TP-LINK®

User Guide

TL-WR710N

Wi-Fi Pocket Router/AP/TV Adapter/Repeater



1910011713 REV1.1.0

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 © 2016 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 radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment has been SAR-evaluated for use in hand. SAR measurements are based on a 5mm spacing from the body and that compliance is achieved at that distance.

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。

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.

CONTENTS

Chapter 7		oduction	
1.1	Ove	rview of the Router	.2
1.2	2 Cor	ventions	.3
1.3	3 Mai	n Features	.3
1.4	l Par	el Layout	.3
Chapter 2	2. Co	nnecting the Router	.5
2.7	l Sys	tem Requirements	.5
2.2	2 Inst	allation Environment Requirements	.5
2.3	3 Cor	necting the Router	.5
	2.3.	1 Wireless Router Mode	.6
	2.3.	2 Access Point Mode	.6
	2.3.	3 Repeater Mode	.7
	2.3.	4 Client Mode	.8
	2.3.	5 WISP Client Router Mode	.8
Chapter :	3. Qu	ck Installation Guide	10
3.′	TCF	P/IP Configuration	10
3.2	2 Qui	ck Installation Guide	13
	3.2.	1 Wireless Router Mode	14
	3.2.	2 Access Point Mode	17
	3.2.	3 Repeater Mode	19
	3.2.	4 Client Mode	21
	3.2.	5 WISP Client Router Mode	23
Chapter 4		nfiguration for Wireless Router Mode	
4.1	l Log	in	27
4.2	2 Stat	us	27
4.3	3 Qui	ck Setup	30
4.4	I WP	S	30
4.8	5 Wo	king Mode	34
4.6	6 Net	work	35
	4.6.	1 WAN	35
	4.6.	2 MAC Clone	44
	4.6.	3 LAN	45

		TL-WR710N Wi-Fi Pocket Router/AP/TV Adapter/Repeate	er
4.7	Wireles	SS	46
	4.7.1	Wireless Settings	46
	4.7.2	Wireless Security	48
	4.7.3	Wireless MAC Filtering	51
	4.7.4	Wireless Advanced	53
	4.7.5	Wireless Statistics	54
4.8	DHCP		55
	4.8.1	DHCP Settings	55
	4.8.2	DHCP Client List	56
	4.8.3	Address Reservation	56
4.9	USB S	ettings	58
	4.9.1	Storage Sharing	58
	4.9.2	Media Server	59
	4.9.3	User Accounts	61
4.10	Forwar	ding	63
	4.10.1	Virtual Servers	63
	4.10.2	Port Triggering	65
	4.10.3	DMZ	67
		UPnP	
4.11	Securit	ty	68
	4.11.1	Basic Security	68
	4.11.2	Advanced Security	69
	4.11.3	Local Management	71
	4.11.4	Remote Management	72
		al Control	
4.13	Access	s Control	75
	4.13.1	Rule	75
	4.13.2	Host	78
	4.13.3	Target	79
		Schedule	
4.14	Advand	ced Routing	83

	4	4.14.1 S	Static Routing List	83
	4	4.14.2 S	System Routing Table	84
4.	.15 I	Bandwidt	th Control	85
	4	4.15.1 C	Control Settings	85
	4	4.15.2 F	Rule List	86
4.	.16	IP & MAC	C Binding	87
	4	4.16.1 E	Binding Setting	87
	4	4.16.2 A	ARP List	89
4.	.17	Dynamic	DNS	89
	4	4.17.1 N	No-IP DDNS	90
	4	4.17.2 C	Comexe.cn DDNS	90
	4	4.17.3 C	Dyndns org DDNS	91
4.	.18	System T	Fools	92
	4	4.18.1 T	īme Settings	93
	4	4.18.2 C	Diagnostic	94
	4	4.18.3 F	Firmware Upgrade	95
	4	4.18.4 F	Factory Defaults	96
	4	4.18.5 E	Backup & Restore	96
	4	4.18.6 ह	Reboot	97
	4	4.18.7 F	Password	97
	4	4.18.8 S	System Log	98
	4	4.18.9 S	Statistics	99
Chapter	5.	Configu	ration for Access Point Mode	.101
5.	.1	Login		101
5.	.2 3	Status		101
5.	.3 (Quick Se	etup	103
5.	.4	WPS		103
5.	.5 \	Working	Mode	107
5.	.6 I	Network.		108
	į	5.6.1 L	AN	108
5.	.7	Wireless		109
	!	5.7.1 V	Vireless Settings	.109

		5.7.2	Wireless Security	111
		5.7.3	Wireless MAC Filtering	114
		5.7.4	Wireless Advanced	116
		5.7.5	Wireless Statistics	117
	5.8	DHCP.		118
		5.8.1	DHCP Settings	118
		5.8.2	DHCP Client List	119
		5.8.3	Address Reservation	120
	5.9	USB Se	ettings	121
		5.9.1	Storage Sharing	121
		5.9.2	Media Server	123
		5.9.3	User Accounts	125
	5.10	System	1 Tools	126
		5.10.1	Diagnostic	126
		5.10.2	Firmware Upgrade	128
		5.10.3	Factory Defaults	129
		5.10.4	Backup & Restore	129
		5.10.5	Reboot	130
		5.10.6	Password	130
		5.10.7	System Log	131
Chapt		-	uration for Repeater Mode	
	6.1	-		
	6.2			
	6.3		Setup	
	6.4		g Mode	
	6.5		k	
	6.6	6.5.1	LAN	
	0.0			
		6.6.1	Wireless Settings	137
		6.6.2	Wireless Security	139
		6.6.3	Wireless MAC Filtering	141
		6.6.4	Wireless Advanced	143

6.7	6.6.5 DHCP.	Wireless Statistics	
	6.7.1	DHCP Settings	145
	6.7.2	DHCP Client List	146
	6.7.3	Address Reservation	147
6.8	USB Se	ettings	148
	6.8.1	Storage Sharing	148
	6.8.2	Media Server	150
	6.8.3	User Accounts	152
6.9	System	ח Tools	153
	6.9.1	Diagnostic	153
	6.9.2	Firmware Upgrade	155
	6.9.3	Factory Defaults	156
	6.9.4	Backup & Restore	156
	6.9.5	Reboot	157
	6.9.6	Password	157
	6.9.7	System Log	
Chapter 7.	Config	juration for Client Mode	160
7.1	Config Login	juration for Client Mode	 160 160
7.1 7.2	Config Login Status.	juration for Client Mode	 160 160 160
7.1 7.2 7.3	Config Login Status . Quick S	Juration for Client Mode	 160 160 160 162
7.1 7.2	Config Login Status . Quick S Workin	juration for Client Mode	160 160 160 162 162
7.1 7.2 7.3 7.4	Config Login Status . Quick S Workin	Juration for Client Mode	160 160 160 162 162 163
7.1 7.2 7.3 7.4	Config Login Status . Quick S Workin Networ 7.5.1	juration for Client Mode Setup g Modek	160 160 162 162 163 163
7.1 7.2 7.3 7.4 7.5	Config Login Status . Quick S Workin Networ 7.5.1	Juration for Client Mode	160 160 162 162 163 163 164
7.1 7.2 7.3 7.4 7.5	Config Login Status . Quick S Workin Networ 7.5.1 Wireles	Juration for Client Mode	160 160 160 162 163 163 164 164
7.1 7.2 7.3 7.4 7.5	Config Login Status . Quick S Workin Networ 7.5.1 Wireles 7.6.1 7.6.2	Juration for Client Mode	160 160 160 162 163 163 164 164 165
7.1 7.2 7.3 7.4 7.5 7.6	Config Login Status . Quick S Workin Networ 7.5.1 Wireles 7.6.1 7.6.2	Juration for Client Mode	160 160 160 162 163 163 164 164 165 167
7.1 7.2 7.3 7.4 7.5 7.6	Config Login Status . Quick S Workin Networ 7.5.1 Wireles 7.6.1 7.6.2 DHCP .	Juration for Client Mode	160 160 160 162 163 163 164 164 165 167 167
7.1 7.2 7.3 7.4 7.5 7.6	Config Login Status . Quick S Workin Networ 7.5.1 Wireles 7.6.1 7.6.2 DHCP. 7.7.1	puration for Client Mode	160 160 160 162 162 163 163 164 165 167 167 167

TL-WR710N Wi-Fi Pocket Router/AP/TV Adapter/Repeater 7.8.1 7.8.2 7.8.3 7.9 7.9.1 7.9.2 7.9.3 7.9.4 7.9.5 7.9.6 7.9.7 Chapter 8. 8.1 8.2 8.3 8.4 8.5 8.5.1 8.5.2 8.5.3 Wireless 198 8.6 8.6.1 8.6.2 8.6.3 8.6.4 8.6.5 8.7 8.7.1 8.7.2 8.7.3 8.8 8.8.1

	8.8.2	Media Server	211
	8.8.3	User Accounts	213
8.9	Forwar	ding	215
	8.9.1	Virtual Servers	215
	8.9.2	Port Triggering	217
	8.9.3	DMZ	219
	8.9.4	UPnP	219
8.10	Securit	y	220
	8.10.1	Basic Security	220
	8.10.2	Advanced Security	221
	8.10.3	Local Management	223
	8.10.4	Remote Management	224
8.11	Parenta	al Control	224
8.12	Access	S Control	227
	8.12.1	Rule	227
	8.12.2	Host	230
	8.12.3	Target	231
	8.12.4	Schedule	233
8.13	Advanc	ed Routing	235
	8.13.1	Static Routing List	235
	8.13.2	System Routing Table	236
8.14	Bandwi	idth Control	237
	8.14.1	Control Settings	237
	8.14.2	Rule List	238
8.15	IP & M	AC Binding	239
	8.15.1	Binding Setting	239
	8.15.2	ARP List	241
8.16	Dynam	ic DNS	241
	8.16.1	No-IP DDNS	242
	8.16.2	Comexe.cn DDNS	242
	8.16.3	Dyndns org DDNS	243
8.17	System	n Tools	244

8.17.1	Time Settings	. 245
8.17.2	Diagnostic	. 246
8.17.3	Firmware Upgrade	. 247
8.17.4	Factory Defaults	. 248
8.17.5	Backup & Restore	. 248
8.17.6	Reboot	. 249
8.17.7	Password	. 249
8.17.8	System Log	. 250
8.17.9	Statistics	. 251
Appendix A: FAQ.		. 253
Appendix B: Confi	guring the PC	. 257
Appendix C: Speci	ifications	. 260
Appendix D: Gloss	sary	. 261

Chapter 1. Introduction

1.1 Overview of the Router

Small enough to fit in the average pocket, the router is uniquely suited to provide robust wireless networking to travelers, students, or anyone else for work or play.

Incredible Speed

The router supports the newest 802.11n standards, and provides backward compatibility with older 802.11b/g standards as well. The up-to-150Mbps wireless speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth.

Multiple Operation Modes

The router supports five operation modes. Wireless Router mode creates an instant private wireless network and share Internet to multiple Wi-Fi devices, which is suitable for most hotel and home network. Access Point mode creates a wireless network for Wi-Fi devices. The wireless devices are exposed to the wired network. Repeater mode extends your home wireless range by copying the same wireless name and password. Client mode works as a wireless adapter for any Ethernet-enabled devices, such as Smart TV, Game Console and PC. WISP Client Router mode accesses the Internet wirelessly in areas with no wired ISP infrastructure

Reliable Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, WiFi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the router provides complete data privacy.

Flexible Access Control

The router 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.

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

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

You can set the parameters according to your demand.

1.3 Main Features

- > Portable design, ideal for travel and home use
- > Built-in power supply design without external power adapter
- > Support Wireless Router, Access Point, Repeater, Client, WISP Client Router modes
- > USB port supports charging for smart phone and tablet
- > USB port supports storage sharing, media server function
- > Pre-encryption prevents unauthorized access from users outside of the network

1.4 Panel Layout



> LED

Status	Indication
Solid Green	The device is working properly.
	Condition 1: System is booting.
Blinking	Condition 2: The Ethernet Cable or USB Device is
	connecting to the product.

- **USB:** The USB port connects to a USB storage device.
- Reset: It is used to reset the Router to its factory defaults. With the Router powered on, use a pin to press and hold the **Reset** button (about 5 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.
- LAN/WAN: This LAN/WAN port works as LAN in AP/Repeater/Client/WISP Client Router mode and as WAN in Wireless Router mode. As LAN, it connects the Router to the local PC; as WAN, it enables you connect the DSL/cable Modem, or Ethernet.
- LAN: This LAN port works as LAN in Wireless Router/ AP/Repeater/Client/WISP Client Router mode. It connects the Router to the local PC.

Chapter 2. Connecting the Router

2.1 System Requirements

- > Each PC in the LAN needs a working Ethernet Adapter
- > TCP/IP protocol must be installed on each PC
- > Web browser, such as Microsoft Internet Explorer 5.0 or later, Mozilla Firefox, Apple Safari
- If the device is configured to Wireless Router/Access Point mode, you also need 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.)

2.2 Installation Environment Requirements

- > Place the Router in a well-ventilated place far from any heater or heating vent
- Place the Router in a location where it can be connected to the various devices as well as to a power source
- > 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°F ~ 104°F)
- > Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

Before installing the Router, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact with your ISP. To connect the Router, please follow the steps below:

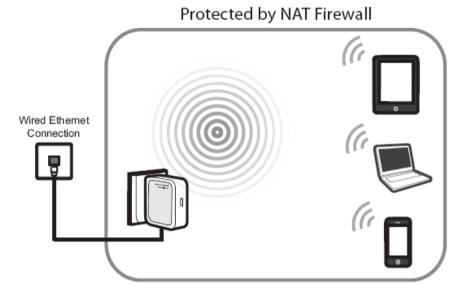
- 1. Power off your PC, Cable/DSL Modem, and the Router.
- 2. Locate an optimum location for the Router. The best place is usually at the center of your wireless network. The place must accord with the <u>Installation Environment Requirements</u>.
- 3. Plug the power plug in the electrical wall socket. The Router will start to work automatically.

After finishing the steps above, please choose the operation mode you need and carry out the corresponding steps. There are five operation modes supported by this router: **Wireless Router**, **Access Point**, **Repeater**, **Client** and **WISP Client Router**.

2.3.1 Wireless Router Mode

As a wireless router, it enables multi-user to share Internet via DSL/Cable Modem.

The default mode of the router is Wireless Router. On this mode, the wired port LAN/WAN works as WAN, it can be connected to DSL Modem or directly connected to a wired network with an Ethernet cable. Computers could connect to the device by both wired way through the wired port LAN and wireless way.



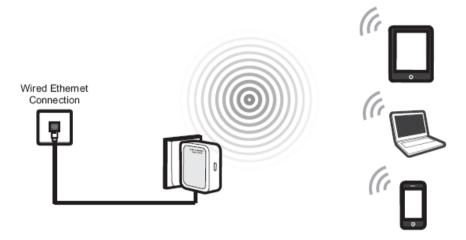
- 1. Connect the LAN/WAN port of the router to the LAN Port on the DSL/Cable Modem.
- 2. Connect the WAN port on the DSL/Cable Modem to the wired Internet.
- 3. Plug the power plug of the router in electrical wall socket.
- 4. Power on the DSL/Cable Modem, PC(s) and notebook(s).

2.3.2 Access Point Mode

As the supplement of wired LAN, the router enables the wired LAN to connect to the Internet wirelessly.

Plug the power plug of the router in electrical wall socket and connect the Ethernet cable correctly, you can surf the Internet by connecting your PC(s) to the Router wirelessly.

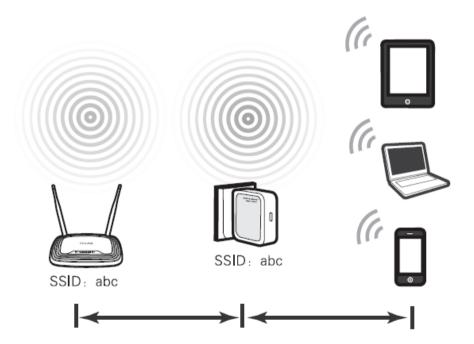
On this mode, the wired port LAN/WAN works as LAN. Computer could connect to the device by either wired or wireless way. The Pre-encryption function is opened by default and the default password is the last unique eight numbers of each Router's MAC address.



- 1. Connect the LAN or LAN/WAN port of the router to the wired network port with an Ethernet cable.
- 2. Plug the power plug of the router in electrical wall socket.
- 3. Power on the PC(s) and notebook(s).

2.3.3 Repeater Mode

The router is used to extend the range of wireless signal of the existing AP or wireless router. On this mode, the wired port LAN/WAN works as LAN. Computer could connect to the device by either wired or wireless way. The SSID of the router should be the same as that of the device you repeat.



- 1. Plug the power plug of the router in electrical wall socket.
- 2. Power on the notebook(s).

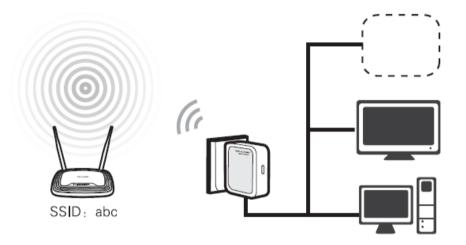
P Note:

It is recommended that you connect a PC/notebook to the LAN port of the Router with an Ethernet cable, and then login the Router from the PC/notebook to set the Router in Repeater mode.

2.3.4 Client Mode

The router is used as a wireless network card to connect the wireless network signal or wireless router.

On this mode, the wired port LAN/WAN works as LAN. Computer could connect to the device by either wired or wireless way.

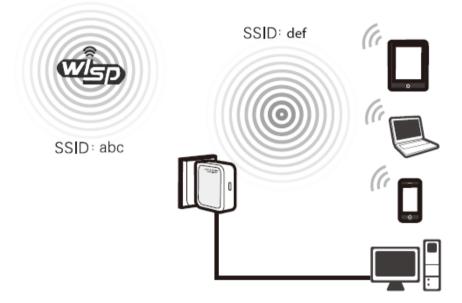


- 1. Connect the PC to the LAN or LAN/WAN port of the router with an Ethernet cable.
- 2. Plug the power plug of the router in electrical wall socket.
- 3. Power on the PC(s).

2.3.5 WISP Client Router Mode

In WISP mode, the router enables multiple users to share Internet connection from WISP.

On this mode, the LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at WISP Client Router mode. The Ethernet port acts as a LAN port.



- 1. Plug the power plug of the router in electrical wall socket.
- 2. Power on the notebook(s).

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the router is 192.168.0.254. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the local PC to the LAN port of the Router. And then you can configure the IP address for your PC as the following steps:

- 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>
- 2) Then the built-in DHCP server will assign IP address for the PC.

Then connect to the Router through wireless connection following the steps below:

1) Click the icon at the bottom of your desktop. Click refresh button, and then select the default SSID of the Router. Click **Connect**.



2) Enter the **Security key**. Click **OK**.

🔮 Connect to a Netwo	rk	×
Type the network	security key	
Security key:	••••••••••••••••••••••••••••••••••••••	
		OK Cancel

3) If you can see **Connected** after the default SSID, you've successfully connected to the wireless network.

Dial-up and VPN	~	•
Wireless Network Conn	ection 6 🔹 🔺	
TP-LINK_Network1	Connected	=
NetworkProfile~	Sail	=
B19DDE_ZLP	lite.	
8877A7	lite.	
1B0F28	lite.	
Infra_KeyTest	lite.	
TP-LINK_1B0F28	lite.	
TP-LINK_B19DDE_ZLP	lite.	
TP-LINK_8877A7	3 41	-
Open Network an	d Sharing Center	
EN 📶 😼	<u>利</u> 心) 10:12 AM 3/29/2011	

Note:

- 1. The default **SSID** and **Password** of your Router are on the label. Both are case-sensitive.
- 2. The pre-encryption function is enabled by default and the default **Network key/Security key** is the **Password** on the label.

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 XP.

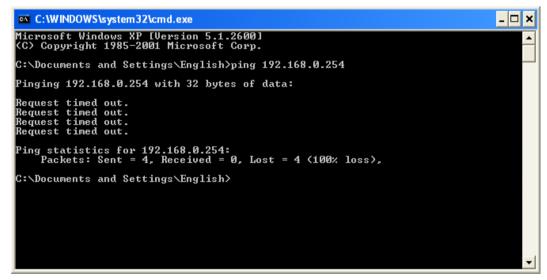
Open a command prompt, and type *ping 192.168.0.254*, and then press Enter.

If the result displayed is similar to the following figure, it means the connection between your PC and the Router has been established well.

C:\WINDOWS\system32\cmd.exe	- 🗆 X
Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.	-
C:\Documents and Settings\English>Ping 192.168.0.254	
Pinging 192.168.0.254 with 32 bytes of data:	
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64 Reply from 192.168.0.254: bytes=32 time<1ms TTL=64 Reply from 192.168.0.254: bytes=32 time<1ms TTL=64 Reply from 192.168.0.254: bytes=32 time<1ms TTL=64	
Ping statistics for 192.168.0.254: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms	
C:\Documents and Settings\English>_	
	-

If the result displayed is similar to the following figure, it means the connection between your
PC and the Deuter has failed.

PC and the Router has failed.



Please check the connection following these steps:

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

Note:

The LED of LAN/WAN ports which you link to on the Router should be lit.

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

P Note:

If the Router's IP address is 192.168.0.254, your PC's IP address must be within the range of 192.168.0.1 ~ 192.168.0.253.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the 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 address http://tplinklogin.net in the address field of the browser.

After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Windows Security
The server tplinklogin.net at TP-LINK 150Mbps Wireless N Mini Pocket Router WR710N requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin ••••• Remember my credentials
OK Cancel

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 a successful login, you can click the **Quick Setup** menu to quickly configure your Router.

uick Setup		
The quick setup will tell you h To continue, please click th	ow to configure the basic network parameters.	
To exit, please click the Exi		
	Exit Next	

3. Click Next, and then Working Mode page will appear.

Working I	Mode
Start >> We	orking Mode >> WAN Connection Type >> Wireless >> Finish
۲	Wireless Router
0	Access Point
0	Repeater
0	Client
0	WISP Client Router
	Back Next

Solution Note:

The Router supports five working modes for multi-user to access the Internet: **Wireless Router**, **Access Point**, **Repeater**, **Client** and **WISP Client Router**. In **Wireless Router** mode, the device enables multiple users to share the Internet connection via ADSL/Cable Modem. In **Access Point** mode, this device can be connected to a wired network and transform the wired access into wireless that multiple devices can share together. In **Repeater** mode, the device will relay data to an associated root AP. In **Client** mode, the device will act as a wireless station to enable wired host(s) to access AP. In **WISP Client Router** mode, the device enables multiple users to share Internet connection from WISP. You can configure your device quickly by the following steps in different modes.

3.2.1 Wireless Router Mode

When you choose Wireless Router on Working Mode page, take the following steps:

1. Click **Next**, and then **WAN Connection Type** page will appear.

Quick Setup - WAN Connection Type	
Start >> Working Mode >> WAN Connection Type >> Wireless >> Finish	
The Quick Setup is preparing to set up your connection type of WAN port.	
The Router will try to detect the Internet connection type your ISP provides if you select the Auto-Detect option. Otherwise, you need to specify the connection type manually.	
Auto-Detect - Let the Router automatically detect the connection type your ISP provides.	
O PPPoE - Usually for ADSL Modem and you will need a PPPoE username and password from your ISP.	
O Dynamic IP - Usually for Cable Modern and the router will automatically obtain an IP address from the DHCP serve	er.
Static IP - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.	
Back Next	

The Router supports three popular ways **PPPoE**, **Dynamic IP** and **Static IP** to connect to the Internet. To make sure the connection type your ISP provides, please refer to the ISP. Make sure the cable is securely plugged into the WAN port before detection.

- Auto Detect If you don't know the connection type your ISP provides, use this option to allow the Quick Setup to search your Internet connection for servers and protocols and determine your ISP configuration.
- > **PPPoE -** For this connection, you will need your account name and password from your ISP.

If you have applied ADSL to realize Dial-up service, you should choose this type. Under this condition, you should fill in both the User Name and Password that the ISP supplied. Please note that these fields are case-sensitive.

Quick Setup - PPPoE		
Start >> Working Mode >> WAN	Connection Type >> Wireles	ss >> Finish
User Name:	username	
Password:		
Confirm Password:		
	Back	Next

- Dynamic IP Your ISP uses a DHCP service to assign your Router an IP address for connecting to the Internet. When the Router connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. If you choose this type of connection, no configuration should be set and you can go on with the wireless configuration.
- Static IP This type of connection uses a permanent, fixed (static) IP address that your ISP assigned. In this type, you should fill in the IP address, Subnet Mask, Default Gateway, and DNS IP address manually, which are specified by your ISP. Then click Next.

Quick Setup - Static IP		
Start >> Working Mode >> WAN (Connection Type >> Wirele	ess >> Finish
IP Address:	0.0.0.0]
Subnet Mask:	0.0.0.0]
Default Gateway:	0.0.0]
Primary DNS:	0.0.0.0]
Secondary DNS:	0.0.0.0	(Optional)
	Back	Next

2. Then, the **Wireless** page will appear. Set the wireless parameters. It is recommended that you rename an SSID, choose a Security Type and enter a Password. Then click **Next**.

