





Wireless AC1750 Dual-band Gigabit Router

Copyright Statement

Tenda[®] is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without prior expressed written permission from Shenzhen Tenda Technology Co., Ltd, any individual or party is not allowed to copy, plagiarize, reproduce, or translate it into other languages.

All photos and product specifications mentioned in this manual are for references only. Upgrades of software and hardware may occur; Tenda reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes. If you would like to know more about our product information, please visit our website at <u>http://www.tendacn.com</u>.



TABLE OF CONTENTS

TABLE OF CONTENTS	2
CHAPTER 1 PRODUCT OVERVIEW	5
1.1 What it does	5
1.2 Features	5
CHAPTER 2 QUICK INTERNET CONNECTION SETUP	7
2.1 PACKAGE CONTENTS	7
2.2 MINIMUM SYSTEM REQUIREMENTS:	7
2.3 HARDWARE INSTALL	8
2.4 WEB UTILITY LOGIN	11
2.5. INTERNET CONNECTION SETUP	14
2.6 VERIFY INTERNET CONNECTION SETTINGS	15
2.7 WIRELESS SETTINGS	19
2.7.1 Wireless-Basic Settings	19
2.7.2 Wireless-Security Settings	20
2.8 CONNECT TO DEVICE WIRELESSLY	21
CHAPTER 3 RUNNING STATUS	24
3.1 WAN STATUS	25
3.2 LAN STATUS	27
3.3 Wireless Status	27
3.4 System Info	29
CHAPTER 4 NETWORK	29
4.1.LAN SETTINGS	
4.2.WAN SETTINGS	31
4.3 DHCP Server	
4.4 DHCP CLIENTS	40
4.5 STATIC ASSIGNMENT	40
4.6 MAC CLONE	41
4.7 Port Mode	42

	44
5.1 IP GROUP	44
5.2 TIME GROUP	45
5.3 CLIENT FILTER	46
5.4 URL FILTER	52
5.5 MAC FILTER	55
5.6 REMOTE WEB MANAGEMENT	59
CHAPTER 6 ADVANCED	61
6.1 VIRTUAL SERVER	61
6.2 DMZ	64
6.3 UPNP	65
6.4 DDNS	66
6.5 ROUTING	69
6.6 STATIC ROUTING	69
6.7 BANDWIDTH SETTINGS	70
CHAPTER 7 WIRELESS SETTINGS	71
7.1 BASIC SETTINGS	72
	12
7.2 WIRELESS SECURITY	76
7.2 Wireless Security	76 81
7.2 WIRELESS SECURITY	76 81 83
7.2 WIRELESS SECURITY	76 81 83 85
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL	76 81 83 85 86
 7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 Guest Network 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST 	76 81 83 85 86 88
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST. 7.8 ADVANCED SETTINGS	72 76 81 83 85 86 88 88 88
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST. 7.8 ADVANCED SETTINGS CHAPTER 8 USB.	72 76 81 83 85 86 88 88 88 90
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST 7.8 ADVANCED SETTINGS CHAPTER 8 USB 8.1 USB STORAGE	72 76 81 83 85 86 88 88 88 90 90
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST. 7.8 ADVANCED SETTINGS CHAPTER 8 USB. 8.1 USB STORAGE 8.2 USB PRINTING	72 76 81 83 85 86 88 88 88 90 90 93
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST. 7.8 ADVANCED SETTINGS CHAPTER 8 USB 8.1 USB STORAGE 8.2 USB PRINTING 8.3 DLNA	72 76 81 83 85 86 88 88 88 90 90 93 01
7.2 WIRELESS SECURITY 7.3 WPS 7.4 WDS 7.5 GUEST NETWORK 7.6 WIRELESS ACCESS CONTROL 7.7 CONNECTION LIST. 7.8 ADVANCED SETTINGS CHAPTER 8 USB. 8.1 USB STORAGE 8.2 USB PRINTING 8.3 DLNA 1 CHAPTER 9 IPTV	76 81 83 85 86 88 88 88 90 90 93 01 02

10.1 TIME & DATE	106
10.2 FIRMWARE UPDATE	107
10.3 BACKUP & RESTORE	108
10.4. RESTORE TO DEFAULT	108
10.5 User Name & Password	109
10.6 Rевоот	109
10.7 STATISTICS	110
10.8 Log	111
APPENDIX 1 CONFIG TCP/IP SETTINGS	111
APPENDIX 2 GLOSSARY	119
APPENDIX 3 TROUBLESHOOTING	125
APPENDIX 4 REMOVE WIRELESS NETWORK FROM YOUR PC	128
APPENDIX 5 SAFETY AND EMISSION STATEMENT	131



CHAPTER 1 PRODUCT OVERVIEW

1.1 What it does

Thanks for purchasing this Tenda W1800R Wireless AC1750 Dual-band Gigabit Router! The Tenda W1800R is a 5th generation dual-band Wi-Fi router that delivers wireless speeds up to 1750Mbps, currently the fastest available. Compatible with next generation WiFi devices and backward compatible with 802.11 a/b/g and n devices, it enables HD streaming throughout your home. The W1800R with simultaneous dual band WiFi technology offers speeds up to 450+1300Mbps and avoids interference, ensuring top WiFi speeds and reliable connections. This makes it ideal for larger homes with multiple devices. In addition, four Gigabit Ethernet ports offer ultra-fast wired connections. Wirelessly access and share USB hard drive and USB printer using the two USB 2.0 ports. Plus, the DLNA media server feature enables sharing of digital media such as music, photos and videos between consumer devices such as computers, TVs, printers, cameras, cell phones, and other multimedia devices.

1.2 Features

- > 2.4GHz: IEEE802.11n, IEEE802.11g, IEEE 802.11b;
- > 5GHz: IEEE 802.11n, IEEE 802.11a, IEEE 802.11ac;
- ➢ IEEE802.3, IEEE802.3u;

Tenda

- Operate in 2.4GHz and 5GHz wireless bands simultaneously;
- Wireless rate up to1.3Gbps;
- > 1 * Gigabit WAN port for Internet connection;
- 3 * Gigabit LAN ports for LAN connection; 1* IPTV port for IPTV service;
- > 2* USB ports for storage or wireless printing service sharing;
- Support DLNA media server;
- > 3* high gain external antennas;
- > WDS support for extending existing wireless coverage;
- Supports WEP, WPA-PSK, WPA2-PSK and Mixed WPA/WPA2-PSK encryption methods to secure your wireless network;
- Hidden/invisible SSID;
 MAC-based wireless access control;
- > WPS one-touch encryption;
- Provides Wireless guest network feature;
- WMM streams your video and audio;
- Combines the function of a wireless AP, router, switch and firewall;
- Provides Internet connection types: Dynamic/ static
 IP,L2TP,PPTP, PPPOE/ PPPOE dual access;
- > Built-in firewall supports domain name/MAC address filter
- SNTP to synchronize local time with Internet time servers;

Tenda

- Bandwidth control;
- Supports UPnP and DDNS features;
- Provides virtual server and DMZ features;
- Provides logs to record device's usage status;

CHAPTER 2 QUICK INTERNET CONNECTION SETUP

2.1 Package Contents

- Unpack the box and verify the following items:
- W1800R Wireless AC1750 Dual-band Gigabit Router;
- Power Adapter
- Quick Install Guide
- Resource CD
- > 3* 5dBi omni-directional antennas
- Ethernet Cable
- If any of the above items are incorrect, missing, or damaged, please contact your Tenda reseller for immediate replacement.

2.2 Minimum System Requirements:

- > 200MHz or better CPU
- ➢ 64MB or larger memory
- Windows 98/2000/XP/Vista/7
- Installed Network Adapter
- > Internet Explorer 6.0 or higher

- Tenda
- > Netscape Navigator 4.7 or higher
- Broadband Internet Service (through xDSL/Cable Modem/Ethernet)

2.3 Hardware Install

1. Connect one end of the included power adapter to the Device and plug the other end into a wall outlet nearby. (Using a power adapter with a different voltage rating than the one included with the Device will cause damage to the Device.)



2. Connect one of the LAN ports on the Device to the NIC port on your PC using an Ethernet cable.



3. Connect the Ethernet cable from your ISP side to device's WAN port.



4. Observe status of LEDs on the device and ensure that they are functioning correctly as stated in the table below.

Front Panel:



LED Overview:

LED	lcon	Status	Description
Power	\bigcirc	Solid	Indicates a proper connection
			to the power supply
Sys	-Q-	Blinking	Indicates system is functioning
			properly
USB		Solid	USB port connected correctly



Wireless AC1750 Dual-band Gigabit Router

WAN	Ø	Solid WAN port connected correctly	
		Blinking	WAN port is transferring data
LAN	3 2 1	Solid	LAN port connected correctly
(1/2/3)		Blinking	LAN port is transferring data
IPTV	Ľ	Solid	IPTV port connected correctly
		Blinking	IPTV port is transferring data
2.4G	2.4GHz	Solid	2.4G wireless radio is on
		Blinking	Data being transferred over
			2.4G wireless network
5G	5GHz	Solid	5G wireless radio is on
		Blinking	Data being transferred over 5G
			wireless network
WPS	5	Blinking	Device is performing WPS
			authentication on a client
			device.
		Off	WPS function is disabled or
			WPS authentication
			negotiation is completed

Back Panel:



Tenda

- USB: USB port for connection to a USB device such as a USB printer or storage device;
- WAN: Internet port (RJ-45) for connection to an Internet-enabled xDSL Modem/Cable Modem or existing Ethernet;
- LAN/1/2/3: 3 LAN ports (RJ-45) for connection to PC's NIC or uplink to a hub, switch or wireless AP;
- IPTV: IPTV port for connection to a network set-top box.
 However such port can function as a LAN port if IPTV STB port is not enabled;
- 5) WPS/Reset: WPS/Reset button; the WPS LED will display a blinking light if you enabled the WPS function from device web utility. Pressing this button for about 7 seconds restores the Device to factory defaults.

2.4 Web Utility Login

The device's default IP is 192.168.0.1. You can change it to accommodate your own needs. Here in this manual, we use the default IP.

Connect you PC to the Device and config your PC's TCP/IP settings following instructions in appendix 1 hereto. And then do as follows to run a Ping command to test connectivity between your PC and the Device.

Click "Start"-> "Run", input "cmd" and press "Enter".



🔄 Run			— ×
	Type the name of a prog resource, and Windows v	ram, folder, docur will open it for you	ment, or Internet 1.
<u>O</u> pen:	cmd		*
	ОК	Cancel	Browse

Enter "ping 192.168.0.1" and press "Enter". If you see the following screen, it means the router is reachable on your PC. If you don't get the following screen, verify router's power supply, Ethernet cable connections and your PC's TCP/IP settings.



Login to Web Utility

Launch a web browser, in the address bar,input 192.168.0.1 and press "Enter".

v 47 X http://192.168.0.1

When connected to the Device successfully, you shall see the login window below. Enter user name and password in corresponding fields on window below (Default user name and password are respectively set to admin).

TENDA W1800R Router	
User Name:	
Password: (Default:admin)	
Login Cancel	

▲ Note:

For security purpose, please change the default user name and password after you logged in to web utility.

You will see the following interface if you entered a correct user name and a correct password.





2.5. Internet Connection Setup

There are 2 Internet connection types on home page: PPPoE and DHCP.

If you used to create a broadband connection on your PC that is directly connected to a modem and provide a user name and a password for Internet access, then select PPPoE, enter the user name and password and then click OK.

Tenda		
		Advanced
	Internet Connection Settings ® PPPOE ODHCP	
	User Name: possosososososososos	
	For other connection types, please click "Advanced"- "Network"- "WAN".	
	Wireless Security Settings 24G Security Key (* 12345678) (Definit: 12345678)	
	OK Cancel	

If you used to access Internet simply by connecting your PC directly to the modem with no need to configure any settings on your PC. Then select DHCP, enter a security key and then click OK.

Tenda			
		\$ 3Adra	nced
	Internet Connection Settings ©PPPOE @DHCP		
	User Name: Password:		
	For other connection types, please click "Advanced"- "Network"-"WAN".		
	Wireless Security Settings 2.4G Security Key 💌 12345678 (Default: 12345678)		
	OK Cancel		

[▲]Note:

DHCP is the default Internet connection type. If you need other connection types, please go to Chapter 4> WAN settings.

2.6 Verify Internet Connection Settings

After finishing settings on home page, click the Advanced button from right top corner there and then click Running Status-> WAN Status to check the Internet connection status.

A. If you find "Connected" and a WAN IP address displayed there (as shown below), you can now connect to the device using an Ethernet cable to access Internet.





