TP-LINK®

User Guide

Archer C7

AC1750 Wireless Dual Band Gigabit 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 © 2015 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT

FC

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

C€1588 ①

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.

National Restrictions

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply (not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Note: Please don't use the product outdoors in France.

5150-5250 MHz

Country	Restriction	Reason/remark
Bulgaria	Not implemented	Planned
Croatia	License required	
Italy		General authorization required if used outside own premises
Luxembourg	None	General authorization required for network and service

supply (not for spectrum)

Russian Federation No info

Note: Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil nedoit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 3 dBi. Antennas not included in this list or having a gain greater than 3 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

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.

CAN ICES-3 (B)/NMB-3(B)

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. s

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un

environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

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。

減少電磁波影響,請妥適使用。

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。



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

EHC

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.

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

This product can be used in the following countries:

TP-LINK[®] TP-LINK TECHNOLOGIES CO., LTD

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: AC1750 Wireless Dual Band Gigabit Router

Model No.: C7

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

EN 55022: 2010 + AC: 2011

EN 55024: 2010

EN 300 328 V1.8.1

EN 301 893 V1.7.1

EN 50385: 2002

EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011+A2:2013

The product carries the CE Mark:

CE1588①

Person is responsible for marking this declaration:

Yang Hongliang Product Manager of International Business

Date of Issue: 2015-6-26

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

Package	e Contents	1
Chapter	r 1. Introduction	2
1.1	1 Overview of the router	2
1.2	2 Conventions	3
1.3	3 Main Features	3
1.4	4 Panel Layout	4
	1.4.1 The Front Panel	4
	1.4.2 The Rear Panel	5
Chapter	r 2. Connecting the router	7
2.1	1 System Requirements	7
2.2	2 Installation Environment Requirements	7
2.3	3 Connecting the router	7
Chapter	r 3. Quick Installation Guide	9
3.1	1 TCP/IP Configuration	9
3.2	2 Quick Installation Guide	10
Chapter	r 4. Configuring the router	22
4.1	1 Login	22
4.2	2 Status	22
4.3	3 Quick Setup	24
4.4	4 Network	24
	4.4.1 WAN	24
	4.4.2 LAN	34
	4.4.3 MAC Clone	34
	4.4.4 IPTV	35
4.5	5 Dual Band Selection	36
4.6	6 Wireless 2.4GHz	37
	4.6.1 Wireless Settings	
	4.6.2 WPS	
	4.6.3 Wireless Security	
	4.6.4 Wireless MAC Filtering	
	4.6.5 Wireless Advanced4.6.6 Wireless Statistics	
4.7		
4./		

CONTENTS

	4.7.1	Wireless Settings	.50
	4.7.2	WPS	.52
	4.7.3	Wireless Security	.55
	4.7.4	Wireless MAC Filtering	.58
	4.7.5	Wireless Advanced	.60
	4.7.6	Wireless Statistics	.61
4.8	Guest	Network	.61
	4.8.1	Wireless Settings	.62
4.9	DHCP		.63
	4.9.1	DHCP Settings	.63
	4.9.2	DHCP Clients List	.64
	4.9.3	Address Reservation	.65
4.10	USB S	ettings	.66
	4.10.1	3G/4G	.66
	4.10.2	Disk Settings	.70
	4.10.3	Folder Sharing	.70
	4.10.4	Print Server	.71
4.11	NAT		.72
4.12	Forwar	rding	.73
	4.12.1	Virtual Servers	.73
	4.12.2	Port Triggering	.75
	4.12.3	DMZ	.77
	4.12.4	UPnP	.78
4.13	Securit	ty	.79
	4.13.1	Basic Security	.79
	4.13.2	Advanced Security	.80
	4.13.3	Local Management	.82
	4.13.4	Remote Management	.83
4.14	Parent	al Control	.84
4.15	Access	s Control	.86
	4.15.1	Rule	.87
	4.15.2	Host	.92
	4.15.3	Target	.93
	4.15.4	Schedule	.96
4.16	Advan	ced Routing	.97
	4.16.1	Static Routing List	.98

4.16.2 System Routing Table	99
4.17 Bandwidth Control	
4.17.1 Control Settings	100
4.17.2 Rules List	100
4.18 IP & MAC Binding	101
4.18.1 Binding Settings	101
4.18.2 ARP List	103
4.19 Dynamic DNS	104
4.19.1 Comexe.cn DDNS	104
4.19.2 Dyndns.org DDNS	105
4.19.3 No-ip.com DDNS	106
4.20 IPv6 Support	107
4.20.1 IPv6 Status	107
4.20.2 IPv6 Setup	
4.21 System Tools	113
4.21 System Tools 4.21.1 Time Settings	
-	114
4.21.1 Time Settings	114 115
4.21.1 Time Settings 4.21.2 Diagnostic	114 115 117
4.21.1 Time Settings4.21.2 Diagnostic4.21.3 Firmware Upgrade	114 115 117 118
 4.21.1 Time Settings 4.21.2 Diagnostic 4.21.3 Firmware Upgrade 4.21.4 Factory Defaults 	114 115 117 118 119
 4.21.1 Time Settings 4.21.2 Diagnostic 4.21.3 Firmware Upgrade 4.21.4 Factory Defaults 4.21.5 Backup & Restore 4.21.6 Reboot 4.21.7 Password 	
 4.21.1 Time Settings 4.21.2 Diagnostic 4.21.3 Firmware Upgrade 4.21.4 Factory Defaults 4.21.5 Backup & Restore 4.21.6 Reboot 4.21.7 Password 4.21.8 System Log 	
 4.21.1 Time Settings 4.21.2 Diagnostic 4.21.3 Firmware Upgrade 4.21.4 Factory Defaults 4.21.5 Backup & Restore 4.21.6 Reboot 4.21.7 Password 	
 4.21.1 Time Settings 4.21.2 Diagnostic 4.21.3 Firmware Upgrade 4.21.4 Factory Defaults 4.21.5 Backup & Restore 4.21.6 Reboot 4.21.7 Password 4.21.8 System Log 	
 4.21.1 Time Settings 4.21.2 Diagnostic 4.21.3 Firmware Upgrade 4.21.4 Factory Defaults 4.21.5 Backup & Restore 4.21.6 Reboot 4.21.7 Password 4.21.8 System Log 4.21.9 Statistics 	
 4.21.1 Time Settings	

Package Contents

The following items should be found in your package:

- > Archer C7 AC1750 Wireless Dual Band Gigabit Router
- > DC Power Adapter for Archer C7 AC1750 Wireless Dual Band Gigabit Router
- > Quick Installation Guide
- > Resource CD for Archer C7 AC1750 Wireless Dual Band Gigabit Router, including:
 - This Guide
 - Other Helpful Information

P 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. Introduction

1.1 Overview of the router

The Archer C7 AC1750 Wireless Dual Band Gigabit Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Powered by 3x3 MIMO technology, the AC1750 Wireless Dual Band Gigabit Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance. Your wireless connections are radio band selectable to avoid interference in your area, and the four built-in Gigabit ports supply high-speed connection to your wired devices.

Incredible Speed

The Archer C7 AC1750 Wireless Dual Band Gigabit Router provides up to 1750Mbps wireless connection with other wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11ac wireless router will give you the unexpected networking experience at speed much faster than 802.11n. It is also compatible with all IEEE 802.11n, IEEE 802.11a, IEEE 802.11b and IEEE 802.11g products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, Wi-Fi Protected Access (WPA2- PSK, WPA- PSK), as well as advanced Firewall protections, the Archer C7 AC1750 Wireless Dual Band Gigabit Router provides complete data privacy.

Flexible Access Control

The Archer C7 AC1750 Wireless Dual Band Gigabit Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Simple Installation

Since the router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the router, please look through this guide to know all the router's functions.

1.2 Conventions

The router or Archer C7 mentioned in this guide stands for Archer C7 AC1750 Wireless Dual Band Gigabit Router without any explanation.

1.3 Main Features

- > Complies with IEEE 802.11ac.
- One 10/100/1000M Auto-Negotiation RJ45 Internet port, four 10/100/1000M Auto-Negotiation RJ45 Ethernet ports, supporting Auto MDI/MDIX.
- > Provides USB ports supporting storage/FTP/Media/Print Server.
- > Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/ Static IP/ PPPoE/ PPTP/ L2TP/ BigPond Internet access.
- Supports simultaneous 2.4GHz and 5GHz connections for 1750Mbps of total available bandwidth.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- > Provides Automatic-connection and Scheduled Connection on certain time to the Internet.
- > Built-in NAT and DHCP server supporting static IP address distributing.
- Supports Parental Control and Access Control.
- > Connects Internet on demand and disconnects from the Internet when idle for PPPoE.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- > Supports Flow Statistics.
- Supports IPv6.
- > Supports firmware upgrade and Web management.
- Supports Tether App to manage the router on smart devices.

1.4 Panel Layout

1.4.1 The Front Panel



Figure 1-1 LEDs on the front panel

The router's LEDs are located on the front panel (View from left to right).

Name	Status	Indication
	Off	Power is off.
(Power) On		Power is on.
	On	The router is initializing or maybe has a system error.
🗮 (System)	Flashing	The router is working properly.
	Off	The router has a system error.
	Off	The wireless function is disabled.
2.4GHz)	Flashing	The wireless function is enabled. The router is working on 2.4GHz radio band.
🕱 (Wireless	Off	The wireless function is disabled.
5GHz)	Flashing	The wireless function is enabled. The router is working on 5GHz radio band.
	Off	There is no device linked to the corresponding port.
♀ (Ethernet) ♀ (Internet)	On	There is a device linked to the corresponding port but there is no activity.
	Flashing	There is an active device linked to the corresponding port.

	Slow Flash	A wireless device is connecting to the network by WPS function. This process will last in the first 2 minutes.
କ୍ଷ [™] (WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Quick Flash	A wireless device failed to be added to the network by WPS function.
O (USB on	Off	No storage device or printer is plugged into the USB port.
the rear panel)	On	A storage device or printer has connected to the USB port.

Table 1-1 The LEDs Description

P Note:

- 1. After a device is successfully added to the network by WPS function, the WPS LED will keep on for about 5 minutes and then turn off.
- 2. The router is set to working concurrently in 2.4GHz and 5GHz by default. If you desire to choose the working frequency, please go to <u>4.5 Dual Band Selection</u>.

1.4.2 The Rear Panel



Figure 1-2 Rear Panel sketch

The following parts are located on the rear panel (View from left to right).

- Power: The Power socket is where you will connect the power adapter. Please use the power adapter provided with this Archer C7 AC1750 Wireless Dual Band Gigabit Router.
- > **On/Off:** The switch for the power.
- > Wireless On/Off: The switch for the wireless function.
- > **USB:** The USB port connects to a USB storage device or a USB printer.

- > Internet: This port is where you will connect the DSL/cable Modem, or Ethernet.
- **Ethernet (1, 2, 3, 4):** These ports (1, 2, 3, 4) connect the router to the local PC(s).

> WPS/Reset:

Pressing this button for less than 5 seconds enables the WPS function. If your client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can press this button to quickly establish a connection between the router and client devices and automatically configure wireless security for your wireless network.

Pressing this button for more than 5 seconds enables the Reset function. With the router powered on, press and hold the **WPS/Reset** button (approximately 8 seconds) until the SYS LED becomes quick-flash from slow-flash. And then release the button and wait the router to reboot to its factory default settings.

> Wireless antenna: To receive and transmit the wireless data.

Chapter 2. Connecting the router

2.1 System Requirements

- > Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the router is connected directly to the Ethernet)
- > 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

- > Place the router in a well-ventilated place far from any heater or heating vent
- > Avoid direct irradiation of any strong light (such as sunlight)
- > Keep at least 2 inches (5 cm) of clear space around the router
- > Operating Temperature: $0^{\circ}C \sim 40^{\circ}C$ ($32^{\circ}F \sim 104^{\circ}F$)
- > Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the router

Before installing the router, make sure your PC is connected to the Internet through the broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

- 1. Power off your modem (if the modem has a backup battery, please remove it too.), and disconnect your existing router if you have one.
- 2. Connect the **Internet** port on your Router to the Modem's LAN port with an Ethernet cable.
- Connect your computer to one of the Ethernet ports labeled 1~4 on the Router with an Ethernet cable.
- 4. Power on the modem and wait for 2 minutes.
- 5. Make sure the **Wireless On/Off** switch is **ON**. Then plug the provided power adapter into the **Power** jack and the other end to a standard electrical wall socket. Press the **On/Off** button to

power on the Router. (Before you power on the Router, please make sure your computer is NOT connected to any other wireless network.)

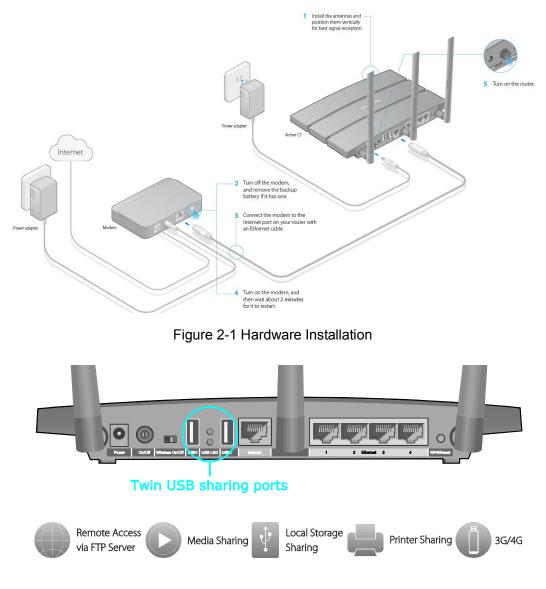


Figure 2-2 USB Installation

P Note:

If you want to use the router to share files or printer, plug the USB storage device to the USB port or connect the printer to the router with a matching cable.

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AC1750 Wireless Dual Band Gigabit Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the router is **192.168.0.1** 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 Ethernet ports of the router and then you can configure the IP address for your PC by the following method: 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 <u>Appendix B: Configuring the PC</u>. 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 between your PC and the router. The following example is in Windows 7 OS.

Open a command prompt, and type *ping tplinkwifi.net*, and then press Enter.

If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the router has been established well.

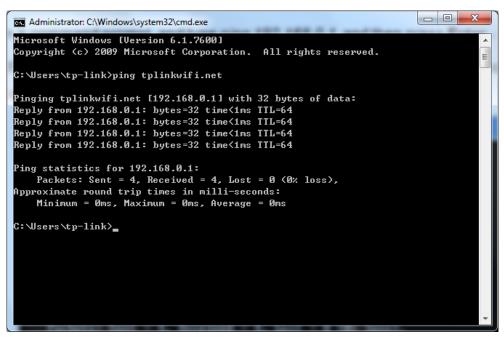


Figure 3-1 Success result of Ping command

If the result displayed is similar to Figure 3-2, it means the connection between your PC and the router failed.

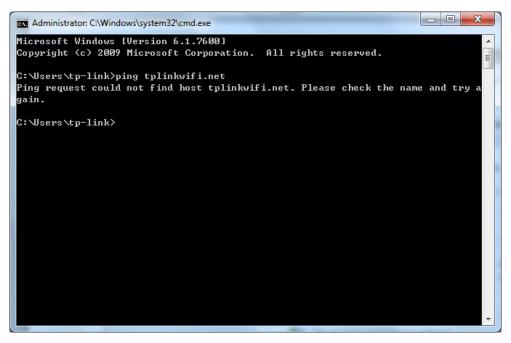


Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

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

P Note:

The 1/2/3/4 LEDs of Ethernet ports which you link to on the router and LEDs on your PC's adapter should be lit.

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

P Note:

If the router's IP address is 192.168.0.1, your PC's IP address must be within the range of $192.168.0.2 \sim 192.168.0.254$.

3. Is the default LAN IP of the router correct?

Note:

If the LAN IP of the modem connected with your router is 192.168.0.x, the default LAN IP of the router will automatically switch from 192.168.0.1 to 192.168.1.1 to avoid IP conflict. Therefore, in order to verify the network connection between your PC and the router, you can open a command prompt, and type *ping 192.168.1.1*, and then press **Enter**.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the AC1750 Wireless Dual Band Gigabit 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 in the default IP address <u>http://tplinkwifi.net</u> in the address field.

	Archer C7 AC1750 Wireless Dua	I Band Gigabit Router
P Archer C7 ×		
← → C		☆ =

Figure 3-3 Log in the router

After a moment, a login window will appear, similar to 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.

<u>*</u>	admin	
p		
	Login	

Figure 3-4 Login Windows

P 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 successful login, the **Quick Setup** page will appear for you to quickly configure your router.

Quick Setup
Run the Quick Setup to manually configure your internet connection and wireless settings.
To continue, please click the Next button.
To exit, please click the Exit button.
Exit Next

Figure 3-5 Quick Setup

3. Click Next, and then WAN Connection Type page will appear, shown in Figure 3-6.

Quick Setup - WAN Connection Type
The Quick Setup is preparing to set up your internet connection, please choose one type below according to your ISP. The detailed description will be displayed after you choose the corresponding type.
Auto-Detect
Dynamic IP (Most Common Cases)
Static IP
PPPoE/Russian PPPoE
L2TP/Russian L2TP
PPTP/Russian PPTP
Note: For users in some areas (such as Russia, Ukraine etc.), please contact your ISP to choose connection type manually.
Back Next

Figure 3-6 WAN Connection Type

The router provides **Auto-Detect** function and supports three popular ways **PPPoE**, **Dynamic IP**, and **Static IP** and to connect to the Internet. It's recommended that you make use of the **Auto-Detect** function. If you are sure of what kind of connection type your ISP provides, you can select the very type and click **Next** to go on configuring.