Quick Setup - Wirel	ess
Start >> Working Mode	>> WAN Connection Type >> Wireless >> Finish
Wireless Radio:	Enable
Wireless Network Name:	TP-LINK 2046F2 (Also called the SSID)
Region:	United States
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.
Mode:	11bgn mixed
Channel Width:	Auto 🔽
Channel:	Auto 🔽
Wireless Security:	
0	Disable Security
۲	WPA-PSK/WPA2-PSK
PSK Password:	1234567890
	(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)
0	No Change
	Back Next

- > Wireless Radio Enable or disable the wireless radio choosing from the pull-down list.
- Wireless Network Name Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the pull-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.
- > **Mode -** Select the desired mode. The default setting is 11bgn mixed.
 - **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.
 When 11bg mixed mode is selected, only 11bg mixed wireless stations can connect to the Router. It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n wireless stations can connect to the Router.

P Note:

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

- Channel Width Select any channel width from the pull-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.
- Channel This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- > Wireless Security You can configure the security settings of your wireless network.
 - **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.
 - WPA-PSK/WPA2-PSK Input the password of your broadcast SSID.
 - No Change If you chose this option, wireless security configuration will not change.
- 3. The **Finish** page is shown as below. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**.

Quick Setup - Finish	
Start >> Working Mode >> Win Congratulations! This d please click other menu	evice is now connecting you to the Internet. For detail settings,
	Back Reboot

3.2.2 Access Point Mode

When you choose Access Point on Working Mode page, take the following steps:

1. Click **Next**, and then **Wireless** page will appear.

Start >> Working Mode >> Wireless	>> Finish	
AP Mode Setting:		
Wireless Network Name(SSID):	TP-LINK_2046F2	(also called SSID)
Region:	United States 🛛 👻	
Warning:	Ensure you select a correct cou Incorrect settings may cause in	
Channel:	Auto 🔽	
Mode:	11bgn mixed 🛛 🖌	
Channel Width:	Auto 🔽	
Wireless Security Mode:	Most Secure(WPA/WPA2-P	sk 🔽
Wireless Password:	1234567890	
	be between 8 and 64 character	imal characters. For Hexadecimal, the length should s; for ASCII, the length should be between 8 and 63 should be of ample length and should not be a

- Wireless Network Name Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the pull-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.
- Channel This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- > **Mode -** Select the desired mode. The default setting is 11bgn mixed.
 - **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.

When 11bg mixed mode is selected, only 11bg mixed wireless stations can connect to the Router. It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n wireless stations can connect to the Router.

P Note:

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

- Channel Width Select any channel width from the pull-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.
- Wireless Security Mode This option should be chosen according to the security configuration of the AP you want to access. It is recommended that the security type is the same as your AP's security type.
- > Wireless Password Input the password of your broadcast SSID.
- 2. Click the **Next** button. You will then see the **Finish** page.

If you don't make any change on the **Wireless** page, you will see the **Finish** page as shown below. Click the **Finish** button to finish the **Quick Setup**.

Quick Setup - Finish	
Start >> Working Mode >> W	/ireless >> Finish
Congratulations! This please click other men	device is now connecting you to the Internet. For detail settings, ius if necessary.
	Back Finish

If there is something changed on the Wireless page, you will see the **Finish** page as shown below. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**.

Quick Setup - Finish	
Start >> Working Mode >> W	ireless >> Finish
Congratulations! This please click other men	device is now connecting you to the Internet. For detail settings, us if necessary.
	Back Reboot

3.2.3 Repeater Mode

When you choose **Repeater Mode** on **Working Mode** page, take the following steps:

1. Click **Next**, and then **Wireless Repeater** page will appear.

Quick Setup - Wireless	
Start >> Working Mode >> Wireless	>> Finish
Repeater Mode Setting:	
Repeater Mode:	💿 Universal Repeater 🔿 WDS Repeater
Wireless Name of Root AP:	TP-LINK_Network (also called SSID)
MAC Address of Root AP:	94-0C-6D-2F-3C-BE
	Survey
	You can click the Survey button to scan the network SSIDs, and then choose the target one to setup the connection.
Region:	United States
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.
Wireless Security Mode:	Most Secure(WPA/WPA2-PSK
	All security settings, for example the wireless password should match the Root AP.
Wireless Password:	
	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters. For good security it should be of ample length and should not be a commonly known pharse.
	Back Next

- Repeater Mode In Repeater mode, the wireless repeater relays signal between its stations and the root AP for greater wireless range.
- Universal Repeater In Repeater mode, the AP with WDS disabled will relay data to an associated root AP. AP function is enabled meanwhile.
- **WDS Repeater** In WDS Repeater mode, the AP with WDS enabled will relay data to an associated root AP. AP function is enabled meanwhile.
- > Wireless Name of Root AP The SSID of AP that you want to access.
- > MAC Address of Root AP The MAC address of AP that you want to access.
- > Survey Click this button, you can search the AP which runs in the environment.
- Region Select your region from the pull-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.
- Wireless Security Mode This option should be chosen according to the security configuration of the AP you want to access. It is recommended that the security type is the same as your AP's security type.
- Wireless Password If the AP your router is going to connect need password, you need to fill the password in this blank.

Click Survey button on the Wireless page, and then AP List page will appear. Find the SSID of the Access Point you want to access, and click Connect in the corresponding row. For example, the third item is selected. The target network's SSID will be automatically filled into the corresponding box.

٩P	Count: 16					
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	6C-E8-73-CA-EE-68		68dB	4	None	Connect
2	94-0C-6D-2F-3C-BE	TP-LINK_Network	47dB	4	WPA2-PSK	Connect
3	84-1B-5E-D7-64-F2	TP-LINK_4234CC	31dB	1	WPA2-PSK	Connect
4	4C-60-DE-32-63-8C	TP-LINK_18F710	30dB	11	WPA2-PSK	Connect
5	6C-E8-73-CA-EE-6A	TP-LINK_D0A761	27dB	4	None	Connect
6	14-E6-E4-E3-87-6A	TP-LINK_TEST	16dB	6	WPA2-PSK	Connect
7	78-52-112-02-DD-A1		15dB	8	MPA-P8K	Connect
_	Back Refresh	880880	1068	4	None	Connect

Note:

If you know the SSID of the desired AP, you can also input it into the field "SSID" manually.

3. Click the **Next** button. You will then see the **Finish** page.

Because something has changed on the **Wireless Repeater** page, you will see the **Finish** page as shown below. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**.

Quick Setup - Finish	
Start >> Working Mode >> Wi	reless >> Finish
Congratulations! This of please click other ment	levice is now connecting you to the Internet. For detail settings, us if necessary.
	Back Reboot

3.2.4 Client Mode

When you choose **Client** on **Working Mode** page, take the following steps:

1. Click **Next**, and then **Wireless Client** page will appear.

Quick Setup - Wireless			
Start >> Working Mode >> Wireless >> Finish			
Client Mode Setting:			
Wireless Name of Root AP:	TP-LINK_Network (also called SSID)		
MAC Address of Root AP:	94-0C-6D-2F-3C-BE		
	You can click the Survey button to scan the network SSIDs, and then choose the target one to setup the connection.		
Region:	United States 👻		
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.		
Wireless Security Mode:	Most Secure(WPA/WPA2-PSK		
	All security settings, for example the wireless password should match the Root AP.		
Wireless Password:			
	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters. For good security it should be of ample length and should not be a commonly known pharse.		
	Back Next		

- > Wireless Name of Root AP Enter the SSID that you want to access.
- > MAC Address of Root AP Enter the MAC address of AP that you want to access.
- > **Survey -** Click this button, you can survey the AP which runs in the environment.
- Region Select your region from the pull-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.
- Wireless Security Mode This option should be chosen according to the security configuration of the AP you want to access. It is recommended that the security type is the same as your AP's security type.
- Wireless Password If the AP your router is going to connect need password, you need to fill the password in this blank.
- Click Survey button on the Wireless page, and then AP List page will appear. Find the SSID of the Access Point you want to access, and click Connect in the corresponding row. For example, the third item is selected. The target network's SSID will be automatically filled into the corresponding box.

Α	∖P List					
AP	Count: 16					
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	6C-E8-73-CA-EE-68		68dB	4	None	Connect
2	94-0C-6D-2F-3C-BE	TP-LINK_Network	47dB	4	WPA2-PSK	Connect
3	84-1B-5E-D7-64-F2	TP-LINK_4234CC	31dB	1	WPA2-PSK	Connect
4	4C-60-DE-32-63-8C	TP-LINK_18F710	30dB	11	WPA2-PSK	Connect
5	6C-E8-73-CA-EE-6A	TP-LINK_D0A761	27dB	4	None	Connect
6	14-E6-E4-E3-87-6A	TP-LINK_TEST	16dB	6	WPA2-PSK	Connect
	78-52-82-82-DD-A1		15dB	8	MPA-PBK	Connect
	Back Refresh	003000	10dB		None	Connect

3. Click the **Next** button. You will then see the **Finish** page. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**.

Quick Setup - Finish	
Start >> Working Mode >> \ Congratulations! This please click other men	device is now connecting you to the Internet. For detail settings,
	Back Reboot

3.2.5 WISP Client Router Mode

When you choose WISP Client Router Mode on Working Mode page, take the following steps:

1. Click **Next**, and then **WAN Connection Type** page will appear.

tart >>	Working Mode >> WAN Connection Type >> Wireless >> Finish
'he Quic	k Setup is preparing to set up your connection type of WAN port.
O PPP	oE - Usually for ADSL Modem and you will need a PPPoE username and password from your ISP.
💿 Dyna	amic IP - Usually for Cable Modem and the router will automatically obtain an IP address from the DHCP server.
Stat	ic IP - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.

The Router supports three popular ways **PPPoE**, **Dynamic IP** and **Static IP** to connect to the Internet. To make sure the connection type your ISP provides, please refer to the ISP. Make sure the cable is securely plugged into the WAN port before detection.

PPPoE - For this connection, you will need your account name and password from your ISP. If you have applied ADSL to realize Dial-up service, you should choose this type. Under this condition, you should fill in both the User Name and Password that the ISP supplied. Please note that these fields are case-sensitive.

Quick Setup - PPPoE		
Start >> Working Mode >> WAN C	onnection Type >> Wireles	es >> Finish
User Name:	username	
Password:	•••••	
Confirm Password:	•••••	
	Back	Next

- Dynamic IP Your ISP uses a DHCP service to assign your Router an IP address for connecting to the Internet. When the Router connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. If you choose this type of connection, no configuration should be set and you can go on with the wireless configuration.
- Static IP This type of connection uses a permanent, fixed (static) IP address that your ISP assigned. In this type, you should fill in the IP address, Subnet Mask, Default Gateway, and DNS IP address manually, which are specified by your ISP. Then click Next.

Quick Setup - Static IP		
Start >> Working Mode >> WAN	Connection Type >> Wire	less >> Finish
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	7
Default Gateway:	0.0.0.0	7
Primary DNS:	0.0.0.0	7
Secondary DNS:	0.0.0.0	(Optional)
	Back	Next

2. You can configure the basic settings for the wireless network on this page.

Start >> Working Mode >> WAN C	onnection Type >> Wireless >> Finish
Client Setting	
SSID:	TP-LINK_Network
BSSID:	94-0C-6D-2F-3C-BE Example:00-1D-0F-11-22-33
	Survey
	Key type is selected.
Key type:	WPA-PSK/WPA2-PSK
WEP Index:	1
Auth type:	open 🗸
Password:	1234567890
AP Setting	
Local SSID:	TP-LINK_2046F2
Wireless Security Mode:	Most Secure(WPA/WPA2-PSK
Wireless Password:	123456789
	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length shou be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters. For good security it should be of ample length and should not be a commonly known pharse.

- SSID 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.
- BSSID 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 survey 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.
- Local SSID Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

- Wireless Security Mode You can configure the security settings of your wireless network.
- > Wireless Password Input the password of your Local SSID.
- Click Survey button on the Wireless page, and then AP List page will appear. Find the SSID of the Access Point you want to access, and click Connect in the corresponding row. For example, the third item is selected. The target network's SSID will be automatically filled into the corresponding box. Then click Next.

А	\P List					
AP	Count: 16					
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	6C-E8-73-CA-EE-68		68dB	4	None	Connect
2	94-0C-6D-2F-3C-BE	TP-LINK_Network	47dB	4	WPA2-PSK	Connect
3	84-1B-5E-D7-64-F2	TP-LINK_4234CC	31 dB	1	WPA2-PSK	Connect
4	4C-60-DE-32-63-8C	TP-LINK_18F710	30dB	11	WPA2-PSK	Connect
5	6C-E8-73-CA-EE-6A	TP-LINK_D0A761	27dB	4	None	Connect
6	14-E6-E4-E3-87-6A	TP-LINK_TEST	16dB	6	WPA2-PSK	Connect
	78-52-82-82-DD-A1		1668	0	WPA-P8K	Connact
	Back Refresh	999999	1068		Nona	Connad

4. The **Finish** page is shown as below. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**.

Quick Setup - Finish	
°	N Connection Type >> Wireless >> Finish
please click other menu	evice is now connecting you to the Internet. For detail settings, Is if necessary.
	Back Reboot

P Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- Away from large metal surfaces.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

Chapter 4. Configuration for Wireless Router Mode

This chapter will show each Web page's key functions and the configuration way for Wireless Router Mode of the router.

4.1 Login

After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.

	Status
	Quick Setup
	WPS
١	Working Mode
I	Network
١	Wireless
	рнср
1	USB Settings
	Forwarding
	Security
١	Parental Control
	Access Control
	Advanced Routing
	Bandwidth Control
	IP & MAC Binding
	Dynamic DNS
	System Tools

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 on Wireless Router Mode. All information is read-only.

Status			
Firmware Version:	3.14.4 Build 130128 Rel.36510n		
Hardware Version:	WR710N v1 00000000		
LAN			
MAC Address:	00-1D-0F-01-06-28		
IP Address:	192.168.0.254		
Subnet Mask:	255.255.255.0		
Wireless			
Working Mode:	Wireless Router		
Wireless Radio:	Enable		
Name (SSID):	TP-LINK_2046F2		
Mode:	11bgn mixed		
Channel Width:	Automatic		
Channel:	Auto (Current channel 6)		
MAC Address:	00-1D-0F-01-06-28		
WDS Status:	Disable		
WAN			
MAC Address:	00-1D-0F-01-06-29		
IP Address:	0.0.0.0	Dynamic IP	
Subnet Mask:	0.0.0.0		
Default Gateway:	0.0.0.0	WAN port is unplugged!	
DNS Server:	0.0.0.0 , 0.0.0.0		
Traffic Statistics			
	Received	Sent	
Bytes:	0	0	
Packets:	0	0	
System Up Time:	0 days 02:50:11	Refresh	

- **Firmware Version -** The version information of the Router's firmware.
- > Hardware Version The version information of the Router's hardware.
- LAN This field displays the current settings or information for the LAN, you can configure them in the Network>LAN page.
 - MAC Address The physical address of the Router, as seen from the LAN.
 - IP Address The LAN IP address of the Router.
 - Subnet Mask The subnet mask associated with LAN IP address.

- Wireless This field displays basic information or status for wireless function, you can configure them in the Wireless > Wireless Settings page.
 - Working Mode The current wireless working mode in use.
 - Wireless Radio Indicates whether the wireless radio feature of the AP is enabled or disabled.
 - Name (SSID) The SSID of the AP.
 - **Mode** The current wireless mode which the Router works on.
 - Channel Width The current wireless channel width in use.
 - Channel The current wireless channel in use.
 - MAC Address The physical address of the Router, as seen from the WLAN.
 - WDS Status The status of WDS connection.
- WAN This field displays the current settings or information for the WAN, you can configure them in the Network > WAN page.
 - MAC Address The physical address of the WAN port, as seen from the Internet.
 - **IP Address** The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to the Internet.
 - Subnet Mask The subnet mask associated with the WAN IP Address.
 - Default Gateway The Gateway currently used by the Router is shown here. When you use Dynamic IP as the connection Internet type, the Renew button will be displayed here. Click the Renew Button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address, Release button will be displayed here. Click the Release button to release the IP address the Router has obtained from the ISP.
- DNS Server The DNS (Domain Name System) server IP addresses currently used by the Router.
- > Traffic Statistics The Router's traffic statistics.
 - Received (Bytes) Traffic that counted in bytes has been received out from the WAN port.
 - Received (Packets) Traffic that counted in packets has been received out from the WAN port.
 - Sent (Bytes) Traffic that counted in bytes has been sent out from the WAN port.
 - Sent (Packets) Traffic that counted in packets has been sent out from the WAN port.
- **System Up Time -** The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

4.4 WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to an existing network quickly by function. The WPS function is only available when the Operation Mode is set to Access Point. Select menu "WPS", you will see the next screen shown below.

WPS (Wi-Fi Protected Se	etup)
WPSStatus:	Enabled Disable WPS
Current PIN:	12345670 Restore PIN Gen New PIN Disable PIN of this Device
Add A New Device:	Add Device

- > WPS Status To enable or disable the WPS function here.
- Current PIN The current value of the device's PIN is displayed here. The default PIN of the device can be found in the label or User Guide.
- > **Restore PIN -** Restore the PIN of the device to its default.
- Gen New PIN Click this button, and then you can get a new random value for the device's PIN. You can ensure the network security by generating a new PIN.
- Disable PIN of this Device WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.
- Add Device You can add a new device to the existing network manually by clicking this button.

To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and device 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.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

Step 1: Keep the WPS Status as **Enabled** and click the **Add Device** button, then the following screen 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

- Step 2: Choose "**Press the button of the new device in two minutes**" and click **Connect**.
- Step 3: For the configuration of the wireless adapter, please choose "**Push the button on my** access point or wireless router" in the configuration utility of the WPS as below, and click **Connect**.

TP-LIN	К				- ×
	WPS		4	2	
Status	WPS	Network	Profile	Advanced	
● Push the	bose a method to j e button on my ac e PIN of my acces	on will guide you th oin a wireless netw cess point or wirele ss point or wireless e into my access p	vork: ess router. router.	g your wireless network outer.	c. Connect

The WPS Configuration Screen of Wireless Adapter

Step 4: Wait for a while until the next screen appears. Click **OK** to complete the WPS configuration.



The WPS Configuration Screen of Wireless Adapter

Method Two: Enter the PIN into my AP

Step 1: For the configuration of the wireless adapter, please choose "Enter the PIN of this device into my access point or wireless router" in the configuration utility of the WPS as below, and click Connect.

	к				
	P s		-	N. S.	
Status	WPS	Network	Profile	Advanced	
Push the Enter the Enter the Enter the	ose a method to e button on my av e PIN of my acce	tion will guide you th join a wireless netw ccess point or wireless ss point or wireless ce into my access p	ork: ess router. router.	g your wireless network	
					Connect

The WPS Configuration Screen of Wireless Adapter

P Note:

In this example, the default PIN code of this adapter is 16952898 as the above figure shown. Step 2: Keep the WPS Status as **Enabled** and click the **Add Device** button. Step 3: Choose "Enter the new device's PIN" and enter the PIN code (take 16952898 for example) of the wireless adapter in the field after PIN as shown in the figure below. Then click Connect.

Add A New Device
Enter the new device's PIN.
PIN: 16952898
Press the button of the new device in two minutes.
Back Connect

Method Three: Enter the PIN from my AP

- Step 1: Get the Current PIN code of the AP (each AP has its unique PIN code. Here takes the PIN code 12345670 of this AP for example).
- Step 2: For the configuration of the wireless adapter, please choose "Enter the PIN of my access point or wireless router" in the configuration utility of the WPS as below, and enter the PIN code of the AP into the field after "Access Point PIN". Then click Connect.

P-LIN Reliable Choice	к				F
Status	WPS	Network	Profile	Advanced	
(((WPS))	This applicat	tion will guide you th	nrough configuring	g your wireless network	¢
		join a wireless netw ccess point or wirele			
	e PIN of my acce	ss point or wireless	router.		
© Enter the	PIN of this devic	ce into my access p	point or wireless r	outer	
				0	Connect

The WPS Configuration Screen of Wireless Adapter

P Note:

The default PIN code of the AP can be found in its label or the WPS configuration screen.

You will see the following screen when the new device has successfully connected to the network.

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

Note:

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

4.5 Working Mode

The Router supports five operation mode types: Wireless Router, Access Point, Repeater, Client and Wireless Client Router. Please select one you want. Click Save to save your choice.

Wireless Router	- Enable multiple users to share Internet connection via ADSL/Cable Modem
🔿 Access Point	- Transform your existing wired network to a wireless network
🔿 Repeater	- Extend your existing wireless coverage by relaying wireless signal
🔿 Client	- Acting as a "Wireless Adapter" to connect your wired devices (e.g. Xbox/PS3) to a wireless network
🔿 WISP Client Route	 Enable multiple users to share Internet connection from WISP

- Wireless Router The wireless Router Mode. In this mode, the device enables multi-user to share Internet via DSL/Cable Modem. The only wired port works as WAN.
- > Access Point The wireless access point mode.
- > Repeater The wireless Repeater Mode. It could extend the range of wireless network.
- Client The Client Mode. The computer connected by Ethernet could get access to an AP by Client mode.
- WISP Client Router In this mode, the device enables multiple users to share Internet connection from WISP.

4.6 Network

Network	
- WAN	
- MAC Clone	
- LAN	

There are three submenus under the Network menu: **WAN**, **MAC Clone** and **LAN**. Click any of them, and you will be able to configure the corresponding function.

4.6.1 WAN

Choose menu "**Network** \rightarrow **WAN**", and then 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 follow:

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 WAN port is unplugged!
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
	Use These DNS Servers
Primary DNS:	0.0.0
Secondary DNS:	0.0.00 (Optional)
occontary bito.	(opening)
Host Name:	TL-WR710N
	Get IP with Unicast DHCP (It is usually not required.)
	Save

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.

P 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**, **Default Gateway** and **DNS** setting, select **Static IP**. The Static IP settings page will appear.

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

- > 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 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. Then you should enter the following parameters:

WAN	
WAN Connection Type:	PPPoE/Russia PPPoE 💌 🛛 Detect
PPPoE Connection:	
User Name:	username
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)
	O Connect Manually
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Disconnected!
	Save Advanced

- > User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Confirm Password Enter again the Password provided by your ISP to ensure the password you entered is correct.
- 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).

PNote:

Only when you have configured the system time on "System Tools \rightarrow Time" 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 below will then appear:

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

- 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.

4. If your ISP provides BigPond Cable connection, please select **BigPond Cable** option. Then you should enter the following parameters:

WAN	
WAN Connection Type:	BigPond Cable
User Name:	username
Password:	
Auth Server:	sm-server
Auth Domain:	
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
Connection Mode:	Onnect 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 Disconnected!
	Save

- > 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,
- 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.
- 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. Then you should enter the following parameters:

WAN	
WAN Connection Type:	L2TP/Russia L2TP 💌
User Name:	username
Password:	
	Connect Disconnect Disconnected!
	💿 Dynamic IP y 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):	1460 (The default is 1460, do not change unless necessary.)
Max Idle Time:	15 minutes (0 means remain active at all times.)
Connection Mode:	Connect on Demand
	Connect Automatically
	Connect Manually
	Save

- > 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:

WAN		
WAN Connection Type:	PPTP/Russia PPTP 🔽	
User Name: Password:	usemame Connect Disconnected!	
	⊙ Dynamic IP _ Static IP	
Server IP Address/Name:		
IP Address: Subnet Mask:	0.0.0.0	
	0.0.0.0	
Gateway: 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): Max Idle Time:	1420(The default is 1420, do not change unless necessary.)15minutes (0 means remain active at all times.)	
Connection Mode:	 Connect on Demand Connect Automatically 	
	Connect Manually	
	Save	

- 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.

4.6.2 MAC Clone

Choose menu "**Network** \rightarrow **MAC Clone**", and then you can configure the WAN MAC address on the screen below:

MAC Clone			
WAN MAC Address:	00-1D-0F-01-06-29	Restore Factory MAC	
Your PC's MAC Address:	6C-62-6D-F7-31-8D	Clone MAC Address	
	Cara		
	Save		

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 WAN 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 To button and this MAC address will fill in the WAN MAC Address field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

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

P Note:

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

2. If you change WAN MAC Address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

4.6.3 LAN

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

LAN		
MAC Address:	00-1D-0F-01-06-28	
IP Address:	192.168.0.254	
Subnet Mask:	255.255.255.0 💌	
IGMP Proxy:	Enable 💌	
Note: IGMP(Internet Group Management Protocol) works for IPTV multicast stream. The device supports both IGMP proxy with enabled or disable option and IGMP snooping.		
	Save	

- MAC Address The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- IP Address Enter the IP address of your Router in dotted-decimal notation (factory default: 192.168.0.254).
- Subnet Mask An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- IGMP Proxy The Internet Group Management Protocol (IGMP) feature allows your devices in LAN can watch TV.
- P Note:
- 1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
- 2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.7 Wireless

Wireless
- Wireless Settings
- Wireless Security
- Wireless MAC Filtering
- Wireless Advanced
- Wireless Statistics

There are five submenus under the Wireless menu: Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced and Wireless Statistics. Click any of them, and you will be able to configure the corresponding function.

4.7.1 Wireless Settings

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

Wireless Settings		
Wireless Network Name:	TP-LINK_2046F2	(Also called the SSID)
Region:	United States 💌	
Warning:	Ensure you select a correct country to cor Incorrect settings may cause interference	
Mode:	11bgn mixed	
Channel Width:	Auto 🛩	
Channel:	Auto 💙	
	🔽 Enable Wireless Router Radio	
	Enable SSID Broadcast	
	Enable WDS Bridging	
	Save	

- Wireless Network Name Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the pull-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.

- > **Mode -** Select the desired mode. The default setting is 11bgn mixed.
- **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.

When 11bg mixed mode is selected, only 11bg mixed wireless stations can connect to the Router. It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n wireless stations can connect to the Router.