B. If "Disconnected" (or "Not connected") and no WAN IP address are displayed (as seen below), connection between the Internet-enabled modem (or broadband service) and your device may have failed. Please double check or re-connect all involved devices and cables properly and then refresh the page. If nothing is wrong, "Connecting" or "Connected" will be displayed.



Upload speed

C. If "Connecting" is displayed and no WAN IP address is seen, try refreshing the page five times. And if it still displays "Connecting" try the following steps:

a. Click the Network menu and then click "MAC Clone". On the MAC Clone interface, click on the "Clone MAC" button, and then click "Save". Settings will take effect after device reboot.



Tenda	
	Status Network Security Advanced Wireless USB IPTV Tools
Network	For Home
LAN Settings	
WAN Settings	MAC Address Clone
DHCP Server	Use this section to coming device's WAIN MAC address. WAIN MAC Address: C8:3A/35.D5:7A/1C Restore to Factory Default MAC Clone MAC
DHCP Clients	Sauce Concol
Static Assignment	Save Galice
MAC Clone	
Port Mode	

b. Go back to the Status screen, refresh it a few times. If you find "Connected" and a WAN IP address displayed there, you can now connect to the device using an Ethernet cable to access Internet. If you still see "Connecting" there, please click Tools-> Reboot to reboot the device.

Tenda									
and the second	Status	Network	Security	Advanced	Wireless	USB	IPTV	Tools	
Tools	🖌 Home	🕑 Exit							
Time& Date									
Firmware Update	Reboot								
Backup&Restore	Reboot	the button below I	to restart your rol	uter.					
Restore to Default									
User Name&Password									
Reboot									
Statistics									
Log									

c. After device reboot, go back to the Status screen, refresh it a few times. If you find "Connected" and a WAN IP address displayed there, you can now connect to the device using an Ethernet cable to access Internet. If you still see "Connecting" after trying above solutions, verify that your PC is able to access



Internet when it is directly connected to the modem and contact our technical staff for help.

2.7 Wireless Settings

2.7.1 Wireless-Basic Settings

If you want to create a WLAN, simply click Wireless-> Basic Settings. Please change the SSID (Wireless Network name), you can name it whatever you like. Leave other options unchanged unless necessary and then click OK. You can also change the SSID and channel settings for the 5G wireless

network if you like.

Tenda						
	Status Network S	Security Advanced	Wireless	USB	IPTV	Tools
Wireless	🖌 Home 💽 Exit					
Basic Settings						
Wireless Security	Basic Settings					
WPS	2.4G Basic Settings	5G Ba	asic Settings			
WDS	Country: America 💌					
Guest Network	2.4GHz wireless network	Tenable				
Wireless Access Control	SSID Broadcast	Enable Disable Disable				
Connection List	SSID	Tenda				
Advanced Settings	802.11 Mode Channel	11b/g/n mixed mode 2437MHz (Channel 6	- -			
	Channel Bandwidth					
	Extension Channel	2417MHz (Channel 2) 🔻			
	WMM Capable	Enable Disable				
	APSD Capable	🛇 Enable 💿 Disable				
			Save	Cancel		



Tenda							
	Status Network	Security	Advanced	Wireless	USB	IPTV	Tools
Wireless	🖌 Home 📝 Exit						
Basic Settings							
Wireless Security	Basic Settings						
WPS	2.4G Basic Settings		<u>5G B</u>	asic Settings			
WDS	Country: America	¥.					
Guest Network	5GHz wireless netwo	rk 🔽 Ena	ible				
Wireless Access Control	SSID Broadcast	Enab	le 💿 Disable				
Connection List	SSID	Tenda	5				
Advanced Settings	802.11 Mode Channel	11a/n	Mode 💌 Hz (Channel 1	49) -			
	Channel Bandwidth	© 20M	IHz © 40MHz	© 80MHz			
	WMM Capable	Enab	ele 💿 Disable				
	APSD Capable	O Enab	ole 🔍 Disable				
				Save	Cancel		

2.7.2 Wireless-Security Settings

If you want to encrypt your wireless network, click

Wireless-Wireless Security, select a band: 2.4G or 5G, and then configure proper security settings. For example: Security Mode: WPA-PSK; Cipher Type: AES; Security Key: enter down to 8 characters. And then click Save.

Tenda								
and the second	Status	Network	Security	Advanced	Wireless	USB	IPTV	Tools
Wireless	🖌 Home	😰 Exit						
Basic Settings								
Wireless Security	Security	Mode						
WPS	1	2.4G Encrypt Typ	<u>2e</u>	<u>5G E</u>	<u>icrypt Type</u>			
WDS	2.4	GHz network SSI	D "Tenda"					
Guest Network	Secur	ity Mode r Type		WPA - PS	K TKIP O TKIP	&AES		
Wireless Access Control	Secur	ity Key		12345678				
Connection List	Key I	Renewal Interval		86400 s	econd			
Advanced Settings					Save	Cancel		



Tenda								
ale su me int	Status	Network	Security	Advanced	Wireless	USB	IPTV	Tools
Wireless	🖌 Home	🗹 Exit						
Basic Settings								
Wireless Security	Security	Mode						
WPS	2	4G Encrypt Typ	e	<u>5G Er</u>	crypt Type			
WDS	5G!	Hz network SSID	"Tenda_5"					
Guest Network	Securi Ciphe	ty Mode r Type		AES O	K TKIP O TKIP	&AES		
Wireless Access Control	Securi	ty Key		12345678				
Connection List	Key F	tenewal Interval		86400 S	econd			
Advanced Settings					Save	Cancel		

2.8 Connect to Device Wirelessly

Having finished above settings, you can search the device's wireless network (SSID) from your wireless devices (notebook, iPad, iPhone, etc) and enter a security key to connect to it wirelessly. If you are using Windows 7 OS, do as follows:

A. Click Start and select Control Panel.



B. Click Network and Internet.



C. Click Network and Sharing Center.



D. Click Change adapter settings.



E. Select a desired wireless connection and click



Connect/Disconnect.



F. Select the desired wireless network, click Connect, enter the security key and then click OK.





🖞 Connect to a Net	work	×
Type the netwo	ork security key	
<u>S</u> ecurity key:	•••••	
	✓ <u>H</u> ide characters	
		OK Cancel

G. You can access Internet via the device when "Connected" appears next to the wireless network name you selected.



CHAPTER 3 RUNNING STATUS

There are 4 subdues under the Status tab: "WAN Status", "LAN Status", "Wireless Status" and "System Info", which are explained in details below.

Tenda
Running Status
WAN Status
LAN Status
Wireless Status
System Info

3.1 WAN Status

This section allows you to view WAN Status, Internet Connection Type, WAN IP, Subnet Mask, Gateway, Primary DNS Server, Secondary DNS Server, MAC Address, WAN Traffic and Connection Duration. It also presents you a vivid impression of WAN traffic usage in a graph.

AN Status	
WAN Status	Connected
Internet Connection Type	PPPoE
WAN IP	10.10.10.10
Subnet Mask	255.255.255.255
Gateway	10.10.10.1
Primary DNS Server	202.96.134.133
Secondary DNS Server	8.8.8.8
MAC Address	C8:3A:35:0B:40:6F
WAN Traffic	Downlink: 0.03KB Uplink: 16.90KB
Connection Duration:	0
Connect	Disconnect
WAN Traffic Graph wan	 Lowmoad speed Upond speed
100 ⁻ 90 ⁻ 80 ⁻ 70 ⁻ 70 ⁻ 70 ⁻ 80 ⁻	

Tenda

WAN Status: Displays WAN connection status. Cable improperly connected: Indicates that the Ethernet cable from your ISP side is not correctly connected to the WAN port on the Device or the Device is not logically connected to your ISP. Connecting: Indicates that the WAN port is correctly

connected and is requesting an IP address from your ISP. Connected: Indicates that the router has been connected to your ISP.

- Internet Connection Type: Displays current Internet connection type.
- WAN IP: Displays WAN (Internet) IP address provided by your ISP.
- Subnet Mask: Displays WAN subnet mask provided by your ISP.
- Gateway: Displays WAN gateway address provided by your ISP.
- Primary DNS Server: Displays primary WAN DNS address provided by your ISP.
- Secondary DNS Server: Displays secondary WAN DNS address (if any) provided by your ISP.
- > MAC Address: Displays WAN MAC address.
- WAN Traffic: Displays current WAN uplink traffic and downlink traffic.

- > Connect: Click to renew current IP address.
- Disconnect: Click to release current IP address and Internet connection will be disconnected.

3.2 LAN Status

Tenda

This section displays information of device LAN IP Address, Subnet Mask, LAN MAC Address, DHCP Server and NAT Entries/NAT.

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
LAN MAC Address	C8:3A:35:0B:40:6F
DHCP Server	Enabled
NAT Entries/NAT	81/ 8192

- > IP Address: Displays current LAN IP address.
- Subnet Mask: Displays current LAN subnet mask.
- > LAN MAC Address: Displays Device's LAN MAC address.
- DHCP Server: Displays whether DHCP server on the device is enabled or not.
- NAT Entries/NAT: Displays the number of NAT entries already used and the number of NAT entries still available.

3.3 Wireless Status

This section displays the status of 2.4G Wireless radio and 5G Wireless radio, Wireless MAC address, SSID, 802.11 Mode,

Country, Channel and Security Mode information.

2.4GHz Wireless Status		
Wireless Radio	Enabled	
Wireless MAC address	C8:3A:35:0B:50:6F	
SSID	Tenda_0B506F	
802.11 Mode	11b/g/n mixed mode	
Country	US	
Channel	Auto	
Security Mode	WPA2 - PSK	
5GHz Wireless Status		
Wireless Radio	Enabled	
Wireless MAC address	C8:3A:35:0E:51:23	
SSID	Tenda_5_0E5123	
802.11 Mode	11a/n mode	
Country	US	
Channel	Auto	
Security Mode	Disabled	

- Wireless Radio: Displays whether wireless is enabled or not.
- Wireless MAC address: Displays the MAC address of the Device's wireless interface.
- SSID: Displays current SSID.
- > 802.11 Mode: Displays currently active network mode.
- Country: Displays the country selected currently.
- Channel: Displays the channel that device is currently operating on.
- Security Mode: Displays current security Mode.

3.4 System Info

This section displays current CPU usage, memory usage, up

time, system time, connected client(s) and firmware version info.

CPU Usage		25
Memory Usage		12
Up Time	05:57:42	
Time	1970-01-01 05:57:34	
Connected Client(s)	1	
Firmware Version	W1800R V1.0.1.0 EN	

- > CPU Usage: Displays current CPU usage.
- Memory Usage: Displays current memory usage.
- > Up Time: Displays the uptime since device is powered up.
- > Time: Displays Device's current system time.
- Connected Client(s): Displays the number of currently connected clients.
- Firmware Version: Displays Device's current firmware version.

CHAPTER 4 NETWORK

Network includes the following five submenus: LAN Settings, WAN Settings, DHCP Server, DHCP Clients, Static Assignment, MAC Clone and Port Mode. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.

Tenda
Network
LAN Settings
WAN Settings
DHCP Server
DHCP Clients
Static Assignment
MAC Clone
Port Mode

4.1.LAN Settings

LAN Settings		
IP Address Subnet Mask	192.168.0.1 255 - 255 - 255 - 0 -	For Example:192.168.1.1 For Example:255.255.0
	Save	Cancel

- IP Address: Device's LAN IP. The default is 192.168.0.1. You can change it according to your need.
- Subnet Mask: Device's LAN subnet mask.

4.2.WAN Settings

There are 6 types of Internet connection: DHCP (Dynamic IP), PPPoE and PPPoE dual access, PPTP, L2TP and Static IP available for your choice.

WAN Settings						
Interface	Connection Status	Info	Edit			
WAN	Connected	DHCP (IP:192.168.30.230/ 255.255.255.0) Gateway:192.168.30.1	Config			

- Interface: Displays the interface used currently;
- Connection Status: Displays WAN current connection status: Disconnected, Connecting or Connected.
- Info: Displays the currently used Internet connection type, gateway, IP address and subnet mask information.

1) DHCP: Select DHCP (Dynamic IP) to obtain IP Address info automatically from your ISP. Select this option if your ISP does not provide you with any IP info.

WAN Settings		
WAN Settings->WAN		
Internet Connection Type	DHCP	
MTU	1500	
	Save Cancel	

> Internet connection Type: Displays a list of available Internet

Tenda

connection types.

MTU: Maximum Transmission Unit. The default value is1500.