- 4. If you select Auto-Detect, the router will automatically detect the connection type your ISP provides. Make sure the cable is securely plugged into the Internet port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the router.
 - 1) If the connection type detected is **Dynamic IP**, the next screen will appear as shown in the below picture. A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will register the MAC address of your computer when you access the Internet for the first time via the cable/ADSL modem they offered. If you add a router into your network to share the Internet, the ISP may not recognize the new MAC address of the router and will not offer the Internet connection any more. Therefore, it is necessary to clone the MAC address of the computer to the router.

	Quick Setup - MAC Clone
	MAC(Media Access Control) address is a unique identifier that identifies your computer or device in the network. Some of the ISPs may register the MAC address of your computer which firstly connects to their services, and would not allow the Internet connection for any new computer or router.TP-LINK router can help you to "clone" or replicate the registered MAC address of your first computer.
	In most of the cases, there is no need to clone the MAC address. But if you can't get the Internet connection after Quick Setup, please run it again and clone the MAC address for a try.
۲	No, I do NOT need to clone MAC address.
	YES, I need to clone MAC address.
No	te: please make sure your current computer is the one initially connected to your modem or ISP's device.
	Back Next

- If you are visiting the Router from the main computer, please select Yes, and then click Next.
- If you are visiting the Router from another computer rather than the main computer, please select No, and then click Next.

```
Solution Note:
```

- 1. It's strongly recommended that you visit and configure the Router from the main computer.
- To find the main computer's MAC, please go to Start > Run on your main computer, type in cmd and press Enter. At the command prompt, enter ipconfig/all and press Enter. The MAC will be displayed as Physical Address.
- If the connection type detected is Static IP, the next screen will appear as shown in Figure 3-7. Configure the following parameters and then click Next to continue.

Quick Setup - Static IP		
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	
Primary DNS:	0.0.0.0	
Secondary DNS:	0.0.0.0	(Optional)
	Back	Next

Figure 3-7 Quick Setup - Static IP

- IP Address This is the WAN IP address as seen by external users on the Internet (including your ISP). Your ISP will provide you with the IP address you need to enter here. Enter the IP address into the field.
- Subnet Mask The Subnet Mask is used for the WAN IP address. Your IPS will provide you with the subnet mask which is usually 255.255.255.0.
- Default Gateway Your ISP will provide you with the Gateway address which is the ISP server's address. Enter the gateway IP address into the box if required.
- > **Primary DNS -** Enter the DNS Server IP address into the box if required.
- Secondary DNS (Optional) If your ISP provides another DNS server, enter it into this field.
- 3) If the connection type detected is **PPPoE/Russian PPPoE**, the next screen will appear as shown in Figure 3-8. Configure the following parameters and then click **Next** to continue.

Disabled	Oynamic IP	Static IP	(For Dual Access/Russia PPPoE)
Back	Next		
			Disabled Dynamic IP Static IP Back Next

Figure 3-8 Quick Setup – PPPoE/Russia PPPoE

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.
- Confirm Password Enter the password again to make sure that the password is correct.

Check the radio button of **Dynamic/Static IP** to activate the secondary connection if your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network.

4) If the connection type detected is **L2TP**/**Russian L2TP**, the next screen will appear as shown in Figure 3-9.Configure the following parameters and then click **Next** to continue.

Quick Setup - L2TP	
User Name:	
Password:	
Confirm Password:	
Server IP Address/Name:	Dynamic IP Static IP
	Back Next

Figure 3-9 Quick Setup – PPTP/Russia PPTP

User Name/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.

Select **Static IP** if IP Address/ Subnet Mask/ Gateway and DNS server address have been provided by your ISP. Then please enter server IP address or domain name provided by your ISP, and also enter the corresponding parameters.

	 Dynamic IP Static IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS:	0.0.0.0

Select **Dynamic IP** if none of the above parameters are provided. Then you just need to enter server IP address or domain name provided by your ISP.

	Oynamic IP	 Static IP 	
Server IP Address/Name:			

5) If the connection type detected is **PPTP/Russian PPTP**, the next screen will appear as shown in Figure 3-10. Configure the following parameters and then click **Next** to continue.

Quick Setup - PPTP	
User Name:	
Password:	
Confirm Password:	
Server IP Address/Name:	Dynamic IP Static IP
	Back Next

Figure 3-10 Quick Setup – L2TP/Russia L2TP

User Name/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.

Select **Static IP** if IP Address/ Subnet Mask/ Gateway and DNS server address have been provided by your ISP. Then please enter server IP address or domain name provided by your ISP, and also enter the corresponding parameters.

	Dynamic IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0
Gateway:	0.0.0.0
DNS:	0.0.0

Select **Dynamic IP** if none of the above parameters are provided. Then you just need to enter server IP address or domain name provided by your ISP.

	Oynamic IP	Static IP	
Server IP Address/Name:]

5. After finishing WAN Connection Type selection, the Dual Band Selection page will appear as shown in Figure 3-11. Here we take "Concurrently with 2.4GHz and 5GHz (802.11a/b/g/n)" for example. Click **Next** to continue.

Quick Setup - Wireles	s Dual Band Selection
The internet setting is finished, ple	ease choose the wireless band of the router:
Concurrently with 2.4GHz and	d 5GHz (802.11a/b/g/n/ac)
Only work in 2.4GHz (802.11)	b/g/n)
Only work in 5GHz (802.11a/	n/ac)
You can also use the Wi-Fi (Dn/Off button on the back panel to completely switch on/off the wireless radio.
	Back Next

Figure 3-11 Quick Setup – Dual Band Selection

- 2.4GHz You can use the 2.4GHz band to connect to many classic wireless devices like gaming consoles, laptops, DVRs, ect.
- 5GHz This band is less crowded and is used for time-sensitive music, video streaming or gaming. Using this band can avoid interference with 2.4GHz networks or noisy devices like cordless phones and microwave ovens.
- 6. Configure the basic parameters for 2.4GHz wireless network in the following screen as shown in Figure 3-12, and then click **Next**.

Quick Setup - Wireless 2	.4GHz	
The Internet setting have been co	ompleted,now please configure wireless settings.	
Wireless Radio:	Enable	
Wireless Network Name:	TP-LINK_A4B4 (Also called the SSII	D)
Region:	United States	
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.	
Wireless Security:		
0	Disable Security	
۲	Enable Security(WPA-PSK/WPA2-PSK)	
PSK Password:	44357207	
	(You can enter ASCII characters between 8 and 63 or Hexadecimal cl between 8 and 64.)	haracters
\odot	No Change	
	(Use the current security settings.)	
	More Advanced Wireless Settings	
	Note: Please use the WiFi switch on this device to enable/disable radi	io.
	Back Next	

Figure 3-12 Quick Setup – Wireless

- > Wireless Radio Displays whether the wireless function is enabled or not.
- Wireless Network Name Also called the SSID (Service Set Identification). Enter a value of up to 32 characters. The same name must be assigned to all wireless devices

in your network. The default SSID is set to be TP-LINK_2.4GHz_XXXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

Region - Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

P Note:

Limited by local law regulations, version for North America does not have region selection option.

- > Wireless Security
 - **Disable Security** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption.
 - Enable Security (WPA-PSK/WPA2-PSK) It's selected by default, with the default PSK password the same as the default PIN code.
 - No Change If you chose this option, wireless security configuration will not change!

The above settings are only for basic wireless parameters. For advanced settings, please check "**More Advanced Wireless Settings**", and then you can set the following parameters.

	More Advanced Wireless Settings
Band:	2.4GHz
Mode:	11bgn mixed T
Channel Width:	Auto 🔻
Channel:	Auto 🔻
	Note: Please use the WiFi switch on this device to enable/disable radio.

- > **Band -** This field displayed the operating frequency being configured.
- > **Mode -** This field determines the wireless mode which the router works on.
 - **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.
- Channel Width Select any channel width from the drop-down list. The default setting is "Auto", which can adjust the channel width for your clients automatically.
- 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. If you select "Auto", then the AP will select the best channel automatically.

7. Configure the basic parameters for 5GHz wireless network in the following screen as shown

The Internet setting have been c	ompleted,now please configure wireless settings.	
Wireless Radio:	Enable	
Wireless Network Name:	TP-LINK_A4B3_5G (Also called the SSID)	
Region:	United States	
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.	
Wireless Security:		
0	Disable Security	
۲	Enable Security(WPA-PSK/WPA2-PSK)	
PSK Password:	44357207	
	(You can enter ASCII characters between 8 and 63 or Hexadecimal character: between 8 and 64.)	
0	No Change	
	(Use the current security settings.)	
	More Advanced Wireless Settings	
	Note: Please use the WiFi switch on this device to enable/disable radio.	

Figure 3-13 Quick Setup – Wireless

- > Wireless Radio Choose from the drop-down list to enable or disable the wireless radio.
- Wireless Network Name Also called the SSID (Service Set Identification). Enter a value of up to 32 characters. The same name must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_5GHz_XXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

P Note:

Limited by local law regulations, version for North America does not have region selection option.

> Wireless Security

- Disable Security The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption.
- Enable Security (WPA-PSK/WPA2-PSK) It's selected by default, with the default PSK password the same as the default PIN code.
- No Change If you chose this option, wireless security configuration will not change!

The above settings are only for basic wireless parameters. For advanced settings, please check "**More Advanced Wireless Settings**", and then you can set the following parameters.

•	More Advanced Wireless Settings
Band:	5GHz
Mode:	11a/n/ac mixed •
Channel:	Auto 🔻
	Note: Please use the WiFi switch on this device to enable/disable radio.

- > **Band** This field displayed the operating frequency being configured.
- > Mode This field determines the wireless mode which the router works on.
 - **11an mixed -** Select if you are using both 802.11a and 802.11n wireless clients.
 - **11a/n/ac mixed** Select if you are using 802.11a, 802.11n and 802.11ac wireless clients.
- 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. If you select "Auto", then the AP will select the best channel automatically.
- 8. Then you will see the **Finish** page.
- If you don't make any change on the Wireless page, you will see the Finish page as shown in Figure 3-14. Click the Finish button to finish the Quick Setup.

Quick Setup - Finish		
Congratulations!		
The basic internet and wireless settings are finished, please click Finish button and test your internet connection.		
If it is failed, please reboot your modem and wait 2 minutes or run the Quick Setup again.		
Back Finish		

Figure 3-14 Quick Setup – Finish

If there is anything changed on the Wireless page, you will see the Finish page as shown in Figure 3-15. Click the Reboot button to make your wireless configuration take effect and finish the Quick Setup.

Quick Setup - Finish				
Congratulations!				
The basic internet and wireless settings are finished, please click Finish button and test your internet connection.				
If it is failed, please reboot your modem and wait 2 minutes or run the Quick Setup again.				
The change of wireless config will not take effect until the Router reboot.				
Back Reboot				

Figure 3-15 Quick Setup – Reboot

Chapter 4. Configuring the router

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

4.1 Login

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

Quick Setup Network Dual Band Selection
Dual Band Selection
Wireless 2.4GHz
Wireless 5GHz
Guest Network
DHCP
USB Settings
NAT
Forwarding
Security
Parental Control
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
IPv6 Support
System Tools
Logout

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

4.2 Status

The Status page provides the current status information about the router. All information is read-only.

a pişanını.			
Firmware Version:	3.14.2 Build 150311 Rel.54891n		
Hardware Version:	0000000		
LAN			
MAC Address:	C0-4A-00-0A-A4-B4		
IP Address:	192.168.0.1		
Subnet Mask:	255.255.255.0		
Wireless 2.4GHz			
Wireless Radio:	Enable		
Name (SSID):	TP-LINK_A4B4		
Mode:	- 11bgn mixed		
Channel:	Auto (Current channel 1)		
Channel Width:	Automatic		
MAC Address:	C0-4A-00-0A-A4-B4		
WDS Status:	Disable		
Wireless 5GHz			
Wireless Radio:	Enable		
Name (SSID):	TP-LINK_A4B3_5G		
Mode:	11a/n/ac mixed		
Channel:	Auto (Current channel 149)		
Channel Width:	Automatic		
MAC Address:	C0-4A-00-0A-A4-B3		
WDS Status:	Disable		
WAN			
MAC Address:	C0-4A-00-0A-A4-B5		
IP Address:	219.134.214.229	PPPoE(Connect Automatically)	
Subnet Mask:	255.255.255.255		
Default Gateway:	219.134.214.229		
DNS Server:	202.96.128.166 , 202.96.134.133		
Online Time:	0 day(s) 00:00:14	Disconnect	
Traffic Statistics			
	Received	Sent	
Bytes:	228603	173320	
Packets:	442	557	

Figure 4-1 Status

4.3 Quick Setup

Please refer to <u>3.2 Quick Installation Guide</u>.

4.4 Network

Network
- WAN
- LAN
- MAC Clone
- IPTV

Figure 4-2 the Network menu

There are four submenus under the Network menu (shown in Figure 4-2): **WAN**, **LAN**, **MAC Clone** and **IPTV**. Click any of them, and you will be able to configure the corresponding function.

4.4.1 WAN

Choose menu "**Network** \rightarrow **WAN**", you can configure the IP parameters of the WAN on the screen below.

1. If your ISP provides the DHCP service, please choose **Dynamic IP** type, and the router will automatically get IP parameters from your ISP. You can see the page as follows.

WAN	
WAN Connection Type:	Dynamic IP Detect
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
	Renew Release
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
	Use These DNS Servers
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0 (Optional)
Host Name:	Archer_C7
	Get IP with Unicast DHCP (It is usually not required.)
	Save

Figure 4-3 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

- MTU Size The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
- Use These DNS Servers If your ISP gives you one or two DNS addresses, select Use These DNS Servers and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Solution Note:

If you find error when you go to a website after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- > Host Name This option specifies the Host Name of the router.
- Get IP with Unicast DHCP A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (It is rarely required.)

Click the Save button to save your settings.

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 4-4.

WAN		
WAN Connection Type:	Static IP	▼ Detect
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	
MTU Size (in bytes):	1500 (The default	is 1500, do not change unless necessary.)
Primary DNS:	0.0.0.0	
Secondary DNS:	0.0.0.0	(Optional)
	Save	

Figure 4-4 WAN - Static IP

- > 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.
- Default Gateway (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- MTU Size The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
- Primary/Secondary DNS (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

Click the Save button to save your settings.

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. And you should enter the following parameters (Figure 4-5):

WAN	
WAN Connection Type:	PPPoE/Russia PPPoE V Detect
PPPoE Connection:	
User Name:	userame
Password:	
Confirm Password:	
Secondary Connection:	◉ Disabled 💿 Dynamic IP 💿 Static IP (For Dual Access/Russia PPPoE)
Wan Connection Mode:	Connect on Demand
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Automatically
	Time-based Connecting
	Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
	Connect Manually
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Disconnect Connected
	Save Advanced

Figure 4-5 WAN - PPPoE

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Secondary Connection It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.

- **Disabled** The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
- **Dynamic IP** You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.
- **Static IP** You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by ISP.
- Connect on Demand In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- Connect Automatically The connection can be re-established automatically when it was down.
- Time-based Connecting The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

P Note:

Only when you have configured the system time on "**System Tools Time Settings**" page, will the **Time-based Connecting** function can take effect.

Connect Manually - You can click the Connect/Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Caution: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-6 will then appear:

PPPoE Advanced Setting	S
MTU Size (in bytes):	(The default is 1480, do not change unless necessary.)
Service Name: AC Name:	
ISP Specified IP Address: Detect Online Interval:	Use IP address specified by ISP 0.0.0.0 0 Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)
Detect Online Interval.	Use the following DNS Servers
Primary DNS:	0.0.0
Secondary DNS:	0.0.0.0 (Optional)
	Save Back

Figure 4-6 PPPoE Advanced Settings

- MTU Size The default MTU size is "1480" bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- Service Name/AC Name The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- ISP Specified IP Address If your ISP does not automatically assign IP addresses to the router during login, please click "Use IP address specified by ISP" check box and enter the IP address provided by your ISP in dotted-decimal notation.
- Detect Online Interval The router will detect Access Concentrator online at every interval. The default value is "0". You can input the value between "0" and "120". The value "0" means no detect.
- Primary DNS/Secondary DNS If your ISP does not automatically assign DNS addresses to the router during login, please click "Use the following DNS servers" check box and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

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

 If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select BigPond Cable. And you should enter the following parameters (Figure 4-7):

WAN	
WAN Connection Type:	BigPond Cable
User Name:	
Password:	
Auth Server:	sm-server
Auth Domain:	
	(The default is 1500 do not share uplose personal)
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
	Connect on Demand
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Automatically
	Connect Manually
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Disconnect Disconnected!
	Save

Figure 4-7 WAN - BigPond Cable

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- > Auth Server Enter the authenticating server IP address or host name.
- > Auth Domain Type in the domain suffix server name based on your location.

e.g.

NSW / ACT - nsw.bigpond.net.au VIC / TAS / WA / SA / NT - vic.bigpond.net.au QLD - qld.bigpond.net.au

- MTU Size The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
- Connect on Demand In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- Connect Automatically The connection can be re-established automatically when it was down.