P Note:

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

- Channel Width Select any channel width from the pull-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.
- Channel This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Enable Wireless Router Radio The wireless radio of the Router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Router. Otherwise, wireless stations will not be able to access the Router.
- Enable SSID Broadcast If you select the Enable SSID Broadcast checkbox, the wireless router will broadcast its name (SSID) on the air.
- Enable WDS You can select 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 below. Make sure the following settings are correct.

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

- 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.
- BSSID (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 survey the AP which runs in the current channel.

- Security Options 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.

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

P Note:

- 1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
 - Near the center of the area in which your wireless stations will operate.
 - In an elevated location such as a high shelf.
 - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
 - Away from large metal surfaces.
- 2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

4.7.2 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).

Wireless Security		
O Disable Security		
WPA/WPA2 - Personal(Recommendation)	nded)	
Version:	Automatic(Recomm	ended) 🔽
Encryption:	Automatic(Recomm	ended) 🔽
Wireless Password:		
	(You can enter ASCII cl	haracters between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period:	0 Sec	onds (Keep it default if you are not sure, minimum is 30, 0 means no updat
O WPA/WPA2 - Enterprise		
Version:	Automatic 🔽	
Encryption:	Automatic 🛛 👻	
Radius Server IP:		
Radius Port:	1812 (1-65535	5, 0 stands for default port 1812)
Radius Password:		
Group Key Update Period:	0 (in s	econd, minimum is 30, 0 means no update)
○ WEP		
Туре:	Automatic 🛛 👻	
WEP Key Format:	Hexadecimal 💌	
Key Selected	WEP Key	Кеу Туре
Key 1: 💿		Disabled 💌
Key 2: 🕓		Disabled 💌
Key 3: 🔵		Disabled 💌
Key 4: 🕓		Disabled 💌
	Save	

- 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. But it's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - 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-PSK/WPA2-PSK** radio button and choose TKIP encryption, you will find a notice in red.

WPA/WPA2 - Personal(Recommended)				
Version:	Automatic(Recommended) 💌			
Encryption:	ТКІР			
Wireless Password:				
	(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 this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.			

- > WPA/WPA2-Enterprise It's based on Radius Server.
 - Version you can choose the version of the WPA security from the pull-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 Automatic, TKIP or AES.
 - Radius Server IP Enter the IP address of the Radius server.
 - Radius Port Enter the port that Radius server used.
 - 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.
 - **Type** you can choose the type for the WEP security on the pull-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 (Password) 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.

4.7.3 Wireless MAC Filtering

Choose menu "Wireless \rightarrow Wireless MAC Filtering", and then you can control the wireless access by configuring the Wireless MAC Filtering function.

Wireless MAC Filtering			
Wireless MAC Filtering:	Enabled 🗌	Disable	
Filtering Rules			
Deny the stations specified by any	enabled entries i	n the list to access.	
 Allow the stations specified by any 	renabled entries i	n the list to access.	
ID MAC Address	Status	Description	Modify
Add New Enable All Dis	sable All	Delete All	
PI	revious	Next	

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

- > MAC Address The wireless station's MAC address that you want to access.
- > Status The status of this entry, either Enabled or Disable.
- **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:

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

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.

- 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** pull-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 **Enabled** button to enable this function.
- 2. Select the radio button "Allow the stations specified by any enabled entries in the list to access" for **Filtering Rules**.
- 3. Delete all or disable all entries if there are any entries already.
- 4. Click the Add New... button.
 - 1) Enter the MAC address 00-0A-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** pull-down list.
 - 4) Click the **Save** button.
 - 5) Click the **Back** button.

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

Filtering Rules							
Deny the stations specified by any enabled entries in the list to access.							
 Allow the stations specif 	ied by any enabled enti	ries in the list to access.					
-							
MAC Address	Status	Description	Modify				
00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete				
	 Deny the stations specifi Allow the stations specifi MAC Address	 Deny the stations specified by any enabled entr Allow the stations specified by any enabled entr MAC Address Status 	 Deny the stations specified by any enabled entries in the list to access. Allow the stations specified by any enabled entries in the list to access. MAC Address Status Description				

4.7.4 Wireless Advanced

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

less Advanced				
Transmit Power:	High	*		
Beacon Interval :	100	(40-1000)		
RTS Threshold:	2346	(256-2346)		
Fragmentation Threshold:	2346	(256-2346)		
DTIM Interval:	1	(1-255)		
	🔽 Enable	WMM		
	🔽 Enable	Enable Short GI		
	📃 Enable	AP Isolation		
	Save	;		

- 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 1-255 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 enabled.
- Enable Short GI This function is recommended for it will increase the data capacity by reducing the guard interval time.
- Enable AP Isolation This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

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.

4.7.5 Wireless Statistics

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

Wire	Wireless Statistics								
	Curre	ent Connected Wireless	Stations numbers: 1	Refresh					
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure				
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	Allow				
		Previous	Next						

- > 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.
- > Configure The button is used for loading the item to the Wireless MAC Filtering list.
 - Allow If the Wireless MAC Filtering function enable, allow the station to access.
 - Deny If the Wireless MAC Filtering function enable, deny the station to access.

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 DHCP

DHCP	
- DHCP	Settings
- DHCP	Client List
- Addre	ess Reservation

There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

4.8.1 DHCP Settings

Choose menu "**DHCP** \rightarrow **DHCP** Settings", and then you can configure the DHCP Server. 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 💿 Enab	e
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:	192.168.0.254	(Optional)
Default Domain:		(Optional)
Primary DNS:	0.0.0.0	(Optional)
Secondary DNS:	0.0.0.0	(Optional)
	Save	

- 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 LAN port of the Router. The default value is 192.168.0.254.
- > 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. 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".

4.8.2 DHCP Client List

Choose menu "DHCP \rightarrow DHCP Client List", and then you can view the information about the clients attached to the Router.

C	DHCP Client List						
ID	Client Name	MAC Address	Assigned IP	Lease Time			
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47			
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32			
	Refresh						

- > 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.

4.8.3 Address Reservation

Choose menu "DHCP \rightarrow Address Reservation", and then you can view and add a reserved address for clients via the next screen. 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.

Address Reservation						
ID 1	MAC Address 00-11-22-33-44-AA	Reserved IP Address 192.168.0.169	Status Enabled	Modify <u>Modify Delete</u>		
Add New Enable All Disable All Delete All						
		Previous Next				

- > 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.
- > **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

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

Add or Modify an Addres	s Reservation Entry
MAC Address: Reserved IP Address: Status:	Enabled V
	Save Back

To modify or delete an existing entry:

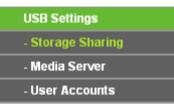
- 1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
- 2. Modify the information.
- 3. Click the **Save** button.

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.

4.9 USB Settings



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

4.9.1 Storage Sharing

Choose menu "**USB Settings**→**Storage Sharing**", you can configure a USB disk drive attached to the router and view volume and share such properties as share name, capacity, used space, and free space on this page as shown below.

Storage	Sharing					
	Service Status:	Started	Stop shared storage wi	th password		
Volume	Capacity	Used	Free	Use%	Shared	
volume1	1.9 GB	1.3 GB	626 MB	67%	Disable	
		Eject Dis	sk Resc	an		

- Service Status Indicates the Network Sharing service's current status. You can click the
 Start button to start the Storage Sharing service and click the Stop button to stop it.
- Volume The volume name of the USB drive the users have access to. Volume 1-8 is mapping to USB port1, and Volume 9-16 is mapping to USB port2.
- > **Capacity -** The storage capacity of the USB driver.
- > **Used -** The used space of the USB driver.
- > **Free -** The available space of the USB driver.
- > **Use% -** The percentage of the used space.
- Shared Indicates the shared or non-shared status of the volume. When the volume is shared, you can click the Disable to stop sharing the volume; when volume is non-shared, you can click the Enable button to share the volume.

Click the Start button to start the Network Sharing service.

Click the Stop button to stop the Network Sharing service.

Click the **Eject Disk** button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Message f	rom webpage		×
?	This operation will disable Media Server.	Are you sure to continue?	
		ОК	Cancel

Click the **Rescan** button to start a new scan.

Follow the instructions below to set up your router as a file server:

- 1. Plug an external USB hard disk drive or USB flash drive into this router.
- 2. Click the **Rescan** button to find the USB drive that has been attached to the router.
- 3. Click the **Start** button to start the Storage Sharing service.
- 4. Click the **Enable** button under **Shared** to enable the disk to share.
- 5. Click the **Open the disk** to visit the sharing disk.

P Note:

- 1. The router can automatically locate new USB drive. But to display the information about your USB device, you need to click the **Rescan** button manually.
- 2. The new settings will not take effect until you restart the service.
- 3. To unplug the USB drive, click **Eject Disk** button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.
- 4. Mounted volumes of each USB port are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.
- 5. If you change the storage settings during the storage connection is established, then the changes will not take effect until the router or the client is rebooted.

4.9.2 Media Server

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

	Server Name: erver Status:	TP-LINK_010628 Stopped Start	
Auto-scan ever	y 2 hours 🔽	Scan All	

- Server Name The name of this Media Server.
- Server Status Indicates the Media Server's current status, started or stopped. You can click the Start button to start the Media Server and click the Stop button to stop it.
- > **Name** The display name of this folder.
- > File System The file system type on the partition can be FAT32 or NTFS.
- > Folder The real full path of the specified folder.
- > Delete You can delete the share folder by click Delete.

To set up your media server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router, and then the screen will appear as shown below.

Wedia Serve	r Setting				
	Server Name: Server Status:	TP-LINK_010628 Stopped Start			
Auto-scan eve		Scan All			
Name	File System		Folder	Delete	

2. Click the **Start** button to start the media server, and then the screen will appear as shown below.

Media Server Setting				
Server Name: Server Status:	TP-LINK_010628 Started Stop			
Auto-scan every 2 hours	Scan All			
Name File Syste	em	Folder	Delete	

3. Click the **Add share folder** button to specify a folder as the search path of media server. The screen will then appear as shown below.

Add New Folder	
Display Name: Partition: Folder Location:	video Share entire partition /my share
Select	Folder
0	photo
۲	video
	Save Back Current No. 1 v page

- > **Display Name** You can enter a display name for the share folder.
- Share entire partition Choose this option and then the folders contained in this partition will all be shared.
- > Folder Location Displays the location of this folder.
- > **Select** Check the radio button to select the folder to share.
- > **Folder** Displays folders that are in current path.
- > **Upper** Click this button to get into the upper folder.
- Save Click this button to save your settings and the page will be redirected to the media server configuration page.
- Back Click this button to discard the settings and just go to the media server configuration page.
- 4. Click the **Scan All** button to scan all the share folders immediately. You can also select the **Auto-scan**, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

P Note:

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

4.9.3 User Accounts

You can specify the user name and password for Storage Sharing users on this page. **Storage Sharing** users can use Internet Explorer to access files on the USB drive.

There are two default user accounts that can access the Storage Sharing. They are Administrator and Guest. Administrator has read/write access to Storage Sharing while Guest has read-only access to Storage Sharing.

User Account Ma	anagement			
Add New User				
User Name	Password	Storage Authority	Modify	
admin	admin	Read and Write	yes	Edit
guest	guest	Read Only	no	<u>Edit</u>
Save				

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

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

- 1. Click Add New User button, and the screen will appear as shown below.
- 2. Self-define a User Name.
- 3. Enter the password in the **Password** field.
- 4. Choose the Storage Authority from the drop-down list, **Read and Write** or **Read Only**.

Add or Modify User Acco	unt
User Name:	admin2
Password:	admin
Storage Authority:	Read and Write 💌
	Save Back

- User Name Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.
- Password Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- Storage Authority Choose Read and Write or Read Only from the drop-down list to assign access authority of Storage Sharing to the user.
- > Save You can click the Save button to save your settings.
- Back You can click the Back button to discard the settings and just go to the media server configuration page.

P Note:

Please restart the service for the new settings to take effect.

If you cannot use the new user name and password to access the shares, press **Windows logo + R** to open the Run dialog box and type **net use \\192.168.0.254 /delete /yes** and press Enter. (192.168.0.254 is your router's LAN IP address. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.0.254 to 192.168.1.254 to avoid IP conflict; in this case, please try **net use \\192.168.1.254 /delete / yes**.)

4.10 Forwarding

Forv	varding	
- Vir	tual Servers	
- Po	rt Triggering	
- DM	IZ	
- UP	nP	

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

4.10.1 Virtual Servers

Choose menu "Forwarding \rightarrow Virtual Servers", and then you can view and add virtual servers. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the 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 be changed when using the DHCP function.

Virtual Servers					
ID Service Port	Internal Port	IP Address	Protocol	Status	Modify
Add New	Enable All Disable All	Delete All			
	Previous	Next			

- Service Port The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- 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 providing 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, either Enabled or Disabled.
- > **Modify -** To modify or delete an existing entry.

To setup a virtual server entry:

- 1. Click the Add New... button, the next screen will pop-up as shown below.
- Select the service port you want to use from the Common Service Port list. If the Common Service Port list does not have the service that you want to use, type the service port number or service port range in the Service Port box.
- 3. Type the IP Address of the computer in the **IP Address** box.
- 4. Select the protocol used for this application, either TCP, UDP, or All.
- 5. Select the **Enabled** to enable the virtual server.
- 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 it blank)	
IP Address:		
Protocol:	All	
Status:	Enabled 💌	
Common Service Port:	Select One	
	Save Back	

Note:

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

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.

P 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.

4.10.2 Port Triggering

Choose menu "Forwarding \rightarrow Port Triggering", and then you can view and add port triggering. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Port Triggeri	ng			
ID Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status Modify
Add New	Enable All Disa	ble All Delete All		
	Pre	vious Next		

Once the Router is configured, the operation is as follows:

- 1. A local host makes an outgoing connection 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.
- 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 Ports 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 that triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- Incoming Protocol The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the Router).
- > Status The status of this entry, either Enabled or Disabled.
- > **Modify -** To modify or delete an existing entry.

To add a new rule, follow the steps below:

- 1. Click the **Add New...** button, the next screen will pop up as shown below.
- 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 **AII**.
- 4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **AII**.
- 5. Select **Enabled** in **Status** field.
- 6. Click the **Save** button to save the new rule.

Add or Modify a Port Trig	gering Entry
Trigger Port: Trigger Protocol:	
Incoming Ports:	
Incoming Protocol: Status:	All V Enabled V
Common Applications:	Select One
	Save Back

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.

P Note:

- 1. When the trigger connection is released, the corresponding opening ports will be closed.
- 2. Each rule is allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
- 3. Incoming Port Range cannot overlap each other.

4.10.3 DMZ

Choose menu "Forwarding \rightarrow DMZ", and then you can view and configure DMZ host. 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. DMZ host forwards all the ports at the same time. 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	
Current DMZ Status:	🔿 Enable 💿 Disable
DMZ Host IP Address:	0.0.0.0
	Save

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

- 1. Check the **Enable** radio button.
- 2. Enter the IP Address of a local host in the DMZ Host IP Address field.
- 3. Click the **Save** button.

P Note:

After you set the DMZ host, the firewall related to the host will not work.

4.10.4 UPnP

Choose menu "Forwarding \rightarrow UPnP", and then you can view the information about UPnP (Universal Plug and Play). The 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.

UPn	P					
Current l	JPnP Status:	Enabled		Disable		
Curr	ent UPnP Setting	gs List				
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
		Refresh				

- Current UPnP Status UPnP can be enabled or disabled by clicking the Enable or Disable button.
- > Current UPnP Settings List This table displays the current UPnP information.

- App Description The description provided by the application in the UPnP request.
- External Port The external port the Router opens for the application.
- **Protocol** The type of protocol the Router opens for the application.
- Internal Port The Internal port the Router opens for local host.
- IP Address The IP address of the UPnP device that is currently accessing the Router.
- **Status** The status of the port is displayed here. "Enabled" means that the port is still active. Otherwise, the port is inactive.

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

4.11 Security

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

There are four submenus under the Security menu: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

4.11.1 Basic Security

Choose menu "Security → Basic Security", you can configure the basic security.

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

- 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 IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.
 - **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, keep the default, **Enable**.
 - L2TP Passthrough Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **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, keep the default, **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, keep the default **Enable**.
 - **TFTP ALG** To allow TFTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - H323 ALG To allow Microsoft NetMeeting clients to communicate across NAT, keep the default Enable.

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

4.11.2 Advanced Security

Choose menu "Security → Advanced Security", you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

TL-WR710N Wi-Fi Pock

Wi-Fi Pocket Router/AP/TV Adapter/Repeater

Advanced Security	
Packets Statistics Interval (5 ~ 60):	10 Seconds
DoS Protection:	⊙ Disable O Enable
Enable ICMP-FLOOD Attack Filtering	
ICMP-FLOOD Packets Threshold (5 \sim 3600):	50 Packets/Secs
Enable UDP-FLOOD Filtering	
UDP-FLOOD Packets Threshold (5 \sim 3600):	500 Packets/Secs
Enable TCP-SYN-FLOOD Attack Filtering	
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600):	50 Packets/Secs
Ignore Ping Packet from WAN Port to Router	
Forbid Ping Packet from LAN Port to Router	
Save Blocked DoS Host List	

- 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.

P Note:

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

4.11.3 Local Management

Choose menu "Security \rightarrow Local Management", you can configure the management rule. 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 a	allowed to access the Router's Web-Based Utility
Only the PCs listed can bro	wse the built-in web pages to perform Administrator tasks
MAC 1:	
MAC 2:	
MAC 3:	
MAC 4:	
Your PC's MAC Address:	6C-62-6D-F7-31-8D Add
	Save

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.

P Note:

If your PC is blocked but you want to access the Router again, press and hold the WPS button for more than 5 seconds to reset the Router to factory defaults.

4.11.4 Remote Management

You can configure the Remote Management function on this page. 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	

- 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 interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65535, 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. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will 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 you use port number 8080, enter in your browser: http://202.96.12.8:8080. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's Web-based utility.

Note:

Be sure to change the router's default password to a very secure password.

4.12 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control. 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 t	e able to access the Inter	net.			
Parental Control:	💿 Disable _O Enab	le			
MAC Address of Parental PC:					
MAC Address of Your PC:	6c-62-6d-17-31-8d	Сору Т	o Above		
	Save				
ID MAC address Webs	ite Description		Schedule	Status	Modify
Add New Enable All	Disable All De	ete All			
	Previous	Next	Current No. 1	🖌 Page	

- 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".
- > Modify Here you can edit or delete an existing entry.

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 below.
- 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 (e.g.www.google.com) will be allowed.
- 5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. 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 return to the previous page.

Add or Modify Parental Co	antrol Entry
Add of Modily Parental Co	na or Enary
The Schedule is based on the time of t	the Router. The time can be set in "System Tools -> <u>Time settings</u> ".
MAC Address of Children's PC:	
All MAC Address in Current LAN:	Please Select
Website Description:	
Allowed Website Name:	
Effective Time:	Anytime V
	The time schedule can be set in "Access Control -> Schedule"
Status:	
or and of	
	Save Back

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.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 Restriction → 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:
 - Click Add New... button.
 - Enter 00-11-22-33-44-AA in the MAC Address of Child PC field.
 - Enter "Allow Google" in the Website Description field.

- Enter "www.google.com" in the Allowed Domain Name field.
- Select "Schedule_1" you create just now from the Effective Time drop-down list.
- 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.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-BB	Allow Google	Schedule_1	~	Edit Delete
	Add New Enable All Disable All Delete A				
		Previous Nex	Current No. 1	🖌 Page	

4.13 Access Control

Access Co	ontrol
- Rule	
- Host	
- Target	
- Schedule	•

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

4.13.1 Rule

Choose menu "Access Control→ Rule", you can view and set Access Restriction rules.

A	Access Control Rule Management					
_	Enable Internet	Access Control				
De	fault Filter Poli	cy				
0	Allow the pack	ets specified by any en	abled access control pol	icy to pass through the F	Router	
۲	Deny the packe	ets specified by any en	abled access control pol	icy to pass through the F	louter	
			Save			
		_				
ID	Rule Name	Host	Target	Schedule	Status	Modify
Se	tup Wizard					
A	dd New	Enable All	isable All Delet	e All		
	Move		ID To			
			Previous	Next Current No	. 1 🔽 Page	

- Enable Internet Access Control Select the check box to enable the Internet Access Restriction 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.
- Action Here displays the action the Router takes to deal with the packets. It could be Allow or Deny. Allow means that the Router permits the packets to go through the Router. Deny means that the Router rejects the packets to go through the Router.
- Status This field displays the status of the rule. Enabled means the rule will take effect, Disabled means the rule will not take effect.
- > **Modify -** Here you can edit or delete an existing rule.

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

- 1. Click the Add New... button and the next screen will pop up as shown below.
- 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 Action field, select Deny or Allow.
- 7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
- 8. 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.

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

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

Add Internet Access Cont	rol Entry
Rule Name:	
Host:	Click Here To Add New Host List.
Target:	Any Target 👻 Click Here To Add New Target List.
Schedule:	Anytime 🔽 Click Here To Add New Schedule.
Status:	Enabled 💌
	Save Back

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 "Access Control → Host" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
- Click "Access Control → Target" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
- Click "Access Control → Schedule" in the left to enter the Schedule Settings 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.
- 4. Click "Access Control → Rule" in the left to return to the Access Restriction Rule Management page. Select "Enable Internet Access Restriction" and choose "Deny the packets not specified by any access Restriction policy to pass through the Router".
- 5. Click Add New... button to add a new rule as follows:
 - In **Rule Name** field, create a name for the rule. Note that this name should be unique, for example Rule_1.
 - In **Host** field, select Host_1.
 - In **Target** field, select Target_1.
 - In **Schedule** field, select Schedule_1.
 - In Action field, select Allow.
 - In **Status** field, select Enabled.
 - Click **Save** to complete the settings.

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

ID	Rule Name	Host	Target	Schedule	Status	Modify
1	Rule_1	Host 1	<u>Target 1</u>	Schedule 1	~	Edit Delete
Se	etup Wizard					
Ē	Add New	Enable All Di	sable All Delete	e All		

4.13.2 Host

Choose menu "Access Control \rightarrow Host", you can view and set a Host list. The host list is necessary for the Access Restriction Rule.

Но	ost Settings		
	Host Description	Information	Modify
		Previous	Next Current No. 1 🔽 Page

- > 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.
 - If you select IP Address,
 - 1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In LAN IP Address field, enter the IP address.

Add or Modify a Host Ent	ry
Mode: Host Description: LAN IP Address:	IP Address
	Save Back

- If you select MAC Address,
 - 1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In MAC Address field, enter the MAC address.

Add or Modify a Host Entry		
Mode: Host Description: MAC Address:	MAC Address	
	Save Back	

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 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, you should first follow the settings below:

- 1. Click **Add New...** button 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.

Host Settings		
ID Host Description 1 Host_1 Add New	Information MAC: 00-11-22-33-44-AA Delete All	Modify Edit Delete
	Previous Next C	current No. 📋 🔽 Page

4.13.3 Target

Choose menu "Access Control \rightarrow Target", you can view and set a Target list. The target list is necessary for the Access Restriction Rule.

Target Settings		
ID Target Description	Information	Modify
Add New Delete All		
	Previous	Next Current No. 1 🗸 Page

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.
 - If you select IP Address,
 - 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.

Add or Modify an Access	Target Entry
Mode:	IP Address
Target Description:	
IP Address:	·
Target Port:	
Protocol:	All 💌
Common Service Port:	Please Select 👻
	Save Back

- If you select Domain Name,
 - 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 Google) in the blank. Any domain name with keywords in it (e.g.<u>www.google.com</u>) will be blocked or allowed. You can enter 4 domain names.

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

3. 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 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 **www.google.com** only, you should first follow the settings below:

- 1. Click Add New... button 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.google.com.
- 5. Click **Save** to complete the settings.

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

Т	arget Settings		
ID 1 - A	Target Description Target_1 Add New Delete All	Information www.google.com	Modify Edit Delete
		Previous N	ext Current No. 1 🗸 Page

4.13.4 Schedule

Choose menu "Access Control → Schedule", you can view and set a Schedule list. The Schedule list is necessary for the Access Restriction Rule.

Sch	edule Settings				
ID Add	Schedule Description	Day	Time	Modify	
	[Prevoius	Next Curr	rent No. 👖 🔽 Page	

- 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 and the next screen will pop up as shown below.
- 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 return to the previous page.

Advance Schedule Settin	Advance Schedule Settings			
Note: The Schedule is based on the	ime of the Router.			
Schedule Description:				
Day:	💿 Everyday i 🔿 Select Days			
	🗸 Mon 🗸 Tue 🗸 Wed 🗸 Thu 🗸 Fri 🗸 Sat 🗸 Sun			
Time:	all day-24 hours: 🔽			
Start Time:	(HHMM)			
Stop Time:	(HHMM)			
	Save Back			

For example: If you desire to restrict the internet activities of 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**, you should first follow the settings below:

- 1. Click Add New... button 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.

S	chedule Settings			
ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete
Æ	Add New Delete All			
	(Prevoius	Next Current No. 1 🔽 P	age

4.14 Advanced Routing

Advanced Routing	
- Static Routing List	
- System Routing Table	

There are two submenus under the Network menu: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

4.14.1 Static Routing List

Choose menu "**Static Routing**", and you can configure the static route. A static route is a pre-determined path that network information must travel to reach a specific host or network.

Stati	c Routing				
ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify
Add I	New Enable All	Disable All Dele	ete All		
	(Previous Ne	ext		

To add static routing entries, follow the steps below.

1. Click Add New..., you will see the following screen.

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

- 2. Enter the following data.
 - Destination Network The Destination IP Address is the address of the network or host that you want to assign to a static route.
 - Subnet Mask The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.
 - 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.

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.