2) Static IP: Select Static IP Address if your ISP provides all the connection info. You will need to enter the provided IP address, subnet mask, gateway address, and DNS address(es) in corresponding fields.

VAN Settings->WAN	
nternet Connection Type	Static IP 💌
P Address	192.168.30.213
ubnet Mask	255.255.255.0
efault Gateway	192.168.30.1
rimary DNS Server	192.168.30.1
econdary DNS Server	202.96.134.133
ITU	1500

- Internet connection Type: Displays a list of available Internet connection types.
- IP Address: Enter the IP address provided by your ISP. Consult your local ISP if you are not clear.
- Subnet mask: Enter the subnet mask provided by your ISP.
 Consult your ISP if you are not clear.
- > Default Gateway: Enter the gateway address provided by

your ISP. Consult your local ISP if you are not clear.

- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- MTU: Maximum Transmission Unit. The factory default is 1500.
- 3) PPPoE: Select PPPoE (Point to Point Protocol over Ethernet)

if your ISP uses a PPPoE connection and provides you with a

PPPoE user name and a PPPoE password. Simply enter them in corresponding fields.

WAN Settings					
WAN Settings->WAN					
Internet Connection Type	PPPOE	•			
User Name					
Password					
MPPE					
MTU	1492				
		Save	Cancel		

- Internet connection Type: Displays a list of available Internet connection types.
- User Name: Enter the PPPoE User Name provided by your ISP. Consult your ISP if you are not clear.
- Password: Enter the PPPoE Password provided by your ISP.
 Consult your ISP if you are not clear.

- MPPE: Select whether to enable the MPPE authentication method.
- MTU: Maximum Transmission Unit. The factory default is 1492.

4) PPTP: Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. The PPTP connects a router to a VPN server. For example: A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.

WAN Settings		
WAN Settings->WAN		
Internet Connection Type	PPTP 💌	
PPTP Server IP	pptp_server	(IP address or domain name)
User Name	pptp_user]
Password	•••••]
Address Mode	Static 💌	
IP Address]
Subnet Mask]
Default Gateway]
Primary DNS Server]
Secondary DNS Server]
MPPE		
MTU	1460]
	Save	Cancel

- Internet connection Type: Displays a list of available Internet connection types.
- > PPTP Server: Enter the IP address of a PPTP server.

Wireless AC1750 Dual-band Gigabit Router

Tenda

- > User Name: Enter your PPTP User Name.
- Password: Enter your Password.
- Address mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- IP Address: Enter the IP address provided by your ISP.
 Consult your local ISP if you are not clear.
- Subnet Mask: Enter the subnet mask provided by your ISP. Consult your ISP if you are not clear.
- Default Gateway: Enter the gateway provided by your ISP.
 Consult your local ISP if you are not clear.
- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- MPPE: Select whether to enable the MPPE authentication method.
- MTU: Maximum Transmission Unit. The factory default is 1460.

5) L2TP: Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server. For example: A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.
| WAN Settings | | |
|--------------------------|---|---|
| WAN Settings->WAN | | |
| Internet Connection Type | L2TP 💌 | |
| L2TP Server IP Address | I2tp_server (IP Address or domain name) |) |
| User Name | I2tp_user | |
| Password | ••••• | |
| Address Mode | Static 💌 | |
| IP Address | | |
| Subnet Mask | | |
| Default Gateway | | |
| Primary DNS Server | | |
| Secondary DNS Server | | |
| MTU | 1458 | |
| | | |
| | Save Cancel | |

- Internet connection Type: Displays a list of available Internet connection types.
- L2TP Server: Enter the L2TP IP address provided by your ISP.
- User Name: Enter your L2TP User Name.
- Password: Enter your Password.
- Address mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- IP Address: Enter the IP address provided by your ISP.
 Consult your local ISP if you are not clear.
- > Default Gateway: Enter the gateway provided by your ISP.

Consult your local ISP if you are not clear.

Tenda

- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- MTU: Maximum Transmission Unit. The factory default is 1458.
- PPPoE Dual Access: Select PPPoE (Point to Point Protocol over Ethernet) Dual Access if your ISP uses a PPPoE Dual Access connection and provides you with a PPPoE user name and a PPPoE password. Simply enter them in corresponding fields. In the mean time, you can also use static address mode or dynamic address mode for MAN access.

WAN Settings	
WAN Settings->WAN	
Internet Connection Type	PPPOE Dual Access
User Name	
Password	
Address Mode	Static 💌
IP Address	
Subnet Mask	
Default Gateway	
MPPE	
MTU	1492
	Save Cancel

Internet connection Type: Displays a list of available Internet connection types.

- User Name: Enter the PPPoE User Name provided by your ISP. Consult your ISP if you are not clear.
- Password: Enter the PPPoE Password provided by your ISP.
 Consult your ISP if you are not clear.
- Address mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- IP Address: Enter the IP address provided by your ISP.
 Consult your local ISP if you are not clear.
- Subnet mask: Enter the subnet mask provided by your ISP.
 Consult your ISP if you are not clear.
- Default Gateway: Enter the gateway address provided by your ISP. Consult your local ISP if you are not clear.
- MPPE: Select whether to enable the MPPE authentication method.
- MTU: Maximum Transmission Unit. The factory default is 1492.

▲Note:

It is not advisable to change the factory default MTU value unless necessary as an improper MTU value may degrade your network performance or even lead to network malfunction.

4.3 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is an

automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this device, it will automatically configure TCP/IP protocol settings for all DHCP-Client-enabled PCs in your LAN, including IP address, subnet mask, gateway and DNS etc.

DHCP Server	🔽 Enable
Start IP Address	192.168.0.100
End IP Address	192.168.0.200
Lease Time	7 days 💌
Primary DNS Server	192.168.0.1
Secondary DNS Server (Optional)	

- DHCP Server: Select whether to enable or disable the Device's DHCP server feature.
- Start IP: Enter the starting IP address for the DHCP server's IP assignment.
- End IP: Enter the ending IP address for the DHCP server's IP assignment.
- Lease Time: The length of time for the IP address lease.
- Primary DNS Server: Specify a primary DNS server address that will be assigned to DHCP clients upon request.
- Secondary DNS Server: Specify a secondary DNS server address that will be assigned to DHCP clients upon request.



[▲]Note:

To apply the DHCP server settings to all PCs on your LAN, you must set all PCs to "Obtain an IP address automatically" and "Obtain DNS server address automatically" respectively.

4.4 DHCP Clients

This section displays a DHCP dynamic client list, which includes host name, IP address, MAC address and lease time info.

DH	CP Client List			
	If you enable the DHCP serve	er feature, DHCP client list will be upd	dated every 5 seconds.	Refresh
	Host name	IP Address	MAC Address	Lease Time
	wwx-PC	192.168.0.128	C8:3A:35:0B:40:6F	6D 23:58:11

- Host name: Displays clients' host names.
- IP Address: Displays IP address(s) that client(s) obtained from the DHCP server.
- > MAC Address: Displays MAC address of a given host.
- Lease Time: Remaining time for a corresponding IP address lease.

4.5 Static Assignment

The DHCP server provides DHCP static IP address reservation feature. If you would like some devices on your network to always have fixed IP addresses, you can use this feature and manually add a static DHCP assignment entry for each such device. For example: If you want a PC at the MAC address of 00:15:58:C0:D4:3F (on your internal network) to always receive the IP address of 192.168.0.150 from the device's DHCP server. First, enter the IP address and MAC address in corresponding fields as seen below. Second, click Add and Save to save your settings.

Static As	signment		
IP Ad MAC	dress Address		Add
ID	IP Address	MAC Address	Action
1	192.168.0.150	Save Cancel	Edit Delete

- IP Address: Enter the IP address for static DHCP assignment.
- MAC Address: Enter the MAC address of a computer to always receive the same IP address you specify.
- Add: Click it to add a new IP-MAC static assignment entry to list.
- > Edit: Click it to change an existing entry.
- > Delete: Click to remove an existing entry.

4.6 MAC Clone

This section allows you to configure Device's WAN MAC address.



Use this section to config device's WAN MAC a	ddress.
WAN MAC Address: C8:3A:35:D5:7A:1C	Restore to Factory Default MAC Clone
	2

- > WAN MAC Address: Config Device's WAN MAC address.
- Restore to Factory Default MAC: Reset Device's WAN MAC to factory default.
- Clone MAC: Click to copy your PC's MAC address to the WAN MAC Address field on the Device.

△Note:

Normally you don't need to change the default WAN MAC value. However, some ISP may bind client PC's MAC address for Internet connection authentication. In this case, simply enter such MAC in the WAN MAC Address field or click the "Clone MAC" button. Note that the WAN MAC address in "Status" interface will be updated accordingly once you changed it.
 Do remember to reboot the router to activate the new WAN MAC. DO NOT use the "Clone MAC" feature unless required by your ISP.

3. Only the MAC addresses of the PCs on LAN can be cloned to the Device.

4.7 Port Mode

This page lets you set speed and duplex mode for device's WAN

port. It is advisable to keep the default settings.

WAN Interface-Speed/Duplex	Auto	-	
	Auto		
	10M full-duplex		
	10M half-duplex		
	100M full-duplex	Save	Cancel
	100M half-duplex		
	1000M full-duplex		
	1000M half-duplex		

- Auto: Keep the default of Auto, unless the cable to the WAN port is excessively long, which may deduce drive capability.
- 10M full-duplex: Select to set WAN port to 10M full-duplex to enhance the driving ability.
- 10M half-duplex: Select to set WAN port to 10M half-duplex. If your WAN port is properly connected but does not function correctly, it may be caused by poor driving capacity of the cable. Please set the WAN port to 10M half-duplex to improve drive capability.
- 100M full-duplex: Select to set WAN port to 100M full-duplex.
- 100M half-duplex: Select to set WAN port to 100M half-duplex.
- 1000M full-duplex: Select to set WAN port to 1000M full-duplex.
- 1000M half-duplex: Select to set WAN port to 1000M half-duplex.

CHAPTER 5 SECURITY

The "Security" tab includes 6 submenus: IP Group, Time Group,

Client Filter, URL Filter ,MAC Filter and Remote Web

Management. Clicking any of them enters corresponding

interface for configuration. Below explains, in details, each such feature.



5.1 IP Group

Here you can set up a IP group and define a name for it or briefly describe it. An IP group determines which IP address or IP addresses specific rules of other related features are to be enabled on.



Add IP Group	
Group Name:	
Group Description:	
IP:	
	Note: You can only either enter a single IP address or specify an IP address range.
Add IP:	- Add Edit Delete Clear
	Save Cancel

- Group Name: Define a name for a corresponding group.
- ➢ Group Description: Briefly describe a corresponding group.
- IP: Displays the added IP address or an IP range;
- Add IP: Enter an identical IP address or two different IP addresses in both fields and then click Add to add a single IP address or a range of IP addresses.
- Edit: Click to edit an existing IP address or IP range.
- > Delete: Click to delete an existing IP address or IP range.
- Clear: Click to clear all info on the page.

5.2 Time Group

Here you can set up a time group and define a name for it or briefly describe it. A time group determines when specific rules of other related features are to take effect.



Add	Time	Gro	oup																					
(Group	Name	e:													_								
(Group	Desci	ription	n:																				
A11	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon																								
Tue																								
Wen																								
Thu																								
Fri																								
Sat																								
Sun																								
											Sa	ve			Cano	el								

- Group Name: Define a name for a corresponding group.
- ➢ Group Description: Briefly describe a corresponding group.

To select a time or time group, simply click corresponding area.

5.3 Client Filter

To better manage PCs in LAN, you can allow or disallow such PCs to access certain ports on Internet using the Client Filter functionality. Before you can set up a client filter rule, you must set an IP group and a time group.

Filter Mode:	Deny 💌 Access to Internet
nable:	
escription:	
P Group:	100_150 💌
ime Group:	All
AN Port Range:	~
otocol:	Both 💌

- ➢ Filter Mode: Select Deny or Allow.
- Enable: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched packets to pass through router).
- > Description: Briefly describe the current rule.
- IP Group: Select an IP group for the corresponding rule to apply to.
- Time Group: Select a time group for the corresponding rule to apply to.
- WAN Port Range: Enter TCP/UDP protocol port number (s);
 it can be a range of ports or a single port.
- Protocol: Select a protocol or protocols for the traffic (TCP/UDP/Both).

Client Filter							
Client Filter: 🔽	Enable						
Note: if a curre	ntly configured rule repeat	ts or overlaps an earlier con	ifigured rule, i	then only the	e previous rule take	s effect.	
Default: Allow	 Access to Internet 						
Filter Mode	IP Group Name	Time Group Name	Port	Protoco1	Description	Enable	Action
Deny	100_150	A11	1-65535	Both	Client_Filter	V	Edit Delete
					Delete	All Add	
		Save	ancel				

All client filter rules will be summarized in a list.

