget my password?

- 1) Restore the GPON router's configuration to its factory default settings. If you don't know how to do that, please refer to **T1**.
- 2) Use the default user name and password: **admin, admin**.
- 3) Try to configure your GPON router once again by following the instructions in [3.2 Quick Installation Guide](#).

T3. What can I do if I cannot access the web-based configuration page?

- 1) Configure your computer's IP Address.

For Mac OS X

- Click the **Apple** icon on the upper left corner of the screen.
- Go to "**System Preferences -> Network**".
- Select **Airport** on the left menu bar, and then click **Advanced** for wireless configuration; or select **Ethernet** for wired configuration.
- In the **Con-figure IPv4** box under **TCP/IP**, select **Using DHCP**.
- Click **Apply** to save the settings.

For Windows 7

- Click "**Start -> Control Panel -> Network and Internet -> View network status -> Change adapter settings**".
- Right-click **Wireless Network Connection** (or **Local Area Connection**), and then click **Properties**.
- Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

For Windows XP

- Click "**Start -> Control Panel -> Network and Internet Connections -> Network Connections**".
- Right-click **Wireless Network Connection** (or **Local Area Connection**), and then click **Properties**.
- Select **Internet Protocol (TCP/IP)**, and then click **Properties**.

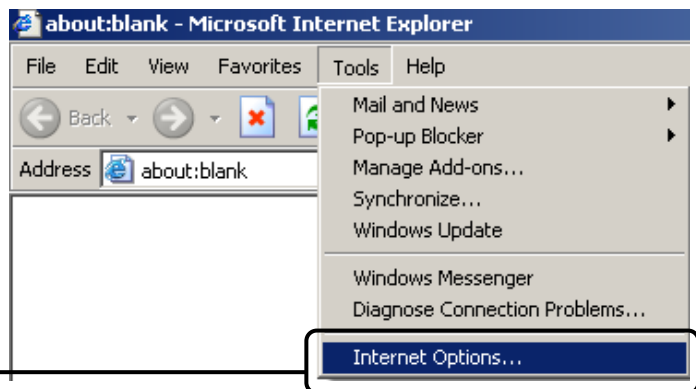
- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

For Windows 8

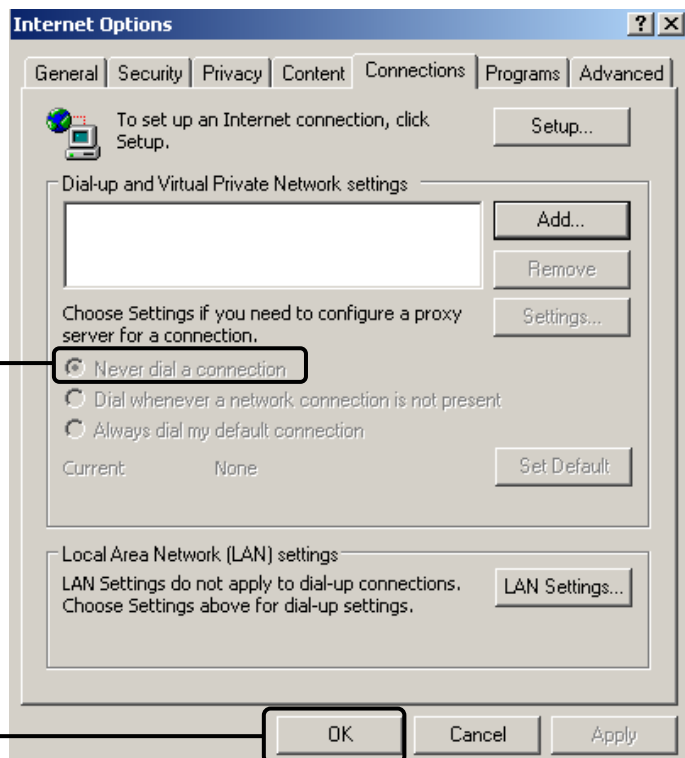
- Move your mouse to the lower right corner and you will see **Search** icon  in the Popups. Go to " -> **Apps**". Type **Control Panel** in the search box and press **Enter**, then you will go to **Control Panel**.
- Click "**View network status and tasks > Change adapter settings**".
- Right-click "**Ethernet**" and then select **Properties**.
- Double-click **Internet Protocol Version 4 (TCP/IPv4)**. Select **Obtain an IP address automatically**, choose **Obtain DNS server address automatically** and then click **OK**.

2) Configure your IE browser

Open your IE browser, click **Tools** tab and you will see the following screen.



Click **Internet Options**



Select **Never dial a connection**

Click **OK**

- 4) Now, try to log on to the Web-based configuration page again after the above settings have been configured. If you still cannot access the configuration page, please restore your GPON router's factory default settings and reconfigure your GPON router following the instructions in [3.2 Quick Installation Guide](#). Please feel free to contact our Technical Support if the problem still exists.

T4. What can I do if I cannot access the Internet?