4.14.2 System Routing Table

Choose menu "Advanced Routing \rightarrow System Routing Table", and you can 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	system Routing Table			
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
2	239.0.0.0	255.0.0.0	0.0.0.0	LAN & WLAN
		Refresh		

- Destination Network The Destination IP Address 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 whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet).

Click the **Refresh** button to refresh the data displayed.

4.15 Bandwidth Control

Bandwidth Control
- Control Settings
- Rule List

There are two submenus under the Bandwidth Control menu. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.15.1 Control Settings

Choose menu "**Bandwidth Control** \rightarrow **Control Settings**", you can configure the Egress Bandwidth and Ingress Bandwidth. 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 Settir	lgs	
Enable Bandwidth Control:		
Line Type:	💿 ADSL 🔿 Other	
Egress Bandwidth:	512	Kbps
Ingress Bandwidth:	2048	Kbps
		_
	Save	

- 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 WAN port.
- > Ingress Bandwidth The download speed through the WAN port.

4.15.2 Rule List

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

Ban	dwidth Control Rule I	_ist					
		Egress Bar	ndwidth(Kbps)	Ingress Bar	ndwidth(Kbps)		
	Description	Min	Max	Min	Мах	- Enable	Modify
	The current list is empty.						
Add	New Delete All]					
Prev	vious Next	Current No. 1	🖌 Page				

- > **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 WAN port, the default is 0.
- Ingress Bandwidth This field displays the max and mix download bandwidth through the WAN 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.

Step 1: Click Add New..., you will see a new screen shown below.

Step 2: Enter the information like the screen shown below.

Bandwidth Control Rule	ettings
Enable: IP Range: Port Range: Protocol:	
Egress Bandwidth: Ingress Bandwidth:	Min Bandwidth(Kbps) Max Bandwidth(Kbps) 0 0 0 0
	Save Back

- > Enable Enable or disable the rule.
- IP Range Interior PC address range. If both are blank (or 0.0.0.0), the domain is no effective.

- Port Range The port range which the Interior PC access the outside PC. If all are blank (or 0), the domain is no effective.
- > **Protocol** Transport layer protocol, here there are All, TCP, UDP.
- Egress Bandwidth The max and the min upload speed which through the WAN port, default number is 0.
- Ingress Bandwidth The max and the min download speed through the WAN port, default number is 0.
- Step 3: Click the Save button.

4.16 IP & MAC Binding

IP & MAC Binding	
- Binding Settings	
- ARP List	

There are two submenus under the IP & MAC Binding menu: **Binding Setting** 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.

4.16.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire.

Bindi	ng Settings				
	ARP Binding:	 Disable Enable Save 			
ID 1	MAC Address 00-0A-EB-00-07-BE	IP Address 192.168.0.173	Bind 🔽	Modify <u>Modify Delete</u>	
Add N	lew Enable All	Disable All	elete All	Find	
		Previous	Next C	urrent No. 📘 💌	Page

- > **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 -** Whether or not enable the ARP binding.
- > **Modify -** Edit or delete item.

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.

IP & MAC Binding Setting	S
Bind: MAC Address: IP Address:	
	Save Back

To add IP & MAC Binding entries:

- 1. Click the **Add New..** button.
- 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:

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

To find an existing entry:

- 1. Click the **Find** button.
- 2. Enter the MAC Address or IP Address.
- 3. Enter the **Find** button in the next page.

Find IP & MAC Binding B	Entry			
MAC Address: IP Address:				
ID	MAC Address	IP Address	Bind Link	
1	00-0A-EB-00-07-BE	192.168.0.173	🗹 <u>To page</u>	
	Find	Back		

Click the Enable All button to make all entries enabled.

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

4.16.2 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 configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries.

AR	² List			
ID 1	MAC Address 6C-62-6D-F7-31-8D	IP Address 192.168.0.100	Status Unbound	Configure Load Delete
2	00-0A-EB-00-07-BE	192.168.0.173	Bound	Load Delete
		Bind All	Load A	ll Refresh

- > MAC Address The MAC address of the controlled computer in the LAN.
- > **IP Address -** The assigned IP address of the controlled computer in the LAN.
- > Status Enabled or Disabled of the MAC address and IP address binding.
- > **Configure -** Load or delete 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.

P 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.

4.17 Dynamic DNS

The Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, 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.no-ip.com</u>, <u>www.comexe.cn</u>, or <u>www.dyndns.org</u>. The Dynamic DNS client service provider will give you a password or key.

4.17.1 No-IP DDNS

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

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

To set up for DDNS, follow these instructions:

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

4.17.2 Comexe.cn DDNS

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

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

To set up for DDNS, follow these instructions:

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

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

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

4.17.3 Dyndns org DDNS

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

DDNS	
Service Provider:	Dyndns (www.dyndns.org) 🖌 <u>Go to register</u>
User Name: Password: Domain Name:	usemame
Connection Status:	DDNS not launching!
	Login Logout Save

To set up for DDNS, follow these instructions:

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

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

Click **Logout** to logout of the DDNS service.

4.18 System Tools

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

There are nine submenus under the System Tools menu: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup and Restore**, **Reboot**, **Password**, **System Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.18.1 Time Settings

Time zone:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore		
Date:	1 1 2013 (MM/DD/YY)		
Time:	1 43 50 (HH/MM/SS)		
NTP Server 1:	0.0.0.0 (Optional)		
NTP Server 2:	0.0.0.0 (Optional)		
Start: End:	Enable Daylight Saving Mar 3rd Sun 2am Nov 2nd Sun 3am		
Daylight Saving Status:	daylight saving is down. 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.		

You can set time manually or get GMT from the Internet for the router on this page:

- > **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.

To set time manually, follow the steps below:

- 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.

For automatic time synchronization:

- 1. Enter the address of the **NTP Server 1 or NTP Server 2**.
- 2. Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

Note:

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, if not, the time limited on these functions will not take effect.

- > The time will be lost if the router is turned off.
- > The router will obtain GMT automatically from Internet if it has already connected to Internet.

4.18.2 Diagnostic

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

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				
This device is ready.				
	Start			

- > **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 pinging/tracerouting the IP address is successful, but pinging/tracerouting 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 Type the destination IP address (such as 202.108.22.5) or Domain name (such as www.baidu.com).
- > **Pings Count -** The number of Ping packets for a Ping connection.
- > Ping Packet Size The size of Ping packet.
- Ping Timeout Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- > Traceroute Max TTL The max number of hops for a Traceroute connection.

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 202.108.22.5 with 64 bytes of data:
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=1 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=2 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=3 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=4
Ping statistics for 202.108.22.5 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milliseconds: Minimum = 1, Maximum = 1, Average = 1

P Note:

Only one user can use this tool at one time. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters. "Traceroute Max TTL" is Traceroute Parameter.

4.18.3 Firmware Upgrade

The page allows you to upgrade the latest version firmware to keep your router up-to-date.

Firmware Upgrade		
File:		Browse
Firmware Version:	3.14.4 Build 130128 Rel.36510n	
Hardware Version:	WR710N v1 00000000	
	Upgrade	

New firmware is posted at <u>www.tp-link.com</u> and can be downloaded for free. If the router is not experiencing difficulties, there is no need to upgrade firmware, unless the new firmware supports a new feature you need.

P Note:

- 1. When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.
- 2. Make sure that your computer is connected to the Internet through the cable when you upgrade the firmware. To upgrade through wireless connection is not allowed.
- 3. Set your IP address as static IP before upgrading.

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

- 1. Download the latest firmware upgrade file from our website <u>http://www.tp-link.com</u>.
- 2. Enter or select the path name where you save the downloaded file on the computer into the **File** blank.
- 3. Click the **Upgrade** button.
- 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 current hardware version.

P Note:

The firmware version must correspond to the hardware. The upgrade process takes a few minutes and the Router will restart automatically when the upgrade is completed. It is important to keep power on during the entire process. Loss of power during the upgrade could damage the Router.

4.18.4 Factory Defaults

This page allows you to restore the factory default settings for the router.

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

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

- > The default User Name: admin
- > The default Password: admin
- > The default access: tplinklogin.net

Note:

Any settings you have saved will be lost when the default settings are restored.

4.18.5 Backup & Restore

This page allows you to save current configuration of router as backup or restore the configuration file you saved before.

Backup & Restor	e	
Configuration Backup: Configuration File:	Backup	Browse Restore

- Click the Backup button to save all configuration settings as a backup file in your local computer.
- > To restore the router's configuration, follow these instructions:
 - Click the **Browse** button to select the backup file which you want to restore.
 - Click the **Restore** button.

P Note:

The current configuration will be covered with the uploading configuration file. The restoration process lasts for 20 seconds and the router will restart automatically. Keep the router on during the restoring process to prevent any damage.

4.18.6 Reboot

This page allows you to reboot the router.

Reboot
Click this button to reboot this device.
Reboot

Click the **Reboot** button to reboot the router.

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

- > Change LAN IP Address. (System will reboot automatically)
- > MAC Clone (system will reboot automatically)
- > DHCP service function.
- > Static address assignment of DHCP server.
- > Web Service Port of the router.
- > Upgrade the firmware of the router (system will reboot automatically).
- > Restore the router's settings to factory default (system will reboot automatically).

4.18.7 Password

This page allows you to change the factory default user name and password of the router.

Password	
The username and password must not exce	eed 14 characters in length and must not include any spaces!
Old User Name:	
Old Password:	
New User Name:	
New Password: Confirm New Password:	
	Save Clear All

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

P Note:

The new user name and password must not exceed 14 characters in length and must 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.

4.18.8 System Log

This page allows you to query the logs of the router.

Sys	System Log								
Auto I	Mail Feature: Di	sabled	Ma	ail Settings					
Log Ty	ype: SHARING	*	Log Le	vel: ALL					
Index	Time	Туре	Level	Log Content					
6	1 st day 01:12:56	SHARING	NOTICE	Network sharing service stopped					
5	1st day 00:11:17	SHARING	INFO	Media server started					
4	1st day 00:08:07	SHARING	NOTICE	Network sharing service started					
3	1 st day 00:08:06	SHARING	NOTICE	Network sharing settings changed					
2	1 st day 00:06:23	SHARING	NOTICE	Network sharing service started					
1	1st day 00:06:20	SHARING	NOTICE Network sharing settings changed						
Time =	2013-01-01 1:55:	47 6948s							
H-Ver =	= WR710N ∨1 000	00000 : S-\	/er = 3.14	I.4 Build 130128 Rel.36510n					
L = 192	2.168.0.254 : M = 2	255.255.25	5.0						
W1 = D	HCP : W = 0.0.0.0	: M = 0.0.0	.0 : G = 0.	0.0.0					
Refresh Save Log Mail Log Clear Log									
	Previous Next Current No. 1 V Page								

- **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. The result will be shown in the later log soon.
- > Clear Log All the logs will be deleted from this device permanently, not just from the page.

4.18.9 Statistics

The Statistics page displays the network traffic of each PC in LAN, including total traffic and traffic of the last **Packets Statistic Interval** seconds.

Statistics								
Current Statistic	s Status:	Disabled	1		Enat	ole		
Packets Statistics Inter	val(5~60):	10 Seconds Auto-refresh		Refre	esh			
Sort	ted Rules:	Sorted I	oy Current Byt	es 💌	Reset	t All	Delete All	
	Tota			Current				
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	Modify
			The current	list is empt	у.			
5 🗸 entries per page. Current No. 1 🗸 Page								
Previous Next								

- Current Statistics Status Enable or Disable. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be ineffective.
- Packets Statistics Interval The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- > **Sorted Rules -** Here displays sort as desired.

Statistics Table:

IP Address		The IP Address displayed with statistics
Packets		The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.
Current Bytes		The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.

ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.		
UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.		
TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.		

Click the Save button to save the Packets Statistic interval value.

Click the Auto-refresh checkbox to refresh automatically.

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

Chapter 5. Configuration for Access Point Mode

This chapter will show each Web page's key functions and the configuration way for Access Point Mode of the router.

5.1 Login

After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.

Status
Quick Setup
WPS
Working Mode
Network
Wireless
DHCP
USB Settings
System Tools

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

5.2 Status

The Status page provides the current status information about the Router on Access Point Mode. All information is read-only.

Status			
Status			
Firmware Version:	3.14.4 Build 130128 Rel.36510n		
Hardware Version:	WR710N v1 00000000		
Wired			
MAC Address:	00-1D-0F-01-06-28		
IP Address:	192.168.0.254		
Subnet Mask:	255.255.255.0		
Wireless			
Working Mode:	Access Point		
Wireless Network Name:	TP-LINK_2046F2		
Channel:	Auto (Current channel 3)		
Mode:	11bgn mixed		
Channel Width:	Automatic		
MAC Address:	00-1D-0F-01-06-28		
Traffic Statistics			
	Received	Sent	
Bytes:	0	32,676	
Packets:	0	79	
System Up Time:	0 days 00:01:34	Refresh	

- > **Firmware Version -** The version information of the Router's firmware.
- > Hardware Version The version information of the Router's hardware.
- Wired This field displays the current settings or information for the LAN, you can configure them in the Network > LAN page.
 - MAC address The physical address of the Router, as seen from the LAN.
 - IP address The LAN IP address of the Router.
 - Subnet Mask The subnet mask associated with LAN IP address.
- Wireless This field displays basic information or status for wireless function, you can configure them in the Wireless > Wireless Settings page.
 - Working Mode The current wireless working mode in use.
 - Wireless Network Name The SSID of the AP.
 - Channel The current wireless channel in use.
 - Mode The current wireless mode which the Router works on.
 - Channel Width The current wireless channel width in use.

- MAC Address The physical address of the Router, as seen from the WLAN.
- > **Traffic Statistics -** The Router's traffic statistics.
 - Received (Bytes) Traffic that counted in bytes has been received out from the WAN port.
 - Received (Packets) Traffic that counted in packets has been received out from the WAN port.
 - Sent (Bytes) Traffic that counted in bytes has been sent out from the WAN port.
 - Sent (Packets) Traffic that counted in packets has been sent out from the WAN port.
- > System Up Time The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

5.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

5.4 WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to an existing network quickly by function. The WPS function is only available when the Operation Mode is set to Access Point. Select menu "WPS", you will see the next screen shown below.

WPS (Wi-Fi Protected Se	WPS (Wi-Fi Protected Setup)				
WPSStatus:	Enabled Disable WPS				
Current PIN:	12345670 Restore PIN Gen New PIN Disable PIN of this Device				
Add A New Device:	Add Device				

- > WPS Status To enable or disable the WPS function here.
- Current PIN The current value of the device's PIN is displayed here. The default PIN of the device can be found in the label or User Guide.
- > **Restore PIN -** Restore the PIN of the device to its default.
- Gen New PIN Click this button, and then you can get a new random value for the device's PIN. You can ensure the network security by generating a new PIN.
- Disable PIN of this Device WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.

Add Device - You can add a new device to the existing network manually by clicking this button.

To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and device 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.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

II. By PBC

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

Step 1: Keep the WPS Status as **Enabled** and click the **Add Device** button, then the following screen 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

- Step 2: Choose "**Press the button of the new device in two minutes**" and click **Connect**.
- Step 3: For the configuration of the wireless adapter, please choose "**Push the button on my** access point or wireless router" in the configuration utility of the WPS as below, and click **Connect**.

	К				- x
	WPS		-		
Status	WPS	Network	Profile	Advanced	
◉ Push th ⊚ Enter th	pose a method to e button on my acce e PIN of my acce	ion will guide you th join a wireless netw ccess point or wireless ss point or wireless ce into my access p	vork: ess router. router.) your wireless network	Connect

The WPS Configuration Screen of Wireless Adapter

Step 4: Wait for a while until the next screen appears. Click **OK** to complete the WPS configuration.

Configuring the wireless network.
(((WPS)))
Successfully connected to the network by WPS!
ОК

The WPS Configuration Screen of Wireless Adapter

Method Two: Enter the PIN into my AP

Step 1: For the configuration of the wireless adapter, please choose "Enter the PIN of this device into my access point or wireless router" in the configuration utility of the WPS as below, and click Connect.

	ĸ				
			A	and a state of the	
Status	WPS	Network	Profile	Advanced	
((WPS)	2	tion will guide you th join a wireless netw		g your wireless network	s
Push the	button on my ad	ccess point or wirele ss point or wireless	ess router.		
~		ce into my access p		outer.	
PIN: 1695	52898	4 2			
					Connect

The WPS Configuration Screen of Wireless Adapter

P Note:

In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

- Step 2: Keep the WPS Status as **Enabled** and click the **Add Device** button.
- Step 3: Choose "Enter the new device's PIN" and enter the PIN code (take 16952898 for example) of the wireless adapter in the field after PIN as shown in the figure below. Then click Connect.

Add A New Device
Enter the new device's PIN.
PIN: 16952898
Press the button of the new device in two minutes.
Back Connect

Method Three: Enter the PIN from my AP

- Step 1: Get the Current PIN code of the AP (each AP has its unique PIN code. Here takes the PIN code 12345670 of this AP for example).
- Step 2: For the configuration of the wireless adapter, please choose "Enter the PIN of my access point or wireless router" in the configuration utility of the WPS as below, and enter the PIN code of the AP into the field after "Access Point PIN". Then click Connect.



Note:

The default PIN code of the AP can be found in its label or the WPS configuration screen.

You will see the following screen when the new device has successfully connected to the network.

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

Note:

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

5.5 Working Mode

The Router supports five operation mode types: Wireless Router, Access Point, Repeater, Client and Wireless Client Router. Please select one you want. Click Save to save your choice.

🔘 Wireless Router	- Enable multiple users to share Internet connection via ADSL/Cable Modem
Access Point	- Transform your existing wired network to a wireless network
🔿 Repeater	- Extend your existing wireless coverage by relaying wireless signal
🔿 Client	- Acting as a "Wireless Adapter" to connect your wired devices (e.g. Xbox/PS3) to a wireless networ
O WISP Client Route	 Enable multiple users to share Internet connection from WISP

- Wireless Router The wireless Router Mode. In this mode, the device enables multi-user to share Internet via DSL/Cable Modem. The only wired port works as WAN.
- > Access Point The wireless access point mode.
- > Repeater The wireless Repeater Mode. It could extend the range of wireless network.
- Client The Client Mode. The computer connected by Ethernet could get access to an AP by Client mode.
- WISP Client Router In this mode, the device enables multiple users to share Internet connection from WISP.

5.6 Network

Network - LAN

There is only one submenu under the Network menu: LAN.

5.6.1 LAN

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

LAN				
MAC Address:	00-1D-0F-01-06-28			
Туре:	Smart IP(DHCP) 🔽			
IP Address:	192.168.0.254			
Subnet Mask:	255.255.255.0 💌			
IGMP Proxy:	Enable 💌			
Note: IGMP(Internet Group Management Protocol) works for IPTV multicast stream. The device supports both IGMP proxy with enable or disable option and IGMP snooping.				
	Save			

MAC Address - The physical address of the LAN ports, as seen from the LAN. The value can not be changed.

- Type Choosing Smart IP (DHCP) to get IP address from DHCP server, or choosing static IP to config IP address manually.
- IP Address Enter the IP address of your system in dotted-decimal notation (factory default -192.168.0.254).
- Subnet Mask An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.
- IGMP Proxy The Internet Group Management Protocol(IGMP) feature allows your devices in LAN can watch TV.

P Note:

- 1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
- 2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, while the Virtual Server and DMZ Host will not take effect until they are re-configured.
- 3. When you choose the **Smart IP(DHCP)** mode, the DHCP Server function will be disabled.

5.7 Wireless



There are five submenus under the Wireless menu: Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced and Wireless Statistics. Click any of them, and you will be able to configure the corresponding function.

5.7.1 Wireless Settings

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

Wireless Settings		
Wireless Network Name:	TP-LINK_2046F2	(Also called the SSID)
Region:	United States 🛛 👻	
Warning:	Ensure you select a correct country to c	
	Incorrect settings may cause interferer	ce.
Channel:	Auto 🗸	
Mode:	11bgn mixed 👻	
Channel Width:	Auto 🔽	
	🔽 Enable Wireless Radio	
	🔽 Enable SSID Broadcast	
	Save	

- Wireless Network Name Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- Region Select your region from the pull-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.
- Channel This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- > **Mode -** Select the desired mode. The default setting is 11bgn mixed.
- **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.

When 11bg mixed mode is selected, only 11bg mixed wireless stations can connect to the Router. It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n wireless stations can connect to the Router.

P Note:

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

Channel Width - Select any channel width from the pull-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.

- Enable Wireless Router Radio The wireless radio of the Router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Router. Otherwise, wireless stations will not be able to access the Router.
- Enable SSID Broadcast If you select the Enable SSID Broadcast checkbox, the wireless router will broadcast its name (SSID) on the air.

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

P Note:

- 1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
 - Near the center of the area in which your wireless stations will operate.
 - In an elevated location such as a high shelf.
 - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
 - Away from large metal surfaces.
- 2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

5.7.2 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).

Wireless Security						
O Disable Security						
WPA/WPA2 - Personal(Recommended)						
Version:	Version: Automatic(Recommended)					
Encryption:	Automatic(Recommended)					
Wireless Password:						
	(You can enter ASCII c	haracters between 8 and 63 or Hexadecimal characters between 8 and 64.)				
Group Key Update Period:	0 Sec	conds (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 stands for default port 1812)					
Radius Password:						
Group Key Update Period:	(in s	econd, minimum is 30, 0 means no update)				
○ WEP						
Туре:	Automatic 🗸 🗸					
WEP Key Format:	Hexadecimal 💌					
Key Selected	WEP Key	Кеу Туре				
Key 1: 💿		Disabled 💌				
Key 2: 🔵		Disabled 💌				
Key 3: 🔵		Disabled 💌				
Key 4: 🔵		Disabled 🗸				
	[Paura]					
	Save					

- 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. But it's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - 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.

WPA/WPA2 - Personal(Recomment	ded)
Version:	Automatic(Recommended) 💌
Encryption:	ТКІР
Wireless Password:	
	(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 this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

- > WPA/WPA2-Enterprise It's based on Radius Server.
 - Version you can choose the version of the WPA security from the pull-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 Automatic, TKIP or AES.
 - Radius Server IP Enter the IP address of the Radius server.
 - Radius Port Enter the port that Radius server used.
 - 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.
 - **Type** you can choose the type for the WEP security on the pull-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 (Password) 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.

5.7.3 Wireless MAC Filtering

Choose menu "Wireless \rightarrow Wireless MAC Filtering", and then you can control the wireless access by configuring the Wireless MAC Filtering function.

Wireless MAC Filtering					
Wireless MAC Filtering:	Enabled	Disable			
Filtering Rules					
Deny the stations specified by any of the station of the statio	enabled entries	s in the list to access.			
Allow the stations specified by any enabled entries in the list to access.					
-					
ID MAC Address	Status	Description	Modify		
Add New Enable All Dis	able All	Delete All			
Pre	evious	Next			

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

- > MAC Address The wireless station's MAC address that you want to access.
- > 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:

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

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.

- 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** pull-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 stations specified by any enabled entries in the list to access" for **Filtering Rules**.
- 3. Delete all or disable all entries if there are any entries already.
- 4. Click the Add New... button.
 - Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the MAC Address field.
 - Enter wireless station A/B in the **Description** field.
 - Select Enabled in the Status pull-down list.
 - Click the Save button.
 - Click the **Back** button.

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

stations specified by a stations specified by a		es in the list to access. es in the list to access.	
stations specified by a	any enabled entrie	es in the list to access.	
	Status	Description	Modify
0-0B	Enabled	wireless station A	Modify Delete
7-5F	Enabled	wireless station B	Modify Delete
	00-0B)7-5F	00-0B Enabled	00-0B Enabled wireless station A

5.7.4 Wireless Advanced

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

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

- 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 1-255 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 enabled.
- Enable Short GI This function is recommended for it will increase the data capacity by reducing the guard interval time.
- Enable AP Isolation This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

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.

5.7.5 Wireless Statistics

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

Wire	eless Statistics						
	Current Connected Wireless Stations numbers: 1 Refresh						
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure		
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	Allow		
		Previous	Next				

- > 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
- > Configure The button is used for loading the item to the Wireless MAC Filtering list.

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.

5.8 DHCP



There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Client List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

5.8.1 DHCP Settings

Choose menu "**DHCP** \rightarrow **DHCP** Settings", and then you can configure the DHCP Server. 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 in the LAN.

DHCP Settings		
DHCP Server:	💿 Disable 🔘 Enat	le
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:	0.0.0.0	(optional)
Default Domain:		(optional)
Primary DNS:	0.0.0.0	(optional)
Secondary DNS:	0.0.0.0	(optional)
	Save	

- 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 LAN port of the Router. The default value is 192.168.0.254.
- > **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.

Note:

- 1. To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
- 2. When you choose the **Smart IP (DHCP)** mode in **Network** → **LAN**, the DHCP Server function will be disabled. You will see the page as below.

Start IP Address: 192.168.0.100 End IP Address: 192.168.0.199 Address Lease Time: 120 Default Gateway: 192.168.0.254 Optional) (Optional) Primary DNS: 192.168.0.254 Secondary DNS: 192.168.0.254	DHCP Server:	O Disable	e 💿 Enable	
Address Lease Time: 120 minutes (1 ~2880 minutes, the default value is 120) Default Gateway: 192.168.0.254 (Optional) Default Domain: (Optional) Primary DNS: 192.168.0.254 (Optional)	Start IP Address:	192.168.0	.100	
Default Gateway: 192.168.0.254 (Optional) Default Domain: (Optional) Primary DNS: 192.168.0.254 (Optional)	End IP Address:	192.168.0	.199	
Default Domain: (Optional) Primary DNS: 192.168.0.254	Address Lease Time:	120	minutes (1	~2880 minutes, the default value is 120)
Primary DNS: 192.168.0.254 (Optional)	Default Gateway:	192.168.0	.254	(Optional)
	Default Domain:			(Optional)
Secondary DNS: 192.168.0.254 (Optional)	Primary DNS:	192.168.0	.254	(Optional)
	Secondary DNS:	192.168.0	.254	(Optional)

5.8.2 DHCP Client List

Choose menu "DHCP \rightarrow DHCP Clients List", and then you can view the information about the clients attached to the Router.