Connect Manually - You can click the Connect/Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Caution: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

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

5. If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option. And you should enter the following parameters (Figure 4-8):

WAN		
WAN Connection Type:	L2TP/Russia L2TP 🔹	
User Name:		
Password:		
	Connect Disconnect Disconnected!	
	Dynamic IP Static IP	
Server IP Address/Name:		
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Gateway:	0.0.0.0	
DNS:	0.0.0.0 , 0.0.0.0	
Internet IP Address:	0.0.0.0	
Internet DNS:	0.0.0.0 , 0.0.0.0	
MTH Size (in hytee):	1460 (The default is 1460, do not change unless necessary.)	
MTU Size (in bytes): Max Idle Time:	1460 (The default is 1460, do not change unless necessary.) 15 minutes (0 means remain active at all times.)	
wax fule fime.	15 minutes (o means remain active at an unies.)	
WAN Connection Mode:	Connect on Demand	
	Connect Automatically	
	Connect Manually	
	Save	

Figure 4-8 WAN - L2TP/Russia L2TP

User Name/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- Dynamic IP/ Static IP Choose either as you are given by your ISP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
- Connect on Demand You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, check the radio button. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Connect Automatically Connect automatically after the router is disconnected. To use this option, check the radio button.
- Connect Manually You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time**, because some applications are visiting the Internet continually in the background.

Click the Save button to save your settings.

6. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 4-9):

WAN	
WAN Connection Type:	PPTP/Russia PPTP 🔹
User Name:	
Password:	
	Connect Disconnect Disconnected!
	Oynamic IP Static IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS:	0.0.0.0 , 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0.0 , 0.0.0.0
MTU Size (in bytes):	1420 (The default is 1420, do not change unless necessary.)
Max Idle Time:	15 minutes (0 means remain active at all times.)
WAN Connection Mode:	Connect on Demand
WAN Connection Mode.	Connect Automatically
	Connect Manually Connect Manually
	oundermanually
	Save

Figure 4-9 PPTP Settings

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Dynamic IP/ Static IP Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Connect on Demand - You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- Connect Automatically Connect automatically after the router is disconnected. To use this option, check the radio button.
- Connect Manually You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications are visiting the Internet continually in the background.

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

P Note:

If you don't know how to choose the appropriate connection type, click the **Detect** button to allow the router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the router can detect are as follows:

- **PPPoE** Connections which use PPPoE that requires a user name and password.
- **Dynamic IP** Connections which use dynamic IP address assignment.
- Static IP Connections which use static IP address assignment.

The router cannot detect PPTP/L2TP/Big Pond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.4.2 LAN

Choose menu "**Network** \rightarrow **LAN**", you can configure the IP parameters of the LAN on the screen as below.

LAN	
MAC Address:	C0-4A-00-0A-A4-B4
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0 ▼
	Save

Figure 4-10 LAN

- MAC Address The physical address of the router, as seen from the LAN. The value can't be changed.
- IP Address Enter the IP address of your router or reset it in dotted-decimal notation (factory default: 192.168.0.1).
- Subnet Mask An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

P Note:

- 1) If you change the IP Address of LAN, you must use the new IP Address to log in the router.
- 2) If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.4.3 MAC Clone

Choose menu "**Network** \rightarrow **MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 4-11:

C Clone		
WAN MAC Address:	C0-4A-00-0A-A4-B5	Restore Factory MAC
Your PC's MAC Address:	D4-3D-7E-BF-61-5F	Clone MAC Address

Figure 4-11 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

WAN MAC Address - This field displays the current MAC address of the Internet port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX format (X is any hexadecimal digit). Your PC's MAC Address - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the Clone MAC Address button and this MAC address will fill in the WAN MAC Address field.

Click **Restore Factory MAC** to restore the MAC address of Internet port to the factory default value. Click the **Save** button to save your settings.

P Note:

Only the PC on your LAN can use the **MAC Address Clone** function.

4.4.4 IPTV

Select "Network \rightarrow IPTV" to go to the setup screen IPTV.

Figure 4-12 IPTV

- > **IGMP Proxy** If you want to watch TV through IGMP, please Enable it.
- > Mode:
 - Automatic There would be no change to the LAN ports, work with IGMP Proxy technology, allowing watch IPTV via wired and wireless connection.

Mode:	Automatic	•
-------	-----------	---

 Bridge - Assign an individual LAN port for IPTV set-top-box, which can get IP address from ISP directly, without any quality loss even when PCs connect with router are downloading torrents at maximum speed, since this LAN port is isolated from other NAT LAN ports.

Mode:	Bridge	T
Port for IPTV:	Disable	•

802.1Q Tag VLAN - ISP would provide the networking service based on 802.1Q Tag VLAN technology. You can assign different VLAN Tag ID for different LAN ports, to connect PC, IPTV set-top-box or IP-phone. Please contact with you ISP to get the VLAN ID information.

Mode:	802.1Q Tag VLAN 🔹
VLAN TAG for Internet Service:	🔵 Disable 💿 Enable
Internet VLAN ID:	1257
Internet VLAN Pri:	0 •
IP-phone VLAN ID:	263
IP-phone VLAN Pri:	0 •
IPTV VLAN ID:	4000
IPTV VLAN Pri:	4 🔻
	Enable Multicast VLAN
LAN1 Mode:	IP-phone ▼
LAN2 Mode:	Internet •
LAN3 Mode:	Internet •
LAN4 Mode:	IPTV V

4.5 Dual Band Selection

Choose menu "**Dual Band Selection**", and you can choose the working frequency for your router. It is recommended that your computers and devices running video and voice applications use the 5GHz band, while your guest access and computers that are only browsing the web use the 2.4GHz band.

Dual Band Selection		
This router supports dual band, please choose the frequency that you would like to work with:		
Concurrently with 2.4GHz and 5GHz (802.11a/b/g/n/ac)		
Only work in 2.4GHz (802.11b/g/n)		
Only work in 5GHz (802.11a/n/ac)		
To turn off the wireless radio, you can switch the Wireless On/Off button located on the back panel of the device to the OFF position.		
Save		

Figure 4-13 Dual Band Selection

- Concurrently with 2.4GHz and 5GHz (802.11a/b/g/n) Choose this option, and then the router will work concurrently in 2.4GHz and 5GHz frequency.
- Only work in 2.4GHz (802.11b/g/n) Choose this option, and then the router will only work in 2.4GHz frequency. You can use the 2.4GHz band to connect to many classic wireless devices like gaming consoles, laptops, DVRs, ect.
- Only work in 5GHz (802.11a/n) Choose this option, and then the router will only work in 5GHz frequency. This band is less crowded and is used for time-sensitive music, video streaming or gaming. Using this band can avoid interference with 2.4GHz networks or noisy devices like cordless phones and microwave ovens.

4.6 Wireless 2.4GHz



Figure 4-14 Wireless menu

There are six submenus under the Wireless menu (shown in Figure 4-14): Wireless Settings, WPS, Wireless Security, Wireless MAC Filtering, Wireless Advanced and Wireless Statistics. Click any of them, and you will be able to configure the corresponding functions.

4.6.1 Wireless Settings

Choose menu "Wireless 2.4GHz \rightarrow Wireless Settings", you can configure the basic settings for the wireless network of 2.4GHz on this page.

Wireless Settings (2.4GHz		
Wireless Network Name: Region:	TP-LINK_A4B4	(Also called the SSID)
Warning:	Ensure you select a correct cou Incorrect settings may cause into	
Mode:	11bgn mixed 🔻	
Channel Width:	Auto 🔻	
Channel:	Auto 🔻	
	Enable SSID Broadcast	
	Enable WDS Bridging	
	Save	

Figure 4-15 Wireless Settings – 2.4GHz

- Wireless Network Name Also called the SSID (Service Set Identification). Enter a value of up to 32 characters. The same name must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_2.4GHz_XXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of

the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the drop-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.

The page at 192.168.0.1 says:		×
Selecting the incorrect country may cause int other devices and violate the applicable law.	erference to	
	ОК]

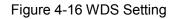


P Note:

Limited by local law regulations, version for North America does not have region selection option.

- > **Mode -** Select the desired mode.
 - **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. It is strongly recommended that you set the Mode to **802.11bgn mixed**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.
- 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.
- Channel This field determines which operating frequency will be used. The default channel is set to Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Enable SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. If you select the Enable SSID Broadcast checkbox, the Wireless router will broadcast its name (SSID) on the air.
- Enable WDS Bridging Check this box to enable WDS. With this function, the router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown in Figure 4-16. Make sure the following settings are correct.

	Enable WDS Bridge	ging
SSID(to be bridged):		
MAC Address(to be bridged):		Example:00-1D-0F-11-22-33
	Survey	
Key type:	None	T
WEP Index:	1	T
Auth type:	open	T
Password:		

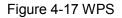


- SSID (to be bridged) The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- MAC Address (to be bridged) The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- > **Survey** 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 router is going to connect needs password, you need to fill the password in this blank.

4.6.2 WPS

Choose menu "Wireless 2.4GHz \rightarrow WPS", you can the screen as shown in Figure 4-17. This section will guide you to add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

WPS (Wi-Fi Protected Setup)		
WPS Status:	Enabled Disable WPS	
Current PIN:	44357207 Restore PIN Gen New PIN Disable Router's PIN	
Add a new device:	Add device	



- > WPS Status Enable or disable the WPS function here.
- Current PIN The current value of the router's PIN is displayed here. The default PIN of the router can be found in the label or User Guide.
- > **Restore PIN -** Restore the PIN of the router to its default.
- Gen New PIN Click this button, and then you can get a new random value for the router's PIN. You can ensure the network security by generating a new PIN.
- Disable router's PIN If this box is checked, and then wireless clients will not be able to connect to the wireless network with PIN code.
- Add device You can add a new device to the existing network manually by clicking this button.

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

P 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 WPS button.

Step 1: Press the WPS/Reset button on the back panel of the router, as shown in Figure 4-18. You can also keep the default WPS status as Enabled and click the Add device button in Figure 4-17. Then choose "Press the button of the new device in two minutes" and click Connect, shown in Figure 4-19.

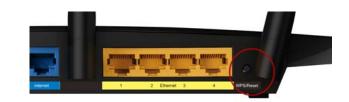


Figure 4-18

Add A New Device
Enter the new device's PIN.
PIN:
Press the button of the new device in two minutes.
Back Connect

Figure 4-19 Add A New Device

- Step 2: Press and hold the WPS button of the client device.
- **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 router.

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

Use this method if your client device does not have the WPS button, but 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 4-17, then Figure 4-20 will appear.

Add A New Device
Enter the new device's PIN.
PIN:
Press the button of the new device in two minutes.
Back Connect

Figure 4-20 Add A New Device

- Step 2: Enter the PIN number from the client device in the field on the WPS screen above. Then click **Connect** button.
- **Step 3: "Connect successfully**" will appear on the screen of Figure 4-20, which means the client device has successfully connected to the router.

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

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

- **Step 1:** On the client device, enter the PIN number listed on the router's Wi-Fi Protected Setup screen, shown in Figure 4-17 (It is also labeled on the bottom of the 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 router.

```
P Note:
```

1) The WPS LED on the 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 router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.6.3 Wireless Security

Choose menu "Wireless 2.4GHz → Wireless Security", you can configure the security settings of your wireless network. There are five wireless security modes supported by the router: WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, and WEP.

Wireless Security		
Disable Security		
WPA/WPA2 - Personal(Re	commended)	
Version:	Automatic (Recommended)	
Encryption:	AES	
PSK Password:	44357207	
	(You can enter ASCII characters	between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period:	0 Seconds (Ke	ep it default if you are not sure, minimum is 30, 0 means no update)
WPA/WPA2 - Enterprise		
Version:	Automatic •	
Encryption:	Automatic •	
Radius Server IP:		
Radius Port:	1812 (1-65535, 0 stands	s for default port 1812)
Radius Password:		
Group Key Update Period:	0 (in second, n	ninimum is 30, 0 means no update)
WEP		
Туре:	Automatic 🔹	
WEP Key Format:	Hexadecimal 🔹	
Key Selected	WEP Key (Password)	Кеу Туре
Key 1: 💿		Disabled T
Key 2:		Disabled T
Key 3:		Disabled ▼
Key 4:		Disabled T
	Save	

Figure 4-21 Wireless Security

- Disable 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 It's the WPA/WPA2 authentication type based on pre-shared passphrase. The router is configured by this security type by default.
 - Version you can choose the version of the WPA-PSK security on the drop-down list. The default setting is Automatic, which can select WPA-PSK (Pre-shared key of WPA) or WPA2-PSK (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
 - Encryption When WPA-PSK or WPA is set as the Authentication Type, you can select either Automatic, or TKIP or AES as Encryption.

P Note:

If you check the **WPA/WPA2-Personal** radio button and choose **TKIP** encryption, you will find a notice in red as shown in Figure 4-22.

WPA/WPA2 - Personal(Re	WPA/WPA2 - Personal(Recommended)			
Version:	Automatic(Recommended)			
Encryption:	TKIP			
PSK Password:	44357207			
	(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)			
Group Key Update Period:	0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)			
	We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.			

Figure 4-22 WPA/WPA2 – Personal

- **PSK Password** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the bottom of the router or can be found in Figure 4-17.
- **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.
 - Version you can choose the version of the WPA security on the drop-down list. The default setting is Automatic, 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 Automatic, or TKIP or AES.

Solution Note:

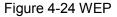
If you check the **WPA/WPA2-Enterprise** radio button and choose **TKIP** encryption, you will find a notice in red as shown in Figure 4-23.

WPA/WPA2 - Enterprise		
Version:	Automatic •	
Encryption:	TKIP	
Radius Server IP:		
Radius Port:	1812 (1-65535, 0 stands for default port 1812)	
Radius Password:		
Group Key Update Period:	0 (in second, minimum is 30, 0 means no update)	
	We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.	

Figure 4-23 WPA/WPA2 - Enterprise

- Radius Server IP Enter the IP address of the Radius server.
- Radius Port Enter the port number of the Radius server.
- Radius 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. If you check this radio button, you will find a notice in red as show in Figure 4-24.

WEF	2		
	Type:	Automatic 🔹	
	WEP Key Format:	Hexadecimal 🔻	
	Key Selected	WEP Key (Password)	Кеу Туре
	Key 1: 💿		Disabled T
	Key 2:		Disabled T
	Key 3:		Disabled v
	Key 4:		Disabled v
		We do not recommend using the WEP 802.11n mode due to the fact that WEF	encryption if the device operates in P is not supported by 802.11n specification.



- **Type** you can choose the type for the WEP security on the drop-down list. The default setting is **Automatic**, which 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.

152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

P 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 MAC Filtering

Choose menu "Wireless 2.4GHz \rightarrow Wireless MAC Filtering", you can control the wireless access by configuring the Wireless MAC Filtering function, shown in Figure 4-25.

Wireless MA	C Filtering			
Wireless N	MAC Filtering: Disabled Enab	ble		
Filtering Ru	les			
Deny tr	ne stations specified by any enabled e	entries in the list to acces	S.	
 Allow the second second	ne stations specified by any enabled e	entries in the list to acces	s.	
ID MAC Add	ress	Status	Description	Modify
Add New	Enable All Disable All	Delete All		
	Previo	Next		

Figure 4-25 Wireless MAC Filtering

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 **"Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-26:

Add or Modify Wireless MAC	Address Filtering entry
MAC Address: Description: Status:	Enabled T
	Save Back

Figure 4-26 Add or Modify Wireless MAC Address Filtering entry

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

- 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: 00-0A-EB-B0-00-0B.
- 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 modify or delete an existing entry:

- 1. Click the **Modify** 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 All button to make all entries enabled

Click the **Disable All** button to make all entries disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the router, but all the other wireless stations cannot access the 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 entries 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 00-0A-EB-B0-00-0B/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:

F	Filtering Rules				
	Deny the stations specified by any enabled entries in the list to access.				
	Allow the stations specified by any enable	oled entries in the lis	at to access.		
ID	MAC Address	Status	Description	Modify	
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete	
2	00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete	

4.6.5 Wireless Advanced

Choose menu "Wireless 2.4GHz \rightarrow Wireless Advanced", you can configure the advanced settings of your wireless network.

Wireless Advanced		
Transmit Power:	High	▼
Beacon Interval :	100	(40-1000)
RTS Threshold:	2346	(1-2346)
Fragmentation Threshold:	2346	(256-2346)
DTIM Interval:	1	(1-255)
	C Enable WMM	
	Enable Short GI	
	Enable	AP Isolation
	Save	9

Figure 4-27 Wireless Advanced

- Transmit Power Here you can specify the transmit power of 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 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the 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 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 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 1-15 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- Enable WMM WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.
- Enable Short GI This function is recommended for it will increase the data capacity by reducing the guard interval time.
- Enabled AP Isolation This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

P 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.

4.6.6 Wireless Statistics

Choose menu "Wireless 2.4GHz → Wireless Statistics", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Wireless Statistics				
	Current Connected Wirele	ess Stations numbers: 1	Refresh	
ID	MAC Address	Current Status	Designed Designed	Saut Dashata
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	C8-85-50-5D-02-40	STA-ASSOC	19773	25714
Previous Next				

Figure 4-28 Wireless Statistics

- > 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.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

P Note:

This page will be refreshed automatically every 5 seconds.

4.7 Wireless 5GHz

Wireless 5GHz
- Wireless Settings
- WPS
- Wireless Security
- Wireless MAC Filtering
- Wireless Advanced
- Wireless Statistics

Figure 4-29 Wireless menu

There are six submenus under the Wireless menu (shown in Figure 4-14): Wireless Settings, WPS, Wireless Security, Wireless MAC Filtering, Wireless Advanced and Wireless Statistics. Click any of them, and you will be able to configure the corresponding functions.