- > Client Filter: Check to enable the feature.
- Default: Default filter mode; select Allow or Deny from the drop-down list. For example, if Deny is selected from the

Default drop-down list (i.e. default mode is "Deny Access to Internet"), then all clients will be denied from accessing Internet at any time. And if Deny is selected from the Filter Mode drop-down list, then all clients will be denied from accessing Internet at any time. However, if Allow is selected from the Filter Mode drop-down list, then only clients whose IP addresses are included in the specified IP group will be allowed to access Internet during the time period specified by the time group in the rule.

Example 1: To forbid PCs at the IP addresses between 192.168.0.100 and 192.168.0.150 inclusive from accessing Internet at any time, do as follows:

Step 1. Set an IP group: 192.168.0.100-192.168.0.150.

Group Name:	100_150
Group Description:	IP_Group
	192.168.0.100-192.168.0.150
1P:	
	Note: You can only either enter a single IP address or specify an IP address rang
Add IP:	Add Edit Delete Clea

Step 2. Set a time group: select "All".



Group Name:										All														
(Group Description:									Time_Group														
A11	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon																								
Tue																								
Wen																								
Thu																								
Fri																								
Sat																								
Sun																								

Step 3. Set a client filter rule as shown below.

Filter Mode:	Deny 💌 Access to Internet
Enable:	
Description:	Client_Filter
IP Group:	100_150
Time Group:	All
WAN Port Range:	1 ~ 65535
Protocol:	Both 💌

Step 4. Enable the Client Filter feature and select "Allow" from the "Default" drop-down list as shown below.



Client Filter:	Enable ly configured rule repeat	ts or overlaps an earlier cor	ifigured rule, t	then only the	previous rule take	s effect.	
Default: Allow [Access to Internet 						
Filter Mode	IP Group Name	Time Group Name	Port	Protocol	Description	Enable	Actio
Deny	100_150	All	1-65535	Both	Client_Filter		Edit De
					Delet	e All Add	
					Delet	e All Add	

Example 2: To allow only the PC at an IP address of 192.168.

0.145 to browse webpages from 8:00 to 18: 00, do as follows:

Step 1. Set an IP group: enter 192.168.0.145 in both fields.

Group Name:	145
Group Description:	IP_Group
	192.168.0.145-192.168.0.145
IP:	
	Note: You can only either enter a single IP address or specify an IP address range.
Add IP:	- Add Edit Delete Clear

Step 2. Set a time group: select "08"-"18" and "Mon"-"Sun".



Group Name:	8_18		
Group Description:	Time_Group		
All 00 01 02 03 04 05 00	07 08 09 10 11 11	2 13 14 15 16 17 18 19 20 21	22 23
Mon			
Tue			
Wen			
Thu			
Fri			
Sat			
Sun			
	Save	Cancel	

Step 3. Set a client filter rule as shown below.

Client Filter	
Filter Mode:	Allow 💌 Access to Internet
Enable:	
Description:	Client_Filter
IP Group:	145 💌
Time Group:	8_18 💌
WAN Port Range:	80 ~ 80
Protocol:	Both 💌
	Save Cancel

Step 4. Enable the Client Filter feature and select "Deny" from the "Default" drop-down list as shown below.



Clie	ent Filter							
	Client Filter: 🗹 En Note: if a currently	nable y configured rule repeats	s or overlaps an earlier confi	gured rule,	then only th	e previous rule take	s effect.	
	Default: Deny 💌	Access to Internet						
	Filter Mode	IP Group Name	Time Group Name	Port	Protocol	Description	Enable	Action
	A11ow	145	8_18	80-80	Both	Client_Filter		Edit Delete
						Delete	All Add	
			Save Ca	ncel				

5.4 URL Filter

To better control LAN PCs, you can use the URL filter functionality to allow or disallow such PC to access certain websites within a specified time range. Before you can set up a URL filter rule, you must set an IP group and a time group.

Add URL Filter Filter Mode:	Denv 💌 Access to Internet
Enable:	
Description:	
IP Group:	100_150
Tome Group:	All
URL String:	(A comma should be put between different domain names. Up to 16 entries allowed!)
	Save Cancel

- Filter Mode: Select Deny or Allow.
- Enable: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched packets to pass through router).
- > Description: Briefly describe the current entry/rule.

- IP Group: Select a proper IP group for the corresponding rule to apply to.
- Time Group: Select a proper time group for the corresponding rule to apply to.
- URL String: Enter domain names or a part of a domain name to be filtered out.

Note:if a currently configured rule repeats or overlaps an earlier configured rule,then only the previous rule takes effect. Default: Deny Recess to Internet Filter Mode IP Group Name Time Group Name URL String Description Enable	
Default: Deny 🔽 Access to Internet Filter Mode IP Group Name Time Group Name URL String Description Enable Datate all def	
Filter Mode IP Group Name Time Group Name URL String Description Enable	
Delete all inde	Action
Delete All Add	
Delete All Add	

All rules will be summarized in a list.

- > URL Filter: Check to enable the feature.
- Default: Default filter mode; select Allow or Deny from the drop-down list. For example, if Deny is selected from the Default drop-down list (i.e. default mode is "Deny Access to Internet"), then all clients will be denied from accessing Internet at any time. And if Deny is selected from the Filter Mode drop-down list, then all clients will be denied from accessing Internet at any time. However, if Allow is selected from the Filter Mode drop-down list, then only clients whose IP addresses are included in the specified IP group will be allowed to access corresponding websites during the time

period specified by the time group in the rule.

If you want to disallow all computers on your LAN to access Google and facebook from 8: 00 to 18: 00 during working days (Monday- Friday), then do as follows:

Step 1. Set an IP group: 192.168.0.2-192.168.0.254.

Broup Name:	2_254
Group Description:	IP_Group
	192.168.0.2-192.168.0.254
7	
P:	
	Note: You can only either enter a single IP address or specify an IP address range.
Add IP:	Add Edit Delete Clear

Step 2. Set a time group: select "08"-"18" and "Mon"-"Fri".

Group Name:									Μ	Mon_Fri_8_18					_									
Group Description:									Time_Group															
A11	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon																								
Tue																								
Wen																								
Thu																								
Fri																								
Sat																								
Sun																								
											Sa	ve			Cano	el								

Step 3. Set a filter rule as shown below.



Filter Mode:	Deny 🔽 Access to Internet
Enable:	V
Description:	URL_Filter
IP Group:	2_254
Tome Group:	Mon_Fri_8_1
TIDI ()	google,facebook (A comma should be put between different domain nam
UKL String:	to 16 entries allowed!)

Step 4. Enable the URL Filter feature and select "Allow" from the "Default" drop-down list as shown below.

		ts or overlaps an earlier conf	figured rule, then only the	previous rule takes e	ffect.	
Default: Allow	Access to Internet					
Filter Mode	IP Group Name	Time Group Name	URL String	Description	Enable	Action
Deny	2_254	Mon_Fri_8 _18	google,facebook	URL_Filte r		Edit Delete
				Delete	All Add	

▲Note:

Each entry can include up to 16 domain names, each of which must be separated by " ".

5.5 MAC Filter

To better manage PCs in LAN, you may use the MAC Address Filter function to allow/disallow such PCs to access to Internet.



Filter Mode	Deny 💌 Access to Internet	
Description		
MAC:	MAC Address list	•
Time:	00 - 00 - 00 - 00 - MAC Address list	
Day:	Everyday Sun Mon Tue Wen Tt 192.168.0.123-8C:64:22:88:2D	:B2

Filter Mode:

Deny Access to Internet: Disallow only specified packets to access Internet; other packets are not restricted. Allow Access to Internet: Allow only specified packets to access Internet; other packets are denied.

- > Description: Briefly describe the current rule.
- MAC: Specify the MAC address of the PC for the corresponding rule to take effect. MAC Address list: Displays MAC addresses of all clients connected to the device. Simply select the desired MAC address and add it to the MAC field. Or you can also add it manually.
- > Time: Specify a time range for a current rule to take effect.
- Day: Select a day or several days for a current rule to take effect.

MAC Filter												
MAC Filter Enab	ole											
Defalut: Deny 💌	Access to Internet											
			Day									
Filter Mode	Filter Mode MAC	Time	Sun	Mon	Tue	Wen	Thu	Fri	Sat	Description	Action	
Deny	22:22:22:22:22:22	00:00-00:00	٧	٧	~	٧	~	٧	٧	MAC Filter	Modify	Delete
									De	lete All Add		
			Sal	10		Cance						
			Sal	le		Cance	51					

All rules will be summarized in a list.

- > MAC Filter: Check to enable the feature.
- Default: Select Allow or Deny from the drop-down list. For example, if Deny is selected from the Default drop-down list (i.e. default mode is "Deny Access to Internet"), then all clients at specified MAC addresses will be denied from accessing Internet at any time. And if Deny is selected from the Filter Mode drop-down list, then all clients at specified MAC addresses will be denied from accessing Internet at any time. However, if Allow is selected from the Filter Mode drop-down list, then only clients at specified MAC addresses will be allowed to access Internet during the time period specified by the time group in the rule.

Example1: To prevent a PC at the MAC address of 00:E0:4C:69:A4:10 from accessing Internet between 8:00 and16:00 during working days (Monday -Friday). Do as follows: Step 1. Set a MAC filter rule as shown below.

Add MAC Filter		
Filter Mode	Deny Access to Internet	
Description	MAC Filter	
MAC:	00 E0 4C 69 A4 10 <= MAC Address list	-
Time:	$08 \bullet 00 \bullet \sim 16 \bullet 00 \bullet$	
Day:	🗆 Everyday 💭 Sun 🖉 Mon 🖉 Tue 🖉 Wen 🗭 Thu 🖉 Fri 🗔 Sta	
	Save Cancel	

Step 2. Enable the MAC Filter feature and select "Allow" from the



"Default" drop-down list as shown below.

MAC Filter TEna	ble										
Defalut: Allow -	Access to Internet										
T1-26-1 2640		Time		Day					D	Action	
Filter iviode	Filter Mode MAC	1 ime	Sun	Mon	Tue	Wen	Thu	Fri	Sat	Description	Action
Deny	00:E0:4C:69:A4:10	08:00-16:00		V	~	٧	V	٧		MAC Filter	Modify Dele
									De	lete All Add	
		Save	(Cancel							

Example2: To allow a PC at the MAC address of

00:E4:A5:44:35:69 to access Internet from Monday to Friday. Do as follows:

Step 1. Set a MAC filter rule as shown below.

Add MAC Filter	
Filter Mode	Allow 💌 Access to Internet
Description	MAC Filter
MAC:	00 E4 A5 44 35 69 <= MAC Address list
Time:	00 • : 00 • ~ 00 • : 00 •
Day:	🗆 Everyday 🔲 Sun 🗹 Mon 🖉 Tue 🖉 Wen 🖉 Thu 🖉 Fri 🗌 Sta
	Save Cancel

Step 2. Enable the MAC Filter feature and select "Deny" from the "Default" drop-down list as shown below.

MA	C Filter												
	MAC Filter: Enabl	e Access to Internet											
	Filter Mode MAC		Time	Day							Description	Action	
	I little Mode	14110	THE	Sun	Mon	Tue	Wen	Thu	Fri	Sat	Description	2101011	
	Allow	00:E4:A5:44:35:69	00:00-00:00		1	~	~	1	1		MAC Filter	Modify	Delete
										De	lete All Add		
			Save	(Cancel								

5.6 Remote Web Management

The Remote Web management allows the Router to be configured from the Internet by a web browser.

mote Web Managem	ient
Enable:	
IP Address:	0.0.0.0
Port:	8080

- Enable: Select whether to enable the Remote Web-based Management feature.
- IP Address: Enter a trusted IP address of a PC from Internet or other external networks which you want to authorize to manage the device remotely via a web browser.
- > Port: Remote admin port; the port used by trusted hosts from

Internet or other external networks to access and manage the device remotely via a web browser.

For example: If you want to allow only the PC at the IP address of 218.88.93.33 from Internet to access Device's web-based utility via port: 8080, then configure the same settings as shown on the screenshot below on your Device.

emote Web Managem	ent
Enable:	
IP Address:	218.88.93.33
Port:	8080
	Save Cancel

[∆]Note:

1. To access the device via port 8080, enter "http://x.x.x.x8080" where "x.x.x.x" represents the the device's Internet IP address and 8080 is the remote admin port. Assuming the device's Internet IP address is 220.135.211.56, then, simply replace the "x.x.x.x" with "220.135.211.56" (namely,

http://220.135.211.56:8080).