D	HCP Client Lis	t		
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32
		Refresh		

> 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.

5.8.3 Address Reservation

Choose menu "DHCP \rightarrow Address Reservation", and then you can view and add a reserved address for clients via the next screen. 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.

Addre	ess Reservation			
ID 1	MAC Address 00-11-22-33-44-AA	Reserved IP Address 192.168.0.169	Status Enabled	Modify <u>Modify Delete</u>
Add N	ew Enable All	Disable All Delete All		
		Previous Next		

- > 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.
- > **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

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

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

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.

5.9 USB Settings

USB Settings	
- Storage Sharing	
- Media Server	
- User Accounts	

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

5.9.1 Storage Sharing

Choose menu "**USB Settings**→**Storage Sharing**", you can configure a USB disk drive attached to the router and view volume and share such properties as share name, capacity, used space, and free space on this page as shown below.

Storage	Sharing					
	Service Status:	Started	Stop hared storage wi	th password		
Volume volume1	Capacity 1.9 GB	Used 1.3 GB	Free 626 MB	Use % 67%	Shared Disable	
		Eject Dis	sk Resc	an		

- Service Status Indicates the Network Sharing service's current status. You can click the Start button to start the Storage Sharing service and click the Stop button to stop it.
- Volume The volume name of the USB drive the users have access to. Volume 1-8 is mapping to USB port1, and Volume 9-16 is mapping to USB port2.
- > **Capacity -** The storage capacity of the USB driver.

- **Used -** The used space of the USB driver.
- > **Free -** The available space of the USB driver.
- > **Use% -** The percentage of the used space.
- Shared Indicates the shared or non-shared status of the volume. When the volume is shared, you can click the **Disable** to stop sharing the volume; when volume is non-shared, you can click the **Enable** button to share the volume.

Click the Start button to start the Network Sharing service.

Click the **Stop** button to stop the Network Sharing service.

Click the **Eject Disk** button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Message f	rom webpage	×
?	This operation will disable Media Server. Are you sure to continue?	
	OK Cancel	

Click the **Rescan** button to start a new scan.

Follow the instructions below to set up your router as a file server:

- 1. Plug an external USB hard disk drive or USB flash drive into this router.
- 2. Click the **Rescan** button to find the USB drive that has been attached to the router.
- 3. Click the Start button to start the Storage Sharing service.
- 4. Click the **Enable** button under **Shared** to enable the disk to share.
- 5. Click the **Open the disk** to visit the sharing disk.

P Note:

- 1. The router can automatically locate new USB drive. But to display the information about your USB device, you need to click the **Rescan** button manually.
- 2. The new settings will not take effect until you restart the service.
- 3. To unplug the USB drive, click **Eject Disk** button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.
- 4. Mounted volumes of each USB port are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.

5. If you change the storage settings during the storage connection is established, then the changes will not take effect until the router or the client is rebooted.

5.9.2 Media Server

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

Media Ser	ver Setting				
	Server Name:	TP-LINK_010628			
	Server Status:	Stopped Start			
Auto-scan	every 2 hours 🔽	Scan All			
Add share fol	der				
Name	File System		Folder	Delete	

- Server Name The name of this Media Server.
- Server Status Indicates the Media Server's current status, started or stopped. You can click the Start button to start the Media Server and click the Stop button to stop it.
- > **Name** The display name of this folder.
- > **File System** The file system type on the partition can be FAT32 or NTFS.
- > Folder The real full path of the specified folder.
- > **Delete** You can delete the share folder by click **Delete**.

To set up your media server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router, and then the screen will appear as shown below.

Media Server Setting					
	Server Name: Server Status:	TP-LINK_010628 Stopped Start			
Auto-scan ex		Scan All			
Name	File System		Folder	Delete	

2. Click the **Start** button to start the media server, and then the screen will appear as shown below.

	Server Name:	TP-LINK 010628			
	Server Status:	Started Stop			
Auto-scan	every 2 hours 🗸	Scan All			
Add share fol	der				
Name	File System		Folder	Delete	

3. Click the **Add share folder** button to specify a folder as the search path of media server. The screen will then appear as shown below.

Add New Folder	
Display Name: Partition: Folder Location:	video Share entire partition /my share
Select	Folder
0	photo
۲	video
0	Save Back Current No. 1 v page

- > **Display Name -** You can enter a display name for the share folder.
- Share entire partition Choose this option and then the folders contained in this partition will all be shared.
- > Folder Location Displays the location of this folder.
- > Select Check the radio button to select the folder to share.
- > **Folder** Displays folders that are in current path.
- > **Upper** Click this button to get into the upper folder.
- Save Click this button to save your settings and the page will be redirected to the media server configuration page.
- Back Click this button to discard the settings and just go to the media server configuration page.
- 4. Click the **Scan All** button to scan all the share folders immediately. You can also select the **Auto-scan**, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

P Note:

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

5.9.3 User Accounts

You can specify the user name and password for Storage Sharing users on this page. **Storage Sharing** users can use Internet Explorer to access files on the USB drive.

There are two default user accounts that can access the Storage Sharing. They are Administrator and Guest. Administrator has read/write access to Storage Sharing while Guest has read-only access to Storage Sharing.

User Account Mar	nagement			
Add New User				
User Name	Password	Storage Authority	Modify	
admin	admin	Read and Write	yes	Edit
guest	guest	Read Only	no	Edit
Save				

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

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

- 1. Click Add New User button, and the screen will appear as shown below.
- 2. Self-define a User Name.
- 3. Enter the password in the **Password** field.
- 4. Choose the Storage Authority from the drop-down list, Read and Write or Read Only.

Add or Modify User Acco	unt
User Name: Password:	admin2
Storage Authority:	Read and Write 💌
	Save Back

User Name - Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.

- Password Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- Storage Authority Choose Read and Write or Read Only from the drop-down list to assign access authority of Storage Sharing to the user.
- > Save You can click the Save button to save your settings.
- Back You can click the Back button to discard the settings and just go to the media server configuration page.

P Note:

Please restart the service for the new settings to take effect.

If you cannot use the new user name and password to access the shares, press **Windows logo + R** to open the Run dialog box and type **net use \\192.168.0.254 /delete /yes** and press Enter. (192.168.0.254 is your router's LAN IP address. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.0.254 to 192.168.1.254 to avoid IP conflict; in this case, please try **net use \\192.168.1.254/delete/yes**.)

5.10 System Tools

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

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

5.10.1 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.

Diagnostic Tools	
Diagnostic Parameters	
Diagnostic Tool:	💿 Ping j 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	
This device is ready.	
	Start

- > **Diagnostic Tool -** Check the radio button to select one diagnostic tool.
 - **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.

P Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting 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 Type the destination IP address (e.g. 202.108.22.5) or Domain name (e.g. http://www.tp-link.com).
- > **Pings Count -** The number of Ping packets for a Ping connection. The default is 4.
- > **Ping Packet Size -** The size of Ping packet. The default is 64.
- Ping Timeout Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime. The default is 800.
- Traceroute Max TTL The max number of hops for a Traceroute connection. 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 202.108.22.5 with 64 bytes of data:
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=1 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=2 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=3 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=4
Ping statistics for 202.108.22.5 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds: Minimum = 1, Maximum = 1, Average = 1

P Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for **Ping** function. Option "Tracert Hops" are used for **Tracert** function.

5.10.2 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:		Browse
Firmware Version:	3.14.4 Build 130128 Rel.36510n	
Hardware Version:	WR710N v1 00000000	
	Upgrade	

- Firmware Version This displays the current firmware version.
- Hardware Version This 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 more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).
- 2. Type the path and file name of the update file into the **File** field, or click the **Browse** button to locate the update file.
- 3. Click the **Upgrade** button.

P Note:

 New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the 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, otherwise, the Router may be damaged.
- 4. The Router will reboot after the upgrading has been finished.

5.10.3 Factory Defaults

Choose menu "System Tools \rightarrow Factory Defaults", 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

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

- > The default **User Name**: admin
- > The default **Password**: admin
- > The default **IP Address**: 192.168.0.254
- > The default **Subnet Mask**: 255.255.255.0

Note:

All changed settings will be lost when defaults are restored.

5.10.4 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.

Backup & Restore	•		
Configuration Backup: Configuration File:	Backup	Browse Restore)

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 locate the update file for the Router, or enter the exact path to the Setting file in the text box.
 - Click the **Restore** button.

P Note:

The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

5.10.5 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 this device.
Reboot

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).

5.10.6 Password

Choose menu "System Tools \rightarrow Password", and then you can change the factory default user name and password of the Router.

Password	
The username and password must not exc Old User Name: Old Password:	eed 14 characters in length and must not include any spaces!
New User Name: New Password: Confirm New Password:	
	Save Clear All

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.

P 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.

Click the Save button when finished.

Click the Clear All button to clear all.

5.10.7 System Log

Choose menu "System Tools → System Log", and then you can view the logs of the Router.

Sys	stem Log			
Auto I	Mail Feature: Di	sabled	Ma	ail Settings
Log T	ype: SHARING	*	Log Le	vel: ALL
Index	Time	Туре	Level	Log Content
6	1 st day 01:12:56	SHARING	NOTICE	Network sharing service stopped
5	1st day 00:11:17	SHARING	INFO	Media server started
4	1 st day 00:08:07	SHARING	NOTICE	Network sharing service started
3	1st day 00:08:06	SHARING	NOTICE	Network sharing settings changed
2	1 st day 00:06:23	SHARING	NOTICE	Network sharing service started
1	1st day 00:06:20	SHARING	NOTICE	Network sharing settings changed
Time =	2013-01-01 1:55:	47 6948s		
H-Ver =	= WR710N ∨1 000	00000 : S-\	/er = 3.14	.4 Build 130128 Rel.36510n
L = 192	2.168.0.254 : M = 2	255.255.25	5.0	
W1 = D	HCP : W = 0.0.0.0	: M = 0.0.0	.0 : G = 0.	0.0.0
R	efresh	Save Log		Mail Log Clear Log
			Pr	evious Next Current No. 1 🔮 Page

- **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. The result will be shown in the later log soon.
- > **Clear Log** All the logs will be deleted from this device permanently, not just from the page.

Chapter 6. Configuration for Repeater Mode

This chapter will show each Web page's key functions and the configuration way for Repeater Mode of the router.

6.1 Login

After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.

Status Quick Setup Working Mode Network Wireless
Working Mode Network
Network
Wireless
DHCP
USB Settings
System Tools

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

6.2 Status

The Status page provides the current status information about the Router on Repeater Mode. All information is read-only.

Firmware Version:	3.14.4 Build 130128 Rel.36510)n	
Hardware Version:	WR710N v1 00000000		
Wired			
MAC Address:	00-1D-0F-01-06-28		
IP Address:	192.168.0.254		
Subnet Mask:	255.255.255.0		
Wireless			
Working Mode:	Universal Repeater		
Wireless Name of Root AP:	TP-LINK_Network		
Channel:	4		
Mode:	11bgn mixed		
Channel Width:	Automatic		
MAC Address:	00-1D-0F-01-06-28		
Traffic Statistics			
	Received	Sent	
Bytes:	0	3,452	
Packets:	0	14	
	0 days 00:02:12		

- > **Firmware Version -** The version information of the Router's firmware.
- > Hardware Version The version information of the Router's hardware.
- Wired This field displays the current settings or information for the LAN, you can configure them in the Network > LAN page.
 - MAC address The physical address of the Router, as seen from the LAN.
 - IP address The LAN IP address of the Router.
 - Subnet Mask The subnet mask associated with LAN IP address.
- Wireless This field displays basic information or status for wireless function, you can configure them in the Wireless > Wireless Settings page.
 - Working Mode The current wireless working mode in use.
 - Wireless Name of Root AP The SSID of Root AP.
 - Channel The current wireless channel in use.
 - Mode The current wireless mode which the Router works on.
 - Channel Width The current wireless channel width in use.

- MAC Address The physical address of the Router, as seen from the WLAN.
- > **Traffic Statistics -** The Router's traffic statistics.
 - Received (Bytes) Traffic that counted in bytes has been received out from the WAN port.
 - Received (Packets) Traffic that counted in packets has been received out from the WAN port.
 - Sent (Bytes) Traffic that counted in bytes has been sent out from the WAN port.
 - Sent (Packets) Traffic that counted in packets has been sent out from the WAN port.
- > System Up Time The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

6.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

6.4 Working Mode

The Router supports five operation mode types: Wireless Router, Access Point, Repeater, Client and Wireless Client Router. Please select one you want. Click Save to save your choice.

Working Mode	
🔿 Wireless Router	- Enable multiple users to share Internet connection via ADSL/Cable Modem
🔘 Access Point	- Transform your existing wired network to a wireless network
Repeater	- Extend your existing wireless coverage by relaying wireless signal
🔘 Client	- Acting as a "Wireless Adapter" to connect your wired devices (e.g. Xbox/PS3) to a wireless network
🔘 WISP Client Router	- Enable multiple users to share Internet connection from WISP
	Save

- Wireless Router The wireless Router Mode. In this mode, the device enables multi-user to share Internet via DSL/Cable Modem. The only wired port works as WAN.
- > Access Point The wireless access point mode.
- > Repeater The wireless Repeater Mode. It could extend the range of wireless network.
- Client The Client Mode. The computer connected by Ethernet could get access to an AP by Client mode.
- WISP Client Router In this mode, the device enables multiple users to share Internet connection from WISP.

6.5 Network

Network

There is only one submenu under the Network menu: LAN.

6.5.1 LAN

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

LAN				
MAC Address:	00-1D-0F-01-06-28			
Type:	Smart IP(DHCP) 🔽			
IP Address:	192.168.0.254			
Subnet Mask:	255.255.255.0 🔽			
IGMP Proxy:	Enable 💌			
Note: IGMP(Internet Group Management Protocol) works for IPTV multicast stream. The device supports both IGMP proxy with enable or disable option and IGMP snooping.				
	Save			

- MAC Address The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- Type Choosing Smart IP (DHCP) to get IP address from DHCP server, or choosing static IP to config IP address manually.
- IP Address Enter the IP address of your system in dotted-decimal notation (factory default -192.168.0.254).
- Subnet Mask An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.
- IGMP Proxy The Internet Group Management Protocol(IGMP) feature allows your devices in LAN can watch TV.

P Note:

- 1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
- 2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

6.6 Wireless



There are five submenus under the Wireless menu: Wireless Settings, Wireless Security, MAC Filtering, Wireless Advanced and Wireless Statistics. Click it, and you will be able to configure the corresponding function.

6.6.1 Wireless Settings

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

Wireless Settings					
Repeater Mode:	💿 Universal Repeater 🔿 WDS Repeater				
Wireless Name of Root AP:	TP-LINK_Network				
MAC Address of Root AP:	94-0C-6D-2F-3C-BE				
Region:	United States				
Warning: Ensure you select a correct country to conform local law.					
	Incorrect settings may cause interference.				
Mode:	11bgn mixed 🔽				
Channel Width:	Auto				
	Enable Wireless Radio				
	Survey				
	Save				

- Repeater Mode In Repeater mode, the wireless repeater relays signal between its stations and the root AP for greater wireless range.
 - Universal Repeater In Repeater mode, the AP with WDS disabled will relay data to an associated root AP. AP function is enabled meanwhile.
 - WDS Repeater In WDS Repeater mode, the AP with WDS enabled will relay data to an associated root AP. AP function is enabled meanwhile.
- > Wireless Name of Root AP The SSID of AP that you want to access.
- > MAC Address of Root AP The MAC address of AP that you want to access.
- > **Survey -** Click this button, you can search the AP which runs in the environment.

- Region Select your region from the pull-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.
- Wireless Security Mode This option should be chosen according to the security configuration of the AP you want to access. It is recommended that the security type is the same as your AP's security type.
- Wireless Password If the AP your router is going to connect need password, you need to fill the password in this blank.

Click **Survey** button on the **Wireless** page, and then **AP List** page will appear. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the third item is selected. The target network's SSID will be automatically filled into the corresponding box.

M.	Count: 16					
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	6C-E8-73-CA-EE-68		68dB	4	None	Connect
2	94-0C-6D-2F-3C-BE	TP-LINK_Network	47dB	4	WPA2-PSK	Connect
3	84-1B-5E-D7-64-F2	TP-LINK_4234CC	31dB	1	WPA2-PSK	Connect
4	4C-60-DE-32-63-8C	TP-LINK_18F710	30dB	11	WPA2-PSK	Connect
5	6C-E8-73-CA-EE-6A	TP-LINK_D0A761	27dB	4	None	Connect
6	14-E6-E4-E3-87-6A	TP-LINK_TEST	16dB	6	WPA2-PSK	Connect
7	78-52-82-02-DD-A1		16dB		MPA-P8K	Connect

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

P Note:

- 1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
 - Near the center of the area in which your wireless stations will operate.
 - In an elevated location such as a high shelf.
 - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
 - Away from large metal surfaces.
- 2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

6.6.2 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).

Wireless Security						
 Disable Security 						
WPA/WPA2 - Personal(Recommended)						
Version:	Automatic(Recomm					
Encryption:	Automatic(Recomm	iended) 🚩				
Wireless Password:						
		characters between 8 and 63 or Hexadecimal characters between 8 and 64.)				
Group Key Update Period:	0 Sec	conds (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 (1-65536	5, 0 stands for default port 1812)				
Radius Password:						
Group Key Update Period:	0 (in s	second, minimum is 30, 0 means no update)				
○ WEP						
Туре:	Automatic 💌					
WEP Key Format:	Hexadecimal 👻					
Key Selected	WEP Key	Кеу Туре				
Key 1: 💿		Disabled 💌				
Key 2:		Disabled 🛩				
Key 3: 🔘		Disabled 🛩				
Key 4: 🔘		Disabled 🛩				
	Save					

- 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. But it's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - 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.

WPA/WPA2 - Personal(Recommend)	led)
Version:	Automatic(Recommended) 🔽
Encryption:	TKIP
Wireless Password:	
	(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period:	O 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 this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

- > WPA/WPA2-Enterprise It's based on Radius Server.
 - Version you can choose the version of the WPA security from the pull-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 Automatic, TKIP or AES.
 - Radius Server IP Enter the IP address of the Radius server.
 - Radius Port Enter the port that Radius server used.
 - 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.
 - **Type** you can choose the type for the WEP security on the pull-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 (Password) 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.

6.6.3 Wireless MAC Filtering

Choose menu "Wireless \rightarrow Wireless MAC Filtering", and then you can control the wireless access by configuring the Wireless MAC Filtering function.

Wireless MAC Filtering			
Wireless MAC Filtering:	Enabled	Disable	
Filtering Rules			
Deny the stations specified by an	v enabled entries i	n the list to access.	
Allow the stations specified by an	iy enabled entries i	n the list to access.	
ID MAC Address	Status	Description	Modify
		Description	Modify

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 access.
- > 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:

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

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** pull-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 stations specified by any enabled entries in the list to access" for **Filtering Rules**.
- 3. Delete all or disable all entries if there are any entries already.
- 4. Click the Add New... button.
 - Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the MAC Address field.
 - Enter wireless station A/B in the **Description** field.
 - Select Enabled in the Status pull-down list.
 - Click the **Save** button.
 - Click the **Back** button.

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

Filtering Rules						
O Deny the stations specified	i by any enabled entr	ries in the list to access.				
 Allow the stations specifie 	d by any enabled enti	ries in the list to access.				
-						
MAC Address	Status	Description	Modify			
00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete			
00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete			
	 Allow the stations specified MAC Address 00-0A-EB-B0-00-0B 	Allow the stations specified by any enabled ent MAC Address O0-0A-EB-B0-00-0B Enabled	 Allow the stations specified by any enabled entries in the list to access. MAC Address Status Description 00-0A-EB-B0-00-0B Enabled wireless station A 			

6.6.4 Wireless Advanced

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

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

- 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 1-255 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 enabled.
- Enable Short GI This function is recommended for it will increase the data capacity by reducing the guard interval time.
- Enable AP Isolation This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

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.

6.6.5 Wireless Statistics

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

Wire	less Statistics						
	Current Connected Wireless Stations numbers: 1 Refresh						
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure		
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	Allow		
		Previous	Next				

- > 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
- > Configure The button is used for loading the item to the Wireless MAC Filtering list.

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.

Note:

This page will be refreshed automatically every 5 seconds.

6.7 DHCP



There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Client List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

6.7.1 DHCP Settings

Choose menu "**DHCP** \rightarrow **DHCP** Settings", and then you can configure the DHCP Server. 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 in 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 (1~28	380 minutes, the default value is 120)
Default Gateway:	0.0.0.0 (0;	otional)
Default Domain:	(0)	otional)
Primary DNS:	0.0.0.0 (0;	otional)
Secondary DNS:	0.0.0.0 (0;	otional)
	Save	

- 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 LAN port of the Router. The default value is 192.168.0.254.
- > 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:

- 1. To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
- 2. When you choose the Smart IP (DHCP) mode in Network → LAN, the DHCP Server function will be disabled. You will see the page as below.

DHCP Server:	🔿 Disable 💿 Er	nable
Start IP Address:	192.168.0.100	
End IP Address:	192.168.0.199	
Address Lease Time:	120 minut	es (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.254	(Optional)
Default Domain:		(Optional)
Primary DNS:	192.168.0.254	(Optional)
Secondary DNS:	192.168.0.254	(Optional)
Note: The DHCP Settings function can (in this situation the device will help yo		ou have choosed Smart IP (DHCP) in Network->LAN ? automaticaly as you need).
	Save	

6.7.2 DHCP Client List

Choose menu "DHCP \rightarrow DHCP Client List", and then you can view the information about the clients attached to the Router.

C	HCP Client Lis	t		
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32
		Refresh		

> 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.

6.7.3 Address Reservation

Choose menu "DHCP \rightarrow Address Reservation", and then you can view and add a reserved address for clients via the next screen. 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.

Addre	ess Reservation			
ID 1	MAC Address 00-11-22-33-44-AA	Reserved IP Address 192.168.0.169	Status Enabled	Modify <u>Modify Delete</u>
Add N	ew Enable All	Disable All Delete All		
		Previous Next		

- > 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.
- > **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

- 1. Click the Add New... button.
- 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 Addres	s Reservation Entry
MAC Address: Reserved IP Address: Status:	Enabled V
	Save Back

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.

6.8 USB Settings

USB Settings
- Storage Sharing
- Media Server
- User Accounts

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

6.8.1 Storage Sharing

Choose menu "**USB Settings**→**Storage Sharing**", you can configure a USB disk drive attached to the router and view volume and share such properties as share name, capacity, used space, and free space on this page as shown below.

Storage	Sharing					
	Service Status:	Started	Stop hared storage wi	th password		
Volume volume1	Capacity 1.9 GB	Used 1.3 GB	Free 626 MB	Use % 67%	Shared Disable	
		Eject Dis	sk Resc	an		

- Service Status Indicates the Network Sharing service's current status. You can click the Start button to start the Storage Sharing service and click the Stop button to stop it.
- Volume The volume name of the USB drive the users have access to. Volume 1-8 is mapping to USB port1, and Volume 9-16 is mapping to USB port2.
- > **Capacity -** The storage capacity of the USB driver.

- **Used -** The used space of the USB driver.
- > Free The available space of the USB driver.
- > **Use% -** The percentage of the used space.
- Shared Indicates the shared or non-shared status of the volume. When the volume is shared, you can click the **Disable** to stop sharing the volume; when volume is non-shared, you can click the **Enable** button to share the volume.

Click the Start button to start the Network Sharing service.

Click the **Stop** button to stop the Network Sharing service.

Click the **Eject Disk** button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Message from webpage	×
This operation will disable Media Server. Are you sure to continue?	
OK	

Click the **Rescan** button to start a new scan.

Follow the instructions below to set up your router as a file server:

- 1. Plug an external USB hard disk drive or USB flash drive into this router.
- 2. Click the **Rescan** button to find the USB drive that has been attached to the router.
- 3. Click the **Start** button to start the Storage Sharing service.
- 4. Click the **Enable** button under **Shared** to enable the disk to share.
- 5. Click the **Open the disk** to visit the sharing disk.

P Note:

- 1. The router can automatically locate new USB drive. But to display the information about your USB device, you need to click the **Rescan** button manually.
- 2. The new settings will not take effect until you restart the service.
- 3. To unplug the USB drive, click **Eject Disk** button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.
- 4. Mounted volumes of each USB port are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.
- 5. If you change the storage settings during the storage connection is established, then the changes will not take effect until the router or the client is rebooted.

6.8.2 Media Server

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

Media Server Setting		
Server Name: Server Status:	TP-LINK_010628 Stopped Start	
Auto-scan every 2 hours 👻	Scan All	
Name File System	Folder	Delete

- > **Server Name -** The name of this Media Server.
- Server Status Indicates the Media Server's current status, started or stopped. You can click the Start button to start the Media Server and click the Stop button to stop it.
- > Name The display name of this folder.
- > File System The file system type on the partition can be FAT32 or NTFS.
- > **Folder** The real full path of the specified folder.
- > **Delete** You can delete the share folder by click **Delete**.

To set up your media server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router, and then the screen will appear as shown below.