4.7.1 Wireless Settings

Choose menu "Wireless 5GHz \rightarrow Wireless Settings", you can configure the basic settings for the wireless network of 5GHz on this page.

Wireless Settings (5GHz)		
Wireless Network Name:	TP-LINK_A4B3_5G	(Also called the SSID)
Region: Warning:	Ensure you select a correct country to	o conform local law
warning.	Incorrect settings may cause interfere	
Mode:	11a/n/ac mixed ▼	
Channel:	Auto 🔻	
	Enable SSID Broadcast	
	Enable WDS Bridging	
	Save	

Figure 4-30 Wireless Settings – 5GHz

- Wireless Network Name Also called the SSID (Service Set Identification). Enter a value of up to 32 characters. The same name must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_5GHz_XXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the drop-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.

The page at 192.168.0.1 says:	×
Selecting the incorrect country may cause interference to other devices and violate the applicable law.	
ок	

Note Dialog

P Note:

Limited by local law regulations, version for North America does not have region selection option.

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

- 11a/n/ac mixed Select if you are using 802.11a, 802.11n and 802.11ac wireless clients. It is strongly recommended that you set the Mode 11a/n/ac mixed, and all of 802.11a, 802.11n and 802.11ac wireless stations can connect to the router
- **11an mixed** Select if you are using both 802.11a and 802.11n wireless clients. It is strongly recommended that you set the Mode **11an mixed**, and all of 802.11a and 802.11n wireless stations can connect to the router.
- Channel This field determines which operating frequency will be used. The default channel is set to Auto, so the router will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Enable SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. If you select the Enable SSID Broadcast checkbox, the Wireless router will broadcast its name (SSID) on the air.
- Enable WDS Bridging Check this box to enable WDS. With this function, the router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown in Figure 4-31. Make sure the following settings are correct.

	Enable WDS Bridging	
SSID(to be bridged):		
MAC Address(to be bridged):		Example:00-1D-0F-11-22-33
	Survey	
Key type:	None	¥
WEP Index:	1	T
Auth type:	open	T
Password:		



- SSID (to be bridged) The SSID of the AP your router is going to connect to as a client.
 You can also use the search function to select the SSID to join.
- MAC Address (to be bridged) The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey** 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 router is going to connect needs password, you need to fill the password in this blank.

4.7.2 WPS

Choose menu "Wireless 5GHz \rightarrow WPS", you can the screen as shown in Figure 4-32. This section will guide you to add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

WPS (Wi-Fi Protected Setup)	
WPS Status:	Enabled Disable WPS
Current PIN:	44357207 Restore PIN Gen New PIN Disable Router's PIN
Add a new device:	Add device

Figure 4-32 WPS

- > WPS Status Enable or disable the WPS function here.
- Current PIN The current value of the router's PIN is displayed here. The default PIN of the router can be found in the label or User Guide.
- > Restore PIN Restore the PIN of the router to its default.
- Gen New PIN Click this button, and then you can get a new random value for the 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.

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

P 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/Reset button on the back panel of the router, as shown in Figure 4-33. You can also keep the default WPS status as Enabled and click the Add device button in Figure 4-32. Then choose "Press the button of the new device in two minutes" and click Connect, shown in Figure 4-34.



Figure 4-33

Add A New Device
Enter the new device's PIN.
PIN:
Press the button of the new device in two minutes.
Back Connect

Figure 4-34 Add A New Device

- **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 router.

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

Use this method if your client device does not have the WPS button, but 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 4-32, then Figure 4-35 will appear.

Add A New Device
PIN:
Press the button of the new device in two minutes.
Back Connect

Figure 4-35 Add A New Device

- 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 4-35, which means the client device has successfully connected to the router.
- III. Enter the router's PIN on your client device

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

- **Step 1:** On the client device, enter the PIN number listed on the router's Wi-Fi Protected Setup screen, shown in Figure 4-32 (It is also labeled on the bottom of the 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 router.

Note:

- 1) The WPS LED on the 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 router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.7.3 Wireless Security

Choose menu "Wireless 5GHz \rightarrow Wireless Security", you can configure the security settings of your wireless network.

There are five wireless security modes supported by the router: WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, and WEP.

Wireless Security		
Disable Security		
WPA/WPA2 - Personal(Re	commended)	
Version:	Automatic (Recommended)	Y
Encryption:	AES	Y
PSK Password:	443572073	
	(You can enter ASCII characte	rs between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period:	0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)
WPA/WPA2 - Enterprise		
Version:	Automatic 🔹	
Encryption:	Automatic 🔹	
Radius Server IP:		
Radius Port:	1812 (1-65535, 0 star	ids for default port 1812)
Radius Password:		
Group Key Update Period:	0 (in second	minimum is 30, 0 means no update)
○ WEP		
Type:	Automatic •	
WEP Key Format:	Hexadecimal 🔹	
Key Selected	WEP Key (Password)	Кеу Туре
Key 1: 💿		Disabled v
Key 2:		Disabled v
Key 3:		Disabled v
Key 4:		Disabled v
	Save	

Figure 4-36 Wireless Security

- Disable 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 It's the WPA/WPA2 authentication type based on pre-shared passphrase. The router is configured by this security type by default.
 - Version you can choose the version of the WPA-PSK security on the drop-down list. The default setting is Automatic, which can select WPA-PSK (Pre-shared key of WPA) or WPA2-PSK (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
 - Encryption When WPA-PSK or WPA is set as the Authentication Type, you can select either Automatic, or TKIP or AES as Encryption.

P Note:

If you check the **WPA/WPA2-Personal** radio button and choose **TKIP** encryption, you will find a notice in red as shown in Figure 4-37.

WPA/WPA2 - Personal(Recommended)				
Version:	Automatic(Recommended)			
Encryption:	TKIP			
PSK Password:	443572073			
	(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)			
Group Key Update Period:	0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)			
	We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.			

Figure 4-37 WPA/WPA2 – Personal

- **PSK Password** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the bottom of the router or can be found in Figure 4-32.
- **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.
 - Version you can choose the version of the WPA security on the drop-down list. The default setting is Automatic, 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 Automatic, or TKIP or AES.

P Note:

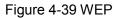
If you check the **WPA/WPA2-Enterprise** radio button and choose **TKIP** encryption, you will find a notice in red as shown in Figure 4-38.

WPA/WPA2 - Enterprise			
Version:	Automatic •		
Encryption:	TKIP		
Radius Server IP:			
Radius Port:	1812 (1-65535, 0 stands for default port 1812)		
Radius Password:			
Group Key Update Period:	0 (in second, minimum is 30, 0 means no update)		
	We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.		

Figure 4-38 WPA/WPA2 - Enterprise

- Radius Server IP Enter the IP address of the Radius server.
- Radius Port Enter the port number of the Radius server.
- Radius 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. If you check this radio button, you will find a notice in red as show in Figure 4-39.

Type:	Automatic 🔹	
WEP Key Format:	Hexadecimal 🔹	
Key Selected	WEP Key (Password)	Кеу Туре
Key 1: 💿		Disabled T
Key 2:		Disabled v
Key 3: 🔵		Disabled v
Key 4:		Disabled ▼



- Type you can choose the type for the WEP security on the drop-down list. The default setting is Automatic, which 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.

152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 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.

4.7.4 Wireless MAC Filtering

Choose menu "Wireless \rightarrow MAC Filtering", you can control the wireless access by configuring the Wireless MAC Filtering function, shown in Figure 4-40.

Wireless MAC Filtering					
Wireless MAC Filtering: Disabled Enable					
Filtering Rules	Filtering Rules				
Deny the stations specified by any enabled en	tries in the list to access				
Allow the stations specified by any enabled en	tries in the list to access				
ID MAC Address	Status	Description	Modify		
Add New Enable All Disable All Delete All					
Previous Next					

Figure 4-40 Wireless MAC Filtering

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 **"Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-41:

Add or Modify Wireless MAC Address Filtering entry			
MAC Address: Description: Status:	Enabled V		
	Save Back		

Figure 4-41 Add or Modify Wireless MAC Address Filtering entry

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

- 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: 00-0A-EB-B0-00-0B.
- 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 modify or delete an existing entry:

- 1. Click the **Modify** 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 All** button to make all entries enabled

Click the **Disable All** button to make all entries disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the router, but all the other wireless stations cannot access the 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 entries 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.
- 5. Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the MAC Address field.
- 6. Enter wireless station A/B in the **Description** field.
- 7. Select Enabled in the Status drop-down list.
- 8. Click the **Save** button.
- 9. 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.				
ID	MAC Address	Status	Description	Modify	
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete	
2	00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete	

4.7.5 Wireless Advanced

Choose menu "Wireless \rightarrow Wireless Advanced", you can configure the advanced settings of your wireless network.

Wireless Advanced			
Transmit Power:	High	•	
Beacon Interval :	100	(40-1000)	
RTS Threshold:	2346	(1-2346)	
Fragmentation Threshold:	2346	(256-2346)	
DTIM Interval:	1	(1-255)	
	C Enable WMM		
	Enable Short GI		
	Enable AP Isolation		
Save			

Figure 4-42 Wireless Advanced

- Transmit Power Here you can specify the transmit power of 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 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the 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 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 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 1-15 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- Enable WMM WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.

- Enable Short GI This function is recommended for it will increase the data capacity by reducing the guard interval time.
- Enabled AP Isolation This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

P 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.

4.7.6 Wireless Statistics

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

Wirel	Wireless Statistics					
	Current Connected Wireless Stations numbers: 1 Refresh					
ID	MAC Address	Current Status	Received Packets	Sent Packets		
1	C8-85-50-5D-02-40	STA-ASSOC	77	60		
		Previous	xt			
		11011040				

Figure 4-43 Wireless Statistics

- > 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.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

P Note:

This page will be refreshed automatically every 5 seconds.

4.8 Guest Network

Guest Network
- Wireless Settings

Figure 4-44 The Guest Network menu

There are one submenu under the Guest Network menu (shown in Figure 4-44): **Wireless Settings**. Click it, and you will be able to configure the corresponding functions.

4.8.1 Wireless Settings

Choose menu "Guest Network \rightarrow Wireless Settings", you can configure the Guest Network Wireless Settings on the page as shown in Figure 4-45.

Guest Network Wireless Settings			
Access And Bandwidth Control			
Allow Guest To Access My Local Network:			
Enable Guest Network Bandwidth Control:			
Egress Bandwidth For Guest Network:	256 Kbps (Range:1~1000000)		
Ingress Bandwidth For Guest Network:	1024 Kbps (Range:1~1000000)		
Wireless 2.4GHz			
Guest Network (2.4G):			
Network Name:	TP-LINK Guest A4B4 (Also called the SSID)		
Wireless Security:	 Disable Security ▼		
Access Time:	Schedule can not be connected.		
	Everyday Select Days		
	Mon Tue Wed Thu Fri Sat Sun		
	All day-24 Hours		
	Start Time: (HHMM)		
	End Time: (HHMM)		
Wireless 5GHz			
Guest Network (5G):			
Network Name:	TP-LINK_Guest_A4B3_5G (Also called the SSID)		
Wireless Security:	Disable Security		
Access Time:	Schedule can not be connected.		
	Everyday Select Days		
	Mon Tue Wed Thu Fri Sat Sun		
	All day-24 Hours		
	Start Time: (HHMM)		
	End Time: (HHMM)		

Figure 4-45 Guest Network Wireless Settings

- Allow Guest To Access My Local Network If enabled, guests can communicate with hosts.
- Enable Guest Network Bandwidth Control If enabled, the Guest Network Bandwidth Control rules will take effect.
- Egress Bandwidth For Guest Network The upload speed through the WAN port for Guest Network.
- Ingress Bandwidth For Guest Network The download speed through the WAN port for Guest Network.
- **Guest Network (2.4G/5G)** Enabled or disable the Guest Network function here.

- Network Name Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your Guest Network.
- > Wireless Security You can configure the security of Guest Network here.
- > Access Time During this time the wireless stations could accessing the AP.

P Note:

The range of bandwidth for Guest Network is calculated according to the setting of Bandwidth Control on the page "Bandwidth Control->Control Settings".

4.9 DHCP

DHCP
- DHCP Settings
- DHCP Clients List
- Address Reservation

Figure 4-46 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-46): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding functions.

4.9.1 DHCP Settings

Choose menu "**DHCP** \rightarrow **DHCP** Settings", you can configure the DHCP Server on the page as shown in Figure 4-47. The 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 router on the LAN.

DHCP Settings				
DHCP Server:	🔵 Disable 💿 Enable			
Start IP Address:	192.168.0.100			
End IP Address:	192.168.0.199			
Address Lease Time:	120 minutes (1~	2880 minutes, the default value is 120)		
Default Gateway:	192.168.0.1	(optional)		
Default Domain:		(optional)		
Primary DNS:	0.0.0.0	(optional)		
Secondary DNS:	0.0.0.0	(optional)		
		_		
	Save			

Figure 4-47 DHCP Settings

- DHCP Server Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- Start IP Address Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- End IP Address Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- Address Lease Time The Address Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- Default Gateway (Optional.) It is suggested to input the IP address of the Ethernet port of the router. The default value is 192.168.0.1.
- > Default Domain (Optional) Input the domain name of your network.
- > **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP or consult your ISP.
- Secondary DNS (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

P Note:

To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically".

4.9.2 DHCP Clients List

Choose menu "DHCP \rightarrow DHCP Clients List", you can view the information about the clients attached to the router in the screen as shown in Figure 4-48.

D	HCP Clients List			
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	WIN7-PC	D4-3D-7E-BF-61-5F	192.168.0.100	01:21:13
2	phone	C8-85-50-5D-02-40	192.168.0.101	01:55:38
Refresh				

Figure 4-48 DHCP Clients List

- > Client Name The name of the DHCP client
- > MAC Address The MAC address of the DHCP client
- > Assigned IP The IP address that the router has allocated to the DHCP client

Lease 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.

4.9.3 Address Reservation

Choose menu "**DHCP** \rightarrow **Address Reservation**", you can view and add a reserved address for clients via the next screen (shown in Figure 4-49). 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.

Addres	ss Reservation			
ID	MAC Address	Reserved IP Address	Status	Modify
Add Ne	w Enable All	Disable All Delete All		
		Previous Next		

Figure 4-49 Address Reservation

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

To Reserve an IP address:

- 1. Click the **Add New...** button. Then Figure 4-50 will pop up.
- 2. Enter the MAC address (in 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.

Add or Modify an Address Reservation Entry		
MAC Address: Reserved IP Address: Status:	Enabled T	
	Save Back	

Figure 4-50 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

- 1. Click the **Modify** 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 All button to make all entries enabled/disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

4.10 USB Settings

USB Settings
- 3G/4G
- Disk Settings
- Folder Sharing
- Print Server

Figure 4-51 The USB Settings menu

There are four submenus under the USB Settings menu (shown in Figure 4-51): **3G/4G**, **Disk Settings**, **Folder Sharing** and **Print Server**. Click any of them, and you will be able to configure the corresponding functions.

4.10.1 3G/4G

Choose menu "**USB Settings** \rightarrow **3G**/**4G**", you can configure parameters for 3G/4G function on the screen below. To use the 3G/4G function, you should first insert your USB modem on the USB port of the Router. There is already much 3G/4G USB modem information embedded in the Router. The USB modem parameters will be set automatically if the card is supported by the Router. If your USB modem inserted is supported by the Router, then "**Identify successfully**" will display in the 3G/4G USB Modem field as shown in the picture below.

3G/4G	
3G/4G USB Modem: Location: Mobile ISP: SIM/UIM PIN:	Identify successfully USA AT&T
Message:	PIN protection is enabled. Please input PIN code.
The current Internet Access is W	AN Preferred. The Connection Mode and Max Idle Time could not be set manually.
Connection Mode:	 Connect on Demand Connect Automatically Connect Manually Max Idle Time: 15 minutes (0 means remain active at all times)
Authentication Type:	Auto PAP CHAP Notice: The default is Auto, do not change unless necessary. Connect Disconnect Connecting
	Advanced Save Modem Settings

Figure 4-52 3G/4G

- > Location Please select the location where you're enjoying the 3G/4G card.
- Mobile ISP Please select the ISP (Internet Service Provider) you apply to for 3G/4G service.
 The Router will show the default Dial Number and APN of that ISP.
- SIM/UIM PIN If the PIN protection is enabled, please input the PIN code here. If you enter it wrong 3 times in a row, it will be locked.
- > Message Displays the PIN information of your SIM/UIM card.
- Connect on Demand You can configure the Router to disconnect your Internet connection after a specified period of the Internet connectivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
 - P Note:

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

- Connect Automatically Connect automatically after the Router is disconnected. To use this option, click the radio button.
- Connect Manually You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you

attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested.

Note:

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

- Authentication Type Some ISPs need a specific authentication type, please confirm it with your ISP or keep it Auto.
 - **Auto-**The Router will have dynamic negotiation with the dialing server and the Autnentication Type need not to be specified. The default type is Auto.
 - PAP-Password Authentication Protocol. This protocol allows the Router to establish authentication with the peer using two handshakes. Select this option if the ISP requires this authentication type.
 - **CHAP-**Challenge Handshake Authentication Protocol. This protocol allows the route to establish authentication with the peer using three handshakes and checking the peer identity periodically. Select this option if the ISP requires this authentication type.

Click the Advanced button to set up the advanced options in the screen as shown in Figure 4-53.