Leaving the IP address field at "0.0.0.0" makes the device remotely accessible to all the PCs on Internet or other external networks; populating it with a specific IP address, say, 218.88.93.33, makes the device only remotely accessible to the PC at the specified IP address.

CHAPTER 6 ADVANCED

The "Advanced" tab includes the following 7 submenus:Virtual Server, DMZ, UPnP, DDNS, Routing, Static Routing and Bandwidth Settings. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



6.1 Virtual Server

The Virtual Server feature grants Internet users access to

services on your LAN. It is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a WAN port on your router for redirection to an internal LAN IP Address.

Virtual Server allows you	to open a single WAN service port and redirect all traffic received through such port to a LAN server at a designated IP
address. It allows remote	computers, such as computers on the Internet, to connect to a specific computer or service within a private local area netwo
(LAN).	
WAN:	WAN
WAN Port:	53 Common Service Port: DNS(53)
LAN Port:	53
Private IP:	
Protocol:	Both 💌
Enable:	

- WAN Port: WAN service port;
- LAN Port: LAN service port;
- Private IP: The IP address of a computer used as a server in LAN.
- Protocol: Includes TCP, UDP and Both. Select "Both" if you are not sure about which protocol to use.
- Enable: The corresponding entry takes effect only if you checked this option.

Well-Known Service Port: The "Well-Known Service Port" lists widely used protocol ports. Simply select a port, an entry ID and click the "Add to" button to populate the selected port to the corresponding fields of the selected entry. In case that you don't find the port you need, enter it manually.

Example: You want to share some large files with your friends who are not in your LAN; however it is not convenient to transfer such large files across network. Then, you can set up your own PC as a FTP server and use the Virtual server to let your friends access these files. Assuming that the static IP address of the FTP server (Namely, your PC) is 192.168.0.10, you want your friends to access this FTP server on the default port of 21 using the TCP protocol, then do as follows:

1. Enter 21 in both WAN Port and LAN Port fields or select FTP from "Well-known Service Port" and an entry ID, 21 will be automatically populated to corresponding fields of the selected entry.

2. Enter 192.168.0.10 in the corresponding field, select "TCP" and then check "Enable" as seen below.

Virtual Server allows you	to open a single WAN service port and redirect all traffic received through such port to a LAN server at a designated IP
address. It allows remote	computers, such as computers on the Internet, to connect to a specific computer or service within a private local area network
(LAN).	
WAN:	WAN -
WAN Port:	21 Common Service Port: FTP(21)
LAN Port:	21
Private IP:	192.168.0.10
Protocol:	TCP -
Enable:	

3. Click "Save" to save your settings.

Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server. xxx.xxx.xxx.xxx is the

router's WAN IP address. Assuming it is 172.16.102.89, then your friends need to enter "ftp://172.16.102.89: 21" in their browsers.

▲Note:

If you include port 80 on this section, you must set the port for remote (web-based) management to a different number than 80, such as 8080, otherwise the virtual server feature may not take effect.

6.2 DMZ

In some cases such as playing Internet games or holding video conferences, you may need to have your computer completely exposed to external networks for implementation of a bidirectional communication. To do so, set it as a DMZ host. Note that you should assign a static IP address to the PC designated as a DMZ host (DHCP Server> DHCP Client List> DHCP Reservation) before using the feature.



> DMZ Host IP address: Enter the IP address of a computer

on your LAN which you want to set as a DMZ host. The DMZ host should be connected to a LAN port on the Device.

- Enable: Check/uncheck to enable/disable the DMZ host feature.
- ▲ Note:

 Once enabled, the DMZ host will no longer be protected by device's firewall and thus may become vulnerable to attacks.
 Users on WAN access the DMZ host through a corresponding WAN IP address.

6.3 UPnP

UPnP (Universal Plug and Play) allows a network device to discover and connect to other devices on the network. With this feature enabled, hosts in LAN can request the device to perform special port forwarding so as to enable external hosts to access resources on internal hosts.

UPnP							
Enable UPnP							
				UPnP Mapping List			
	ID	Remote Host	WAN Port	LAN Host	LAN Port	Protocol	Description
Refresh							
			Save	Cancel			

- Enable UPnP: Check/uncheck to enable/disable the UPnP feature.
- > UPnP Mapping List: Displays info of external/internal port,

private (internal) IP, protocol and description, etc.

Note: UPnP works in Windows XP, Windows ME or later (NOTE: Operational system needs to be integrated with or installed with Directx 9.0) or in an environment with installed application software that supports UPnP.

6.4 DDNS

Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. We use a numeric IP address allocated by Internet Service Provider (ISP) to connect to Internet: the address may either be stable ("static"), or may change from one session on the Internet to the next ("dynamic"). However, a numeric address is inconvenient to remember: an address which changes unpredictably makes connection impossible. The DDNS provider allocates a static host name to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software running on a computer or network device at that address; the provider distributes the association between the host name and the address to the Internet's DNS servers so that they may resolve DNS gueries. Thus, uninterrupted access to devices and services whose numeric IP address may change is maintained.

66

DDNS	
DDNS Settings	Enable DDNS
DDNS Server Provider	no-ip.com 💌 Register
User Name	
Password	
Domain Name	(Optional)
Connection Status	Disconnected
	Save Cancel

- > DDNS Settings: Enable/Disable the DDNS feature.
- DDNS Server Provider: Select your DDNS service provider from the drop-down menu.
- User Name: Enter the DDNS user name registered with your DDNS service provider.
- Password: Enter the DDNS Password registered with your DDNS service provider.
- Domain Name: Enter the DDNS domain name with your DDNS service provider.
- Connection Status: Displays current status of connection with the DDNS server.

Click "Save" to save your settings.

For example: If you have registered a DDNS service from no-ip.com for a web server on the host at 192.168.0.10 and get



below info:

User Name	Tenda
Password	123456
Domain Name	tenda.zapto.org

First set a mapping rule on Virtual Server interface (For details, see Virtual Server section) and then enter the registered user name, password and domain name as shown below:

DDNS	
DDNS Settings	I Enable DDNS
DDNS Server Provider	no-ip.com 💌 Register
User Name	Tenda
Password	
Domain Name	tenda.zapto.org (Optional)
Connection Status	Disconnected
	Save Cancel

Click Save to save the settings. Simply input

"http://tenda.zapto.org" in a launched web browser and your web server will be accessible.

6.5 Routing

This section displays the routing table content.

Destination Network	Subnet Mask	Gateway	metric	Interface
10.10.10.1	255.255.255.255	0.0.0.0	0	ppp1
192.168.2.0	255.255.255.0	0.0.0.0	0	br1
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
127.0.0.0	255.0.0.0	0.0.0.0	0	10
0.0.00	0.0.0.0	10.10.10.1	0	ppp1

6.6 Static Routing

Use this section to customize static routes of data through your network.

Add Static Routing		
Destination Network: Subnet Mask: Gateway:		
	Save	Cancel

- Destination Network: The IP address of a destination network.
- Subnet Mask: The Subnet Mask that corresponds to the specified destination IP address.
- Gateway: The IP address for next hop.

6.7 Bandwidth Settings

To better manage bandwidth allocation and optimize network

performance, use the Bandwidth Control feature.

Bandwidth Settings				
O Disable Bandwidth Allocation				
 Custom Bandwidth Allocation 				
IP Range	Upstream	Downstream	Description	Enable Action
				Delete All Add
		Save	Cancel	

Enable the bandwidth control feature, click Add and below

screen will appear:

Bandwidth Control				
Enable	If disabled, settings below will only be saved instead of being activated.			
IP Range	-			
Upstream Bandwidth Limit	KByte(Total)			
Downstream Bandwidth limit	KByte(Total)			
P2P Download Control	🔲 Regulates P2P download rate to ensure ea	nsure each user a guaranteed share of bandwidth.		
Attaction 3 (e.f.	 Each member of the IP range shall utilize 	$\ensuremath{\bigcirc}$ All members of the IP range shall share the allocated		
Anocation Mode	the allocated bandwidth individually.	bandwidth collectively.		
Allocation Policy	$\ensuremath{\bigcirc}$ Uitize only allocated bandwidth	 Utilize more bandwidth if available 		
Description				
	Save Cance	el		

- Enable: Check/uncheck to enable/disable current entry. When disabled, corresponding entry will not take effect though existing in fact.
- > IP Range: Enter a single IP or an IP range.
- Upstream Bandwidth Limit: Max uplink traffic.

- > Downstream Bandwidth Limit: Max downlink traffic.
- P2P Download Control: Regulates P2P download rate to ensure each user a guaranteed share of bandwidth.
- Allocation Mode: Select either "Individual (Each member of the IP range shall utilize the allocated bandwidth individually)" or "Collective (All members of the IP range shall share the allocated bandwidth collectively)";
- Allocation Policy: Select either "Utilize only the allocated bandwidth" or "Utilize more bandwidth if available".
- > Description: Briefly describe the current rule.

CHAPTER 7 WIRELESS SETTINGS

The "Wireless" tab includes 8 submenus: Basic Settings, Wireless Security, WPS, WDS, Guest Network, Wireless Access Control, Connection List and Advanced Settings. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.
Tenda
Wireless
Basic Settings
Wireless Security
WPS
WDS
Guest Network
Wireless Access Control
Connection List
Advanced Settings

7.1 Basic Settings

This section allows you to manage your wireless network (2.4G or 5G). You can select your country (Unavailable for 5G wireless network), config wireless network name (SSID), network mode and channel settings, etc the way you want.

Basic Settings--2.4G



Basic Settings	
2.4G Basic Settings	5G Basic Settings
Country: Germany 💌	
2.4GHz wireless network	☑ Enable
SSID Broadcast	Enable
SSID	Tenda_00904C
802.11 Mode	11b/g/n mixed mode 💌
Channel	2462MHz (Channel 11)
Channel Bandwidth	
Extension Channel	2442MHz (Channel 7)
WMM Capable	
APSD Capable	🛇 Enable 🔘 Disable
	Save Cancel

- Select 2.4G Basic Settings or 5GHz Basic Settings to configure basic settings on corresponding band.
- Country: Select your country from the drop-down list. There are 11 options available.
- 2.4GHz Wireless Network: Check/uncheck to enable/disable the 2.4GHz wireless feature. If disabled, all 2.4GHz-based features will be disabled accordingly.
- SSID Broadcast: This option is enabled By default. Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to see what's available. When disabled,



wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.

- SSID: A SSID (Service Set Identifier) is the unique name of a wireless network.
- 802.11 Mode: Select a right mode according to your wireless client. The default mode is 11b/g/n mixed.
- Channel: For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
- Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of 20/40M frequency band; when there are only non-11n wireless clients, select 20M frequency band mode; when the wireless network mode is 11n mode, please select 20/40 frequency band to boost its throughput.
- Extension Channel: Available only in 11b/g/n mixed mode.
- WMM Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data (such as video or audio).
- > ASPD Capable: Select to enable/disable the auto power

saving mode.

Basic Settings--5G

Basic Settings	
2.4G Basic Settings	<u>5G Basic Settings</u>
Country: America 👻	
5GHz wireless network	✓ Enable
SSID Broadcast	Enable O Disable
SSID	Tenda_5_00A04C
802.11 Mode	11a/n mode 💌
Channel	5200MHz (Channel 40)
Bandwidth	© 20MHz ◎ 40MHz ◎ 80MHz
WMM Capable	Enable Disable Disable
APSD Capable	© Enable 💿 Disable
	Save Cancel

- Select 2.4G Basic Settings or 5GHz Basic Settings to configure basic settings on corresponding band.
- 5GHz Wireless Network: Check/uncheck to enable/disable the 5GHz wireless feature. If disabled, all 5GHz-based features will be disabled accordingly.
- SSID Broadcast: This option is enabled By default. Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to see what's available. When disabled, wireless clients will have to first know this SSID and

manually enter it on their devices if they want to connect to the SSID.

- SSID: A SSID (Service Set Identifier) is the unique name of a wireless network; it is configurable.
- 802.11 Mode: Select a right mode according to your wireless client. The default mode is 11a/n.
- Channel: For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
- Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. For best throughput, 80MHz is recommended.
- WMM Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data (such as video or audio).
- ASPD Capable: Select to enable/disable the auto power saving mode. By default, this option is disabled.

7.2 Wireless Security

This section allows you to encrypt your wireless network to block unauthorized accesses and malicious packet sniffing.