Media Server Setting Server Name: Server Status:	TP-LINK_010628 Stopped Start		
Auto-scan every 2 hours V Add share folder	Scan All		
Name File System	F	older	Delete

2. Click the **Start** button to start the media server, and then the screen will appear as shown below.

	Server Name:	TP-LINK 010628			
	Server Status:	Started Stop			
Auto-scan	every 2 hours 🗸	Scan All			
Add share fol	der				
Name	File System		Folder	Delete	

3. Click the **Add share folder** button to specify a folder as the search path of media server. The screen will then appear as shown below.

Add New Folder	
Display Name: Partition:	video
Folder Location:	/my share
Select	Folder
0	photo
۲	video
	Save Back Current No. 1 v page

- > **Display Name -** You can enter a display name for the share folder.
- Share entire partition Choose this option and then the folders contained in this partition will all be shared.
- > Folder Location Displays the location of this folder.
- > Select Check the radio button to select the folder to share.
- > Folder Displays folders that are in current path.
- > **Upper** Click this button to get into the upper folder.
- Save Click this button to save your settings and the page will be redirected to the media server configuration page.
- Back Click this button to discard the settings and just go to the media server configuration page.
- 4. Click the Scan All button to scan all the share folders immediately. You can also select the Auto-scan, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

P Note:

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

6.8.3 User Accounts

You can specify the user name and password for Storage Sharing users on this page. **Storage Sharing** users can use Internet Explorer to access files on the USB drive.

There are two default user accounts that can access the Storage Sharing. They are Administrator and Guest. Administrator has read/write access to Storage Sharing while Guest has read-only access to Storage Sharing.

User Account Management				
Add New User				
User Name	Password	Storage Authority	Modify	
admin	admin	Read and Write	yes	Edit
guest	guest	Read Only	no	Edit
Save				

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

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

- 1. Click Add New User button, and the screen will appear as shown below.
- 2. Self-define a User Name.
- 3. Enter the password in the **Password** field.
- 4. Choose the Storage Authority from the drop-down list, Read and Write or Read Only.

Add or Modify User Acco	unt
User Name:	admin2
Password:	admin
Storage Authority:	Read and Write 💌
	Save Back

User Name - Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.

- Password Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- Storage Authority Choose Read and Write or Read Only from the drop-down list to assign access authority of Storage Sharing to the user.
- Save You can click the Save button to save your settings.
- Back You can click the Back button to discard the settings and just go to the media server configuration page.

P Note:

Please restart the service for the new settings to take effect.

If you cannot use the new user name and password to access the shares, press **Windows logo + R** to open the Run dialog box and type **net use \\192.168.0.254 /delete /yes** and press Enter. (192.168.0.254 is your router's LAN IP address. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.0.254 to 192.168.1.254 to avoid IP conflict; in this case, please try **net use \\192.168.1.254 /delete / yes**.)

6.9 System Tools

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

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

6.9.1 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.

Diagnostic Tools	
Diagnostic Parameters	
Diagnostic Tool:	💿 Ping i 🔿 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	
This device is ready.	
	Start

- > **Diagnostic Tool -** Check the radio button to select one diagnostic tool.
 - **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.

P Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting 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 Type the destination IP address (e.g. 202.108.22.5) or Domain name (e.g. http://www.tp-link.com).
- > **Pings Count -** The number of Ping packets for a Ping connection. The default is 4.
- > **Ping Packet Size -** The size of Ping packet. The default is 64.
- Ping Timeout Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime. The default is 800.
- Traceroute Max TTL The max number of hops for a Traceroute connection. 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 202.108.22.5 with 64 bytes of data:
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=1 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=2 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=3 Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=4
Ping statistics for 202.108.22.5 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1

P Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for **Ping** function. Option "Tracert Hops" are used for **Tracert** function.

6.9.2 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:		Browse
Firmware Version:	3.14.4 Build 130128 Rel.36510n	
Hardware Version:	WR710N v1 00000000	
	Upgrade	

- Firmware Version This displays the current firmware version.
- Hardware Version This 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 more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).
- 2. Type the path and file name of the update file into the **File** field, or click the **Browse** button to locate the update file.
- 3. Click the **Upgrade** button.

P Note:

 New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the 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, otherwise, the Router may be damaged.
- 4. The Router will reboot after the upgrading has been finished.

6.9.3 Factory Defaults

Choose menu "System Tools \rightarrow Factory Defaults", 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

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

- > The default **User Name**: admin
- > The default **Password**: admin
- > The default IP Address: 192.168.0.254
- > The default **Subnet Mask**: 255.255.255.0

Note:

All changed settings will be lost when defaults are restored.

6.9.4 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.

Backup & Restore	•			
Configuration Backup: Configuration File:	Backup	Browse	Restore)

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 locate the update file for the Router, or enter the exact path to the Setting file in the text box.
 - Click the **Restore** button.

P Note:

The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

6.9.5 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 this device.
Reboot

Some settings of the Router will take effect only after rebooting, including:

- > 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.

6.9.6 Password

Choose menu "System Tools \rightarrow Password", and then you can change the factory default user name and password of the Router.

Password	
The username and password must not exc	eed 14 characters in length and must not include any spaces!
Old User Name:	
Old Password:	
New User Name:	
New Password:	
Confirm New Password:	
	Save Clear All

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.

P 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.

Click the **Save** button when finished.

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

6.9.7 System Log

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

System Log					
Auto	Mail Feature: Di	sabled	Ma	ail Settings	
Log T	ype: SHARING	*	Log Le	vel: ALL	
Index	Time	Туре	Level	Log Content	
6	1st day 01:12:56	SHARING	NOTICE	Network sharing service stopped	
5	1st day 00:11:17	SHARING	INFO	Media server started	
4	1 st day 00:08:07	SHARING	NOTICE	Network sharing service started	
3	1 st day 00:08:06	SHARING	NOTICE	Network sharing settings changed	
2	1 st day 00:06:23	SHARING	NOTICE	Network sharing service started	
1	1 st day 00:06:20	SHARING	NOTICE	OTICE Network sharing settings changed	
Time =	2013-01-01 1:55:	47 6948s			
H-Ver	= WR710N ∨1 000	00000 : S-\	/er = 3.14	I.4 Build 130128 Rel.36510n	
L = 192	2.168.0.254 : M = 2	255.255.25	5.0		
W1 = 0	HCP : W = 0.0.0.0	: M = 0.0.0	.0 : G = 0.	0.0.0	
Refresh Save Log Mail Log Clear Log					
Previous Next Current No. 1 V Page					

- > **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. The result will be shown in the later log soon.
- > Clear Log All the logs will be deleted from this device permanently, not just from the page.

Chapter 7. Configuration for Client Mode

This chapter will show each Web page's key functions and the configuration way for Client Mode of the router.

7.1 Login

After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.

Status Quick Setup Working Mode Network Wireless DHCP USB Settings System Tools	
Working Mode Network Wireless DHCP USB Settings	Status
Network Wireless DHCP USB Settings	Quick Setup
Wireless DHCP USB Settings	Working Mode
DHCP USB Settings	Network
USB Settings	Wireless
	DHCP
System Tools	USB Settings
	System Tools

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

7.2 Status

The Status page provides the current status information about the Router on Client Mode. All information is read-only.

Status			
Firmware Version:	3.14.4 Build 130128 Rel.365	10n	
Hardware Version:	WR710N v1 00000000		
Wired			
MAC Address:	00-1D-0F-01-06-28		
IP Address:	192.168.0.254		
Subnet Mask:	255.255.255.0		
Wireless			
Working Mode:	Client		
Wireless Name of Root AP:	TP-LINK_network		
Channel:	11		
Mode:	11bgn mixed		
Channel Width:	Automatic		
MAC Address:	00-1D-0F-01-06-28		
Traffic Statistics			
	Received	Sent	
Bytes:	0	444	
Packets:	0	4	
System Up Time:	0 days 00:01:54	Refresh	1

- > **Firmware Version -** The version information of the Router's firmware.
- > Hardware Version The version information of the Router's hardware.
- Wired This field displays the current settings or information for the LAN, you can configure them in the Network > LAN page.
 - MAC address The physical address of the Router, as seen from the LAN.
 - IP address The LAN IP address of the Router.
 - Subnet Mask The subnet mask associated with LAN IP address.
- Wireless This field displays basic information or status for wireless function, you can configure them in the Wireless > Wireless Settings page.
 - Working Mode The current wireless working mode in use.
 - Wireless Name of Root AP The SSID of Root AP.
 - Channel The current wireless channel in use.
 - Mode The current wireless mode which the Router works on.
 - Channel Width The current wireless channel width in use.

- MAC Address The physical address of the Router, as seen from the WLAN.
- > **Traffic Statistics -** The Router's traffic statistics.
 - Received (Bytes) Traffic that counted in bytes has been received out from the WAN port.
 - Received (Packets) Traffic that counted in packets has been received out from the WAN port.
 - Sent (Bytes) Traffic that counted in bytes has been sent out from the WAN port.
 - Sent (Packets) Traffic that counted in packets has been sent out from the WAN port.
- > System Up Time The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

7.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

7.4 Working Mode

The Router supports five operation mode types: Wireless Router, Access Point, Repeater, Client and Wireless Client Router. Please select one you want. Click Save to save your choice.

Working Mode			
O Wireless Router	- Enable multiple users to share Internet connection via ADSL/Cable Modem		
🔿 Access Point	- Transform your existing wired network to a wireless network		
🔿 Repeater	- Extend your existing wireless coverage by relaying wireless signal		
 Client 	- Acting as a "Wireless Adapter" to connect your wired devices (e.g. Xbox/PS3) to a wireless network		
🔘 WISP Client Router	- Enable multiple users to share Internet connection from WISP		
	Save		

- Wireless Router The wireless Router Mode. In this mode, the device enables multi-user to share Internet via DSL/Cable Modem. The only wired port works as WAN.
- > Access Point The wireless access point mode.
- > Repeater The wireless Repeater Mode. It could extend the range of wireless network.
- Client The Client Mode. The computer connected by Ethernet could get access to an AP by Client mode.
- WISP Client Router In this mode, the device enables multiple users to share Internet connection from WISP.

7.5 Network

```
Network
```

There is only one submenu under the Network menu: LAN.

7.5.1 LAN

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

LAN				
MAC Address:	00-1D-0F-01-06-28			
Type:	Smart IP(DHCP)			
IP Address:	192.168.0.254			
Subnet Mask:	255.255.255.0 🔽			
IGMP Proxy:	Enable 💌			
Note: IGMP(Internet Group Management Protocol) works for IPTV multicast stream. The device supports both IGMP proxy with enable or disable option and IGMP snooping.				
	Save			

- MAC Address The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- Type Choosing Smart IP (DHCP) to get IP address from DHCP server, or choosing static IP to config IP address manually.
- IP Address Enter the IP address of your system in dotted-decimal notation (factory default -192.168.0.254).
- Subnet Mask An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.
- IGMP Proxy The Internet Group Management Protocol(IGMP) feature allows your devices in LAN can watch TV.

P Note:

- 1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
- 2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, while the Virtual Server and DMZ Host will not take effect until they are re-configured.
- 3. When you choose the **Smart IP (DHCP)** mode, the DHCP Server function will be disabled.

7.6 Wireless



There are two submenus under the Wireless menu: **Wireless Settings** and **Wireless Security**. Click any of them, and you will be able to configure the corresponding function.

7.6.1 Wireless Settings

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

eless Settings			
Enable WDS			
Wireless Name of Root AP:	TP-LINK Network		
MAC Address of Root AP:	94-0C-6D-2F-3C-BE		
Region:	United States		
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.		
	🗹 Enable Wireless Radio		
	Survey		
	Save		

- Enable WDS The AP client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consisting of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please enable this option.
- > Wireless Name of Root AP Enter the SSID of AP that you want to access.
- > MAC Address of Root AP Enter the MAC address of AP that you want to access.
- Region Select your region from the pull-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.
- Enable Wireless Radio The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP, otherwise, wireless stations will not be able to access the AP.
- > **Survey** Click this button, you can search the APs.
- P Note:

- 1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
 - Near the center of the area in which your wireless stations will operate.
 - In an elevated location such as a high shelf.
 - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
 - Away from large metal surfaces.
- 2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

7.6.2 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).

Wireless Security				
O Disable Security				
WPA/WPA2 - Personal(Recomment)	WPA/WPA2 - Personal(Recommended)			
Version:	Automatic(Recomm	ended) 💌		
Encryption:	Automatic(Recomm	ended) 🔽		
Wireless Password:				
	(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)			
Group Key Update Period:	0 Sec	onds (Keep it default if you are not sure, minimum is 30, 0 means no update)		
O WPA/WPA2 - Enterprise				
Version:	Automatic 👻			
Encryption:	Automatic			
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)			
○ WEP				
Туре:	Automatic 💌			
WEP Key Format:	Hexadecimal 👻			
Key Selected	WEP Key	Кеу Туре		
Key 1: 💿		Disabled 💌		
Key 2:		Disabled 💌		
Key 3: 🔵		Disabled 💌		
Key 4: 🔘		Disabled 💌		
	Save			

- 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. But it's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - 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.

Solution Note:

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

WPA/WPA2 - Personal(Recomment)	ided)
Version:	Automatic(Recommended) 💌
Encryption:	ТКІР
Wireless Password:	
	(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 this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

- > WPA /WPA2-Enterprise It's based on Radius Server.
 - Version you can choose the version of the WPA security from the pull-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 Automatic, TKIP or AES.
 - Radius Server IP Enter the IP address of the Radius server.
 - Radius Port Enter the port that Radius server used.
 - 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.
 - **Type** you can choose the type for the WEP security on the pull-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 (Password) 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.

7.7 DHCP



There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Client List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

7.7.1 DHCP Settings

Choose menu "**DHCP** \rightarrow **DHCP** Settings", and then you can configure the DHCP Server. 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 in the LAN.

DHCP Settings		
DHCP Server:	💿 Disable 🔘 Enal	ole
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:	0.0.0.0	(optional)
Default Domain:		(optional)
Primary DNS:	0.0.0.0	(optional)
Secondary DNS:	0.0.0.0	(optional)
	Save	

- 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 LAN port of the Router. The default value is 192.168.0.254.
- > **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:

- 1. To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically". This function will take effect until this device reboots.
- 2. When you choose the **Smart IP (DHCP)** mode in **Network** → **LAN**, the DHCP Server function will be disabled. You will see the page as below.

DHCP Server:	🔿 Disable 💿 Ena	able
Start IP Address:	192.168.0.100	
End IP Address:	192.168.0.199	
Address Lease Time:	120 minute	s (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.254	(Optional)
Default Domain:		(Optional)
Primary DNS:	192.168.0.254	(Optional)
Secondary DNS:	192.168.0.254	(Optional)

7.7.2 DHCP Client List

Choose menu "DHCP \rightarrow DHCP Client List", and then you can view the information about the clients attached to the Router.

C	HCP Client Lis	t			
ID	Client Name	MAC Address	Assigned IP	Lease Time	
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47	
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32	
	Refresh				

- > 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.

7.7.3 Address Reservation

Choose menu "DHCP \rightarrow Address Reservation", and then you can view and add a reserved address for clients via the next screen. 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.

			Status	Modify
00-11	1-22-33-44-AA	192.168.0.169	Enabled	Modify Delete

- > 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.
- > **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

- 1. Click the **Add New...** button. Then figure shown below 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 V	
	Save Back	

To modify or delete an existing entry:

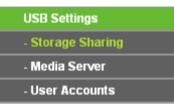
- 1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
- 2. Modify the information.
- 3. Click the **Save** button.

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.

7.8 USB Settings



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

7.8.1 Storage Sharing

Choose menu "**USB Settings**→**Storage Sharing**", you can configure a USB disk drive attached to the router and view volume and share such properties as share name, capacity, used space, and free space on this page as shown below.

Storage	Sharing					
	Service Status:	Started	Stop hared storage wi	th password		
Volume	Capacity	Used	Free	Use%	Shared	
volume1	1.9 GB	1.3 GB	626 MB	67%	Disable	

- Service Status Indicates the Network Sharing service's current status. You can click the
 Start button to start the Storage Sharing service and click the Stop button to stop it.
- Volume The volume name of the USB drive the users have access to. Volume 1-8 is mapping to USB port1, and Volume 9-16 is mapping to USB port2.
- > **Capacity -** The storage capacity of the USB driver.
- > **Used -** The used space of the USB driver.
- > **Free -** The available space of the USB driver.
- > **Use% -** The percentage of the used space.
- Shared Indicates the shared or non-shared status of the volume. When the volume is shared, you can click the Disable to stop sharing the volume; when volume is non-shared, you can click the Enable button to share the volume.

Click the Start button to start the Network Sharing service.

Click the Stop button to stop the Network Sharing service.

Click the **Eject Disk** button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Message f	rom webpage		— ×
?	This operation will disable Media Server.	Are you sure to continue?	
		OK Ca	ncel

Click the **Rescan** button to start a new scan.

Follow the instructions below to set up your router as a file server:

- 1. Plug an external USB hard disk drive or USB flash drive into this router.
- 2. Click the **Rescan** button to find the USB drive that has been attached to the router.
- 3. Click the **Start** button to start the Storage Sharing service.
- 4. Click the **Enable** button under **Shared** to enable the disk to share.
- 5. Click the **Open the disk** to visit the sharing disk.

P Note:

- 1. The router can automatically locate new USB drive. But to display the information about your USB device, you need to click the **Rescan** button manually.
- 2. The new settings will not take effect until you restart the service.
- 3. To unplug the USB drive, click **Eject Disk** button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.
- 4. Mounted volumes of each USB port are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.
- 5. If you change the storage settings during the storage connection is established, then the changes will not take effect until the router or the client is rebooted.

7.8.2 Media Server

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

	Server Name: Server Status:	TP-LINK_010628 Stopped Start		
Auto-scan		Scan All		
lame	File System		Folder	Delete

- **Server Name -** The name of this Media Server.
- Server Status Indicates the Media Server's current status, started or stopped. You can click the Start button to start the Media Server and click the Stop button to stop it.
- > **Name** The display name of this folder.
- > File System The file system type on the partition can be FAT32 or NTFS.
- > Folder The real full path of the specified folder.
- > **Delete** You can delete the share folder by click **Delete**.

To set up your media server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router, and then the screen will appear as shown below.

Media Server Setting			
Server Name: Server Status:	TP-LINK_010628 Stopped Start		
Auto-scan every 2 hours Y	Scan All		
Name File System		Folder	Delete

2. Click the **Start** button to start the media server, and then the screen will appear as shown below.

Media Server Setting			
Server Name: Server Status:	TP-LINK_010628 Started Stop		
Auto-scan every 2 hours Y	Scan All		
Name File System		Folder	Delete

3. Click the **Add share folder** button to specify a folder as the search path of media server. The screen will then appear as shown below.

Add New Folder	
Display Name:	video
Partition:	Share entire partition
Folder Location:	/my share
Select	Folder
0	<u>photo</u>
۲	video
	Save Back Current No. 1 v page

- > Display Name You can enter a display name for the share folder.
- Share entire partition Choose this option and then the folders contained in this partition will all be shared.
- > Folder Location Displays the location of this folder.
- > **Select** Check the radio button to select the folder to share.
- > **Folder** Displays folders that are in current path.
- > **Upper** Click this button to get into the upper folder.
- Save Click this button to save your settings and the page will be redirected to the media server configuration page.
- Back Click this button to discard the settings and just go to the media server configuration page.
- 4. Click the Scan All button to scan all the share folders immediately. You can also select the Auto-scan, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

Note:

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

7.8.3 User Accounts

You can specify the user name and password for Storage Sharing users on this page. **Storage Sharing** users can use Internet Explorer to access files on the USB drive.

There are two default user accounts that can access the Storage Sharing. They are Administrator and Guest. Administrator has read/write access to Storage Sharing while Guest has read-only access to Storage Sharing.

User Account Mar	nagement			
Add New User				
User Name	Password	Storage Authority	Modify	
admin	admin	Read and Write	yes	Edit
guest	guest	Read Only	no	Edit
Save				

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

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

- 1. Click Add New User button, and the screen will appear as shown below.
- 2. Self-define a User Name.
- 3. Enter the password in the **Password** field.
- 4. Choose the Storage Authority from the drop-down list, **Read and Write** or **Read Only**.

Add or Modify User Acco	unt
User Name:	admin2
Password:	admin
Storage Authority:	Read and Write 💌
	Save Back

- User Name Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.
- Password Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- Storage Authority Choose Read and Write or Read Only from the drop-down list to assign access authority of Storage Sharing to the user.
- Save You can click the Save button to save your settings.
- Back You can click the Back button to discard the settings and just go to the media server configuration page.

P Note:

Please restart the service for the new settings to take effect.

If you cannot use the new user name and password to access the shares, press **Windows logo + R** to open the Run dialog box and type **net use \\192.168.0.254 /delete /yes** and press Enter. (192.168.0.254 is your router's LAN IP address. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.0.254 to 192.168.1.254 to avoid IP conflict; in this case, please try **net use \\192.168.1.254 /delete / yes**.)

7.9 System Tools

5	System Tools
	Diagnostic
	Firmware Upgrade
	Factory Defaults
	Backup & Restore
	Reboot
	Password
	System Log

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

7.9.1 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.

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				

- > **Diagnostic Tool -** Check the radio button to select one diagnostic tool.
 - **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.

P Note:

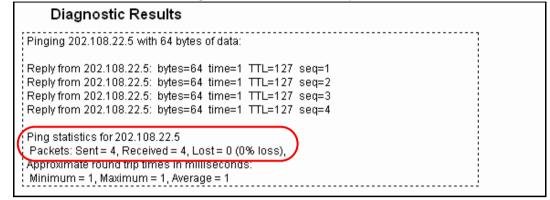
You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by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

- IP Address/Domain Name Type the destination IP address (e.g. 202.108.22.5) or Domain name (e.g.http://www.tp-link.com).
- > **Pings Count -** The number of Ping packets for a Ping connection. The default is 4.
- > **Ping Packet Size -** The size of Ping packet. The default is 64.
- Ping Timeout Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime. The default is 800.
- Traceroute Max TTL The max number of hops for a Traceroute connection. 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.



P Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for **Ping** function. Option "Tracert Hops" are used for **Tracert** function.

7.9.2 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:		Browse
Firmware Version:	3.14.4 Build 130128 Rel.36510n	
Hardware Version:	WR710N v1 00000000	
	Upgrade	

- Firmware Version This displays the current firmware version.
- Hardware Version This 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 more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).
- 2. Type the path and file name of the update file into the **File** field, or click the **Browse** button to locate the update file.
- 3. Click the **Upgrade** button.

P Note:

- New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the 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, otherwise, the Router may be damaged.
- 4. The Router will reboot after the upgrading has been finished.

7.9.3 Factory Defaults

Choose menu "System Tools \rightarrow Factory Defaults", 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

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

- > The default **User Name**: admin
- > The default **Password**: admin
- > The default IP Address: 192.168.0.254
- > The default Subnet Mask: 255.255.255.0

P Note:

All changed settings will be lost when defaults are restored.

7.9.4 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.

Backup & Restor	re			
Configuration Backup: Configuration File:	Backup	Browse	Restore	

- 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 locate the update file for the Router, or enter the exact path to the Setting file in the text box.
 - Click the **Restore** button.

P Note:

The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

7.9.5 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 this device.
Reboot

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.

7.9.6 Password

Choose menu "System Tools \rightarrow Password", and then you can change the factory default user name and password of the Router.

Password		
The username and password must not exce	ed 14 characters in length and must not include any spaces!	
Old User Name:		
Old Password:		
New User Name:		
New Password:		
Confirm New Password:		
	Save Clear All	

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.

P 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.

Click the Save button when finished.

Click the Clear All button to clear all.

7.9.7 System Log

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

System Log				
Auto	Mail Feature: Di	sabled	Ma	ail Settings
Log T	ype: SHARING	*	Log Le	vel: ALL
Index	Time	Туре	Level	Log Content
6	1st day 01:12:56	SHARING	NOTICE	Network sharing service stopped
5	1st day 00:11:17	SHARING	INFO	Media server started
4	1 st day 00:08:07	SHARING	NOTICE	Network sharing service started
3	1 st day 00:08:06	SHARING	NOTICE	Network sharing settings changed
2	1 st day 00:06:23	SHARING	NOTICE	Network sharing service started
1	1 st day 00:06:20	SHARING	NOTICE	Network sharing settings changed
Time =	2013-01-01 1:55:	47 6948s		
H-Ver	H-Ver = WR710N ∨1 00000000 : S-Ver = 3.14.4 Build 130128 Rel.36510n			
L = 192	L = 192.168.0.254 : M = 255.255.255.0			
W1 = 0	W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0			
	Defresh Save Log Mail Log Clear Log			
Refresh Save Log Mail Log Clear Log				
			Pr	evious Next Current No. 1 V Page

- > **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. The result will be shown in the later log soon.
- > Clear Log All the logs will be deleted from this device permanently, not just from the page.

Chapter 8. Configuration for WISP Client Router Mode

This chapter will show each Web page's key functions and the configuration way for WISP Client Router Mode of the router.

8.1 Login

After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.

Status
Quick Setup
WPS
Working Mode
Network
Wireless
DHCP
USB Settings
Forwarding
Security
Parental Control
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
System Tools

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

8.2 Status

The Status page provides the current status information about the Router on WISP Client Router Mode. All information is read-only.