3G/4G Advanced Settings	3
Location:	USA
Mobile ISP:	AT&T
	Set the Dial Number, APN, Username and Password manually
Dial Number:	*99#
APN:	broadband
Username:	WAP@CINGULAR.COM (Optional)
Password:	······ (Optional)
MTU Size (in bytes):	1480 (The default is 1480, do not change unless necessary)
	Use The Following DNS Servers
Primary DNS:	202.96.128.166
Secondary DNS:	202.96.134.133 (Optional)
	Save Back

Figure 4-53 3G/4G Advanced Settings

Location / Mobile ISP – These two fields will display the location and the ISP you have selected in the previous page (shown in Figure 4-52). While you tick the below option Set the Dial Number, APN, Username and Password manually, there will be no specific information in these two fields.

- Set the Dial Number, APN, Username and Password manually Tick the checkbox and then you are able to fill in the Dial Number and APN blanks below, if your ISP is not listed in the Mobile ISP field in the previous page (Figure 4-52).
- > Dial Number Enter the Dial Number provided by your ISP.
- > APN Enter the APN (Access Point Name) provided by your ISP.
- > Username/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- MTU Size The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- Use the following DNS Servers If your ISP specify a DNS server IP address for you, click the checkbox, and fill the Primary DNS and Secondary DNS blanks below. The Secondary DNS is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.
- Primary DNS (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
- Secondary DNS (Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

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

Click the **Back** button to return the previous page.

Click the **Modem Settings** button (in Figure 4-52) if your 3G/4G USB Modem is not supported by the Router, and then you will see the screen as shown in Figure 4-54. Parameters of your USB modem can be configured on this page.

3G/4G USB Modem Settings			
ID	Vendor	Model	Delete
Add New	Delete All		
		Back	

Figure 4-54 3G/4G USB Modem Settings

There is already much 3G/4G USB modem information embedded in the Router. The USB modem parameters will be set automatically if the card is supported by the Router. But when the Router finds the card you just insert "unknown" to it, it will prompt you to set these parameters. The Router can identify your "unknown" card if the correct parameters are in the list. We suggest you to do the "3G/4G USB Modem Setting" only in such circumstance.

To add 3G/4G USB Modem entries, follow the steps below.

1. Download a most recent 3G/4G USB modem configuration file from our website (http://www.tp-link.com).

- 2. Click the Add New... button in Figure 4-54, and then you will see Figure 4-55.
- 3. Click **Browse...** to select the path name where you save the downloaded file on the computer into the File blank.
- 4. Click the **Upload** button to upload the configuration.

Upload 3G/4G USB Modem Configuration File		
File:	Choose File No file chosen	
Please Note: If you restore the router's factory setting, the bin file will be lost. In the event that you do lose the bin file, you will need to re-upload it, or download our latest firmware from <u>www.tp-link.com</u> . The updated firmware will be installed into your 3G/4G router and restore all of its functions.		
[Upload Back	

Figure 4-55 Add or Modify a 3G/4G USB Modem Entry

4.10.2 Disk Settings

Choose menu "**USB Settings**→**Disk Settings**", you can Click the **Scan** button to display the information of the USB storage device connected to the router. Click the **Safely Remove** button to remove the USB storage device safely from the router. Select the **Active** checkbox, and then the corresponding USB storage device is active.

Di	sk Settings			
	Scan			
sda_s	SanDisk:			Safely Remove
ID	Volume	Capacity	Free Space	Active
1	volume9	7.5 GB	4.0 GB	

Figure 4-56 Disk Settings

4.10.3 Folder Sharing

Choose menu "**USB Settings**→**Folder Sharing**". Focus on the Sharing Account section. Choose to use Login Account (admin) or use Following Account you set and click Save.

Folder Sharing					
Sharin	g Account				
Prepare the sharing acc		the sharing contents.	You can use the login user	r account or set a new u	iser account as the
Use Log	gin Account				
Use Fol	lowing Account				
	Username:	admin			
	Password:	•••••			
Conf	irm Password:	•••••			
		Save			
Sharin	g Setting				
Network/M	edia Server Name:	TP-LINK_0AA4	34		
Enable	Access Method		Link		Port
•	Network Neighbor	hood	\\192.168.0.1		
	FTP		ftp://192.168.0.1:21		21
	FTP (Remote)		ftp://219.134.215.42:21	Edit	21
	Sharing Mode:	Sharing All	Sharing Floders		
	Authentication:				
		Save			

Figure 4-57 Media Server Setting

Focus on the Sharing Setting section.

- Network/Media Server Name Name of the USB drive connected to the router. Network Connection is enabled by default.
- > Enable The Access Method is active if the Enable box is selected.
- > Access Method Available methods to access the storage device.
- **FTP** FTP client(s) accessing from the home network.
- **FTP (Remote)** FTP client(s) accessing from the Internet remotely.
- > Link Access the storage device by clicking on the link or entering it into a web browser.
- > Sharing Mode Select to share all or specific folders.
- Share All Share all active folders. Select the Require Login check box to require users to log in with a username and password.
- Share Selected Folders You may select which folders to share on the network.

4.10.4 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 4-58 Pint Server Setting

There are two 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 service 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.

4.11 NAT

Choose "**NAT**", and you can enable or disable the NAT and Hardware NAT Control feature. The NAT Rules and Hardware NAT will work properly only when the NAT Control feature is enabled.

NA	NAT Control Setting				
Note:	Make sure the NAT is enable if yo	u want the Hardware NAT configuration take effect			
	Current NAT Status:	💿 Enable 🔵 Disable			
	Current Hardware NAT Status:	Enable Disable			
		Save			

Figure 4-59 The Forwarding menu

- Enable NAT Control If enabled, the NAT function and the Forwarding configuration will take effect.
- Disable NAT Control If disabled, neither NAT function nor Forwarding configuration will take effect.
- > Enable Hardware NAT Control If enabled, the Hardware NAT feature will take effect.
- > **Disable Hardware NAT Control** If disabled, neither Hardware NAT feature will take effect.

4.12 Forwarding

Forwarding
- Virtual Servers
- Port Triggering
- DMZ
- UPnP

Figure 4-60 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-60): **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 4-61). 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. If you want the Virtual Servers configuration take effect, please make sure the NAT is enabled.

V	Virtual Servers					
Note	Note: Make sure the nat is enable if you want the Virtual Servers configuration take effect					
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
A	dd New	Enable All Disable Al	Delete All			
		Previous	Next			

Figure 4-61 Virtual Servers

- 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).
- Internal Port The Internal Service Port number of the PC running the service application. You can leave it blank if the Internal Port is the same as the Service Port, or enter a specific port number when Service Port is a single one.
- > **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 router).
- > **Status** The status of this entry, "Enabled" means the virtual server entry is enabled.
- > **Common Service Port** Some common services already exist in the drop-down list.
- > Modify To modify or delete an existing entry.

To setup a virtual server entry:

- 1. Click the **Add New...** button. (pop-up Figure 4-61)
- 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. Enter the IP address of the computer running the service application in the **IP Address** field.
- 4. Select the protocol used for this application in the **Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
- 5. Select the **Enabled** option in the **Status** drop-down list.
- 6. Click the **Save** button.

Add or Modify a Virtual Server Entry			
Service Port:	(XX-XX or XX)		
Internal Port:	(XX, Only valid for single Service Port or leave a blank)		
IP Address:			
Protocol:	ALL		
Status:	Enabled		
Common Service Port:	Select One		
	Save Back		

Figure 4-62 Add or Modify a Virtual Server Entry

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 **Modify** or **Delete** as desired on the **Modify** column.

Click the Enable/ Disable All button to make all entries enabled/ disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

Note:

If you set the service port of the virtual server as 80, you must set the Web management port on **Security** \rightarrow **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 4-63). 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 router.

Port Triggering						
Note: Make sure t	Note: Make sure the nat is enable if you want the Port Triggering configuration take effect					
ID Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify	
Add New	Enable All Dis	able All Delete A	All			
	Pre	vious Next				

Figure 4-63 Port Triggering

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 4-64.
- Select a common application from the Common Applications drop-down list, then the Trigger Port field and the Incoming Ports field will be automatically filled. If the Common Applications do not have the application you need, enter the Trigger Port and the Incoming 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 **Enabled** in **Status** field.
- 6. Click the **Save** button to save the new rule.

Add or Modify a Port Trigger	ing Entry
Trigger Port:	
Trigger Protocol:	ALL V
Incoming Ports:	
Incoming Protocol:	ALL V
Status:	Enabled v
Common Applications:	Select One
	Save Back

Figure 4-64 Add or Modify a Triggering Entry

- 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 router).
- Incoming 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.
- Incoming Protocol The protocol used for Incoming Port, either TCP, UDP, or ALL (all protocols supported by the router).
- **Status** The status of this entry, Enabled means the Port Triggering entry is enabled.
- Common Applications Some popular applications already listed in the drop-down list of Incoming Protocol.

To modify or delete an existing entry:

- 1. Find the desired entry in the table.
- 2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to make all entries enabled.

Click the **Disable All** button to make all entries disabled.

Click the Delete All button to delete all entries

Once the 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 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. Incoming Ports ranges cannot overlap each other.

4.12.3 DMZ

Choose menu "Forwarding \rightarrow DMZ", and then you can view and configure DMZ host in the screen (shown in Figure 4-65). 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 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	DMZ				
Note: Make sure the nat is enable if you	u want the DMZ configuration take effect				
Current DMZ Status: DMZ Host IP Address:	 Enable Disable 0.0.0 				
	Save				

Figure 4-65 DMZ

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

- 1. Click the **Enable** button.
- 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 4-66). 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.

UP	UPnP					
Note:	Note: Make sure the nat is enable if you want the UPnP configuration take effect					
Currer	it UPnP Status:			Enabled	Disabl	e
Cu	Current UPnP Settings List					
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
		Refresh				

Figure 4-66 UPnP Setting

- 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 router opened for the application.
 - **Protocol** The type of protocol which is opened.
 - Internal Port The port which the 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 Security

Security
- Basic Security
- Advanced Security
- Local Management
- Remote Management

Figure 4-67 The Security menu

There are four submenus under the Security menu as shown in Figure 4-67: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding functions.

4.13.1 Basic Security

Choose menu "Security \rightarrow Basic Security", and then you can configure the basic security in the screen as shown in Figure 4-68.

Basic Security				
Firewall				
	SPI Firewall:	Enable Disable		
VPN				
	PPTP Passthrough:	💿 Enable 💿 Disable		
	L2TP Passthrough:	Enable O Disable		
	IPSec Passthrough:	Enable Disable		
ALG				
	FTP ALG:	Enable Disable		
	TFTP ALG:	Enable Disable		
	H323 ALG:	Enable Disable		
	RTSP ALG:	💿 Enable 💿 Disable		
	SIP ALG:	Enable O Disable		
		Save		

Figure 4-68 Basic Security

- Firewall A firewall protects your network from the outside world. Here you can enable or disable the router's firewall.
 - SPI Firewall SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- VPN VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the 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 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 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 router, click **Enable**.
- 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, H323 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**.
 - H323 ALG To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.
 - **RTSP ALG** To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.
 - **SIP ALG** To allow some customers to share multimedia data through NAT, click Enable.

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

4.13.2 Advanced Security

Choose menu "Security \rightarrow Advanced Security", and then you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 4-69.

Advanced Security	
Packets Statistics Interval (5 ~ 60):	10 V Seconds
DoS Protection:	Disable Enable
Enable ICMP-FLOOD Attack Filtering	
ICMP-FLOOD Packets Threshold (5 ~ 3600):	50 Packets/s
Enable UDP-FLOOD Filtering	
UDP-FLOOD Packets Threshold (5 ~ 3600):	500 Packets/s
Enable TCP-SYN-FLOOD Attack Filtering	
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600):	50 Packets/s
Ignore Ping Packet From WAN Port	
Forbid Ping Packet From LAN Port	
Save Blocked DoS Host List	

Figure 4-69 Advanced Security

- Packets Statistics Interval (5~60) The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- DoS Protection Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

Note:

Dos Protection will take effect only when the **Traffic Statistics** in "System Tool \rightarrow Statistics" is enabled.

- Enable ICMP-FLOOD Attack Filtering Enable or Disable the ICMP-FLOOD Attack Filtering.
- ICMP-FLOOD Packets Threshold (5~3600) The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the router will startup the blocking function immediately.
- > Enable UDP-FLOOD Filtering Enable or Disable the UDP-FLOOD Filtering.

- UDP-FLOOD Packets Threshold (5~3600) The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the router will startup the blocking function immediately.
- Enable TCP-SYN-FLOOD Attack Filtering Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- TCP-SYN-FLOOD Packets Threshold (5~3600) The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the router will startup the blocking function immediately.
- Ignore Ping Packet From WAN Port Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the router.
- Forbid Ping Packet From LAN Port Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.

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

Click the **Blocked DoS Host List** button to display the DoS host table by blocking.

4.13.3 Local Management

Choose menu "Security \rightarrow Local Management", and then you can configure the management rule in the screen as shown in Figure 4-70. The management feature allows you to deny computers in LAN from accessing the router.

Local Management	
Management Rules	
All the PCs on the LAN are allo	owed to access the Router's Web-Based Utility
Only the PCs listed can brows	e the built-in web pages to perform Administrator tasks
MAC 1:	
MAC 2:	
MAC 3:	
MAC 4:	
Your PC's MAC Address:	D4-3D-7E-BF-61-5F Add
	Save

Figure 4-70 Local Management

By default, the radio button "All the PCs on the LAN are allowed to access the router's Web-Based Utility" is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the router's Web-Based Utility locally from inside the network, check the radio button "Only the PCs listed can browse the built-in web pages to perform Administrator tasks", and then enter each MAC Address in a separate field. The format for the MAC Address is

XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

After click the **Add** button, your PC's MAC Address will be placed in the list above.

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

Note:

If your PC is blocked but you want to access the router again, use a pin to press and hold the **WPS/Reset** button (hole) on the back panel for about 5 seconds to reset the router's factory defaults on the router's Web-Based Utility.

4.13.4 Remote Management

Choose menu "Security \rightarrow Remote Management", and then you can configure the Remote Management function in the screen as shown in Figure 4-71. This feature allows you to manage your router from a remote location via the Internet.

Remote Management		
Web Management Port: Remote Management IP Address:	80	(Enter 255.255.255.255 for all)
	Save	

Figure 4-71 Remote Management

- Web Management Port Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.
- Remote Management IP Address This is the current address you will use when accessing your router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the router from internet.

Note:

 To access the router, you should type your router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web-based utility. 2. Be sure to change the router's default password to a very secure password.

4.14 Parental Control

Choose menu "**Parental Control**", and then you can configure the parental control in the screen as shown in Figure 4-72. 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.

Parental Control Settings				
Non-Parental PCs not listed will not be able	e to access the Internet.			
Parental Control:	Disable Enable			
MAC Address of Parental PC1:				
MAC Address of Parental PC2:				
MAC Address of Parental PC3:				
MAC Address of Parental PC4:				
MAC Address of Your PC:	D4-3D-7E-BF-61-5F	Copy To Above		
	Save			
ID MAC address Website D	escription	Schedul	e Enable	Modify
Add New Enable All Di	sable All Delete All]		
		-		
	Previous Ne	xt Current No	. 1 🔻 Page	

Figure 4-72 Parental Control Settings

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

1. Click the Add New... button and the next screen will pop-up as shown in Figure 4-73.

Add or Modify Parental Control Entry		
The Schedule is based on the time of the Ro	outer. The time can be set in "System Tools -> <u>Time settings</u> ".	
MAC Address of Child PC:		
All MAC Address In Current LAN:	please select	
Website Description:		
Allowed Domain Name:		
Effective Time:		
Effective Time:	Anytime	
	The time schedule can be set in "Access Control -> <u>Schedule</u> "	
Status:	Enabled •	
	Save Back	

Figure 4-73 Add or Modify Parental Control Entry

- **Parental Control** Check **Enable** if you want this function to take effect; otherwise, check **Disable**.
- 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 Your PC This field displays the MAC address of the PC that is managing this 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.
- Website Description Description of the allowed website for the PC controlled.
- Schedule The time period allowed for the PC controlled to access the Internet. For detailed information, please go to "Access Control → Schedule".
- Enable Check this option to enable a specific entry.
- Modify Here you can edit or delete an existing entry.
- Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the MAC Address of Child PC field, or you can choose the MAC address from the All Address in Current LAN drop-down list.
- 3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the **Website Description** field.
- Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the Allowed Domain Name field. Any domain name with keywords in it (www.tp-link.com) will be allowed.
- 5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want. If there are not suitable schedules for you, click the **Schedule** in red below to go to the Advance Schedule Settings page and create the schedule you need.
- 6. In the Status field, you can select **Enabled** or **Disabled** to enable or disable your entry.
- 7. Click the **Save** button.

Click the Enable All button to enable all the rules in the list.

Click the **Disable All** button to disable all the rules in the list.

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

Click the **Next** button to go to the next page, or click the **Previous** button to return to the previous page.

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.tp-link.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below.

- Click "Parental Control" menu on the left to enter the Parental Control Settings page. Check Enable and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.
- Click "Access Control Schedule" on the left to enter the Schedule Settings page. Click Add New... button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.
- 3. Click "**Parental Control**" menu on the left to go back to the Add or Modify Parental Control Entry page:
 - 1) Click **Add New...** button.
 - 2) Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
 - 3) Enter "Allow Google" in the Website Description field.
 - 4) Enter "www.google.com" in the **Allowed Domain Name** field.
 - 5) Select "Schedule_1" you create just now from the **Effective Time** drop-down list.
 - 6) In **Status** field, select Enable.
- 4. Click **Save** to complete the settings.