The security feature applies to both 2.4GHz wireless and 5GHz

wireless networks. Depending on which band your wireless

network is operating on, select the right option: 2.4G or 5G.

ancel
a

Six security modes are available: None (Disable), Open, Shared and WPA-PSK, WPA2-PSK and Mixed WPA-PSK/WPA2-PSK.

1、 Open

WEP is intended to provide data confidentiality comparable to that of a traditional wired network.

Security Mode		
2.4G Encrypt Type	5G Encrypt Type	
2.4GHz network SSID "Tenda_00A04C"		
Security Mode	Open 💌	
Default key	key 1 💌	
WEP key1	ASCII	ASCII 🗸
WEP key2	ASCII	ASCII 🗸
WEP key3	ASCII	ASCII 👻
WEP key4	ASCII	ASCII 🗸
	Save Cancel	

- Security Mode: Select a proper security mode from the drop-down list.
- > Default Key: Select a key from the preset keys 1-4 for

current use.

2、 Shared

WEP is intended to provide data confidentiality comparable to

that of a traditional wired network.

Security Mode		
2.4G Encrypt Type	5G Encrypt Type	
2.4GHz network SSID "Tenda_00A04	IC"	
Security Mode	Shared	
Encryption type	WEP -	
Default key	key 1 💌	
WEP key1	ASCII	ASCII -
WEP key2	ASCII	ASCII -
WEP key3	ASCII	ASCII -
WEP key4	ASCII	ASCII -
	Save Cancel	

- Security Mode: Select a proper security mode from the drop-down list.
- Encrypt Type: WEP by default.
- Default Key: Select a key from the preset keys 1-4 for current use.
- 3、WPA-PSK

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only Tenda

authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.

Security Mode	
2.4G Encrypt Type	<u>5G Encrypt Type</u>
2.4GHz network SSID "Tenda_0E51	23"
Security Mode	WPA - PSK
Cipher Type	◉ AES ◎ TKIP ○ TKIP&AES
Security Key	12345678
Key Renewal Interval	86400 Seconds
	Save Cancel

- Security Mode: Select a proper security mode from the drop-down list.
- Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- > Key Renewal Interval: Enter a valid time period for the key.
- 4、WPA2-PSK

WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. It is more secured than WPA and WEP.



curity Mode	
2.4G Encrypt Type	<u>5G Encrypt Type</u>
2.4GHz network SSID "Tenda_0E5	5123"
Security Mode	WPA2 - PSK
Cipher Type	◉ AES ◎ TKIP ◎ TKIP&AES
Security Key	12345678
Key Renewal Interval	86400 Seconds

- Security Mode: Select a proper security mode from the drop-down list.
- Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- > Key Renewal Interval: Enter a valid time period for the key.
- 3、Mixed WPA/WPA2-PSK

Mixed WPA/WPA2-PSK provides both WPA-PSK WPA2-PSK security modes with AES, TKIP and TKIP&AES cipher types.



2.4G Encrypt Type	5G Encrypt Type
2.4GHz network SSID "Tenda	_0E5123"
Security Mode	Mixed WPA/WPA2 - PSK 💌
Cipher Type	◉ aes ☉ tkip ☉ tkip&aes
Security Key	12345678
Key Renewal Interval	86400 Seconds

- Security Mode: Select a proper security mode from the drop-down list.
- Cipher Type: Select AES (advanced encryption standard), TKIP or TKIP (temporary key integrity protocol) &AES.
- Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- > Key Renewal Interval: Enter a valid time period for the key.

7.3 WPS

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a secure wireless home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. Simply enter a PIN code or press the software PBC button or hardware WPS button (if any) and a secure wireless connection is established.



8 Mode		
2.4G WPS	<u>5G WPS</u>	
2.4GHz wireless network		
2.4GHz SSID	Tenda_00A04C	
Enable WPS	🗇 Disable 🔍 Enable	
WPS Mode	© PBC ◎ PIN 0000000	
		Reset OOB

- > Enable WPS: Select to enable/disable the WPS encryption.
- > WPS Mode: Select PBC (Push-Button Configuration) or PIN.
- Reset OOB: When clicked, the WPS LED turns off; WPS function will be disabled automatically; WPS server on the Router enters idle mode and will not respond to client's WPS connection request.

Operation Instructions:

PBC: (Before you start the following operations, make sure you have enabled the WPS feature on the device from the web utility.) Press the hardware WPS button on the device for 1 second and if the WPS LED keeps blinking for about 2 minutes, it indicates that PBC encryption mode is successfully enabled. And an authentication will be performed between your device and the other WPS/PBC-enabled wireless client during this time; if it succeeds, the wireless client connects to your device, and the WPS LED turns off. Repeat steps mentioned above if you want to add more wireless clients to the device.

PIN: To use this option, you must know the PIN code from the

Tenda

wireless client and enter it in the corresponding field on your device while using the same PIN code on client side for such connection.

Note: To use the WPS encryption, the wireless adapter must be WPS-capable. The PIN code can be found on the label attached to device.

7.4 WDS

WDS (Wireless Distribution System) feature can be used to extend your existing 2.4G or 5G wireless network coverage. Here we present you how to config such feature in 2.4GHz, which also applies to 5GHz.

WDS Mode	
2.4G WDS	<u>5G WDS</u>
WDS Mode	Repeater Mode 💌
AP MAC address	
AP MAC address	
Open scan	
	Save Cancel

- Select 2.4G WDS or 5G WDS.
- > WDS Mode: Select Disable or Repeater Mode.
- > AP MAC address: Displays the MAC address of the router

Tenda

that is successfully bridged.

For example: select Repeater Mode and click Open Scan to scan all available wireless networks (To ensure that both devices involved communicate through the same channel, set the channel to "Auto" before scanning.).

2.4G W	<u>/DS</u>	5G WDS			
WDS Mode		Repeater Mode 💌			
AP MAC ad	Idress				
AP MAC ad	ldress				
se scan					
Select	SSID	MAC address	Channel	Security	Signal strengt
\odot	wangwenxiu_wwx	C8:3A:35:28:28:28	0	none	
0	wangwenxiu_wwx fltmap	C8:3A:35:28:28:28 C8:3A:35:4B:DC:B8	6	none	77
0	wangwenxiu_wwx fltmap N4	C8:3A:35:28:28 C8:3A:35:4B:DC:B8 C8:3A:35:5C:6B:28	6 7	none wep/wpa	77 82
O O O O	wangwenxiu_wwx fltmap N4 Tenda_C8CCC0	C8:3A:35:28:28 C8:3A:35:4B:DC:B8 C8:3A:35:5C:6B:28 00:00:00:C8:CC:C0	6 7 4	none none wep/wpa none	77 77 82 77
© © © ©	wangwenxiu_wwx fltmap N4 Tenda_C8CCC0 Tenda	C8:3A:35:28:28:28 C8:3A:35:4B:DC:B8 C8:3A:35:5C:6B:28 00:00:00:C8:CC:C0 00:10:18:A9:08:5E	6 7 4 11	none wep/wpa none none	77 77 82 77 73
	wangwenxiù_wwx fltmap N4 Tenda_C&CCCO Tenda Tenda 888888	C8:3A:35:28:2828 C8:3A:35:4B:DC:B8 C8:3A:35:5C:6B:28 00:00:00:C8:CC:C0 00:10:18:A:90:8:E 00:90:4C:88:88:88	6 7 4 11 10	none wep/wpa none none wep/wpa	77 77 82 77 73 82

Simply check the wireless network you want to connect to. After successfully completing settings on the Device, repeat above operations on the other device. When the two devices added each other's MAC address, the WDS may be implemented successfully.

[∆]Note:

1. WDS feature can only be implemented between 2
 WDS-capable wireless devices. Plus, SSID, channel, security



settings and security key must be exactly the same on both such devices.

Note that you may need to change one of the router's LAN IP to avoid an IP address collision. It is advisable to disable the DHCP server on either of the two routers involved.

7.5 Guest Network

The Guest Network feature allows guests to access Internet and other users on the guest network while disallowing them to access Device web manager, users on master network and clients behind the LAN ports. Thus the wireless master network is secured. You can find the guest network available in both 2.4G and 5G networks. Here we present you how to config such feature on 2.4GHz band, which also applies to 5GHz.

Guest Network	
2.4G Custom Network	<u>5G Custom Network</u>
2.4GHz wireless network	
Guest Network	Enable
SSID Broadcast	Enable
AP Isolation	Enable
SSID	Tenda_5_2_00A04D
Security Mode	Disable 💌
	Save Cancel

Tenda

- > Select 2.4GHz or 5GHz Guest Network.
- Guest Network: Select to enable/disable the guest network feature.
- SSID Broadcast: This option is enabled By default. Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to see what's available. When disabled, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.
- AP Isolation: If enabled, clients connecting to the guest network will be mutually inaccessible.
- SSID : A SSID (Service Set Identifier) is the unique name of a wireless network.
- Security Mode: Select a proper security mode to encrypt the guest network. For details, see section 7.2 hereof.

7.6 Wireless Access Control

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your 2.4G or 5G wireless network. Here we present you how to config such feature in 2.4GHz band, which also applies to 5GHz network.



ddresses to connect to your wireless network
ddresses to connect to your wireless networ
Action
Add

Filter Mode:

Allow Access to Wireless Network: Allow only PCs at specified MAC addresses to connect to your wireless network.

Deny Access to Wireless Network: Block only PCs at specified MAC addresses from connecting to your wireless network.

- MAC address: Specify the MAC address that is to be filtered out.
- > Add: Click to add specified MAC address to the MAC list.

Example: To allow only the PC at the MAC address of 00:E8:C8:A4:56:75 to connect to your wireless network, do as follows:



Wireless Access Control		
2.4G Wireless Access Control	5G Wireless Access Control	
2.4GHz network SSID "Tenda_00A04C"		
The Wireless Access Control feature can be used to	o allow or disallow clients at specified MA	C addresses to connect to your wireless network.
Wireless Access Control A	Allow 💌 Access to Wireless Network	
MAC ad	ddress	Action
00 : E8 : C8 :	A4 : 56 : 75	Add
	00:E8:C8:A4:56:75	Delete
	Save Cancel	

A. Enter 00:E8:C8:A4:56:75 in the MAC address field and then click Add.

B. The MAC address will then be displayed in the MAC list. Now click the Save button.

7.7 Connection List

This interface displays the information of currently connected wireless clients (if any).



7.8 Advanced Settings

This section allows you to config advanced settings, including AP Isolation, Beacon interval, Fragment threshold, RTS threshold

and DTIM interval, etc, for both 2.4G and 5G wireless networks.

Advanced Settings	
2.4G Advanced Settings	5G Advanced Settings
AP Isolation	Enable
Beacon Interval	100 ms (range: 20 - 999,default: 100)
Fragment Threshold	2346 (range: 256 - 2346, default: 2346)
RTS Threshold	2347 (range: 1 - 2347, default: 2347)
DTIM Interval	3 (range: 1 - 16384, default: 1)
	Save Cancel

- > AP Isolation: Isolates clients connecting to master SSID.
- Beacon Interval: A time interval between any 2 consecutive Beacon packets sent by an Access Point to synchronize a wireless network. Do NOT change the default value of 100 unless necessary.
- Fragment Threshold: Specify a Fragment Threshold value. Any wireless packet exceeding the preset value will be divided into several fragments before transmission. DO NOT change the default value of 2346 unless necessary.
- RTS Threshold: If a packet exceeds such set value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference. For normal SOHO, it is recommended to keep the default value unchanged; otherwise, device performance may be degraded.

Tenda

DTIM Interval: A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive at device's buffer, the device will send DTIM (delivery traffic indication message) and DTIM interval to wake clients up for receiving these packets.

CHAPTER 8 USB

The Router provides two USB interfaces for USB device connection. The "USB" tab includes three submenus: "USB Storage" "USB Printer" and DLNA.



8.1 USB Storage

The storage sharing feature allows you to share files on the storage device attached to the Device.



Device Name	W1800R	
Workgroup	Workgroup	
	Add Edit Delete	

- Enable: Check/uncheck to enable/disable storage sharing feature.
- Device Name: Define a meaningful name to you for the device.
- > Workgroup: Define a work group name for the device.
- Add: Click to add a user account. Up to 5 accounts can be added.
- > Edit: Click to edit an existing account.
- > Delete: Click to delete an existing account.

Operation Instructions:

Before sharing files on a USB storage device, you must create a user account.