	System Up Time:	0 days 00:02:38	Refresh
	Packets:	0	0
	Bytes:	0	0
		Received	Sent
Traffic S	tatistics		
	Subnet Mask:	0.0.0.0	Renew
	IP Address:	0.0.0.0	Dynamic IP
Seconda	ary Connection		
	Online Time:	0 day(s) 00:00:00	Connecting
	DNS Server:	0.0.0.0,0.0.0.0	
	Default Gateway:	0.0.0.0	
	Subnet Mask:	0.0.0.0	
	IP Address:	0.0.0.0	PPPoE(Connect Automatically)
	MAC Address:	00-1D-0F-01-06-29	
WAN			
	Client Status:	Run	
	MAC Address:	00-1D-0F-01-06-28	
	Channel Width:	Automatic	
	Mode:	11bgn mixed	
	Channel:	4	
	Name (SSID):	TP-LINK_2046F2	
	Wireless Radio:	Enable	
Wireless	Working Mode:	WISP Client Router	
	Subnet Mask:	255.255.255.0	
	IP Address:	192.168.0.254	
LAN	MAC Address:	00-1D-0F-01-06-28	
H	lardware Version:	WR710N v1 00000000	
F	irmware Version:	3.14.4 Build 130128 Rel.36510n	
F	irmware Version:	3.14.4 Build 130128 Rel.36510n	

- > **Firmware Version -** The version information of the Router's firmware.
- > Hardware Version The version information of the Router's hardware.
- LAN This field displays the current settings or information for the LAN, you can configure them in the Network>LAN page.
 - MAC Address The physical address of the Router, as seen from the LAN.

- IP Address The LAN IP address of the Router.
- Subnet Mask The subnet mask associated with LAN IP address.
- Wireless This field displays basic information or status for wireless function, you can configure them in the Wireless > Wireless Settings page.
 - Working Mode The current wireless working mode in use.
 - Wireless Radio Indicates whether the wireless radio feature of the AP is enabled or disabled.
 - Name (SSID) The SSID of the AP.
 - Channel The current wireless channel in use.
 - **Mode** The current wireless mode which the Router works on.
 - Channel Width The current wireless channel width in use.
 - MAC Address The physical address of the Router, as seen from the WLAN.
 - Client Status The status of Client.
- WAN This field displays the current settings or information for the WAN, you can configure them in the Network > WAN page.
 - MAC Address The physical address of the WAN port, as seen from the Internet.
 - **IP Address** The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to the Internet.
 - Subnet Mask The subnet mask associated with the WAN IP Address.
 - Default Gateway The Gateway currently used by the Router is shown here. When you use Dynamic IP as the connection Internet type, the Renew button will be displayed here. Click the Renew Button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address, Release button will be displayed here. Click the Release button to release the IP address the Router has obtained from the ISP.
 - **DNS Server** The DNS (Domain Name System) server IP addresses currently used by the Router.
 - Online Time The time that you online. When you use PPPoE as WAN connection type, the online time is displayed here. Click the Connect or Disconnect button to connect to or disconnect from Internet.
- Secondary Connection Besides PPPoE, if you use an extra connection type to connect to a local area network provided by ISP, then parameters of this secondary connection will be shown in this area.
 - **IP Address** The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to the Internet.
 - Subnet Mask The subnet mask associated with the WAN IP Address.

Click the **Release** to delete the network parameters, and click the **Renew** button to obtaining network parameters.

- > Traffic Statistics The Router's traffic statistics.
 - Received (Bytes) Traffic that counted in bytes has been received out from the WAN port.
 - Received (Packets) Traffic that counted in packets has been received out from the WAN port.
 - Sent (Bytes) Traffic that counted in bytes has been sent out from the WAN port.
 - Sent (Packets) Traffic that counted in packets has been sent out from the WAN port.
- > System Up Time The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

8.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

8.4 Working Mode

The Router supports five operation mode types: Wireless Router, Access Point, Repeater, Client and Wireless Client Router. Please select one you want. Click Save to save your choice.

Working Mode	
 Wireless Router 	- Enable multiple users to share Internet connection via ADSL/Cable Modem
🔘 Access Point	- Transform your existing wired network to a wireless network
Repeater	- Extend your existing wireless coverage by relaying wireless signal
🔘 Client	- Acting as a "Wireless Adapter" to connect your wired devices (e.g. Xbox/PS3) to a wireless network
WISP Client Router	- Enable multiple users to share Internet connection from WISP
	Save

- Wireless Router The wireless Router Mode. In this mode, the device enables multi-user to share Internet via DSL/Cable Modem. The only wired port works as WAN.
- > Access Point The wireless access point mode.
- > Repeater The wireless Repeater Mode. It could extend the range of wireless network.
- Client The Client Mode. The computer connected by Ethernet could get access to an AP by Client mode.
- WISP Client Router In this mode, the device enables multiple users to share Internet connection from WISP.

8.5 Network

Network	
- WAN	
- MAC Clone	
- LAN	

There are three submenus under the Network menu: **WAN**, **MAC Clone** and **LAN**. Click any of them, and you will be able to configure the corresponding function.

8.5.1 WAN

Choose menu "**Network** \rightarrow **WAN**", and then 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 follow:

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 WAN port is unplugged!
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:	TL-WR710N
	Get IP with Unicast DHCP (It is usually not required.)
	Save

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.

P 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**, **Default Gateway** and **DNS** setting, select **Static IP**. The Static IP settings page will appear.

WAN	
WAN Connection Type:	Static IP
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	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

- > 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 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. Then you should enter the following parameters:

WAN	
WAN Connection Type:	PPPoE/Russia PPPoE 💌 Detect
PPPoE Connection:	
User Name:	username
Password:	
Confirm Password:	
Secondary Connection:	💿 Disabled O 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.)
	Onnect 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 Disconnected!
	Save Advanced

- > User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Confirm Password Enter again the Password provided by your ISP to ensure the password you entered is correct.
- 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 \rightarrow Time" 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 below will then appear:

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

- 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.

4. If your ISP provides BigPond Cable connection, please select **BigPond Cable** option. Then you should enter the following parameters:

WAN	
WAN Connection Type:	BigPond Cable
User Name:	username
Password:	
Auth Server:	sm-server
Auth Domain:	
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
Connection Mode:	Onnect 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

- > 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,
- 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.
- 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. Then you should enter the following parameters:

WAN	
WAN Connection Type:	L2TP/Russia L2TP 💌
User Name:	username
Password:	
	Connect Disconnect Disconnected!
	💿 Dynamic IP j 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 lutes).	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.)
Max fale filme:	15 minutes (o means remain acuve at an unres.)
Connection Mode:	Onnect on Demand
	O Connect Automatically
	Connect Manually
	Save

- > 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:

WAN		
WAN Connection Type:	PPTP/Russia PPTP 🔽	
User Name: Password:	usemame Connect Disconnected!	
	⊙ Dynamic IP _ Static IP	
Server IP Address/Name:		
IP Address: Subnet Mask:	0.0.0.0	
	0.0.0	
Gateway: DNS:	0.0.0.0 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): Max Idle Time:	1420(The default is 1420, do not change unless necessary.)15minutes (0 means remain active at all times.)	
Connection Mode:	 Connect on Demand Connect Automatically 	
	Connect Manually	
	Save	

- 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.

8.5.2 MAC Clone

Choose menu "**Network** \rightarrow **MAC Clone**", and then you can configure the WAN MAC address on the screen below:

MAC Clone			
WAN MAC Address:	00-1D-0F-01-06-29	Restore Factory MAC	
Your PC's MAC Address:	6C-62-6D-F7-31-8D	Clone MAC Address	
	Cara		
	Save		

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 WAN 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 To button and this MAC address will fill in the WAN MAC Address field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

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

P Note:

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

2. If you change WAN MAC Address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

8.5.3 LAN

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

LAN	
MAC Address:	00-1D-0F-01-06-28
IP Address:	192.168.0.254
Subnet Mask:	255.255.255.0 💌
IGMP Proxy:	Enable 💌
Note: IGMP(Internet Group Management Protocol) works for IPTV multicast stream. The device supports both IGMP proxy with enabled or disable option and IGMP snooping.	
	Save

- MAC Address The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- IP Address Enter the IP address of your Router in dotted-decimal notation (factory default: 192.168.0.254).
- Subnet Mask An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- IGMP Proxy The Internet Group Management Protocol (IGMP) feature allows your devices in LAN can watch TV.
- P Note:
- 1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
- 2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

8.6 Wireless

Wireless
- Wireless Settings
- Wireless Security
- Wireless MAC Filtering
- Wireless Advanced
- Wireless Statistics

There are five submenus under the Wireless menu: Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced and Wireless Statistics. Click any of them, and you will be able to configure the corresponding function.

8.6.1 Wireless Settings

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

Wireless Settings	
Wilciess Octaings	
Client Setting	
SSID:	TP-LINK_Network
BSSID:	94-0C-6D-2F-3C-BE Example:00-1D-0F-11-22-33
	Survey
Key type:	WPA-PSK/WPA2-PSK
WEP Index:	1
Auth type:	open
Password:	1234567890
AP Setting	
Local SSID:	TP-LINK_2046F2
	Enable Wireless Router Radio
	🗹 Enable SSID Broadcast
	Disable Local Wireless Access
	Save

- 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. But it's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on pre-shared passphrase.

- 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-PSK/WPA2-PSK** radio button and choose TKIP encryption, you will find a notice in red.

WPA/WPA2 - Personal(Recommended)		
Version:	Automatic(Recommended)	
Encryption:	TKIP	
Wireless Password:		
	(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)	
Group Key Update Period:	O 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 this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.	

- > WPA/WPA2-Enterprise It's based on Radius Server.
 - Version you can choose the version of the WPA security from the pull-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 Automatic, TKIP or AES.
 - Radius Server IP Enter the IP address of the Radius server.
 - Radius Port Enter the port that Radius server used.
 - 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.
 - **Type** you can choose the type for the WEP security on the pull-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 (Password) 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.

8.6.2 Wireless Security

Wireless Security		
 Disable Security 		
WPA/WPA2 - Personal(Recomment	ded)	
Version:	Automatic(Recomm	ended) 💌
Encryption:	Automatic(Recomm	ended) 🔽
Wireless Password:		
		haracters between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period:	0 Se	conds (Keep it default if you are not sure, minimum is 30, 0 means no update)
O WPA/WPA2 - Enterprise		
Version:	Automatic 🔽	
Encryption:	Automatic 🔽	_
Radius Server IP:		
Radius Port:	1812 (1-6553	5, 0 stands for default port 1812)
Radius Password:		
Group Key Update Period:	0 (in :	second, minimum is 30, 0 means no update)
○ WEP		
Туре:	Automatic 💌	
WEP Key Format:	Hexadecimal 💌	
Key Selected	WEP Key	Кеу Туре
Key 1: 💿		Disabled 💌
Key 2:		Disabled 💌
Key 3: 🔿		Disabled 💌
Key 4: 🔿		Disabled 💌
	Save	

- 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. But it's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - 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.

WPA/WPA2 - Personal(Recommended)		
Version:	Automatic(Recommended) 💌	
Encryption:	ТКІР	
Wireless Password:		
	(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 this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.	

- > WPA/WPA2-Enterprise It's based on Radius Server.
 - Version you can choose the version of the WPA security from the pull-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 Automatic, TKIP or AES.
 - Radius Server IP Enter the IP address of the Radius server.
 - Radius Port Enter the port that Radius server used.
 - 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.
 - **Type** you can choose the type for the WEP security on the pull-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 (Password) 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.

8.6.3 Wireless MAC Filtering

Choose menu "Wireless \rightarrow Wireless MAC Filtering", and then you can control the wireless access by configuring the Wireless MAC Filtering function.

Wireless MAC Filtering			
Wireless MAC Filtering:	Enabled (Disable	
Filtering Rules			
Oeny the stations specified by ar	y enabled entries	in the list to access.	
Allow the stations specified by an example.	ny enabled entries	; in the list to access.	
ID MAC Address	Status	Description	Modify
Add New Enable All	isable All	Delete All	
F	Previous	Next	

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 access.
- > 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:

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

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.

- 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** pull-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 stations specified by any enabled entries in the list to access" for **Filtering Rules**.
- 3. Delete all or disable all entries if there are any entries already.
- 4. Click the Add New... button.
 - 1) Enter the MAC address 00-0A-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** pull-down list.
 - 4) Click the **Save** button.
 - 5) Click the **Back** button.

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

iltering Rules			
O Deny the stations specifi	ed by any enabled entr	ries in the list to access.	
 Allow the stations specif 	ied by any enabled enti	ries in the list to access.	
-			
MAC Address	Status	Description	Modify
00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete
	 Deny the stations specifi Allow the stations specifi MAC Address	 Deny the stations specified by any enabled entr Allow the stations specified by any enabled entr MAC Address Status 	 Deny the stations specified by any enabled entries in the list to access. Allow the stations specified by any enabled entries in the list to access. MAC Address Status Description

8.6.4 Wireless Advanced

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

Vireless Advanced				
Transmit Power:	High 🔽			
Beacon Interval :	100 (40-1000)			
RTS Threshold:	2346 (256-234)	0		
Fragmentation Threshold:	2346 (256-234)	0		
DTIM Interval:	1 (1-255)			
	 Enable WMM Enable Short GI 			
	📃 Enable AP Isolation			
	Save			

- 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 1-255 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 enabled.
- Enable Short GI This function is recommended for it will increase the data capacity by reducing the guard interval time.
- Enable AP Isolation This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

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.

8.6.5 Wireless Statistics

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

Wire	eless Statistics				
	Curre	ent Connected Wireless	Stations numbers: 1	Refresh	
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	Allow
		Previous	Next		

- > 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.
- > Configure The button is used for loading the item to the Wireless MAC Filtering list.
 - Allow If the Wireless MAC Filtering function enable, allow the station to access.
 - Deny If the Wireless MAC Filtering function enable, deny the station to access.

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.

8.7 DHCP

DHCP	
- DHCF	P Settings
- DHCF	P Client List
- Addr	ess Reservation

There are three submenus under the DHCP menu: **DHCP Settings**, **DHCP Client List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function.

8.7.1 DHCP Settings

Choose menu "**DHCP** \rightarrow **DHCP** Settings", and then you can configure the DHCP Server. 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 in the LAN.

DHCP Settings		
DHCP Server:	🔿 Disable 💿 Enabl	e
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:	192.168.0.254	(Optional)
Default Domain:		(Optional)
Primary DNS:	0.0.0.0	(Optional)
Secondary DNS:	0.0.0.0	(Optional)
	Save	

- 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 LAN port of the Router. The default value is 192.168.0.254.
- > 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. 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".

8.7.2 DHCP Client List

Choose menu "DHCP \rightarrow DHCP Client List", and then you can view the information about the clients attached to the Router.

DHCP Client List						
ID	Client Name	MAC Address	Assigned IP	Lease Time		
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47		
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32		
		Refresh				

- > 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.

8.7.3 Address Reservation

Choose menu "DHCP \rightarrow Address Reservation", and then you can view and add a reserved address for clients via the next screen. 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.

Addr	ess Reservation			
ID 1	MAC Address 00-11-22-33-44-AA	Reserved IP Address 192.168.0.169	Status Enabled	Modify <u>Modify Delete</u>
Add N	lew Enable All	Disable All Delete All		
		Previous Next		

- > 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.
- > **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

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

Add or Modify an Addres	s Reservation Entry
MAC Address: Reserved IP Address: Status:	Enabled V
	Save Back

To modify or delete an existing entry:

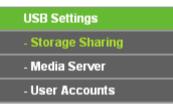
- 1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
- 2. Modify the information.
- 3. Click the **Save** button.

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.

8.8 USB Settings



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

8.8.1 Storage Sharing

Choose menu "**USB Settings**→**Storage Sharing**", you can configure a USB disk drive attached to the router and view volume and share such properties as share name, capacity, used space, and free space on this page as shown below.

Storage	Sharing					
	Service Status:	Started [Stop shared storage wi	th password		
Volume	Capacity	Used	Free	Use%	Shared	
volume1	1.9 GB	1.3 GB	626 MB	67%	Disable	
		Eject Di	sk Resc	an		

- Service Status Indicates the Network Sharing service's current status. You can click the
 Start button to start the Storage Sharing service and click the Stop button to stop it.
- Volume The volume name of the USB drive the users have access to. Volume 1-8 is mapping to USB port1, and Volume 9-16 is mapping to USB port2.
- > **Capacity -** The storage capacity of the USB driver.
- > **Used -** The used space of the USB driver.
- > **Free -** The available space of the USB driver.
- > **Use% -** The percentage of the used space.
- Shared Indicates the shared or non-shared status of the volume. When the volume is shared, you can click the Disable to stop sharing the volume; when volume is non-shared, you can click the Enable button to share the volume.

Click the Start button to start the Network Sharing service.

Click the Stop button to stop the Network Sharing service.

Click the **Eject Disk** button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Message f	rom webpage		×
?	This operation will disable Media Server.	Are you sure to continue?	
		ОК	Cancel

Click the **Rescan** button to start a new scan.

Follow the instructions below to set up your router as a file server:

- 1. Plug an external USB hard disk drive or USB flash drive into this router.
- 2. Click the **Rescan** button to find the USB drive that has been attached to the router.
- 3. Click the **Start** button to start the Storage Sharing service.
- 4. Click the **Enable** button under **Shared** to enable the disk to share.
- 5. Click the **Open the disk** to visit the sharing disk.

P Note:

- 1. The router can automatically locate new USB drive. But to display the information about your USB device, you need to click the **Rescan** button manually.
- 2. The new settings will not take effect until you restart the service.
- 3. To unplug the USB drive, click **Eject Disk** button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.
- 4. Mounted volumes of each USB port are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.
- 5. If you change the storage settings during the storage connection is established, then the changes will not take effect until the router or the client is rebooted.

8.8.2 Media Server

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

	Server Name: Server Status:	TP-LINK_010628 Stopped Start		
Auto-scan		Scan All		
Name	File System		Folder	Delete

- **Server Name -** The name of this Media Server.
- Server Status Indicates the Media Server's current status, started or stopped. You can click the Start button to start the Media Server and click the Stop button to stop it.
- > **Name** The display name of this folder.
- > File System The file system type on the partition can be FAT32 or NTFS.
- > Folder The real full path of the specified folder.
- > **Delete** You can delete the share folder by click **Delete**.

To set up your media server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router, and then the screen will appear as shown below.

	Server Name: Server Status:	TP-LINK_010628 Stopped Start		
Auto-scan every 2 hours Scan All				
Name	File System		Folder	Delete

2. Click the **Start** button to start the media server, and then the screen will appear as shown below.

Media Server Setting				
Server Name: Server Status:	TP-LINK_010628 Started Stop			
Auto-scan every 2 hours V	Scan All			
Name File System	1	Folder	Delete	

3. Click the **Add share folder** button to specify a folder as the search path of media server. The screen will then appear as shown below.

Add New Folder	
Display Name: Partition: Folder Location:	video Share entire partition /my share
Select	Folder
0	photo
۲	video
	Save Back Current No. 1 v page

- > **Display Name** You can enter a display name for the share folder.
- Share entire partition Choose this option and then the folders contained in this partition will all be shared.
- > Folder Location Displays the location of this folder.
- > **Select** Check the radio button to select the folder to share.
- > **Folder** Displays folders that are in current path.
- > **Upper** Click this button to get into the upper folder.
- Save Click this button to save your settings and the page will be redirected to the media server configuration page.
- Back Click this button to discard the settings and just go to the media server configuration page.
- 4. Click the **Scan All** button to scan all the share folders immediately. You can also select the **Auto-scan**, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

P Note:

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

8.8.3 User Accounts

You can specify the user name and password for Storage Sharing users on this page. **Storage Sharing** users can use Internet Explorer to access files on the USB drive.

There are two default user accounts that can access the Storage Sharing. They are Administrator and Guest. Administrator has read/write access to Storage Sharing while Guest has read-only access to Storage Sharing.

User Account Management				
Add New User				
User Name	Password	Storage Authority	Modify	
admin	admin	Read and Write	yes	Edit
guest	guest	Read Only	no	Edit
Save				

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

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

- 1. Click Add New User button, and the screen will appear as shown above.
- 2. Self-define a User Name.
- 3. Enter the password in the **Password** field.
- 4. Choose the Storage Authority from the drop-down list, **Read and Write** or **Read Only**.

Add or Modify User Acco	unt
User Name: Password: Storage Authority:	admin2 admin Read and Write 💌
	Save Back

- User Name Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.
- Password Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- Storage Authority Choose Read and Write or Read Only from the drop-down list to assign access authority of Storage Sharing to the user.
- Save You can click the Save button to save your settings.
- Back You can click the Back button to discard the settings and just go to the media server configuration page.

P Note:

Please restart the service for the new settings to take effect.

If you cannot use the new user name and password to access the shares, press **Windows logo + R** to open the Run dialog box and type **net use \\192.168.0.254 /delete /yes** and press Enter. (192.168.0.254 is your router's LAN IP address. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.0.254 to 192.168.1.254 to avoid IP conflict; in this case, please try **net use \\192.168.1.254 /delete / yes**.)

8.9 Forwarding

Forwarding
- Virtual Servers
- Port Triggering
- DMZ
- UPnP

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

8.9.1 Virtual Servers

Choose menu "Forwarding \rightarrow Virtual Servers", and then you can view and add virtual servers. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the 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 be changed when using the DHCP function.

Virtual Servers					
ID Service Port	Internal Port	IP Address	Protocol	Status	Modify
Add New	Enable All Disable All	Delete All			
	Previous	Next			

- Service Port The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- 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 providing 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, either Enabled or Disabled.
- > **Modify -** To modify or delete an existing entry.

To setup a virtual server entry:

- 1. Click the Add New... button, the next screen will pop-up as shown below.
- Select the service port you want to use from the Common Service Port list. If the Common Service Port list does not have the service that you want to use, type the service port number or service port range in the Service Port box.
- 3. Type the IP Address of the computer in the **IP Address** box.
- 4. Select the protocol used for this application, either TCP, UDP, or All.
- 5. Select the **Enable** to enable the virtual server.
- 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 it blank)	
IP Address:		
Protocol:	All	
Status:	Enabled	
Common Service Port:	Select One	
	Save Back	

Note:

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

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.

P 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.

8.9.2 Port Triggering

Choose menu "Forwarding \rightarrow Port Triggering", and then you can view and add port triggering. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Port Triggering				
ID Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status Modify
Add New	Enable All Disa	ble All Delete All		
	Pre	vious Next		

Once the Router is configured, the operation is as follows:

- 1. A local host makes an outgoing connection 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.
- 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 Ports 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 that triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- Incoming Protocol The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the Router).
- > Status The status of this entry, either Enabled or Disabled.
- > **Modify -** To modify or delete an existing entry.

To add a new rule, follow the steps below:

- 1. Click the **Add New...** button, the next screen will pop-up as shown below.
- 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 **AII**.
- 4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **AII**.
- 5. Select **Enable** in **Status** field.
- 6. Click the **Save** button to save the new rule.

Add or Modify a Port Triggering Entry		
 Trigger Port:		
Trigger Protocol:	All 💌	
Incoming Ports:		
Incoming Protocol:	All 💌	
Status:	Enabled 🔽	
Common Applications:	Select One	
	Save Back	

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.

P Note:

- 1. When the trigger connection is released, the corresponding opening ports will be closed.
- 2. Each rule is allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
- 3. Incoming Port Range cannot overlap each other.

8.9.3 DMZ

Choose menu "Forwarding \rightarrow DMZ", and then you can view and configure DMZ host. 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. DMZ host forwards all the ports at the same time. 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	
Current DMZ Status:	🔿 Enable 💿 Disable
DMZ Host IP Address:	0.0.0.0
	Save

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

- 1. Check the **Enable** radio button.
- 2. Enter the IP Address of a local host in the DMZ Host IP Address field.
- 3. Click the **Save** button.

P Note:

After you set the DMZ host, the firewall related to the host will not work.

8.9.4 UPnP

Choose menu "Forwarding \rightarrow UPnP", and then you can view the information about UPnP (Universal Plug and Play). The 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.

UPn	Р					
Current l	JPnP Status:	Enabled		Disable		
Curr	ent UPnP Setting	js List				
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
		Refresh				

- Current UPnP Status UPnP can be enabled or disabled by clicking the Enable or Disable button.
- > Current UPnP Settings List This table displays the current UPnP information.

- App Description The description provided by the application in the UPnP request.
- External Port The external port the Router opens for the application.
- **Protocol -** The type of protocol the Router opens for the application.
- Internal Port The Internal port the Router opens for local host.
- IP Address The IP address of the UPnP device that is currently accessing the Router.
- **Status** The status of the port is displayed here. "Enabled" means that the port is still active. Otherwise, the port is inactive.

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

8.10 Security

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

There are four submenus under the Security menu: **Basic Security**, **Advanced Security**, **Local Management and Remote Management**. Click any of them, and you will be able to configure the corresponding function.

8.10.1 Basic Security

Choose menu "Security → Basic Security", you can configure the basic security.

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

- 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 IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.
 - **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, keep the default, **Enabled**.
 - L2TP Passthrough Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enabled**.
 - **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, keep the default, **Enabled**.
- 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, keep the default **Enable**.
 - **TFTP ALG** To allow TFTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - H323 ALG To allow Microsoft NetMeeting clients to communicate across NAT, keep the default Enable.

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

8.10.2 Advanced Security

Choose menu "Security → Advanced Security", you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

TL-WR710N Wi-Fi Pocke

Wi-Fi Pocket Router/AP/TV Adapter/Repeater

Advanced Security	
Packets Statistics Interval (5 ~ 60):	10 Seconds
DoS Protection:	⊙ Disable O Enable
Enable ICMP-FLOOD Attack Filtering	
ICMP-FLOOD Packets Threshold (5 \sim 3600):	50 Packets/Secs
Enable UDP-FLOOD Filtering	
UDP-FLOOD Packets Threshold (5 \sim 3600):	500 Packets/Secs
Enable TCP-SYN-FLOOD Attack Filtering	
TCP-SYN-FLOOD Packets Threshold (5 \sim 3600):	50 Packets/Secs
Ignore Ping Packet from WAN Port to Router	
Forbid Ping Packet from LAN Port to Router	
Save Blocked DoS Host List	

- 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.