Then you will go back to the **Parental Control Settings** page and see the following list, as shown in Figure 4-74.

ID	MAC address	Webs	site Description		Schedule	Enable	Modify
1	D4-3D-7E-BF-61-5F	allow	tp-link		Permanent		Edit Delete
	Add New En	able All	Disable All	Delete All			

Figure 4-74 Parental Control Settings

4.15 Access Control

Access Control
- Rule
- Host
- Target
- Schedule

Figure 4-75 Access Control

There are four submenus under the Access Control menu as shown in Figure 4-75: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.15.1 Rule

Choose menu "Access Control \rightarrow Rule", and then you can view and set Access Control rules in the screen as shown in Figure 4-76.

Internet Access Control Rule Management				
Enable Internet Access Control				
Default Filter Policy				
Allow the packets specified by any enal	bled access control policy	/ to pass through the Rou	uter	
Deny the packets specified by any enal	oled access control policy	to pass through the Rou	uter	
	Save			
ID Rule Name Host	Target	Schedule	Enable	Modify
Setup Wizard				
Add New Enable All Dis	sable All Delete	All		
		To ID		
Move		To ID		
	Previous	Next Current	No. 1 🔻 Page	

Figure 4-76 Access Control Rule Management

- Enable Internet Access Control Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- > Rule Name Here displays the name of the rule and this name is unique.
- > 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.
- Enable Here displays the status of the rule, enabled or not. Check this option to enable a specific entry.
- > Modify Here you can edit or delete an existing rule.
- > Setup Wizard Click the Setup Wizard button to create a new rule entry.
- > Add New... Click the Add New... button to add a new rule entry.
- > Enable All Click the Enable All button to enable all the rules in the list.
- > Disable All Click the Disable All button to disable all the rules in the list.
- > Delete All Click the Delete All button to delete all the entries in the table.
- Move You can change the entry's order as desired. Enter in the first box the ID number of the entry you want to move and in the second box another ID number, and then click the Move button to change the entries' order.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

There are two methods to add a new rule.

Method One:

1. Click Setup Wizard button and the next screen will appear as shown in Figure 4-77.

Quick Setup - Create a Host	Entry
Mode: Host Description: LAN IP Address:	IP Address
	Back Next

Figure 4-77 Quick Setup – Create a Host Entry

- **Host Description** In this field, create a unique description for the host (e.g. Host_1).
- Mode Here are two options, IP Address and MAC Address. You can select either of them from the drop-down list.

If the IP Address is selected, you can see the following item:

LAN IP Address - Enter the IP address or address range of the host in dotted-decimal format (e.g. 192.168.0.23).

If the MAC Address is selected, you can see the following item:

- MAC Address Enter the MAC address of the host in XX-XX-XX-XX-XX format (e.g. 00-11-22-33-44-AA).
- Click Next when finishing creating the host entry, and the next screen will appear as shown in Figure 4-78.

Quick Setup - Create an Acc	ess Target Entry
Mode: Target Description: IP Address: Target Port: Protocol:	IP Address
Common Service Port:	please select ▼
	Back Next

Figure 4-78 Quick Setup – Create an Access Target Entry

- Target Description In this field, create a description for the target. Note that this description should be unique (e.g. Target_1).
- Mode Here are two options, IP Address and Domain Name. You can choose either of them from the drop-down list.

If the IP Address is selected, you will see the following items:

- IP Address Enter the IP address (or address range) of the target (targets) in dotted-decimal format (e.g. 192.168.0.23).
- Target Port Specify the port or port range for the target. For some common service ports, you can make use of the Common Service Port item below.
- Protocol Here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
- Common Service Port Here lists some common service ports. Select one from the drop-down list and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.

If the Domain Name is selected, you will see the following items:

- Domain Name Here you can enter 4 domain names, either the full name or the keywords (for example, tp-link). Any domain name with keywords in it (www.tp-link.com) will be blocked or allowed.
- 3. Click **Next** when finishing creating the access target entry, and the next screen will appear as shown in Figure 4-79.

Quick Setup - Create an Advanced Schedule Entry		
Note: The Schedule is based on the time of	f the Router.	
Schedule Description:		
Day:	💿 Everyday 💿 Select Days	
	🕜 Mon 🥑 Tue 🥥 Wed 🕜 Thu 🕜 Fri 🕜 Sat 🖉 Sun	
Time:	all day-24 hours: 🖉	
Start Time:	(HHMM)	
Stop Time:	(HHMM)	
	Back Next	

Figure 4-79 Quick Setup – Create an Advanced Schedule Entry

- Schedule Description In this field, create a description for the schedule. Note that this description should be unique (e.g. Schedule_1).
- **Day** Choose Select Days and select the certain day (days), or choose Everyday.

- > Time Select "24 hours", or specify the Start Time and Stop Time yourself.
- Start Time Enter the start time in HHMM format (HHMM are 4 numbers). For example 0800 is 8:00.
- Stop Time Enter the stop time in HHMM format (HHMM are 4 numbers). For example 2000 is 20:00.
- 4. Click **Next** when finishing creating the advanced schedule entry, and the next screen will appear as shown in Figure 4-80.

Quick Setup - Create an Inter	met Access Control Entry
Rule Name:	
Host:	00-11-22-33-44-AA 🔻
Target:	Target_1 ▼
Schedule:	Schedule_1 •
Status:	Enabled •
	Back Finish

Figure 4-80 Quick Setup - Create an Internet Access Control Entry

- Rule In this field, create a name for the rule. Note that this name should be unique (e.g. Rule_1).
- Host In this field, select a host from the drop-down list for the rule. The default value is the Host Description you set just now.
- Target In this filed, select a target from the drop-down list for the rule. The default value is the Target Description you set just now.
- Schedule In this field, select a schedule from the drop-down list for the rule. The default value is the Schedule Description you set just now.
- Status In this field, there are two options, Enabled or Disabled. Select Enabled so that the rule will take effect. Select Disabled so that the rule won't take effect.
- 5. Click **Finish** to complete adding a new rule.

Method Two:

- 1. Click the **Add New...** button and the next screen will pop up as shown in Figure 4-81.
- 2. Give a name (e.g. Rule_1) for the rule in the **Rule Name** field.
- 3. Select a host from the Host drop-down list or choose "Click Here To Add New Host List".
- 4. Select a target from the **Target** drop-sown list or choose "**Click Here To Add New Target List**".

- 5. Select a schedule from the **Schedule** drop-down list or choose "**Click Here To Add New Schedule**".
- 6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
- 7. Click the **Save** button.

Add Internet Access Control	Entry
Rule Name: Host: Target: Schedule: Status:	00-11-22-33-44-AA Click Here To Add New Host List. Any Target Click Here To Add New Target List. Anytime Click Here To Add New Schedule. Enabled
	Save Back

Figure 4-81 Add Internet Access Control Entry

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

- Click the submenu Rule of Access Control in the left to return to the Rule List page. Select Enable Internet Access Control and choose "Allow the packets specified by any enabled access control policy to pass through the router".
- 2. We recommend that you click **Setup Wizard** button to finish all the following settings.
- 3. Click the submenu **Host of Access Control** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
- 4. Click the submenu **Target of Access Control** in the left to enter the Target List page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
- Click the submenu Schedule of Access Control in the left to enter the Schedule List page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
- 6. Click the submenu **Rule of Access Control** in the left, Click **Add New...** button to add a new rule as follows:
 - 1) In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
 - 2) In Host field, select Host_1.
 - 3) In Target field, select Target_1.
 - 4) In Schedule field, select Schedule_1.

- 5) In Status field, select **Enabled**.
- 6) Click **Save** to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

ID	Rule Name	Host	Target	Schedule	Enable	Modify
1	rule_1	00-11-22-33-44-AA	Target 1	Schedule 1		Edit Delete

4.15.2 Host

Choose menu "Access Control \rightarrow Host", and then you can view and set a Host list in the screen as shown in Figure 4-82. The host list is necessary for the Access Control Rule.

Ho	st Settings		
ID 1 Ad	Host Description 00-11-22-33-44-AA d New Delete All	Information IP: 192.168.0.23	Modify Edit Delete
		Previous	Current No. 1 ▼ Page

Figure 4-82 Host Settings

- > Host Description Here displays the description of the host and this description is unique.
- > Information Here displays the information about the host. It can be IP or MAC.
- > **Modify -** To modify or delete 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.
 - 1) If you select IP Address, the screen shown is Figure 4-83.
 - In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - In LAN IP Address field, enter the IP address.
 - 2) If you select MAC Address, the screen shown is Figure 4-84.
 - In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - In MAC Address field, enter the MAC address.
- 3. Click the **Save** button to complete the settings.

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

Click the **Next** button to go to the next page, or click the **Previous** button to return to the previous page.

Add or Modify a Host Entry	
Mode: Host Description: LAN IP Address:	IP Address • 00-11-22-33-44-AA 192.168.0.23
	Save Back

Figure 4-83 Add or Modify a Host Entry

Add or Modify a Host Entry	
Mode: Host Description:	MAC Address host_1
MAC Address:	00-11-22-33-44-AA
	Save Back

Figure 4-84 Add or Modify a Host Entry

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

- 1. Click **Add New...** button in Figure 4-82 to enter the Add or Modify a Host Entry page.
- 2. In Mode field, select MAC Address from the drop-down list.
- 3. In **Host Description** field, create a **unique** description for the host (e.g. Host_1).
- 4. In **MAC Address** field, enter 00-11-22-33-44-AA.
- 5. Click **Save** to complete the settings.

Then you will go back to the Host Settings page and see the following list.

ID	Host Description	Information	Modify
1	00-11-22-33-44-AA	IP: 192.168.0.23	Edit Delete

4.15.3 Target

Choose menu "Access Control \rightarrow Target", and then you can view and set a Target list in the screen as shown in Figure 4-85. The target list is necessary for the Access Control Rule.

T	arget Settings		
ID 1 A	Target Description Target_1 dd New Delete All	Information 192.168.0.23/21/TCP	Modify Edit Delete
		Previous Next Current No. 1	

Figure 4-85 Target Settings

- Target Description Here displays the description about the target and this description is unique.
- > Information The target can be IP address, port, or domain name.
- > **Modify -** To modify or delete 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** or **Domain Name**.
- 3. If you select **IP Address**, the screen shown is Figure 4-86.

Add or Modify an Access Target Entry		
Mode: Target Description: IP Address: Target Port: Protocol:	IP Address	
Common Service Port:	please select ▼	
	Save Back	

Figure 4-86 Add or Modify an Access Target Entry

- 1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
- 2) In **IP Address** field, enter the IP address of the target.
- 3) Select a common service from Common Service Port drop-down list, so that the Target Port will be automatically filled. If the Common Service Port drop-down list doesn't have the service you want, specify the Target Port manually.
- 4) In **Protocol** field, select TCP, UDP, ICMP or ALL from the drop-down list.
- 4. If you select **Domain Name**, the screen shown is Figure 4-87.

Archer C7 AC1750 Wireless Dual Band Gigabit Router

Add or Modify an Access Target Entry		
Mode: Target Description: Domain Name:	Domain Name	
	Save Back	

Figure 4-87 Add or Modify an Access Target Entry

- 1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
- 2) In Domain Name field, enter the domain name, either the full name or the keywords (for example, tp-link) in the blank. Any domain name with keywords in it (<u>www.tp-link.com</u>) will be blocked or allowed. You can enter 4 domain names.
- 5. Click the **Save** button.

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

Click the **Next** button to go to the next page, or click the **Previous** button to return to the previous page.

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access <u>www.tp-link.com</u> only, you should first follow the settings below:

- 1. Click **Add New...** button in Figure 4-85 to enter the Add or Modify an Access Target Entry page.
- 2. In Mode field, select Domain Name from the drop-down list.
- 3. In **Target Description** field, create a unique description for the target (e.g. Target_1).
- 4. In **Domain Name** field, enter www.tp-link.com.
- 5. Click **Save** to complete the settings.

Then you will go back to the Target Settings page and see the following list.

ID	Target Description	Information	Modify
1	Target_1	192.168.0.23/21/TCP	Edit Delete
2	tp-link	www.tp-link.com	Edit Delete

4.15.4 Schedule

Choose menu "Access Control \rightarrow Schedule", and then you can view and set a Schedule list in the next screen as shown in Figure 4-88. The Schedule list is necessary for the Access Control Rule.

Sc	Schedule Settings			
ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Every Day	00:00 - 24:00	Edit Delete
Ad	Id New Delete All			
		Prevoius Nex	Current No. 1 V Page	

Figure 4-88 Schedule Settings

- Schedule Description Here displays the description of the schedule and this description is unique.
- > **Day** Here displays the day(s) in a week.
- > **Time** Here displays the time period in a day.
- > Modify Here you can edit or delete an existing schedule.

To add a new schedule, follow the steps below:

- 1. Click **Add New...** button shown in Figure 4-88 and the next screen will pop-up as shown in Figure 4-89.
- 2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
- 3. In **Day** 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 **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page, or click the **Previous** button to return to the previous page.

Add or Modify Schedule Entry		
Note: The Schedule is based on the time o	f the Router.	
Schedule Description:		
Day:	everyday Select Days	
	🖉 Mon 🖉 Tue 🥑 Wed 🥑 Thu 🥑 Fri 🥑 Sat 🥥 Sun	
Time:	all day-24 hours: 🕜	
Start Time:	(HHMM)	
Stop Time:	(HHMM)	
	Save Back	

Figure 4-89 Advanced Schedule Settings

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access <u>www.google.com</u> only from **18:00 to 20:00** on **Saturday** and **Sunday**, you should first follow the settings below:

- 1. Click **Add New...** button shown in Figure 4-88 to enter the Advanced Schedule Settings page.
- 2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
- 3. In **Day** field, check the Select Days radio button and then select Sat and Sun.
- 4. In **Time** field, enter 1800 in Start Time field and 2000 in Stop Time field.
- 5. Click **Save** to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Every Day	00:00 - 24:00	Edit Delete

4.16 Advanced Routing



Figure 4-90 Advanced Routing

There are two submenus under the Advanced Routing menu as shown in Figure 4-90: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

4.16.1 Static Routing List

Choose menu "Advanced Routing \rightarrow Static Routing List", and then you can configure the static route in the next screen (shown in Figure 4-91). A static route is a pre-determined path that network information must travel to reach a specific host or network.

Static	Routing				
-					
ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify
Add N	ew Enable All	Disable All Delete All			
		Previous Next			

Figure 4-91 Static Routing

To add static routing entries:

1. Click Add New... shown in Figure 4-91, you will see the following screen.

Add or Modify a Static Route	Entry			
Destination Network:				
Subnet Mask:				
Default Gateway:				
Status:	Enabled	•		
	Save		Back	

Figure 4-92 Add or Modify a Static Route Entry

- 2. Enter the following data:
 - Destination Network The Destination Network 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.
 - Default Gateway This is the IP Address of the gateway device that allows for contact between the router and the network or host.
- 3. Select Enabled or Disabled for this entry on the Status drop-down list.
- 4. Click the **Save** button to make the entry take effect.

Other configurations for the entries:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.16.2 System Routing Table

Choose menu "Advanced Routing System Routing Table", and then you can view the System Routing Table in the next screen (shown in Figure 4-93). System routing table views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

S	ystem Routing Table			
ID	Destination Network	Subnet Mask	Gateway	Interface
1	219.134.212.1	255.255.255.255	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	239.0.0.0	255.0.0.0	0.0.0.0	LAN & WLAN
4	0.0.0.0	0.0.0.0	219.134.212.1	WAN
		Refresh		

Figure 4-93 System Routing Table

- Destination Network The Destination Network is the address of the network or host to which the static route is assigned.
- Subnet Mask The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway This is the IP address of the gateway device that allows for contact between the router and the network or host.
- Interface This interface tells you either the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), or on the WAN (Internet).

4.17 Bandwidth Control

Bandwidth Control	
- Control Settings	
- Rules List	

Figure 4-94 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 4-94: **Control Settings** and **Rules List**. 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 Control Settings

Choose menu "**Bandwidth Control** \rightarrow **Control Settings**", and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

Bandwidth Control Settings		
Enable Bandwidth Control:		
Line Type:	ADSL Other	
Egress Bandwidth:	512	Kbps
Ingress Bandwidth:	2048	Kbps
	Save	

Figure 4-95 Bandwidth Control Settings

- Enable Bandwidth Control Check this box so that the Bandwidth Control settings can take effect.
- Line Type Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- > Egress Bandwidth The upload speed through the Internet port.
- > Ingress Bandwidth The download speed through the Internet port.

4.17.2 Rules List

Choose menu "**Bandwidth Control** \rightarrow **Rules List**", and then you can view and configure the Bandwidth Control rules in the screen below.

l	Bandwidth Control Rules	List					
	Description	Egress Bar	ndwidth(Kbps)	Ingress Ba	ndwidth(Kbps)	Enable	Modify
ID	Description	Min	Мах	Min	Max	Enable	Moully
			The current list is	empty.			
1	Add New Delete All						
	Previous Next	Now is the 1 🔻	page				

Figure 4-96 Bandwidth Control Rules List

- > **Description -** This is the information about the rules such as address range.
- Egress bandwidth This field displays the max and mix upload bandwidth through the Internet port, the default is 0.