- 1. Create account:
- 1). Click "Add" to display a dialogue box as seen below:



ble	
ice Name	W1800R
lgroup	Wor User Name
C	Password Comfirm Password
	Ok Cancel

2) a. Enter a user name and a password, which will be used to authenticate users trying to access the USB storage device for sharing files. b. Re-type to confirm password. Click the "OK" button and below screen will appear:

Device Name W1800R Workgroup Workgroup	
Workgroup Workgroup	
ID Add Edit Delete	
1 tenda	
ĸ	

2. Set Access Right

Select a desired account, click Disk and select sda1 or sdb1.

Select a proper access right:

Read/Write: The right to Read and Write.

Read: The right to Read.

No right: No right to share corresponding file.

Click "Save" to apply all settings.

Enable					
Device Name	W1800R				
Workgroup	Workgroup				
ID	Add Edit	Delete			
1	tenda				
Disk					
Disk_sdal					
Disk_sdb1					
ishare		r/wO	RO	NO	
LAN_Realtek_v5.	780_XP-32	R/WO	RO	NO	
recycle.{645FF04	0-5081-101B-9F08-				
00AA002F954E}		r/wO	R③	NO	
share		R/WO	RO	NO	
Tenda		r/wO	RO	NO	
abcdefghijklm	nopqrstuvwxyz	0123			
456789		R/W③	RO	NO	
test		R/WO	RO	NO	

3. Access shared file

To access resources on such storage device, double click "My Computer" on your PC and enter \\192.168.0.1.

8.2 USB Printing

The USB printing service allows you to connect a USB printer to the device and thus all clients on your network can print anything they want on their PCs. The Router can identify a printer automatically as long as it is successfully connected.



Disconnected	
Save	Cancel
	Disconnected Save

Enable Printer: Check/uncheck to enable/disable USB printing service.

Operation Instructions:

- 1. Correctly connect your USB printer to the USB port on the device.
- 2. Enable Printing Service

USB Printer		
Enable Printer		
Printer	EPSON ME 350 Series	
	Save	Cancel

3. On your PC (connected to the device), click

"Start"——"Settings"——"Printers and Faxes" and select "Add a printer" on appearing window.

Wireless AC1750 Dual-band Gigabit Router





4. Click "Next".





5. Select "Local printer attached to this computer" and click ""Next.

Add Printer Wizard
Local or Network Printer The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use: Local printer attached to this computer Automatically detect and install my Plug and Play printer A network printer, or a printer attached to another computer To set up a network printer that is not attached to a print server, use the "Local printer" option.
< <u>B</u> ack <u>N</u> ext > Cancel

6. Select "Create a new port", Type of port: "Standard TCP/IP



Port" and click "Next".

Add Printer Wizard
Select a Printer Port Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
O Use the following port: LPT1: (Recommended Printer Port) ▼
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
© Create a new port: Type of port: Local Port Local Port Microsoft Document Imaging Writer Monitor Standard TCP//P Port < Back Next > Cancel

7. Click "Next".



8. Enter Router's LAN IP address and click "Next".



Add Standard TCP/IP Printer P	ort Wizard	×
Add Port For which device do you want t	o add a port?	
Enter the Printer Name or IP add	dress, and a port name for the desired device.	
Printer Name or IP <u>A</u> ddress:	192.168.0.1	
<u>P</u> ort Name:	IP_192.168.0.1	
	< <u>B</u> ack Next>	Cancel

9. Click "Standard" under Device Type and select "Generic Network Card", then click "Next".

Add Standard T	CP/IP Printer Port Wizard
Additional Por The device	t Information Required could not be identified.
The detected de 1. The device is 2. The address of Either correct the previous wizard p	vice is of unknown type. Be sure that: properly configured. on the previous page is correct. address and perform another search on the network by returning to the page or select the device type if you are sure the address is correct.
Device Type-	
⊙ <u>S</u> tandard	Generic Network Card 💌
O <u>C</u> ustom	Settings
	< <u>B</u> ack <u>N</u> ext > Cancel

10. Click "Finish".

Add Standard TCP/IP Printer Port Wizard 🛛 🛛 🔀			
	Completing the Add Standard TCP/IP Printer Port Wizard You have selected a port with the following characteristics.		
	SNMP: Protocol: Device: Port Name: Adapter Type:	No RAW, Port 9100 192.168.0.1 IP_192.168.0.1 Generic Network Card	
	To complete th	is wizard, click Finish.	
		< <u>B</u> ack Finish Cancel	

11. Select "Have Disk".

Add Printer Wizard			
Install Printer Software The manufacturer and model o	determine which printer software to use.		
Select the manufacturer an disk, click Have Disk. If you compatible printer software.	d model of your printer. If your printer came with an installation ar printer is not listed, consult your printer documentation for		
Manufacturer Agfa Alps Apollo Apple APS-PS	Printers		
Image: Second state of the second s			
	< <u>B</u> ack <u>N</u> ext > Cancel		

12. Click "Browse", select corresponding drive file and click

"Open". At last click "OK".

Install F	rom Disk	×
-	Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.	OK Cancel
	Copy manufacturer's files from: F:\Documents and Settings\user\Desktop\Driver\ V	Browse

13. Click "Next".

Add Printer Wizard
Install Printer Software The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Printers ■ EPSON ME 350 Series
This driver is digitally signed. <u>I ell me why driver signing is important</u>
< <u>B</u> ack

14. Define a name for the printer and click "Next".



Add Printer Wizard
Name Your Printer You must assign a name to this printer.
Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.
Printer name:
EPSON ME 350 Series
Do you want to use this printer as the default printer?
<u>⟨B</u> ack <u>N</u> ext > Cancel

15. Click "Finish".

Add Printer Wizard			
	Completing the Add Printer Wizard		
	You have successfully completed the Add Printer Wizard. You specified the following printer settings:		
	Name:	EPSON ME 350 Series	
	Share name:	<not shared=""></not>	
	Port:	IP_192.168.0.1	
	Model:	EPSON ME 350 Series	
	Default	Yes	
	Test page:	Yes	
	To close this wizard, click Finish.		
		< <u>B</u> ack Finish Cancel	

8.3 DLNA

The (DLNA) is responsible for defining interoperability guidelines to enable sharing of digital media such as music, photos and videos between consumer devices such as computers, TVs,

printers, cameras, cell phones, and other multimedia devices.

DLNA Server		
Enable		
Media Server Name:	Tenda DLN	IA Server
	Save	Cancel

- > Enable: Check to enable the DLNA feature;
- Media Server Name: This option is configurable. You can change it according to your own needs.

For example: To play multimedia files that are stored on a USB storage attached to the device on your smart phone. Do as follows:

- 1. Connect the USB storage to the device.
- 2. Enable the DLNA feature on the device.
- 3. Change the DLNA server name if you like.
- 4. Start the DLNA client on your smart phone to perform a scan.
- 5. Select a multimedia file to play on your smart phone.

CHAPTER 9 IPTV

The IPTV feature makes it possible to enjoy online videos on your TV set via a set-top box while surfing Internet concurrently without mutual interference.

IPTV		
Enable		
Enable IPTV STB Port		
	Save	Cancel

- Enable: Check/uncheck to enable/disable the IPTV feature. Multicast IPTV is supported in this mode and IPTV port is still functioning as a LAN port.
- Enable IPTV STB Port: Check/uncheck to enable/disable the IPTV-specific port. This mode applies to various forms of IPTV and the IPTV port only provides IPTV service instead of as a LAN port.
- See below for the network topology:





- ▲ Note:
- If you enabled both options mentioned above, then note below: (a). Set IPTV set-top box's connection type to DHCP/dynamic IP or static IP (IMPORTANT: Note that the set-top box's IP address should be on the same IP net segment as router's LAN IP.) if the set-top box is connected to any port of LAN ports 1-3. (b). Select the dialup mode provided by your ISP if the set-top box is connected to the IPTV-specific port.
- After the IPTV port is set for IPTV purpose, PC that connects to such port will not be able to obtain an IP address or access Internet. So think twice before you start. Plus, LAN ports1-3 can only be used as LAN ports to connect PCs instead of an IPTV set-top box.

3. The IPTV feature is currently not supported on WLAN.

CHAPTER 10 TOOLS

The "Tools" tab includes 8 submeus: Time & Date, Firmware Update, Backup & Restore, Restore to Default, User Name & Password, Reboot, Statistics and Log. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



10.1 Time & Date

This section lets you configure, update, and maintain the correct time on the internal system clock. You can either select to set the time and date manually or automatically obtain the GMT time from Internet. Note that the GMT time is obtained only when Device is connected to Internet. You can also configure the system time manually.

This section assists you in setting the device's current time; you can either select to set the time and date manually or update it from Internet
automatically.
Note: The configured time and date settings lose when the device is powered off. However, it will be updated automatically when the router connects to the
Internet. To activate time-based features(e.g.firewall), the time and date information shall be set correctly first, either manually or automatically.
Sync with Internet time servers Sync Interval: 2 hours
Time Zone: (GMT+01:00)Paris,Berlin,Belgium,Vienna,Rome,Switzerland 💌
(Note: GMT time will be updated automatically only when the device is connected to Internet.)
Please input time and date:
1970 year 01 month 01 day 00 hour 27 minute 20 second Copy Local Time

- Sync with Internet time servers: Time and date will be updated automatically from Internet.
- Sync Interval: Specify a time interval for periodical update of time and date info from Internet.
- > Time Zone: Select your current time zone.
- Copy Local Time: Click it to copy your PC's time to the device.

10.2 Firmware Update

Firmware upgrade is released periodically to improve the functionality of your device and also to add new features. If you run into a problem with a specific feature of the device, log on to our website (www.tendacn.com) to download the latest firmware to update your device.

Firmware Update	
Use this section to update your router's software for better functionality or new features.	
Select a Software File: Upgrade	
Current System Version: W1800R_V1.0.0.0_EN; Release Date:Oct 22 2012	
Note: do not power off the router while upgrading, otherwise it may be permanently damaged. Upgrading takes a few minutes. When it it complete, the	
device will reboot automatically.	

To update firmware, do as follows:

- 1. Click "Browse" to locate and select the firmware file and "Update" to update your Device.
- > 2. Device restarts automatically when upgrade completes.

▲ Note:

Note: DO NOT disconnect device from power supply or the operating PC while update is in process, otherwise it may be permanently damaged. When it is complete, the device will reboot automatically. Update takes a few minutes. Please wait.
10.3 Backup & Restore

Backup & Restore					
Use this section to backup current settings	or restore previ	ious settings.			
Save Settings to Local Hard Drive:	Backup				
Load Settings from Local Hard Drive:			Browse	Restore	

- Backup settings: To backup settings, click the "Backup" button and specify a directory to save settings to your local hardware.
- Restore settings: To restore settings, click Browse to locate and select a configuration file and then click Restore.

10.4. Restore to Default

Restor to Default
To restore factory defaults, click the "Restore to Factory Default" button below.
Restore to Factory Default

Click the "Restore to Factory Default" button to reset Device to

factory default settings.

Default IP Address: 192.168.0.1

Default Subnet Mask: 255.255.255.0

Default User Name: admin

Default Password: admin

10.5 User Name & Password

Use this section to change	your login user name and password.	
Note: User name and pas	word can only include letters, numbers	or underscore!
Old User Name		
Old Password		
New User Name		
New Password		
Confirm New Password		

This section allows you to change login password and user name for accessing Device's Web-based management interface.

Both login password and user name are preset to "admin" by default. To change either or both, do as follows: 1. Enter your current user name and password in Old User Name and Old Password fields. 2. Enter a new user name and a new password in New User Name and New Password fields. 3. Click "Save".

▲ Note:

For security purpose, it is highly recommended that you change the default login password and user name.

10.6 Reboot

This section allows you to reboot the device.



To restart your device, click the "Reboot" button. Following

screen will appear:

Click the button below to rest	art your router.
poot	
	Rebooting, please wait12%

10.7 Statistics

Statistics displays current traffic of clients on your LAN.

Rate U1	nit: KB/s (Kbyte per second	Refresh		Disp	lay In descending	order of downst	ream rate
ID	IP Address	↑Packets	îBytes	↓Packets	↓Bytes	↑Rate	↓Rate
1	192.168.0.100	46537	1.53M	46532	1.53M	20.00	20.00
2	192.168.0.128	6	0M	0	0M	0.00	0.00

- Enable Traffic Statistics: Determine whether to enable the Traffic Statistics feature on internal users.
- > Refresh: Click it to update statistic data.

▲ Note:

Enabling the Traffic Statistics feature may degrade router's performance. So, do not enable it unless necessary.

10.8 Log

The Syslog option allows you to view all events that occur upon system startup and check whether there is attack present in your network. The logs are classified into 3 types: "All", "System "and "WAN".