P Note:

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

8.10.3 Local Management

Choose menu "Security \rightarrow Local Management", you can configure the management rule. 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 	allowed to access the Router's Web-Based Utility
Only the PCs listed can bro	wse the built-in web pages to perform Administrator tasks
MAC 1:	
MAC 2:	
MAC 3:	
MAC 4:	
Your PC's MAC Address:	6C-62-6D-F7-31-8D Add
	Save

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.

P Note:

If your PC is blocked but you want to access the Router again, press and hold the WPS button for more than 5 seconds to reset the Router to factory defaults.

8.10.4 Remote Management

You can configure the Remote Management function on this page. 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	

- 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 interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65535, 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. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will 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 you use port number 8080, enter in your browser: http://202.96.12.8:8080. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's Web-based utility.

Note:

Be sure to change the router's default password to a very secure password.

8.11 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control. 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 t	e able to access the Inter	rnet.			
Parental Control:	💿 Disable 🔵 Enal	ole			
MAC Address of Parental PC:					
MAC Address of Your PC:	6c-62-6d-f7-31-8d	Copy	To Above		
	Save				
ID MAC address Webs	ite Description		Schedule	Status	Modify
Add New Enable All	Disable All De	elete All			
	Previous	Next	Current No. 1	🗸 Page	

- 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 Restriction→ Schedule".
- > **Modify -** Here you can edit or delete an existing entry.

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 below.
- 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 (e.g.<u>www.google.com</u>) will be allowed.
- 5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. 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 return to the previous page.

Add or Modify Parental Co	ntrol Entry
Add of modily Farental oc	
The Schedule is based on the time of	the Router. The time can be set in "System Tools -> <u>Time settings</u> ".
MAC Address of Children's PC:	
All MAC Address in Current LAN:	Please Select
Website Description:	
Allowed Website Name:	
Effective Time:	Anytime 🔽
	The time schedule can be set in "Access Control -> <u>Schedule</u> "
Status:	Enabled 💌
	Save Back

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.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 Restriction → 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:
 - Click Add New... button.
 - Enter 00-11-22-33-44-AA in the MAC Address of Child PC field.
 - Enter "Allow Google" in the Website Description field.

- Enter "www.google.com" in the Allowed Domain Name field.
- Select "Schedule_1" you create just now from the Effective Time drop-down list.
- 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.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-BB	Allow Google	Schedule_1	\checkmark	Edit Delete
	Add New Enable All Disable All Delete All				
		Previous Nex	Current No. 1	🖌 Page	

8.12 Access Control

Access Cor	itrol
- Rule	
- Host	
- Target	
- Schedule	

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

8.12.1 Rule

Choose menu "Access Control→ Rule", you can view and set Access Restriction rules.

Acce	Access Control Rule Management					
📃 Enal	ble Internet	Access Control				
Default	t Filter Polic	у.				
🔿 Allov	w the packe	ts specified by any en:	abled access control po	icy to pass through the F	Router	
💿 Den	<mark>iy</mark> the packe	ts specified by any ena	abled access control pol	icy to pass through the F	touter	
			Save			
ID Ru	ile Name	Host	Target	Schedule	Status	Modify
	Wizard					
Jeruh	Wizaru					
1 bbA	New	Enable All D	isable All Delet	e All		
Mo	ove		ID To			
			Previous	Next Current No	. 1 💙 Page	

- Enable Internet Access Restriction Select the check box to enable the Internet Access Restriction 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.
- Action Here displays the action the Router takes to deal with the packets. It could be Allow or Deny. Allow means that the Router permits the packets to go through the Router. Deny means that the Router rejects the packets to go through the Router.
- Status This field displays the status of the rule. Enabled means the rule will take effect, Disabled means the rule will not take effect.
- > Modify Here you can edit or delete an existing rule.

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

- 1. Click the Add New... button and the next screen will pop up as shown below.
- 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 Action field, select Deny or Allow.
- 7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
- 8. 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.

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

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

Add Internet Access Cont	rol Entry
Rule Name:	
Host:	Click Here To Add New Host List.
Target:	Any Target 👻 Click Here To Add New Target List.
Schedule:	Anytime 🔽 Click Here To Add New Schedule.
Status:	Enabled 💌
	Save Back

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 "Access Restriction → Host" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
- Click "Access Restriction → Target" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
- Click "Access Restriction → Schedule" in the left to enter the Schedule Settings 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.
- 4. Click "Access Restriction → Rule" in the left to return to the Access Restriction Rule Management page. Select "Enable Internet Access Restriction" and choose "Deny the packets not specified by any access Restriction policy to pass through the Router".
- 5. Click Add New... button to add a new rule as follows:
 - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
 - In **Host** field, select Host_1.
 - In **Target** field, select Target_1.
 - In **Schedule** field, select Schedule_1.
 - In Action field, select Allow.
 - In **Status** field, select Enabled.
 - Click **Save** to complete the settings.

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

ID	Rule Name	Host	Target	Schedule	Status	Modify
1	Rule_1	<u>Host 1</u>	<u>Target 1</u>	Schedule 1	>	Edit Delete
Se	etup Wizard					
	Add New	Enable All Di	sable All Delete	e All		

8.12.2 Host

Choose menu "Access Control \rightarrow Host", you can view and set a Host list. The host list is necessary for the Access Restriction Rule.

Но	ost Settings		
	Host Description	Information	Modify
		Previous	Next Current No. 1 🗸 Page

- > 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.
 - If you select IP Address,
 - 1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In LAN IP Address field, enter the IP address.

Add or Modify a Host Ent	ry
Mode: Host Description: LAN IP Address:	IP Address
	Save Back

- If you select MAC Address,
 - 1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In MAC Address field, enter the MAC address.

Add or Modify a Host Entry		
Mode: Host Description: MAC Address:	MAC Address	
	Save Back	

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 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, you should first follow the settings below:

- 1. Click **Add New...** button 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.

ł	Host Settings				
ID 1	Host Description Host_1 Add New Delete All	Information MAC: 00-11-22-33-44-AA	Modify Edit Delete		
		Previous Next	Current No. 1 🔽 Page		

8.12.3 Target

Choose menu "Access Control \rightarrow Target", you can view and set a Target list. The target list is necessary for the Access Restriction Rule.

Target Settings		
ID Target Description	Information	Modify
	Previous	Next Current No. 1 🖌 Page

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.
 - If you select IP Address,
 - 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.

Add or Modify an Access	Target Entry
Mode:	IP Address
Target Description: IP Address:	
Target Port:	
Protocol:	All 💌
Common Service Port:	Please Select 💌
	Save Back

- If you select Domain Name,
 - 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 Google) in the blank. Any domain name with keywords in it (e.g.<u>www.google.com</u>) will be blocked or allowed. You can enter 4 domain names.

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

3. 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 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 **www.google.com** only, you should first follow the settings below:

- 1. Click Add New... button 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.google.com.
- 5. Click **Save** to complete the settings.

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

Target Settings			
ID 1 - A	Target Description Target_1 Add New Delete All	Information www.google.com	Modify Edit Delete
		Previous	Current No. 1 🗸 Page

8.12.4 Schedule

Choose menu "Access Control \rightarrow Schedule", you can view and set a Schedule list. The Schedule list is necessary for the Access Restriction Rule.

Sch	edule Settings				
ID Add	Schedule Description	Day	Time	Modify	
	[Prevoius	Next Curr	rent No. 👖 🔽 Page	

- 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 and the next screen will pop-up as shown below.
- 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 return to the previous page.

Advance Schedule Settin	Advance Schedule Settings					
Note: The Schedule is based on the	Note: The Schedule is based on the time of the Router.					
Schedule Description:	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					

For example: If you desire to restrict the internet activities of 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**, you should first follow the settings below:

- 1. Click **Add New...** button to enter the Advanced Schedule Settings page.
- 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.

S	Schedule Settings						
ID	Schedule Description	Day	Time	Modify			
1	Schedule_1 Add New Delete All	Sat Sun	18:00 - 20:00	Edit Delete			
	(Prevoius	Next Current No. 1 🛩 F	°age			

8.13 Advanced Routing

Advanced Routing	
- Static Routing List	
- System Routing Table	

There are two submenus under the Network menu: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

8.13.1 Static Routing List

Choose menu "Static Routing", and you can configure the static route. A static route is a pre-determined path that network information must travel to reach a specific host or network.

Stati	ic Routing				
ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify
Add	New Enable All	Disable All Dele	ete All		
	(Previous Ne	ext		

To add static routing entries, follow the steps below.

1. Click Add New..., you will see the following screen shown below 错误!未找到引用源。.

l or Modify a Static Ro	
Destination Network:	
Subnet Mask:	
Default Gateway:	
Status:	Enabled 🔽
	Save Back

- 2. Enter the following data.
 - Destination Network The Destination IP Address is the address of the network or host that you want to assign to a static route.
 - Subnet Mask The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.
 - 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.

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.

8.13.2 System Routing Table

Choose menu "Advanced Routing \rightarrow System Routing Table", and you can 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	System Routing Table					
ID	Destination Network	Subnet Mask	Gateway	Interface		
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN		
2	239.0.0.0	255.0.0.0	0.0.0.0	LAN & WLAN		
		Refresh				

- Destination Network The Destination IP Address 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 whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet).

Click the **Refresh** button to refresh the data displayed.

8.14 Bandwidth Control

Bandwidth Control
- Control Settings
- Rule List

There are two submenus under the Bandwidth Control menu. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

8.14.1 Control Settings

Choose menu "**Bandwidth Control** \rightarrow **Control Settings**", 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 Settin	igs	
Enable Bandwidth Control:		
Line Type:	💿 ADSL 🔵 Other	
Egress Bandwidth:	512	Kbps
Ingress Bandwidth:	2048	Kbps
		_
	Save	

- 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 WAN port.
- > Ingress Bandwidth The download speed through the WAN port.

8.14.2 Rule List

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

Bandwidth Control Rule List							
		Egress Bar	ndwidth(Kbps)	Ingress Bar	ndwidth(Kbps)		
	Description	Min	Max	Min	Мах	- Enable	Modify
The current list is empty.							
Add New Delete All							
Prev	vious Next	Current No. 1	🖌 Page				

- > **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 WAN port, the default is 0.
- Ingress Bandwidth This field displays the max and mix download bandwidth through the WAN 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.

Step 1: Click Add New..., you will see a new screen shown below.

Step 2: Enter the information like the screen shown below.

Bandwidth Control Rule	ettings
Enable: IP Range: Port Range: Protocol:	
Egress Bandwidth: Ingress Bandwidth:	Min Bandwidth(Kbps) Max Bandwidth(Kbps) 0 0 0 0
	Save Back

- > Enable Enable or disable the rule.
- IP Range Interior PC address range. If both are blank (or 0.0.0.0), the domain is no effective.

- Port Range The port range which the Interior PC access the outside PC. If all are blank (or 0), the domain is no effective.
- > **Protocol** Transport layer protocol, here there are All, TCP, UDP.
- Egress Bandwidth The max and the min upload speed which through the WAN port, default number is 0.
- Ingress Bandwidth The max and the min download speed through the WAN port, default number is 0.
- Step 3: Click the Save button.

8.15 IP & MAC Binding

IP & MAC Binding	
- Binding Settings	
- ARP List	

There are two submenus under the IP & MAC Binding menu: **Binding Setting** 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.

8.15.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire.

Bindi	ng Settings				
	ARP Binding:	 Disable O Enable Save 			
1D 1	MAC Address 00-0A-EB-00-07-BE	IP Address 192.168.0.173	Bind 🔽	Modify Modify Delete	
Add N			Delete All	Find	
		Previous	Next C	urrent No. 1 💌	Page

- > **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 -** Whether or not enable the ARP binding.
- > **Modify -** Edit or delete item.

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.

IP & MAC Binding Setting	S
Bind: MAC Address: IP Address:	
	Save Back

To add IP & MAC Binding entries:

- 1. Click the **Add New..** button.
- 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:

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

To find an existing entry:

- 1. Click the **Find** button.
- 2. Enter the MAC Address or IP Address.
- 3. Enter the **Find** button in the next page.

Find IP & MAC Binding B	Entry			
MAC Address: IP Address:				
ID	MAC Address	IP Address	Bind Link	
1	00-0A-EB-00-07-BE	192.168.0.173	🗹 <u>To page</u>	
	Find	Back		

Click the Enable All button to make all entries enabled.

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

8.15.2 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 configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries.

AR	² List			
ID 1	MAC Address 6C-62-6D-F7-31-8D	IP Address 192.168.0.100	Status Unbound	Configure Load Delete
2	00-0A-EB-00-07-BE	192.168.0.173	Bound	Load Delete
		Bind All	Load A	ll Refresh

- > MAC Address The MAC address of the controlled computer in the LAN.
- > **IP Address -** The assigned IP address of the controlled computer in the LAN.
- > Status Enabled or Disabled of the MAC address and IP address binding.
- > **Configure -** Load or delete item.
- **Load -** Load the item to the IP & MAC Binding list.
- > **Delete -** Delete the item.
- 1. Click the **Bind All** button to bind all the current items, available after enable.
- 2. Click the Load All button to load all items to the IP & MAC Binding list.
- 3. Click the **Refresh** button to refresh all items.

P 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.

8.16 Dynamic DNS

The Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, 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.no-ip.com</u>, <u>www.comexe.cn</u>, or <u>www.dyndns.org</u>. The Dynamic DNS client service provider will give you a password or key.

8.16.1 No-IP DDNS

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

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

To set up for DDNS, follow these instructions:

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

8.16.2 Comexe.cn DDNS

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

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

To set up for DDNS, follow these instructions:

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

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

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

8.16.3 Dyndns org DDNS

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

DDNS	
Service Provider:	Dyndns (www.dyndns.org) 🔽 <u>Go to register</u>
User Name: Password: Domain Name:	username
Connection Status:	Enable DDNS DDNS not launching! Login
	Save

To set up for DDNS, follow these instructions:

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

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

Click Logout to logout of the DDNS service.

8.17 System Tools

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

There are nine submenus under the System Tools menu: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup and Restore**, **Reboot**, **Password**, **System Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

8.17.1 Time Settings

Time zone:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore		
Date:	1 1 2013 (MM/DD/YY)		
Time:	1 43 50 (HH/MM/SS)		
NTP Server 1:	0.0.0.0 (Optional)		
NTP Server 2:	0.0.0.0 (Optional)		
Start:	Enable Daylight Saving Mar 👻 3rd 💙 Sun 💙 2am 💌		
End:	Nov 🖌 2nd 🗹 Sun 🖌 3am 🖌		
Daylight Saving Status:	daylight saving is down.		
	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.		

You can set time manually or get GMT from the Internet for the router on this page:

- > **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.

To set time manually, follow the steps below:

- 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.

For automatic time synchronization:

- 1. Enter the address of the **NTP Server 1 or NTP Server 2**.
- 2. Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

Note:

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, if not, the time limited on these functions will not take effect.

- > The time will be lost if the router is turned off.
- > The router will obtain GMT automatically from Internet if it has already connected to Internet.

8.17.2 Diagnostic

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

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	
This device is ready.	
	Start

- > **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 pinging/tracerouting the IP address is successful, but pinging/tracerouting 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 Type the destination IP address (such as 202.108.22.5) or Domain name (such as www.baidu.com).
- > **Pings Count -** The number of Ping packets for a Ping connection.
- > Ping Packet Size The size of Ping packet.
- Ping Timeout Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- > Traceroute Max TTL The max number of hops for a Traceroute connection.

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 202.108.22.5 with 64 bytes of data:	į
	ł
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=1	1
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=2	
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=3	÷
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=4	ł
Ping statistics for 202.108.22.5	
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),	ł
Approximate round trip times in milliseconds:	1
; Minimum = 1, Maximum = 1, Average = 1	j

P Note:

Only one user can use this tool at one time. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters. "Traceroute Max TTL" is Traceroute Parameter.

8.17.3 Firmware Upgrade

The page allows you to upgrade the latest version firmware to keep your router up-to-date.

Firmware Upgrade		
File:		Browse
Firmware Version:	3.14.4 Build 130128 Rel.36510n	
Hardware Version:	WR710N v1 00000000	
	Upgrade	

New firmware is posted at <u>www.tp-link.com</u> and can be downloaded for free. If the router is not experiencing difficulties, there is no need to upgrade firmware, unless the new firmware supports a new feature you need.

P Note:

- 1. When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.
- 2. Make sure that your computer is connected to the Internet through the cable when you upgrade the firmware. To upgrade through wireless connection is not allowed.
- 3. Set your IP address as static IP before upgrading.

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

- 1. Download the latest firmware upgrade file from our website <u>http://www.tp-link.com</u>.
- 2. Enter or select the path name where you save the downloaded file on the computer into the **File** blank.
- 3. Click the **Upgrade** button.
- 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 current hardware version.

P Note:

The firmware version must correspond to the hardware. The upgrade process takes a few minutes and the Router will restart automatically when the upgrade is completed. It is important to keep power on during the entire process. Loss of power during the upgrade could damage the Router.

8.17.4 Factory Defaults

This page allows you to restore the factory default settings for the router.

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

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

- > The default User Name: admin
- > The default Password: admin
- > The default access: tplinklogin.net

Note:

Any settings you have saved will be lost when the default settings are restored.

8.17.5 Backup & Restore

This page allows you to save current configuration of router as backup or restore the configuration file you saved before.

Backup & Restore	9		
Configuration Backup: Configuration File:	Backup	Browse	Restore

Click the Backup button to save all configuration settings as a backup file in your local computer.

- > To restore the router's configuration, follow these instructions:
 - Click the **Browse** button to select the backup file which you want to restore.
 - Click the **Restore** button.

P Note:

The current configuration will be covered with the uploading configuration file. The restoration process lasts for 20 seconds and the router will restart automatically. Keep the router on during the restoring process to prevent any damage.

8.17.6 Reboot

This page allows you to reboot the router.

Reboot
Click this button to reboot this device.
Reboot

Click the **Reboot** button to reboot the router.

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

- > Change LAN IP Address. (System will reboot automatically)
- > MAC Clone (system will reboot automatically)
- > DHCP service function.
- > Static address assignment of DHCP server.
- > Web Service Port of the router.
- > Upgrade the firmware of the router (system will reboot automatically).
- > Restore the router's settings to factory default (system will reboot automatically).

8.17.7 Password

This page allows you to change the factory default user name and password of the router.

Password	
The username and password must not exc Old User Name: Old Password:	eed 14 characters in length and must not include any spaces!
New User Name: New Password: Confirm New Password:	
	Save Clear All

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

Note:

The new user name and password must not exceed 14 characters in length and must 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.

8.17.8 System Log

This page allows you to query the logs of the router.

Sy	stem Log						
Auto	Mail Feature: Di	sabled	Ma	ail Settings			
Log T	ype: Sharing	*	Log Lev	vel: ALL			
Index	Time	Туре	Level	Log Content			
6	1st day 01:12:56	SHARING	NOTICE	Network sharing service stopped			
5	1st day 00:11:17	SHARING	INFO	Media server started			
4	1 st day 00:08:07	SHARING	NOTICE	Network sharing service started			
3	1 st day 00:08:06	SHARING	NOTICE	Network sharing settings changed			
2	1st day 00:06:23	SHARING	NOTICE	Network sharing service started			
1	1 st day 00:06:20	06:20 SHARING NOTICE Network sharing settings changed					
	2013-01-01 1:55:						
H-Ver	= WR710N v1 000	00000 : S-V	/er = 3.14	I.4 Build 130128 Rel.36510n			
L = 192	2.168.0.254 : M = 2	255.255.25	5.0				
W1 = C	HCP : W = 0.0.0.0	: M = 0.0.0	.0 : G = 0.	0.0.0			
Refresh Save Log Mail Log Clear Log							
	Previous Next Current No. 1 V Page						

> **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. The result will be shown in the later log soon.
- > Clear Log All the logs will be deleted from this device permanently, not just from the page.

8.17.9 Statistics

The Statistics page displays the network traffic of each PC in LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

Statistics								
Current Statistic Packets Statistics Inter		Disable of 10	l V Seconds refresh		Enab			
Sort	ted Rules:	Sorted I	oy Current Byt	es 💙	Reset		Delete All	
	Tota	1			Current			
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN TX	Modify
			The current	list is empty	Ι.			
5 💌 entries per p	age. CurrentՒ	10. 1 <u>v</u>	Page					
		Prev	/ious	Next				

- Current Statistics Status Enable or Disable. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be ineffective.
- Packets Statistics Interval The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- > **Sorted Rules -** Here displays sort as desired.

Statistics Table:

IP Address		The IP Address displayed with statistics		
Total	Packets	The total amount of packets received and transmitted by the router.		
	Bytes	The total amount of bytes received and transmitted by the router.		
	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.		
Current	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.		
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.		

UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.
TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

Click the Save button to save the Packets Statistic interval value.

Click the Auto-refresh checkbox to refresh automatically.

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

Appendix A: FAQ

1. How do I configure the Router to access the Internet by ADSL users?

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Log in 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 and the "Confirm Password" field, and finish it by clicking Connect.

WAN	
WAN Connection Type:	PPPoE/Russia PPPoE 💌 🛛 Detect
PPPoE Connection:	
User Name:	username
Password:	
Confirm Password:	

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.

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 Disconnected!

P 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 the Internet by Ethernet users?

- Log in 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, log in 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 is to 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.

MAC Clone		
WAN MAC Address: Your PC's MAC Address:	00-1D-0F-01-06-29 6C-62-6D-F7-31-8D	Clone MAC Address
	Save	

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

- 1) If you start NetMeeting as a sponsor, you don't need to do anything with the Router.
- 2) 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.

N	/irtual Server	'S				
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 Dis	able All Delete	All		
		IP	revious Next	:		

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

P 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	
Current DMZ Status: DMZ Host IP Address:	Enable Disable 192.168.0.169
	Save

- 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:	88	
Remote Management IP Address:	0.0.0.0	(Enter 255.255.255.255 for all)
	Save	

P Note:

If the above configuration takes effect, configure to the Router by typing 192.168.0.188 (the Router's LAN IP address: Web Management Port) in the address field of the Web browser.

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 "88" 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.

Virtual Servers	5					
ID Service Port	Internal Port	IP Address 192.168.0.188	Protocol All	Status Enabled	Modify Modify Delete	
Add New		able All Delete				
	Pr	revious Next	:			
Add or Modify	a Virtual Server E	ntry				
Se	ervice Port:	(XX-XX or)	∞)			
Internal Port: (XX, Only valid for single Service Port or leave it blank)						
I	P Address:					
	Protocol: All	*				
	Status: Enab	ed 💙				
Common Se	ervice Port:Sele	ect One	~			
		Save Back	<			

5. The wireless stations cannot connect to the Router.

- 1) Make sure the "Enable Wireless Router Radio" is checked.
- 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 PC

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 necessary.

1. Configure TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, 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.

LAN or High-Speed Internet		
	Wireless Network Connection 49 Connected	
(i) (i)	Disable View Available Wireless Networks Status Repair	
	Bridge Connections	
	Create Shortcut Delete	
	Rename Properties	

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

🔟 Wireless Network Connection 49 Properties 👘 🕐 🔀				
General Advanced				
Connect using:				
EZ Connect N 150Mbps Wireless N L				
This connection uses the following items:				
Image: Construction of the state of th				
I <u>n</u> stall <u>U</u> ninstall P <u>r</u> operties				
Description				
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.				
 ✓ Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity 				
OK Cancel				

- 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, Choose Obtain DNS server automatically, as shown in the figure below:

Internet Protocol (TCP/IP) Properties				
General Alternate Configuration				
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.				
Obtain an IP address automatically				
Use the following IP address: —				
IP address:	· · · · · · ·			
S <u>u</u> bnet mask:				
Default gateway:	· · · · ·			
O <u>b</u> tain DNS server address automatically				
O Use the following DNS server addresses:				
Preferred DNS server:	· · · · ·			
Alternate DNS server:				
	Ad <u>v</u> anced			
	OK Cancel			

P Note:

For Windows 98 OS or before, the PC and Router may need to be restarted.

7) Click **OK** to keep your settings.

Appendix C: Specifications

General				
Standards	IEEE 802.11n, 802.11b, 802.11g			
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP			
Port	One 10/100Mbps LAN/WAN port One 10/100Mbps LAN port			
CablingType	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)			
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)			
LED	SYS			
Dimensions (L×W×H)	81mm x 71mm x 28mm			
Safety & Emissions	FCC, CE			
Wireless				
Frequency Band	2.4~2.4835GHz			
Radio Data Rate	 11n: up to 150Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11b: 11/5.5/2/1M (Automatic) 			
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)			
Modulation	DBPSK, DQPSK, CCK, 16-QAM, 64-QAM, BPSK, QPSK			
Security	64/128/152-bit WEP, WPA/WPA2, WPA2-PSK/WPA-PSK			
Sensitivity @PER	135M: -70dBm@10% PER 65M: -73dBm@10% PER 54M: -76dBm@10% PER 6M: -92dBm@10% PER			
Mode	Wireless Router Mode, Access Point Mode, Repeater Mode, Client Mode, WISP Client Router Mode			
Environmental and Physical				
Temperature	Operating: 0°C~40°C (32°F~104°F)			
remperature	Storage: -40°C~70°C(-40°F~158°F)			
Humidity	Operating: 10% - 90% RH, Non-condensing			
	Storage: 5% - 90% RH, Non-condensing			

Appendix D: Glossary

- 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.