- Ingress bandwidth This field displays the max and mix download bandwidth through the Internet port, the default is 0.
- > Enable This displays the status of the rule.
- > Modify Click Modify to edit the rule. Click Delete to delete the rule.

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

- 1. Click **Add New...** shown in Figure 4-96, you will see a new screen shown in Figure 4-97.
- 2. Enter the information like the screen shown below.

Bandwidth Control Rule Sett	ings	
Enable:		
IP Range:	-	
Port Range:	· · · · · · · · · · · · · · · · · · ·	
Protocol:	ALL 🔻	
	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
Egress Bandwidth:	0	0
Ingress Bandwidth:	0	0
	Save Back	

Figure 4-97 Bandwidth Control Rule Settings

3. Click the **Save** button.

4.18 IP & MAC Binding

IP & MAC Binding	
- Binding Settings	
- ARP List	

Figure 4-98 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 4-98): **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 4-99).

	ARP Binding:	Disable Enable	Save	
MAC Address IP Address Bind Modif	IAC Address	IP Address	Bind	Modify
00-E0-4C-00-07-BE 192.168.0.4 🗹 Modify	0-E0-4C-00-07-BE	192.168.0.4		Modify Delete

Figure 4-99 Binding Setting

- > **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.
- **Bind** Check this option to enable ARP binding for a specific device.
- > **Modify -** 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 **Modify** 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 4-100).

IP & MAC Binding Settings	
Bind:	
MAC Address:	
IP Address:	
	Save Back

Figure 4-100 IP & MAC Binding Setting (Add & Modify)

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

- 1. Click the **Add New...** button as shown in Figure 4-99.
- 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 **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry, follow the steps below.

- 1. Click the **Find** button as shown in Figure 4-99.
- 2. Enter the MAC Address or IP Address.

3. Click the **Find** button in the page as shown in Figure 4-101.

Find IP & MAC Binding Entry				
MAC Address:				
IP Address:				
ID	MAC Address	IP Address	Bind	Link
	Now the	e current list is empty		
	Find	Back		

Figure 4-101 Find IP & MAC Binding Entry

Click the Enable All button to make all entries enabled.

Click the **Delete All** button to delete all 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 4-102).

ARP	List			
D	MAC Address	IP Address	Status	Configure
1	D4-3D-7E-BF-61-5F	192.168.0.100	Unbound	Load Delete
2	C8-85-50-5D-02-40	192.168.0.101	Unbound	Load Delete
		Bind All	Load All	Refresh

Figure 4-102 ARP List

- 1. MAC Address The MAC address of the controlled computer in the LAN.
- 2. IP Address The assigned IP address of the controlled computer in the LAN.
- 3. Status Indicates whether or not the MAC and IP addresses are bound.
- 4. **Configure -** Load or delete an item.
 - **Load -** Load the item to the IP & MAC Binding list.
 - **Delete -** Delete the item.

Click the **Bind All** button to bind all the current items, available after enable.

Click the Load All button to load all items to the IP & MAC Binding list.

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

Note:

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

4.19 Dynamic DNS

Choose menu "Dynamic DNS", and you can configure the Dynamic DNS function.

The 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 <u>www.comexe.cn</u>, <u>www.dyndns.org</u>, or <u>www.no-ip.com</u>. The Dynamic DNS client service provider will give you a password or key.

4.19.1 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is <u>www.comexe.cn</u>, the page will appear as shown in Figure 4-103.

DDNS	
Service Provider:	Comexe (www.comexe.cn)
Domain Name:	
User Name:	username
Password:	
Connection Status:	 Enable DDNS DDNS not launching! Logout
	Save

Figure 4-103 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** your dynamic DNS service provider gave.

- 2. Enter the **User Name** for your DDNS account.
- 3. Enter the **Password** for your DDNS account.
- 4. Click the **Login** button to login the DDNS service.

Connection Status -The status of the DDNS service connection is displayed here.

Click Logout to log out of the DDNS service.

P Note:

If you want to login again with another account after a successful login, please click the **Logout** button, then input your new username and password and click the **Login** button.

4.19.2 Dyndns.org DDNS

If the dynamic DNS **Service Provider** you select is <u>www.dyndns.org</u>, the page will appear as shown in Figure 4-104.

DDNS	
Service Provider:	Dyndns (www.dyndns.com) V Go to register
User Name:	username
Password:	•••••
Domain Name:	
	Enable DDNS
Connection Status:	DDNS not launching!
	Login Logout
	Save

Figure 4-104 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

- 1. Enter the User Name for your DDNS account.
- 2. Enter the **Password** for your DDNS account.
- 3. Enter the **Domain Name** you received from dynamic DNS service provider.
- 4. Click the **Login** button to login to the DDNS service.

Connection Status - The status of the DDNS service connection is displayed here.

Click Logout to logout of the DDNS service.

Note:

If you want to login again with another account after a successful login, please click the **Logout** button, then input your new username and password and click the **Login** button.

4.19.3 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is <u>www.no-ip.com</u>, the page will appear as shown in Figure 4-105.

DDNS	
Service Provider:	No-IP (www.no-ip.com) Go to register
User Name:	username
Password:	•••••
Domain Name:	
Connection Status:	 Enable DDNS DDNS not launching! Login Logout
	Save

Figure 4-105 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

- 1. Enter the **User Name** for your DDNS account.
- 2. Enter the **Password** for your DDNS account.
- 3. Enter the **Domain Name** you received from dynamic DNS service provider.
- 4. Click the **Login** button to login to the DDNS service.

Connection Status - The status of the DDNS service connection is displayed here.

Click **Logout** to log out the DDNS service.

P Note:

If you want to login again with another account after a successful login, please click the **Logout** button, then input your new username and password and click the **Login** button.

4.20 IPv6 Support

IPv6 Support	
- IPv6 Status	
- IPv6 Setup	

Figure 4-106 IPv6 Support

There are two submenus under the IPv6 Support menu (shown in Figure 4-106): **IPv6 Status** and **IPv6 Setup**. Click either of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.20.1 IPv6 Status

IPv6 Status	
WAN	
Connection Type:	DHCPv6
IPv6 Address:	:
IPv6 Default Gateway:	:
Primary IPv6 DNS:	:
Secondary IPv6 DNS:	
LAN	
IPv6 Address Assign Type:	SLAAC
IPv6 Address:	:
Link-local Address:	fe80::c24a:ff:fe0a:a4b4/64

Figure 4-107 IPv6 Status

The **IPv6 Status** page displays the router's current IPv6 status and configuration. All information is read-only.

- > WAN
 - Connection Type The IPv6 connection way for WAN
 - IPv6 Address The WAN IPv6 address
 - IPv6 Default Gateway The router's default gateway
 - **Primary IPv6 DNS** The primary IPv6 DNS address
 - Secondary IPv6 DNS The secondary IPv6 DNS address

> LAN

 IPv6 Address Assign Type - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

SLAAC

IPv6 Address Prefix -The Prefix of IPv6 Address

DHCPv6 Server

Release Time - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.

IPv6 Address - Displays the LAN IPv6 Address.

4.20.2 IPv6 Setup

WAN Setup	
Enable IPv6:	
WAN Connection Type:	DHCPv6
۲	Get non-temporary IPv6 address.
0	Get IPv6 prefix delegation.
IPv6 Address:	3ffe::7702:f8f:adb1:8048
	Renew Release
O	Get IPv6 DNS Server Automatically
Primary IPv6 DNS:	2000::ff
Secondary IPv6 DNS:	2000::fe
0	Use the following IPv6 DNS Servers
LAN Setup	
IPv6 Address Assign Type:	SLAAC 🗸
IPv6 Address Prefix:	2001:db8:ffff:1:: /64
LAN IPv6 Address:	2001:db8:ffff.1:12f1:a2ff.fe7c:d39b/64
	Save

Figure 4-108 Enable/Disable IPv6

- Enable IPv6 Tick the checkbox to enable the IPv6 function. It's enabled by default.
- WAN Connection Type Choose the correct WAN connection type based on your ISP network topology.
 - DHCPv6 Connections which use dynamic IPv6 address assignment.
 - Static IPv6 Connections which use static IPv6 address assignment.
 - **PPPoEv6** Connections which use PPPoEV6 that requires a user name and password.

• **Tunnel 6to4** - Connections which use 6to4 address assignment.

Different types of WAN connection require you to do different settings. Below are the detailed explanations for the respective type.

1) DHCPv6

WAN Setup	
Enable IPv6:	N
WAN Connection Type:	DHCPv6
o	Get non-temporary IPv6 address.
0	Get IPv6 prefix delegation.
IPv6 Address:	3ffe::7702:f8f:adb1:8048
	Renew Release
۲	Get IPv6 DNS Server Automatically
Primary IPv6 DNS:	2000::ff
Secondary IPv6 DNS:	2000::fe
0	Use the following IPv6 DNS Servers
LAN Setup	
IPv6 Address Assign Type:	SLAAC 🗸
IPv6 Address Prefix:	2001:db8:ffff:1:: /64
LAN IPv6 Address:	2001:db8:ffff:1:12f1:a2ff:fe7c:d39b/64
	Save

Figure 4-109 DHCPv6

- **Get non-temporary IPv6 address** Get a non-temporary IPv6 address from the ISP.
- Get IPv6 prefix delegation Get a temporary IPv6 address and IPv6 prefix from the ISP, the temporary IPv6 address is set to the WAN port, and the LAN port advertise IPv6 address by RADVD or DHCPs.
- > IPv6 Address The IPv6 address assigned by your ISP dynamically.

Click the Renew button to renew the IPv6 parameters from your ISP.

Click the Release button to release the IPv6 parameters from your ISP.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- > Primary IPv6 DNS Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- Secondary IPv6 DNS Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.

P Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- Get IPv6 with Unicast DHCP A few ISPs' DHCP servers do not support the broadcast applications. If you can't get the IPv6 Address normally, you can choose Unicast. (You generally need not to check this option).
- IPv6 Address Assign Type There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

SLAAC

• IPv6 Address Prefix -The Prefix of IPv6 Address

DHCPv6 Server

- Release Time the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- IPv6 Address Displays the LAN IPv6 Address.

2) Static IPv6

WAN Setup	
Enable IPv6: WAN Connection Type:	Static IPv6
IPv6 Address: Default Gateway:	2001: db8:1000:1::100 :: (Optional)
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
Primary DNS:	2001:4860:4860::8888 (Optional)
Secondary DNS:	2001:4860:4860::8888 (Optional)
LAN Setup	
IPv6 Address Assign Type:	SLAAC Y
IPv6 Address Prefix:	2001:db8:ffff:1:: /64
LAN IPv6 Address:	2001:db8:ffff:1:12f1:a2ff.fe7c:d39b/64
	Save



> **IPv6 Address** - Enter the IPv6 address in dotted-decimal notation provided by your ISP.

- Default Gateway Enter the default gateway in dotted-decimal notation provided by your ISP.
- MTU Size The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- > **Primary DNS** Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- Secondary DNS Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.
- IPv6 Address Assign Type There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

SLAAC

• IPv6 Address Prefix -The Prefix of IPv6 Address

DHCPv6 Server

- Release Time the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- IPv6 Address Displays the LAN IPv6 Address.

3) PPPoEv6

Enable IPv6:	
WAN Connection Type:	PPPoEv6
User Name:	username
Password:	•••••
Confirm Password:	•••••
Get IPv6 Address Way:	Get non-temporary IPv6 address 💌
IPv6 Address:	3ffe::dd58:46eb:22f:637
	Connect Disconnect Connected!
N Setup	
Pv6 Address Assign Type:	SLAAC 🗸
IPv6 Address Prefix:	2001:db8:ffff:1:: /64
LAN IPv6 Address:	2001:db8:ffff:1:20a:ebff:fe13:919/64

Figure 4-111 PPPoEv6

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Get IPv6 Address Way

- **Get non-temporary IPv6 address** Get a non-temporary IPv6 address by DHCPv6 from the ISP.
- **Get IPv6 prefix delegation** Get a prefix delegation IPv6 address by DHCPv6 from the ISP, and the clients in LAN create IPv6 address with the delegation.
- Use IP address specified by ISP Input a static IPv6 address from the ISP

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

IPv6 Address Assign Type - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

SLAAC

• IPv6 Address Prefix -The Prefix of IPv6 Address

DHCPv6 Server

- Release Time the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- IPv6 Address Displays the LAN IPv6 Address.
- 4) Tunnel 6to4

WAN Setup	
Enable IPv6:	
WAN Connection Type:	Tunnel 6to4
Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
Tunnel Address:	
MTU Size (in bytes):	1480 (The default is 1480, do not change unless necessary.)
	Use the following IPv6 DNS Servers
Primary IPv6 DNS:	2001:4860:4860::8888
Secondary IPv6 DNS:	2001:4860:4860::8888 (Optional)
LAN Setup	
IPv6 Address Assign Type:	SLAAC
IPv6 Address Prefix:	2001:db8:ffff:1:: /64
LAN IPv6 Address:	2001:db8:ffff:1:12f1:a2ff.fe7c:d39b/64
Message:	
	Save

Figure 4-112 Tunnel 6to4

Address/Subnet Mask/Default Gateway - the IPv4 address/ subnet mask/ default gateway assigned, in dotted-decimal notation.

MTU Size - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1480 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- Primary IPv6 DNS Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- Secondary IPv6 DNS Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.
- IPv6 Address Assign Type There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

SLAAC

IPv6 Address Prefix -The Prefix of IPv6 Address

DHCPv6 Server

- Release Time the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- IPv6 Address Displays the LAN IPv6 Address.

4.21 System Tools

System Tools
- Time Settings
- Diagnostic
- Firmware Upgrade
- Factory Defaults
- Backup & Restore
- Reboot
- Password
- System Log
- Statistics

Figure 4-113 The System Tools menu

Choose menu "System Tools", and you can see the submenus under the main menu: Time Settings, Diagnostic, Firmware Upgrade, Factory Defaults, Backup & Restore, Reboot, Password, System Log and Statistics. Click any of them, and you will be able to configure the corresponding functions. The detailed explanations for each submenu are provided below.

4.21.1 Time Settings

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

Time Settings	
Time zone:	(GMT-08:00) Pacific Time
Date:	6 16 2015 (MM/DD/YY)
Time:	1 58 33 (HH/MM/SS)
NTP Server 1:	0.0.0.0 (Optional)
NTP Server 2:	0.0.0.0 (Optional)
	Get GMT
	Enable Daylight Saving
Start:	2015 Mar ▼ 3rd ▼ Sun ▼ 2am ▼
End:	2015 Nov ▼ 2nd ▼ Sun ▼ 3am ▼
Daylight Saving Status:	
	Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers
	or entering the customized server (IP Address or Domain Name) in the above frames.
	Save

Figure 4-114 Time settings

- > 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 I / NTP Server II Enter the address or domain of the NTP Server I or NTP Server II, and then the router will get the time from the NTP Server preferentially. In addition, the router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.
- > Enable Daylight Saving Check the box to enable the Daylight Saving function.
- Start The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- End The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- > Daylight Saving Status Displays the status whether the Daylight Saving is in use.

To set time manually:

- 1. Select your local time zone.
- 2. Enter the **Date** in Month/Day/Year 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 I or NTP Server II.
- 3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

To set Daylight Saving:

- 1. Check the box to enable Daylight Saving.
- 2. Select the start time from the drop-down lists in the **Start** field.
- 3. Select the end time from the drop-down lists in the **End** field.
- 4. Click the **Save** button to save the settings.

Enable Daylight Saving					
Start:	2015 Mar ▼ 3rd ▼ Sun ▼ 2am ▼				
End:	2015 Nov ▼ 2nd ▼ Sun ▼ 3am ▼				
Daylight Saving Status:	daylight saving is down.				

Figure 4-115 Time settings

Note:

- 1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.
- 2. The time will be lost if the router is turned off.
- 3. The router will automatically obtain GMT from the Internet if it is configured accordingly.
- 4. The Daylight Saving will take effect one minute after the configurations are completed.

4.21.2 Diagnostic

Choose menu "System Tools \rightarrow Diagnostic", and then you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

Archer C7 AC1750 Wireless Dual Band Gigabit Router

Diagnostic Tools	
Diagnostic Parameters	
Diagnostic Tool:	Ping Traceroute
IP Address/ Domain Name:	
Ping Count:	4 (1-50)
Ping Packet Size:	64 (4-1472 Bytes)
Ping Timeout:	800 (100-2000 Milliseconds)
Traceroute Max TTL:	20 (1-30)
Diagnostic Results	
The Router is ready.	
	Start

Figure 4-116 Diagnostic Tools

- > Diagnostic Tool Check the radio button to select one diagnostic too.
- Ping This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
- **Traceroute** This diagnostic tool tests the performance of a connection.

Note:

You can use ping / traceroute to test both numeric IP address or domain name. If ping / traceroute the IP address is successful, but ping / traceroute the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- IP Address/Domain Name Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- > Pings Count Specifies the number of Echo Request messages sent. The default is 4.
- > Ping Packet Size Specifies the number of data bytes to be sent. The default is 64.
- > **Ping Timeout -** Time to wait for a response, in milliseconds. The default is 800.

Traceroute Max TTL - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click **Start** to check the connectivity of the Internet.