			Type of logs to display: All
	Log C	ontent	
1970-01-01 00:00:11	system	DHCP_GUEST Server Start	
1970-01-01 00:00:11	system	DHCP Server Start	
h Clear			
	1970-01-01 00:00:11 1970-01-01 00:00:11 Clear	Log C 1970-01-01 00:00:11 system 1970-01-01 00:00:11 system	Log Content 1970-01-01 00:00:11 system DHCP_GUEST Server Start 1970-01-01 00:00:11 system DHCP Server Start Clear

APPENDIX 1 CONFIG TCP/IP SETTINGS

If you are using Windows XP,do as follows:

1. From the PC you are currently using, click Start and select

Control Panel;





2. Click Network and Internet Connections.





3. Right-click on the Local .Area Connection and select Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.

🖢 Local Area Connection Properties 🛛 🔹 👔 🔀
General Authentication Advanced
Connect using:
Realtek RTL8139 Family PCI Fast Etł Configure
This connection uses the following items:
Gient for Microsoft Networks File and Printer Sharing for Microsoft Networks GoS Packet Scheduler
✓ There Protocol (TCP/IP)
Install Uninstall Properties
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. Select "Obtain an IP address automatically" or "Use the following IP address".
- a. "Obtain an IP address automatically"

ernet Protocol (1)	PUB) Pro	perties			1
ieneral					
You can get IP setting this capability. Otherwi the appropriate IP setti	s assigned au se, you need I ngs.	tomatically to ask you	if your n r network	etwork su administ	ipports rator for
Obtain an IP add	ress automatic	ally			
OUse the following	IP address: -				
IP address:					
Subnet mask:					٦
Default gateway:					
Obtain DNS serv.	er address au	tomatically			
OUse the following	DNS server a	addresses:			
Preferred DNS serv	er:				
Alternate DNS serve	er:				
				Adv	anced
		ĺ	OK		Cancel

b. Use the following IP address"

IP address: Enter 192.168.0.xxx where xxx can be any number

between 2 and 254).

Subnet mask: Enter 255.255.255.0.

Default gateway: Enter 192.168.0.1.

Preferred DNS server: Set Preferred (Primary) DNS the same as

the LAN IP address of your Device (192.168.0.1) if you don't

know your local DNS server address (Or consult your ISP). The

Alternate (Secondary) DNS is not needed or you may enter one from your ISP.

Click OK twice to save your settings.

nternet Protocol (TCP/IP) Pro	operties 🔹 👔 👔
General	
You can get IP settings assigned a this capability. Otherwise, you need the appropriate IP settings.	utomatically if your network supports d to ask your network administrator for
🔘 Obtain an IP address automa	tically
Our of the following IP address:	
IP address:	192.168.0.2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192.168.0.1
Obtain DNS server address a	utomatically
─⊙ Use the following DNS server	r addresses:
Preferred DNS server:	192.168.0.1
Alternate DNS server:	
	Advanced
	OK Cancel

If you are using Windows 7, do as follows:

From the PC you are currently using, click Start-> Control Panel-> Network and Internet-> Network and Sharing

Center-> Change adapter settings;



> Right click "Local Area Connection" and select "Properties".



Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".



Local Area Connection 2 Properties
Networking Sharing
Connect using:
Realtek RTL8139/810x Family Fast Ethernet NIC
Configure
This connection uses the following items:
Client for Microsoft Networks
🗹 📇 QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

- Select "Obtain an IP address automatically" or "Use the following IP address".
- a. "Obtain an IP address automatically"

nternet Protocol Version 4 (TCP/IPv	/4) Pr	opert	ies		? <mark>X</mark>
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 automatic	ally				
Use the following IP address:					
IP address:					
Subnet mask:					
Default gateway:					
Obtain DNS server address auto	omatio	ally			
Use the following DNS server a	ddress	ies			
Preferred DNS server:					
Alternate DNS server:					
Validate settings upon exit				Adva	nced
			ОК		Cancel

b. Use the following IP address".

IP address: Enter 192.168.0.xxx where xxx can be any number

between 2 and 254). Subnet mask: Enter 255.255.255.0.

Default gateway: Enter 192.168.0.1.

Preferred DNS server: Set Preferred (Primary) DNS the same as

the LAN IP address of your Device if you don't know your local

DNS server address (Or consult your ISP). The Alternate

(Secondary) DNS is not needed or you may enter one from your ISP.

Click OK twice to save your settings.



In this section, we present you how to config your PC's TCP/IP settings.

Before you start, make sure your PC has an installed NIC. If not, please install one first.

APPENDIX 2 GLOSSARY

DLNA

The (DLNA) is a non-profit collaborative trade organization established by Sony in June 2003, that is responsible for defining interoperability guidelines to enable sharing of digital media such as music, photos and videos between consumer devices such as computers, TVs, printers, cameras, cell phones, and other multimedia devices. DLNA uses Universal Plug and Play (UPnP) for media management, discovery and control.[4] UPnP defines the type of device that DLNA supports ("server", "renderer", "controller") and the mechanisms for accessing media over a network. The DLNA guidelines then apply a layer of restrictions over the types of media file format, encodings and resolutions that a device must support.

11AC

IEEE 802.11ac is a wireless computer networking standard of 802.11, currently under development, providing high-throughput wireless local area networks on the 5 GHz band. Theoretically, the 802.11ac specification will enable multi-station WLAN throughput of at least 1 gigabit per second and a maximum single link throughput of at least 500 megabits per second (500 Mbit/s). This is accomplished by extending the air interface concepts embraced by 802.11n: wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to 8), multi-user MIMO,

and high-density modulation (up to 256 QAM).

Channel

Channel

A communication channel, also known as channel, refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel. It is used to transfer an information signal, such as a digital bit stream, from one or more transmitters to one or more receivers. If there is only one AP in the range, select any channel you like. The default is Auto.

If there are several APs coexisting in the same area, it is advisable that you select a different channel for each AP to operate on, minimizing the interference between neighboring APs. For example, if 3 American- standard APs coexist in one area, you can set their channels respectively to 1, 6 and 11 to avoid mutual interference. Frequency interference rarely exists over 5 G band, which has more channels and greater frequency span.

SSID

SSID

Service set identifier (SSID) is used to identify a particular 802.11 wireless LAN. It is the name of a specific wireless network. To let

your wireless network adapter roam among different APs, you must set all Aps' SSID to the same name.

WPA/WPA2

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network.

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA. Currently, WPA is supported by Windows XP SP1.

PPPOE

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. Integrated PPP protocol implements authentication, encryption, and compression functions that traditional Ethernet can not provide and can also be used in the cable modem and digital subscriber line (DSL) and Ethernet that provide access service to

the users. Essentially, it is a protocol that allows to establish a point-to-point tunnel between two Ethernet interfaces within an Ethernet broadcast domain.

DNS

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A Domain Name Service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. WDS

A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. All base stations in a wireless distribution system must be configured to use the same radio channel, method of encryption (none, WEP, or WPA) and the same encryption keys. They may be configured to different service set identifiers. WDS also requires every base station to

be configured to forward to others in the system. WDS may also be considered a repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging).WDS may be incompatible between different products (even occasionally from the same vendor) since it is not certified by the Wi-Fi Alliance. WDS may provide two modes of wireless AP-to-AP connectivity:• Wireless bridging, in which WDS APs communicate only with each other and don't allow wireless clients or stations (STA) to access them• Wireless repeating, in which APs communicate with each other and with wireless STAs. DMZ

In computer security, a DMZ (sometimes referred to as a perimeter networking) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, although communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal

123

network clients. Any services such as Web servers, Mail servers, FTP servers and VoIP servers, etc that are being provided to users on the external network can be placed in the DMZ.

APPENDIX 3 TROUBLESHOOTING

This section provides solutions to problems that may occur during installation and operation of the device. Read the following if you are running into problems. If your problem is not covered here, please feel free to go to www.tendacn.com to find a solution or email your problems to support@tenda.com.cn orsupport02@tenda.com.cn. We will be more than happy to help you out as soon as possible.

1. Q: I entered the device's LAN IP address in the web browser but cannot access the utility. What should I do?

Check whether device is functioning correctly. The Sys LED should blink a few seconds after device is powered up. If it does not light up, then some internal faults may have occurred. Verify physical connectivity by checking whether a corresponding port's link LED lights up. If not, try a different cable. Note that an illuminated light does NOT ALWAYS indicate successful connectivity.

Run the "ping 192.168.0.1" command. If you get replies from 192.168.0.1, open your browser and verify that Proxy server is disabled. In case that ping fails, press and hold the "WPS/RESET" button on your device for 7 seconds to restore factory default settings, and then run "ping192.168.0.1" again.
4) Contact our technical support for help if the problem still exists

after you tried all the above.

2. Q: What should I do if I forget the login password to my device?

A: Reset your device by pressing the WPS/Reset button for over7 seconds. Note: All settings will be deleted and restored tofactory defaults once you pressed the WPS/Reset button.

3. Q: My computer shows an IP address conflict error after having connected to the device. What should I do?

A: 1) Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

2) The default IP address of the device is 192.168.0.1; make sure this address is not used by another PC or device. In case that two computers or devices share the same IP addresses, change either to a different address.

4. Q: I cannot access Internet and send/receive emails; what should I do?

This problem mainly happens to users who use the PPPoE or Dynamic IP Internet connection type. You need to change the MTU size (1492 by default). In this case, go to "WAN Settings" to change the MTU value from default 1480 to 1450 or 1400, etc.

5. Q: How do I share resources on my computer with users on Internet through the device?

A: To let Internet users access internal servers on your LAN such

as e-mail server, Web, FTP, via the device, use the "Virtual Server" feature. To do so, follow steps below:

Step 1: Create your internal server, make sure the LAN users can access these servers and you need to know related service ports, for example, port for Web server is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Enter device web utility and click Virtual Server.

Step 3: Input the Start Port/External Port, say, 80.

Step 5: Input the internal server's IP address. For example,

assuming that your Web server's IP address is 192.168. 0.10, then simply input it.

Select a proper protocol type: TCP, UDP, or Both depending on which protocol(s) your internal host is using.

Click Enable and save your settings.

For your reference, we collected a list of some well-known service ports as follows:

Server	Protocol	Service Port
Web Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	ТСР	1503、1720
		File
MSN Messenger	TCP/UDP	Send:6891-6900(TCP)
		Voice:1863、6901(TCP)

		Voice:1863、5190(UDP)
PPTP VPN	TCP	1723
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110

APPENDIX 4 REMOVE WIRELESS NETWORK FROM YOUR PC

If you change wireless settings on your wireless device, you must remove them accordingly your PC; otherwise, you may not be able to wirelessly connect to the device. Below describes how to do remove a wireless network from your PC.

If you are using Windows XP, do as follows:

1. Right click "My Network Places" and select "Properties".





2. Click Wireless Network Connection and then select

Properties.

	b <u>e</u> 🔹 🖈 🖈)
2	Disable	<u>ام</u>
Loca Conne	View Available Wireless Networks	_lan
	Status	
	Repair	
	Bridge Connections	
	Create Shortcut	
	Delete	I
	Rename	
	Properties	

3. Click "Wireless Networks", select the item under "Preferred networks" and then click the Remove button.

🕂 Local Area Connection 4 Properties 🛛 🔹 💽
General Wireless Networks Advanced
✓ Use <u>W</u> indows to configure my wireless network settings
Available networks:
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.
View Wireless Networks
Preferred networks: Automatically connect to available networks in the order listed below:
Tenda (Automatic)
Move <u>d</u> own
Add <u>R</u> emove Properties
Learn about <u>setting up wireless network</u> Advanced
OK Cancel

If you are using Windows 7, do as follows:

1. Click Network from your desktop and select Properties.

letwork	Open
	Map network drive
	Disconnect network drive
	Create shortcut
	Delete
	Properties

2. Select "Manage Wireless Networks".



3. Click the wireless connection and select "Remove network".



APPENDIX 5 SAFETY AND EMISSION STATEMENT

NCC Notice

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、加大功率或變更設計之特性及功能。 低功率射頻電機之作用不得影響飛航安全及幹擾合法通信; 經發 現有幹擾現象時,應立即停用,並改善至無幹擾時方得繼續使 用。 前項合法通信,指依電信規定作業之無線電信。 低功率射 頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設 備之幹擾。

5.25~5.35GHz 限室內使用 (802.11a used)

FC

FCC Statement

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause

undesired operation.

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 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.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement

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

NOTE:

(1)The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable



CE Mark Warning

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

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

NOTE:

(1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable

"The product can be used without restrictions in the following countries: all EU member states except France and Norway. The product can be used with limitations in the following countries: France (for indoor use only) and Norway (20 km in the center of Ny-Liesund)."