- 1) Check to see if all the connectors are connected well, including the Fiber line, Ethernet cables and power adapter, based on the LEDs described previously.
- 2) Check to see if the GPON router is registered correctly based on the GPON LED described previously and if the Authentication status is Registered in System Status page. If not, please enter the GPON SN or GPON Password described in step 2 again and wait for approximately 2 minutes or try to unplug the fiber and then connect it again. If the problem still exists, please consult your ISP to make sure if you have entered the correct GPON SN or GPON Password.
- 3) Check to see if the dialing software used in step 3 installed correctly and make sure the account username and password are correct.
- 4) If you still cannot access the Internet, please restore your GPON router to its factory default settings and reconfigure it by following the instructions in [3.2 Quick Installation Guide](#).
- 5) Please feel free to contact our Technical Support if the problem still exists.

Note:

For more details about Troubleshooting and Technical Support contact information, please log on to our Technical Support Website: <http://www.tp-link.com/en/support>.

Appendix C: Telephony Features

This section introduces what the following features are used for.

Call Holding

This feature allows you to put a call on hold, in which case the call is not ended but no verbal communication is available.

To put a call on hold, press the **FLASH** button. To return to the original call, press the **FLASH** button again.

Call Transfer

This feature allows you to redirect the current call to another phone by using the **FLASH** button and dialing the destination number.

To transfer a call, please follow the steps below:

1. Press **FLASH** button to put the current call on hold.
2. Dial the destination number.

Note: To quit the transfer, press the **FLASH** button again to return to the original call before hearing the ringback tone.

3. Hang up when hearing the ringback tone or wait for the newly called party to answer and then hang up. Now the call is successfully transferred.

Call Waiting

With this feature enabled, if a calling party places a call to you while you are busy, you are able to suspend the current call and switch to the new incoming call.

To switch to the new incoming call, press **FLASH** followed by the number 2. The first call will be automatically put on hold. You can switch between the two calls by pressing **FLASH** followed by the number 2.

USB Voice Mail

With this feature enabled, the caller will be prompted to leave a voice message upon the call or when there is no response for a certain time.

Call Forwarding

This feature allows an incoming call to be redirected to a specified party. There are three call forwarding features, including Call Forwarding Unconditionally, Call Forwarding on Busy and Call Forwarding on No Answer.

- ✓ With Call Forwarding Unconditionally enabled, no matter whether the called party is busy or not, the incoming call will be redirected to the specified party.
- ✓ With Call Forwarding on Busy enabled, the incoming call will be redirected to the specified party when the called party is busy.
- ✓ With Call Forwarding on No Answer enabled, the incoming call will be redirected to the specified party when there is no response for a certain time.

Anonymous Calling

This feature allows you to make a call without your phone number or ID being displayed on the called party's phone.

Anonymous Call Blocking

With this feature enabled, all anonymous calls will be blocked.

Speed Dial

This feature allows you to create short numbers for your frequently used telephone numbers to make your dialing more convenient. You just need to press one or two digits and the key # instead of the original phone number to make a call.

Warm Line

With this feature enabled, a call will be automatically directed to a specified party without taking any additional action when the phone goes off-hook for a certain time. To use this feature, you need to set warm line numbers first on the web management page.

DND (Do Not Disturb)

With this feature enabled, all the incoming calls will be blocked and the caller will hear the busy tone.

Three-way Call

This feature allows three people to communicate at the same time.

To set up a three-way call, please follow the steps below:

1. Press the **FLASH** button to put the first call on hold.
2. Dial the destination number.
3. Wait for the third party to answer and then press **FLASH** followed by the number 3. Now the three-way call is successfully set up.
4. To drop yourself out of the call, simply hang up.

A three-way call can also be set up during a call with Call Waiting enabled. When hearing the call waiting tone during a call, press **FLASH** followed by the number 3.

Note: The call will end if the initiator of the three-way call hangs up. However, the call will not end if anyone of the other two parties hangs up. The left two parties remain connected to each other.

Appendix D: Telephone Operation

The table below guides you to configure some frequently used call features using keypads on your telephone. For the features mentioned in this table, please refer to **Telephony Features** in **Appendix C**.

Code	Description	Usage
*20	Listen to voice messages stored in your USB storage device.	Pick up the phone to dial this code and then follow the voice prompts for the operations below: Press 0 to listen to new messages. Press 1 to listen to the previous message. Press 2 to listen to the current message again. Press 3 to listen to the next message. Press 4 to delete the current message.
*60	Disable Call Waiting.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*61	Enable Call Waiting.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*62	With Call Waiting enabled, disable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number.
*63	With Call Waiting disabled, enable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number.
*99	Enable Redial on busy.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number. If the called party is busy, the number will be dialed again and again until there is response. To end the dialing, hang up and then pick up your phone.
*70	Disable all the call forwarding features.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.