The **Diagnostic Results** page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

```
Diagnostic Results
Pinging www.baidu.com [180.97.33.107] with 64 bytes of data:
Reply from 180.97.33.107: bytes=64 time=42 TTL=55 seq=1
Reply from 180.97.33.107: bytes=64 time=41 TTL=55 seq=2
Reply from 180.97.33.107: bytes=64 time=43 TTL=55 seq=3
Reply from 180.97.33.107: bytes=64 time=42 TTL=55 seq=4
Ping statistics for www.baidu.com
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 41, Maximum = 43, Average = 42
```

Figure 4-117 Diagnostic Results

Note:

- 1. Only one user can use the diagnostic tools at one time.
- 2. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters, and "Traceroute Max TTL" is Traceroute Parameter.

4.21.3 Firmware Upgrade

Choose menu "System Tools \rightarrow Firmware Upgrade", and then you can update the latest version of firmware for the router on the following screen.

Firmware Upgrade	
File: Firmware Version: Hardware Version:	Choose File No file chosen 3.14.2 Build 150311 Rel.54891n 00000000
	Upgrade

Figure 4-118 Firmware Upgrade

- > 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 router's current hardware version.

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

- 1. Download a most recent firmware upgrade file from our website (www.tp-link.com).
- 2. Click **Choose File** to select the downloaded file.
- 3. Click the **Upgrade** button.
- 4. The router will reboot while the upgrading has been finished.

Note:

- New firmware versions are posted at <u>www.tp-link.com</u> 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 router rather than the
 configuration, you can try to upgrade the firmware.
- 2) When you upgrade the 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 router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the router.
- 4) The firmware version must correspond to the hardware.
- 5) The upgrade process takes a few moments and the router restarts automatically when the upgrade is complete.

4.21.4 Factory Defaults

Choose menu "System Tools \rightarrow Factory Defaults", and then and you can restore the configurations of the router to factory defaults on the following screen.

Factory Defaults
Click the following button to reset all configuration settings to their default values.
Restore

Figure 4-119 Restore Factory Default

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.

4.21.5 Backup & Restore

Choose menu "System Tools \rightarrow Backup & Restore", and then you can save the current configuration of the router as a backup file and restore the configuration via a backup file as shown in Figure 4-120.

Backup & Restor	e	
Backup: File:	Backup Choose File No file chosen	Restore

Figure 4-120 Backup & Restore Configuration

- Click the Backup button to save all configuration settings as a backup file in your local computer.
- > To upgrade the 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 router will restart automatically then. Keep the power of the router on during the process, in case of any damage.

4.21.6 Reboot

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

Reboot	
Click this button to reboot the device.	
	Reboot

Figure 4-121 Reboot the router

Some settings of the 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 router (system will reboot automatically).
- Restore the router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

4.21.7 Password

Choose menu "System Tools \rightarrow Password", and then you can change the factory default user name and password of the router in the next screen as shown in Figure 4-122.

Password	
Username and password can contain b	etween 1 - 15 characters and may not incluede spaces.
Old User Name:	
Old Password:	
New User Name:	
New Password:	
Confirm New Password:	
	Save Clear All

Figure 4-122 Password

It is strongly recommended that you should change the factory default user name and password of the router, because all users who try to access the router's Web-based utility or Quick Setup will be prompted for the router's default user name and password.

Note:

The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

4.21.8 System Log

Choose menu "System Tools \rightarrow System Log", and then you can view the logs of the router.

Sys	System Log						
Auto Mail Feature: Disabled Mail Settings Log Type: ALL V Log Level: ALL V							
Index	Time	Туре	Level	Log Content			
1	Jun 16 02:15:34	NULL	NULL	anonymous_enable=NO write_enable=YES local_enable=YES no_anon_plassword=YES anon_upload_enable=YES anon_mkdir_write_enable=YES user_config_dir=%s connect_from_port_20=YES asci			
H-Ver L = 192 W1 = F	2.168.0.1 : M = 25	000000 55.255.	00 : S- 255.0 5.42 : I	Ver = 3.14.2 Build 150311 Rel.54891n M = 255.255.255.255 : G = 219.134.215.42 Mail Log Clear Log Previous Next Current No. 1 V Page			

Figure 4-123 System Log

- > Auto Mail Feature Indicates whether auto mail feature is enabled or not.
- Mail Settings Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 4-124.

Mail Account Settings	
From:	
To:	
SMTP Server:	
	Authentication
	Enable Auto Mail Feature
۲	Everyday, mail the log at 18 : 00
	Mail the log every 48 hours
	Save Back

Figure 4-124 Mail Account Settings

- From Your mail box address. The router would connect it to send logs.
- **To -** Recipient's address. The destination mailbox where the logs would be received.

- **SMTP Server** Your smtp server. It corresponds with the mailbox filled in the **From** field. You can log on the relevant website for help if you are not clear with the address.
- **Authentication** Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

Note:

Only when you select **Authentication**, do you have to enter the User Name and Password in the following fields.

- User Name Your mail account name filled in the From field. The part behind @ is included.
- **Password -** Your mail account password.
- Confirm The Password Enter the password again to confirm.
- Enable Auto Mail Feature Select it to mail logs automatically. You could mail the current logs either at a specified time every day or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field as shown in Figure 4-124.

Click **Save** to keep your settings.

Click **Back** to return to the previous page.

- **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.
- Save Log Click to save all the logs in a txt file.
- Mail Log Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- > **Clear Log -** All the logs will be deleted from the router permanently, not just from the page.

Click the **Next** button to go to the next page, or click the **Previous** button to return to the previous page.

4.21.9 Statistics

Choose menu "System Tools \rightarrow Statistics", and then you can view the statistics of the router, including total traffic and current traffic of the last Packets Statistic Interval.

Current Statistics Status: Packets Statistics Interval(5~60):		Enabled			C	isable		
		Auto-refresh			R	efresh		
Sorted R	ules:	Sorted by	Current By	tes 🔻	R	eset All	Delet	e All
	To	otal			Current			
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	Modify
192.168.0.100 D4-3D-7E-BF-61-5F	34	13928	0	319	0/0	0/0	0/0	Reset Delete
5 v entries per page. Current No. 1 v page								
D4-3D-7E-BF-61-5F 34 13928 0 319 0/0 0/0 0/0 Reset Delete								

Figure 4-125 Statistics

- Current Statistics Status Enable or Disable. The default value is disabled. To enable it, click the Enable button. If it is disabled, the function of DoS protection in Security settings will be disabled.
- Packets 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.
- > **Sorted Rules -** Choose how the displayed statistics are sorted.

Select the Auto-refresh checkbox to refresh automatically.

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

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

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

IP/MAC A	Address	The IP and MAC address are displayed with related statistics.
Total	Packets	The total number of packets received and transmitted by the router.
	Bytes	The total number of bytes received and transmitted by the router.
	Packets The total number of packets received and transmitted in the Packets Statistic interval seconds.	
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
Current	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".
	TCP 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".
Modifi	Reset	Reset the value of he entry to zero.
Modify	Delete	Delete the existing entry in the table.

Statistics Table:

There would be 5 entries on each page. Click **Previous** to return to the previous page and **Next** to the next page.

Appendix A: FAQ

- 1. How do I configure the router to access Internet by ADSL users?
 - 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
 - Connect the Ethernet cable from your ADSL Modem to the Internet port on the router. The telephone cord plugs into the Line port of the ADSL Modem.
 - 3) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "PPPoE/Russia PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, type password in the "Confirm Password" field again, finish by clicking "Connect".

PPPoE/Russia PPPoE	Detect
username	
•••••	
•••••	
	•••••

Figure A-1 PPPoE Connection Type

4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Connect Manually" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.

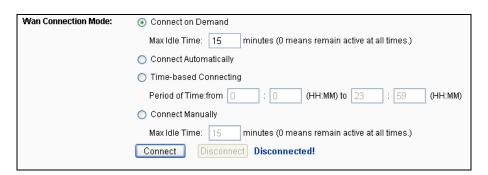


Figure A-2 PPPoE Connection Mode

Note:

- 1. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- 2. If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access Internet by Ethernet users?

- Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "Dynamic IP" for "WAN Connection Type", finish by clicking "Save".
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC's MAC address is proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

00-08-01-00-00-05	Restore Factory MAC
00-19-66-80-54-2B	Clone MAC Address
Save	
	00-19-66-80-54-28

Figure A-3 MAC Clone

3. I want to use Netmeeting, what do I need to do?

- 1) If you start Netmeeting as a host, you don't need to do anything with the router.
- If you start as a response, you need to configure Virtual Server or DMZ Host and make sure the H323 ALG is enabled.
- 3) How to configure Virtual Server: Log in to the router, click the "Forwarding" menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Servers" page, click Add New.... Then on the "Add or Modify a Virtual Server Entry" page, enter "1720" for the "Service Port" blank, and your IP address for the "IP Address" blank, taking 192.168.0.169 for an example, remember to Enable and Save.

٧	Virtual Servers					
Note: Make sure the nat is enable if you want the Virtual Servers configuration take effect						
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	1720	1720	192.168.0.169	ALL	Enabled	Modify Delete
Add New Enable All Disable All Delete All						
		Pr	evious Nex	t		

Figure A-4 Virtual Servers

Add or Modify a Virtual S	Server Entry
Service Port:	1720 (XX-XX or XX)
Internal Port:	(XX, Only valid for single Service Port or leave it blank)
IP Address:	192.168.0.169
Protocol:	ALL
Status:	Enabled 💌
Common Service Port:	Select One
	Save Back

Figure A-5 Add or Modify a Virtual server Entry

Note:

Your opposite side should call your WAN IP, which is displayed on the "Status" page.

4) How to enable DMZ Host: Log in to the router, click the "Forwarding" menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click Enable radio button and type your IP address into the "DMZ Host IP Address" field, using 192.168.0.169 as an example, remember to click the Save button.

DMZ		
lote: Make sure the nat is enable if you want the DMZ configuration take effect		
Current DMZ Status:	💿 Enable 🔘 Disable	
DMZ Host IP Address:	192.168.0.169	
	Save	

Figure A-6 DMZ

5) How to enable H323 ALG: Log in to the router, click the "Security" menu on the left of your browser, and click "Basic Security" submenu. On the "Basic Security" page, check the Enable radio button next to H323 ALG. Remember to click the Save button.

Basic Security	
Firewall	
SPI Firewall:	💿 Enable 🔵 Disable
VPN	
PPTP Passthrough:	Enable Disable
L2TP Passthrough:	Enable O Disable
IPSec Passthrough:	Enable O Disable
ALG	
FTP ALG:	Enable O Disable
TFTP ALG:	Enable O Disable
H323 ALG:	Enable O Disable
RTSP ALG:	Enable O Disable
SIP ALG:	Enable O Disable
	Save

Figure A-7 Basic Security

4. I want to build a WEB Server on the LAN, what should I do?

- 1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.
- 2) To change the WEB management port number: Log in to the router, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click Save and reboot the router.

Remote Management		
Web Management Port: Remote Management IP Address:	88	(Enter 255.255.255.255 for all)
	Save	

Figure A-8 Remote Management

Note:

If the above configuration takes effect, you can visit and configure the router by typing <u>http://192.168.0.1:88</u> (the router's LAN IP address: Web Management Port) in the address field of the Web browser. If the LAN IP of the modem connected with your router is 192.168.0.x, the default LAN IP of the router will automatically switch from 192.168.0.1 to 192.168.1.1 to avoid IP conflict; in this case, please try <u>http://192.168.1.1:88</u>.

3) Log in to the router, click the "Forwarding" menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Servers" page, click Add New..., then on the "Add or Modify a Virtual Server" page, enter "80" into the blank next to the "Service Port", and your IP address next to the "IP Address", assuming 192.168.0.188 for an example, remember to Enable and Save.

١	Virtual Servers					
Not	Note: Make sure the nat is enable if you want the Virtual Servers configuration take effect					
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	1720	1720	192.168.0.169	ALL	Enabled	Modify Delete
	Add New Enable All Disable All Delete All					
		Pr	evious Nex	t		

Figure A-9 Virtual Servers

Add or Modify a Virtual S	erver Entry
Service Port:	80 (XX-XX or XX)
Internal Port:	(XX, Only valid for single Service Port or leave it blank)
IP Address:	192.168.0.188
Protocol:	ALL
Status:	Enabled
Common Service Port:	Select One
	Save Back

Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

- 1) Make sure the "Wireless router Radio" is enabled.
- 2) Make sure that the wireless stations' SSID accord with the router's SSID.
- Make sure the wireless stations have right KEY for encryption when the router is encrypted.

4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PCs

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
- 2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
- 3) Right click the icon that showed below, select Properties on the prompt page.

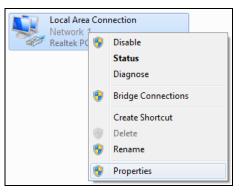


Figure B-1

4) In the prompt page that showed below, double click on the Internet Protocol (TCP/IP).

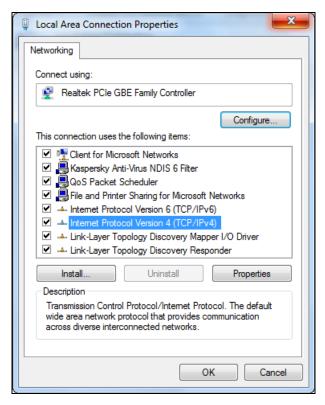


Figure B-2

- 5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.
- 6) Select **Obtain an IP address automatically** and **Obtain DNS server automatically**, as shown in the Figure below:

Internet Protocol Version 4 (TCP/IPv4) P	roperties			? <mark>×</mark>	
General Alternate Configu	ation					
this capability. Otherwise,	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
Obtain an IP address	automatically					
Ouse the following IP a	ddress:					
IP address:						
Subnet mask:				$\sim 10^{-1}$		
Default gateway:						
Obtain DNS server ad	dress automa	atically				
- Use the following DNS	server addre	esses:				
Preferred DNS server:				$\sim 10^{-1}$		
Alternate DNS server:						
Validate settings upo	n exit		(Advan	ced	
			OK		Cancel	

Figure B-3

Appendix C: Specifications

General			
	IEEE 802.11ac. IEEE 802.11n.	IEEE 802.11g, IEEE 802.11b, IEEE	
Standards	802.11a, IEEE 802.11e, IEEE 802.11i, IEEE 802.1X, IEEE 802.3X,		
	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab		
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP		
	1 10/100/1000M Auto-Negotiatio	n Internet RJ45 port:	
Ports	4 10/100/1000M Auto-Negotiat	ion Ethernet RJ45 ports supporting	
	Auto MDI/MDIX; 2 USB ports supporting storage/FTP/Media/Print Server;		
	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m)		
	EIA/TIA-568 100 Ω STP (maximum 100m)		
	100BASE-TX: UTP category 5, 5e cable (maximum 100m)		
Cabling Type	EIA/TIA-568 100Ω STP (maximum 100m)		
	1000BASE-TX: UTP category 5,	5e cable (maximum 100m)	
	EIA/TIA-568 100	Ω STP (maximum 100m)	
LEDs	Power, System, Wireless 2.4G	Hz, Wireless 5GHz, Ethernet (1-4),	
LLDS	Internet, WPS		
Safety & Emissions	FCC, CE		
Wireless			
Frequency Band*	2.4GHz, 5GHz		
	11b: 1/2/5.5/11Mbps 11a/g: 6/9/12/18/24/36/48/54/Mbps		
Radio Data Rate	11n: 45/90/135/180/270/360/405/450Mbps		
	11ac: up to 1.3Gbps		
Frequency Expansion	DSSS (Direct Sequence Spread	Spectrum)	
Modulation	11ac: 256-QAM for OFDM		
Modulation	11n/g/a: QPSK,BPSK,16-QAM, 64-QAM for OFDM 11b: CCK,DQPSK,DBPSK		
Security	WEP, WPA/WPA2, WPA2-PSK/V	VPA-PSK	
	5G:	2.4G:	
	11a 6Mbps: -96dBm	11g 54M: -77dBm	
	11a 54Mbps: -79dBm	11n HT20: -74dmB	
Sensitivity @PER	11ac HT20: -71dBm	11n HT40: -72dBm	
	11ac HT40: -66dBm		
	11ac HT40:-66dBm 11ac HT80:-63dBm		
Environmental and Ph	11ac HT80: -63dBm		
	11ac HT80: -63dBm		
Environmental and Ph Temperature	11ac HT80: -63dBm Tysical	·°F)	
	11ac HT80: -63dBm ysical Operating: 0℃~40℃ (32°F~104	·°F) 8°F)	

* Only 2.412GHz~2.462GHz is allowed to be used in USA, which means only channel 1~11 is available for American users to choose.

Appendix D: Glossary

- 802.11ac IEEE 802.11ac is a wireless computer networking standard of 802.11.This specification will enable multi-station WLAN throughput of at least 1 gigabit per second .This is accomplished by extending the air interface concepts embraced by 802.11n: wider RF bandwidth, more MIMO spatial streams, multi-user MIMO, and high-density modulation (up to 256 QAM).
- 802.11n 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- 802.11b The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- 802.11g specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- DDNS (Dynamic Domain Name System) The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- DHCP (Dynamic Host Configuration Protocol) A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- DMZ (Demilitarized Zone) A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- DNS (Domain Name System) An Internet Service that translates the names of websites into IP addresses.
- > **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- DSL (Digital Subscriber Line) A technology that allows data to be sent or received over existing traditional phone lines.
- > **ISP** (Internet Service Provider) A company that provides access to the Internet.

- MTU (Maximum Transmission Unit) The size in bytes of the largest packet that can be transmitted.
- NAT (Network Address Translation) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- PPPoE (Point to Point Protocol over Ethernet) PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- WEP (Wired Equivalent Privacy) A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- Wi-Fi A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- WLAN (Wireless Local Area Network) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.