*71	Enable Call Forwarding on No Answer.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*72	Enable Call Forwarding on Busy.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*73	Enable Call Forwarding Unconditionally.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*69	Dial the last incoming number.	Pick up the phone to dial this code. The last incoming number will be dialed automatically.
*68	Dial the last outgoing number.	Pick up the phone to dial this code. The last outgoing number will be dialed automatically.
*78	Enable Warm Line.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*79	Disable Warm Line.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*80	Enable Anonymous Call Blocking.	Pick up your phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*81	Disable Anonymous Call Blocking.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*82	With Anonymous Calling disabled, enable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number.
*90	With Anonymous Calling enabled, disable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number.
*83	Enable Anonymous Calling.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.

*84	Disable Anonymous Calling.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*86	Enable DND (Do Not Disturb).	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*87	Disable DND (Do Not Disturb).	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.

Appendix E: Technical Support

Technical Support

- For more troubleshooting help, go to:
<http://www.tp-link.com/en/support/faq>
- To download the latest Firmware, Driver, Utility and User Guide, go to:
<http://www.tp-link.com/en/support/download>
- For all other technical support, please contact us by using the following details:

Global

Tel: +86 755 2650 4400
 Fee: Depending on rate of different carriers, IDD.
 E-mail: support@tp-link.com
 Service time: 24hrs, 7 days a week

USA/Canada

Toll Free: +1 866 225 8139
 E-mail: support.usa@tp-link.com (USA)
 support.ca@tp-link.com (Canada)
 Service time: 24hrs, 7 days a week

Turkey

Tel: 0850 7244 488 (Turkish Service)
 Fee: Depending on rate of different carriers.
 E-mail: support.tr@tp-link.com
 Service time: 09:00 to 21:00, 7 days a week

Ukraine

Tel: 0800 505 508
 Fee: Free for Landline; Mobile: Depending on rate of different carriers
 E-mail: support.ua@tp-link.com
 Service time: Monday to Friday, 10:00 to 22:00

Brazil

Toll Free: 0800 608 9799 (Portuguese Service)
 E-mail: suporte.br@tp-link.com
 Service time: Monday to Friday, 09:00 to 20:00;
 Saturday, 09:00 to 15:00

Indonesia

Tel: (+62) 021 6386 1936
 Fee: Depending on rate of different carriers.
 E-mail: support.id@tp-link.com
 Service time: Monday to Friday, 09:00 to 12:00,
 13:00 to 18:00 *Except public holidays

Australia/New Zealand

Tel: NZ 0800 87 5465 (Toll Free)
 AU 1300 87 5465 (Depending on 1300 policy.)
 E-mail: support.au@tp-link.com (Australia)
 support.nz@tp-link.com (New Zealand)
 Service time: 24hrs, 7 days a week

Germany/Austria

Tel: +49 1805 875 465 (German Service)
 +49 1805 TPLINK
 +43 820 820 360
 Fee: Landline from Germany: 0.14EUR/min.
 Landline from Austria: 0.20EUR/min.
 E-mail: support.de@tp-link.com
 Service time: Monday to Friday, 09:00 to 12:30
 and 13:30 to 18:00. GMT+1 or GMT+2 (DST in
 Germany) *Except bank holidays in Hesse

Singapore

Tel: +65 6284 0493
 Fee: Depending on rate of different carriers.
 E-mail: support.sg@tp-link.com
 Service time: 24hrs, 7 days a week

UK

Tel: +44 (0) 845 147 0017
 Fee: Landline: 1p-10.5p/min, depending on the time of day. Mobile: 15p-40p/min, depending on your mobile network.
 E-mail: support.uk@tp-link.com
 Service time: 24hrs, 7 days a week

Italy

Tel: +39 023 051 9020
 Fee: Depending on rate of different carriers.
 E-mail: support.it@tp-link.com
 Service time: Monday to Friday, 09:00 to 13:00;
 14:00 to 18:00

Malaysia

Toll Free: 1300 88 875 465
 Email: support.my@tp-link.com
 Service time: 24hrs, 7 days a week

Poland

Tel: +48 (0) 801 080 618
 +48 223 606 363 (if calls from mobile phone)
 Fee: Depending on rate of different carriers.
 E-mail: support.pl@tp-link.com
 Service time: Monday to Friday, 09:00 to 17:00.
 GMT+1 or GMT+2 (DST)

France

Tel: 0820 800 860 (French service)
 Fee: 0.118 EUR/min from France
 Email: support.fr@tp-link.com
 Service time: Monday to Friday, 09:00 to 18:00
 *Except French Bank holidays

Switzerland

Tel: +41 (0) 848 800 998 (German Service)
 Fee: 4-8 Rp/min, depending on rate of different time.
 E-mail: support.ch@tp-link.com
 Service time: Monday to Friday, 09:00 to 12:30 and
 13:30 to 18:00. GMT+1 or GMT+2 (DST)

Russian Federation

Tel: 8 (499) 754 5560 (Moscow NO.)
 8 (800) 250 5560 (Toll-free within RF)
 E-mail: support.ru@tp-link.com
 Service time: From 09:00 to 21:00 (Moscow time)
 *Except weekends and holidays in RF